

RMUTT HPE Aruba Networking campus associate

Aruba Campus Network Training • 26 ส.ค. 2569

Agenda (1/3)

Overview Aruba Solution

Network devices & roles

Campus architecture

CX / Gateway / AP portfolio

Agenda (2/3)

Module 1 : Aruba Switch

Switch series, stacking, PoE

Lab 1: Device management

Lab 2: LAG & VLAN

Lab 3: Layer 3 Routing

Knowledge check?

Agenda (3/3)

Module 2 : Controller + AP

Controller & AP onboarding

WLAN: PSK & MAC auth

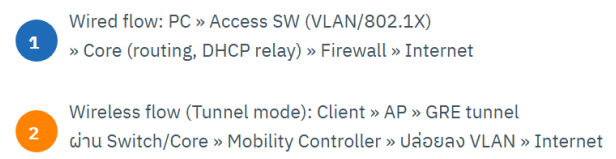
WLAN: 802.1X

WLAN: Captive portal (Guest)

Role & Policy · Q & A

Switch + Controller + AP · Device roles & traffic flow — RMUTT / Commserv Siam · 26 ต.ค. 2569

Switch + Controller + AP · Device roles & traffic flow — RMUTT / Commserv Siam · 26 ต.ค. 2569



■ Copper 1G
 ■ 10G / LAG (Fiber)
 ■ GRE Tunnel (AP — MC)
 ■ RADIUS (802.1X / MAC Auth)
 ■ Wireless (SSID)
 หัวข้อ: Campus architecture · Traffic flow & device roles (10:30 น.)

Network Devices

Networking devices: switch

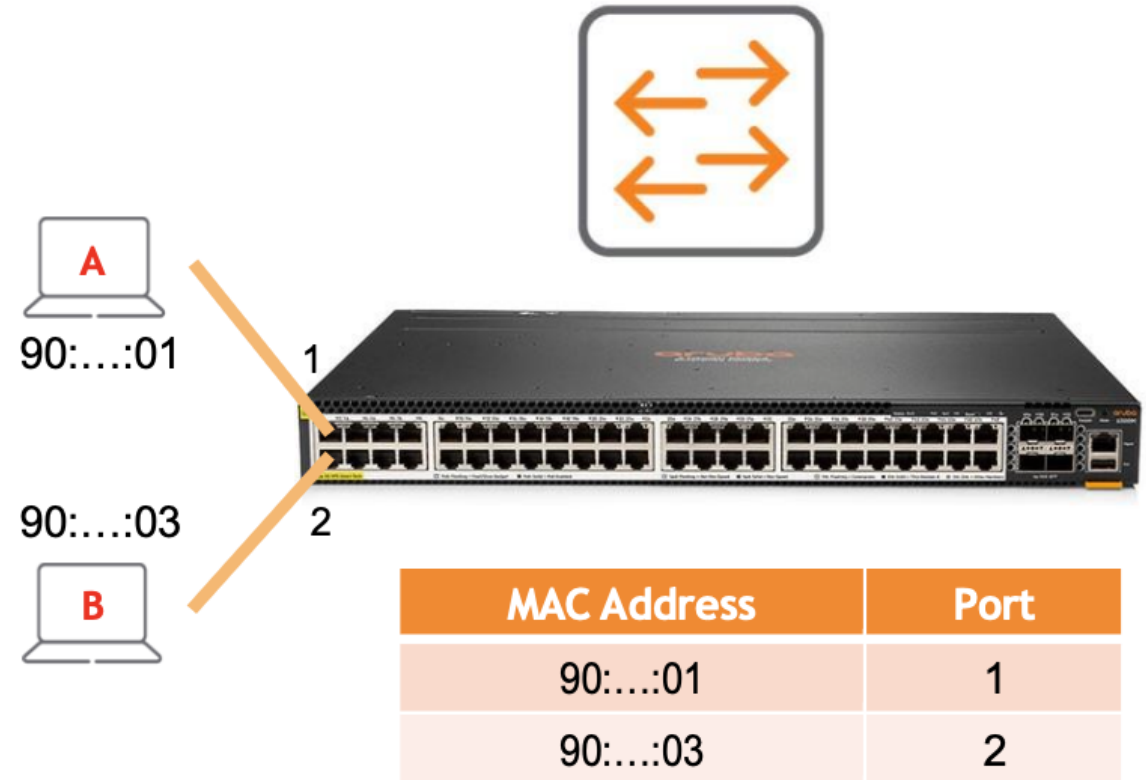
L2 device: Forwards Ethernet frames based on destination MAC addresses

Multiple ports connect endpoints

- PCs, printers, cameras, and more
- Commonly 8, 24, 48, or more physical ports
- Transparent to endpoints

Special L2 protocols

- Performance, reliability, security
- STP, LLDP, 802.1Q



Networking devices: router

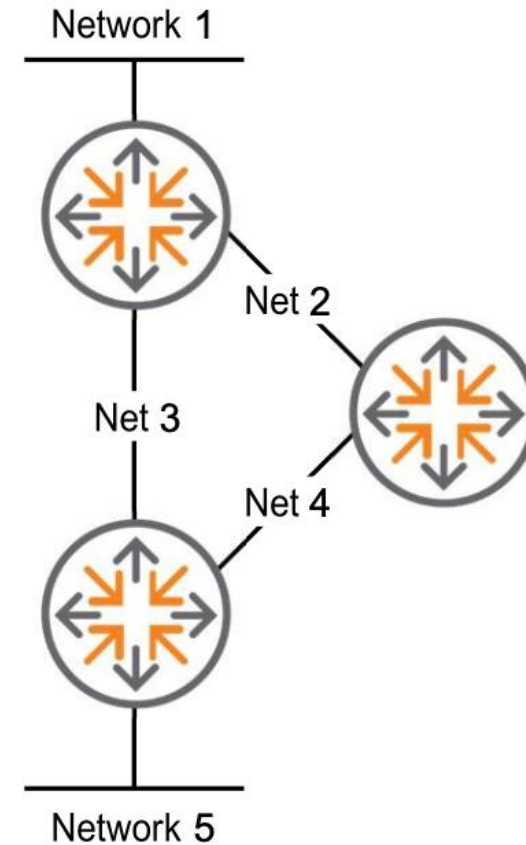
Layer 3 device: Forwards packets based on destination IP address

Functionality and features

- Connect separate networks into an inter-network
- Offer WAN connectivity to networks

L3 routing protocols

- Learn all possible paths, choose a best path
- RIP, OSPF, BGP



Networking devices: multi-layer switch

Performs both L2 switching and L3 routing

L3 Routing

- Internal routing functionality
- Runs RIP, OSPF, BGP

L2 Switching

- Multiple ports connect endpoints
- Uses STP, LLDP, VLANs



Networking devices: access point

Enables wireless users to access wired resources and roam about

Functionality

- Bridges wireless devices and wired networks.
- Transform Ethernet into Wi-Fi frames and back



Varieties of APs

- Internal or external antennas
- Single or Dual Ethernet Ports
- Indoor or outdoor



Networking devices: firewall

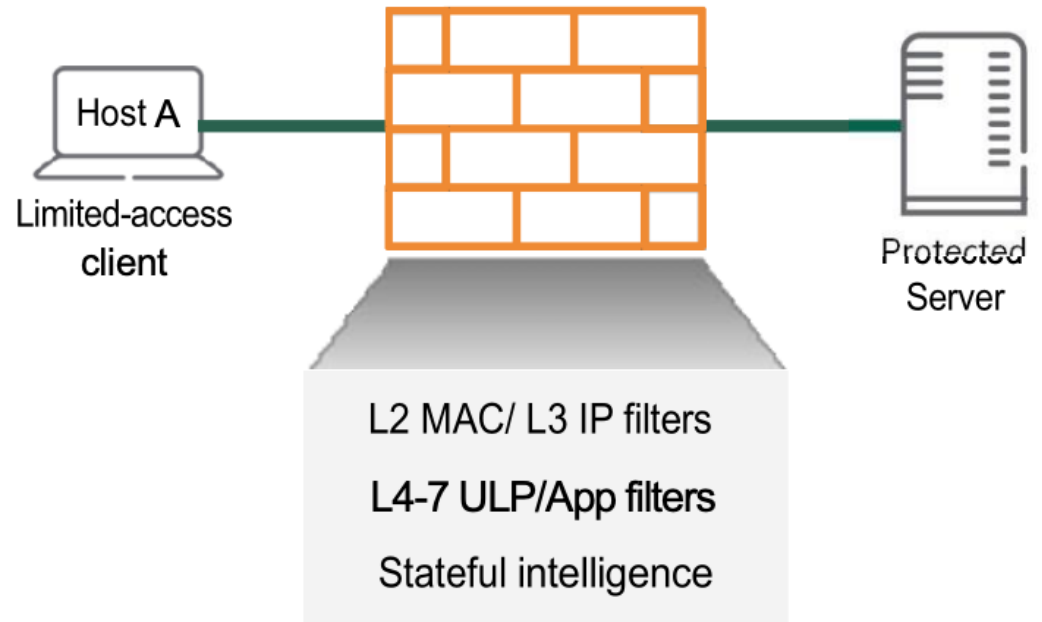
L2-7 filtering and security

Functionality

- Block unauthorized/inappropriate access
- Permit authorized/appropriate access

Types

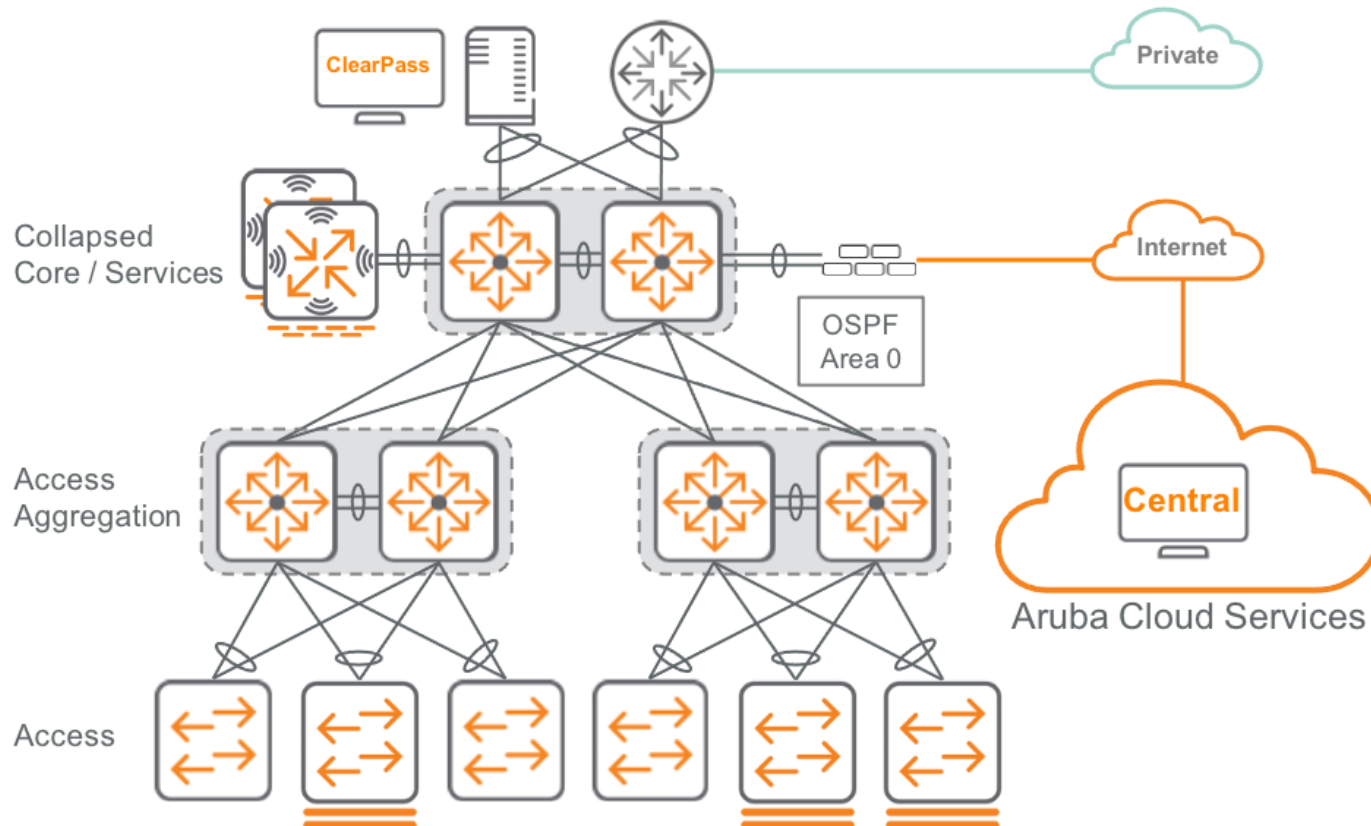
- Stateless vs Stateful
- Functionality built into switches, gateways



Introduction switch

CX switching solutions for all networks

For branch, campus, mid and large enterprises, SMB, and data center networks



Data Center

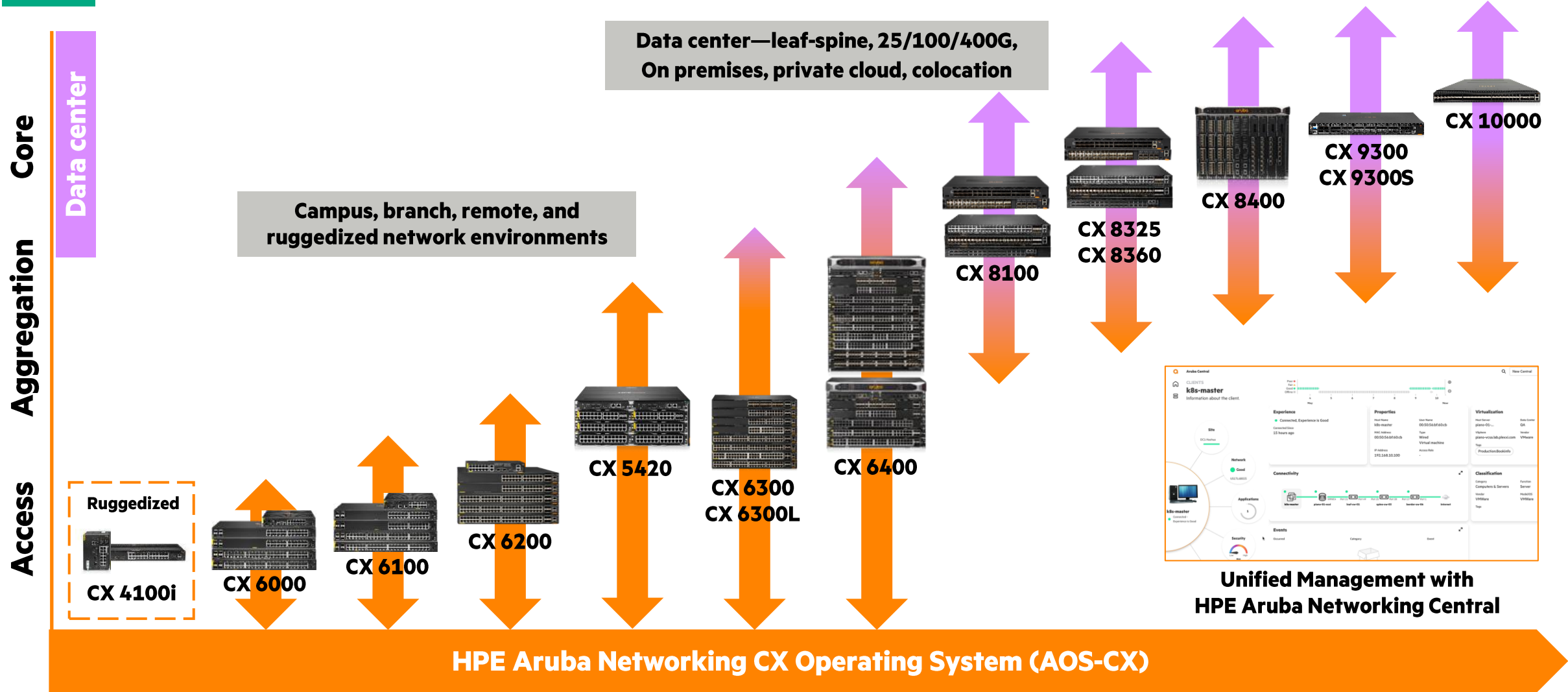
Enterprise Core

Aggregation and Distribution

Campus and Branch Access

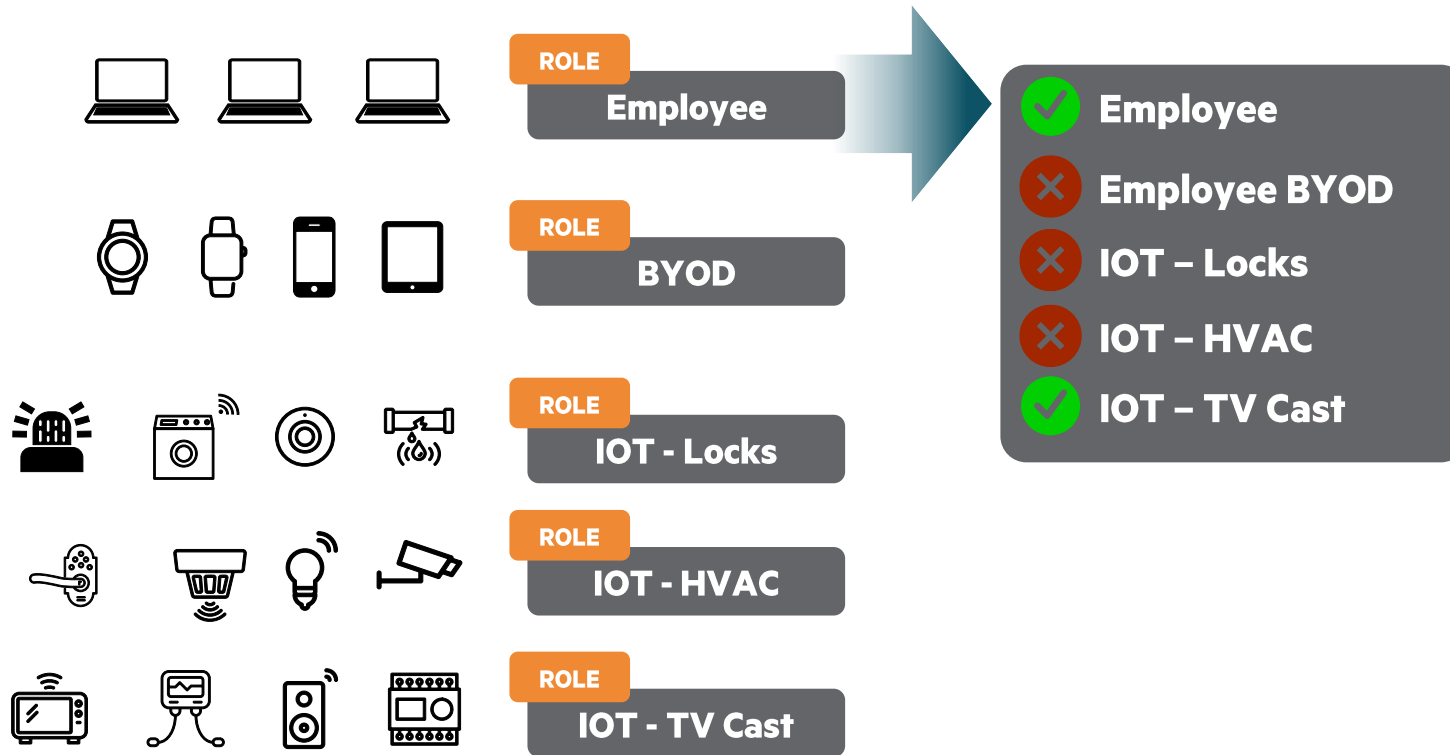
Ruggedized

HPE Aruba Networking CX switch portfolio



One common operating model from campus edge to DC

HPE Aruba Networking User Roles



DYNAMIC SEGMENTATION

Software defined approach eliminates VLAN sprawl and simplifies policy implementation

Delivers wired, wireless, and SD-WAN micro-segmentation needed for securing end-user and IoT devices

AP platforms for comprehensive campus and branch connectivity

Wi-Fi 7

Wi-Fi 6E

Wi-Fi 6

AOS-10
BASED



Mid-range Wi-Fi 7 730 Series (AP-734/735)

Tri-band support
2x2:2SS (8RU), 9.4Gbps,
2x 5GE, 2xUSB, embedded GPS &
barometer, 2 x IoT radios
Ultra tri-band filtering

AOS-10
BASED



Flagship Wi-Fi 7 750 Series (AP-734/735)

Tri-band support
4x4:4SS (8RU), 18.8Gbps,
2x 10GE, 2xUSB, embedded GPS &
barometer, 2 x IoT radios
Ultra tri-band filtering



Entry level Wi-Fi 6E 610 Series (AP-615)

Dual-radio/tri-band
2x2:2SS (8RU), 3.6Gbps,
1x 2.5GE, USB, embedded GPS



Mid-range Wi-Fi 6E 630 Series (AP-634/635)

Tri-band support
2x2:2SS (8RU), 3.9Gbps,
2x 2.5GE, USB, embedded GPS, UTB



Flagship Wi-Fi 6E 650 Series (AP-654/655)

Tri-band support
4x4:4SS (8RU), 7.8Gbps,
2x 5.0 GE, USB, embedded GPS, UTB



Entry level Wi-Fi 6 500 Series (AP-503)

Dual-radio 2x2:2SS, 1.5Gbps, 1x
1GE, USB



Entry level Wi-Fi 6 500 Series (AP-505/504)

Dual-radio 2x2:2SS (8RU), 1.5Gbps, 1x
1GE, USB, DC, BLE/Zigbee, IPM, FTM



Mid-range Wi-Fi 6 510 Series (AP-515/514)

Dual-radio 2x2:2SS (2.4GHz), 4x4:4SS (5GHz),
2.7Gbps, 1x2.5GE + 1xGE, USB, DC, BLE/Zigbee,
IPM, FTM



High-performance Wi-Fi 6 530 Series (AP-535/534)

Dual-radio 4x4:4SS, 3.98Gbps, 2x 5GE, USB,
DC, BLE/Zigbee, IPM, FTM



Flagship Wi-Fi 6 550 Series (AP-555/554)

Dual-radio 4x4:4SS (2.4GHz) 4x4:4SS x2 or
8x8:8SS (5GHz), 5.4Gbps, 2x 5GE, USB, DC,
BLE/Zigbee, IPM, FTM

< Low-density to high-density, demanding environments >

Always-on, always available enterprise networking

Resilient, scalable architecture that eliminates downtime for business continuity

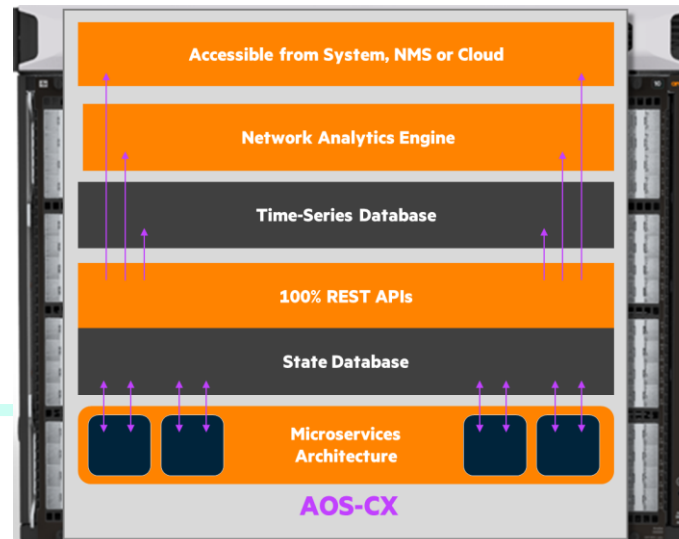


Resilient networks are designed to remain always-on, ensuring uptime for **business continuity** when every moment matters.

- Management and operations
- Physical platform redundancy
- Physical design redundancy
- Logical design redundancy
- Disaster recovery
- Software upgrades

Resilient by design

AOS-CX is a modern, cloud-native, and modular operating system built to be database-centric with independent micro-services and state synchronization.



VSX Live Upgrades

Hot Patching

VSF ISSU

Built-in analytics

Rollout validated configs

Clusters & Stacking

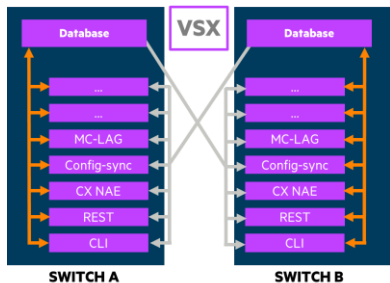
Hot-swappable parts

Always-on PoE

CX creates business continuity across the network thru SW and HW

Resilient, scalable architecture by design

VSX Live Upgrades



ISSU orchestrated upgrades to eliminate maintenance windows

Rollout validated configs

Automated rollouts with NetEdit or Central Multi-Editor

VSF ISSU & hot patching

Minimize downtime during upgrades across a stack

Clustering & Stacking

Grow quickly, simplify mgmt., extend distances with long range trvrs.

Built-in analytics

Visibility and alerts for faster troubleshooting and MTTR

Always-on PoE

Continuous power for IoT and APs during switch updates

Redundant and hot-swappable parts

Power supplies, fans, management, and fabric

Virtual Switching Framework (VSF)

For resilient and scalable campus and branch access networks

Simplified Management with virtual switch stack

Grow your network quickly

Go further with stacking across campus and site using long range transceivers

Fast stack with CX Mobile App that auto-detects potential stack members for a virtualized stack with just a few taps

Configure a stack quickly within Central UI



CX 6300

10-unit CX 6300 stack

Flexibility to combine 6300M and 6300F models

Uses 10/25/50 GbE uplinks

CX 6200

8-unit CX 6200 stack

Flexibility to combine 6200M and 6200F models

Uses 10GbE uplinks

* 6300L only stacks with other 6300L models.
6200 and 6300 mixed stack not allowed

In-Service Software Upgrades (ISSU) with VSF Stacking

Rapid, interruption-less software upgrades for stacked CX 6300 switches¹

What is an ISSU?

- Software upgrades within a release, without traffic interruption. The data plane will keep forwarding traffic during entire upgrade process
- Requires conductor and standby as part of the VSF stack.
- Supports up to 10-member stack

Benefits

- Increase availability during upgrade
- Data plane is not affected and keeps forwarding traffic
- Maintain end-points and application connectivity through the upgrade process
- Includes bug/vulnerability fixes and new features

Total Downtime: 0%

Customer starts ISSU, and observes system ready validation

Standby and members update, then connect to standby database

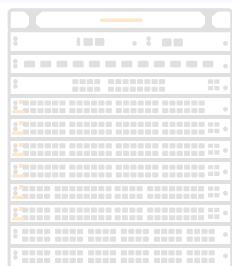
Database sync from active conductor to standby occurs

Switchover from active conductor to standby, new active takes over

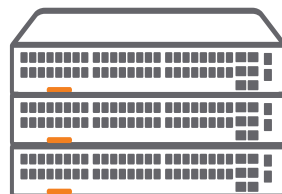
Former active updates & becomes new standby without reboot

¹ VSF ISSU not available on CX 6300L switch models

Configurations
Supported



Chassis



Stack



Standalone

CX 6200 Switch Series

Lite Layer 3 stackable access switches for branch offices and SMBs

Flexible growth with stackable gigabit connectivity with fast 1/10G uplinks

Power IoT & Wi-Fi devices with up to 1440W Class 4 to Class 6 PoE

Scalable growth with **8 member VSF stacking**

Real-time monitoring and troubleshooting with **Network Analytics Engine (NAE)**

Simple and secure access with **Dynamic Segmentation** that automates user and device policy

CX portfolio benefits

Advanced configs and programmability with AOS-CX

Single pane of glass Central across wired, wireless, WAN

Flexible management via Web GUI, CLI, NetEdit, Central

Limited lifetime warranty and options for adv.TAC support

11

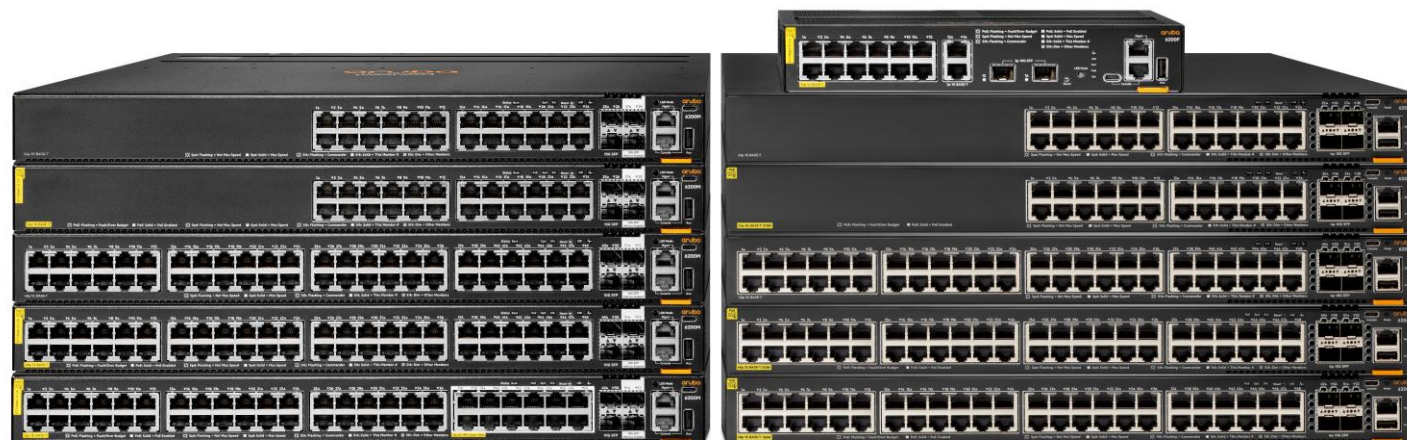
Fixed switches
(power & fans)

5

Modular switches
(power & fans)

4

Built-in 1 and 1/10
GbE uplinks



CX 6300 Switch Series

Powerful Layer 3 stackable switches ready for demanding environments

Flexible growth with stackable gigabit connectivity with fast **10/25/50GbE¹ uplinks**, high density SFP+

Built for IoT and Wi-Fi 6 with up to **2880W Class 6 and Class 8 PoE** and HPE Smart Rate **multi-gigabit** Ethernet

Real-time monitoring and troubleshooting with **Network Analytics Engine (NAE)**

Simple and secure access with **Dynamic Segmentation**; campus and branch fabric with **VXLAN and BGP EVPN**

Power-to-port airflow for cost-effective **1GbE ToR and OOBM data center** deployments

CX portfolio benefits

Advanced configs and programmability with AOS-CX

Single pane of glass Central across wired, wireless, WAN

Flexible management via Web GUI, CLI, NetEdit, Central

Limited lifetime warranty and options for adv.TAC support

4
Fixed power switches

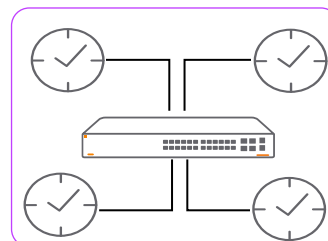
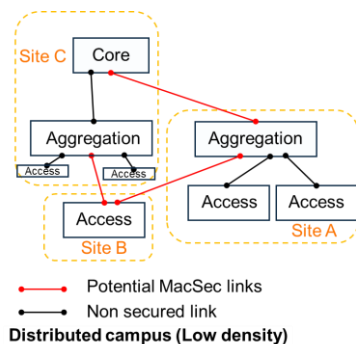
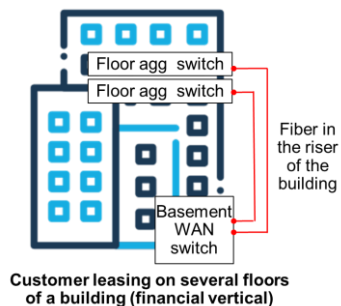
12
Modular power switches

2880W
60W and 90W PoE



10 member
VSF stacking

Bringing performance and versatility to campus networks

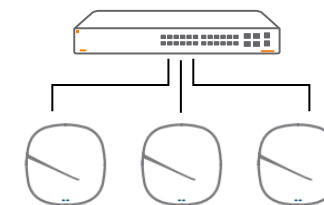


Synchronization and validation across systems

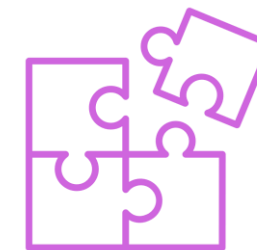


Video conferencing and multimedia consumption

Time synchronization and Audio Video Bridging support with precision time protocol (PTP) boundary clock (BC) and transparent clock (TC).

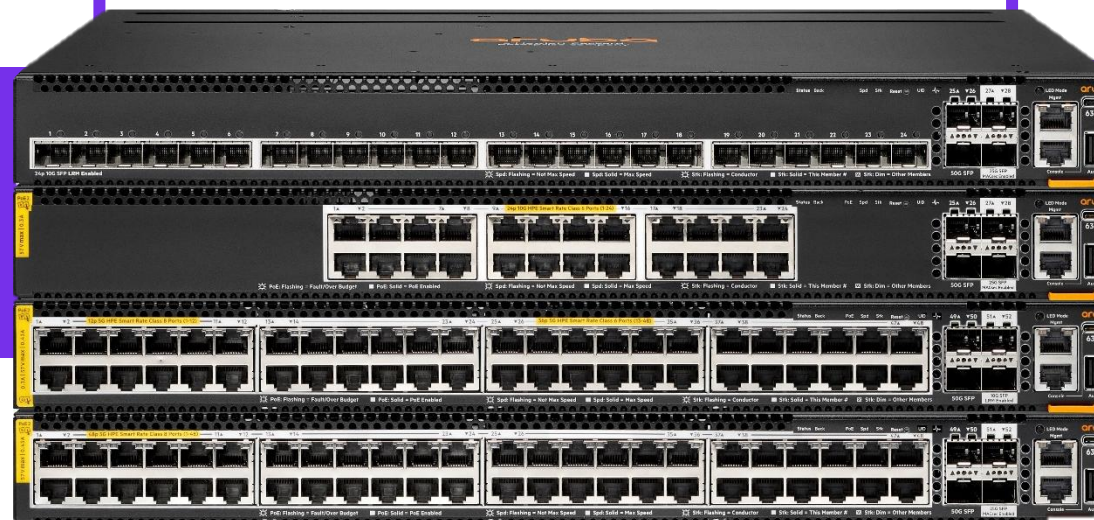


Next-gen 802.3bt enabled wireless access points



Internet of things devices and systems, like smart lighting

Stronger data link layer security with standards-based MACsec 256 encryption and authentication on uplinks and downlinks.



More performance, power, and connectivity options with up to 10G Smart Rate, Class 8 (90W) PoE, and LRM support.

HPE Aruba Networking CX Switches – End-to-end portfolio

Always-on Reliability

- HA with ISSU, HW, SW resiliency
- Proactive analytics

Switching Solution for Any Network

Strong, scalable switching portfolio for branch, campus, mid and large enterprises, SMB, and data center networks

Secure Access

- Dynamic Segmentation
- Campus- branch fabric EVPN/VXLAN
- NetConductor

Simplified Operations

- Single OS from access to core to DC
- Smart automation for flawless configs with NetEdit
- Built-in analytics with deep visibility and clear alerts
- Management flexibility (Cloud, on-prem, Web GUI, CLI, NetEdit, AFC)
- Unified cloud-based single pane of glass management for wired, WLAN, SD-WAN

HPE Aruba Networking CX Switches



Technology Innovation

- AOS-CX: Programmable, modern, designed to scale access to DC
- NAE: built-in analytics monitor, baseline, troubleshoot
- NetEdit: error-free automated rollouts
- VSX live upgrades, VSF rolling stack, & Hot Patching: HA during upgrades
- In-house ASICs: high-performance, programmable agility
- Central: Unified, AIOps, NetConductor

Faster Troubleshooting

- NAE built-in for monitoring, alerts, troubleshooting and root cause analysis
- Central integration with AI insights

Scalable, High-Performance Enterprise Switching

High-density fixed and modular switches with non-blocking architecture, speeds from 1G to 400G, extended table sizes, high power PoE, multi-gig, 80 Plus power supplies, fiber and copper transceivers and DACs

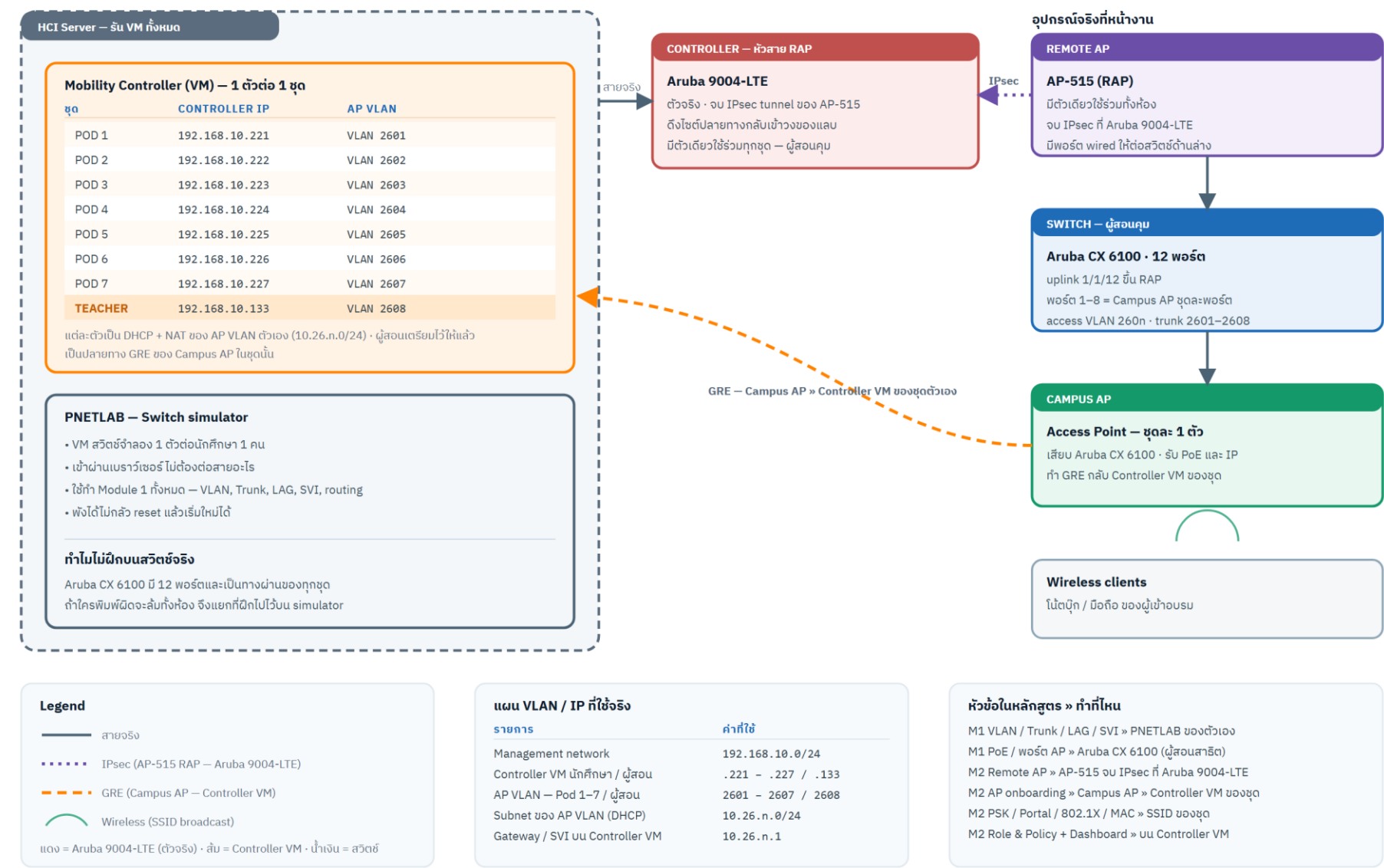
Customer First, Customer Last

- Industry leading warranty
- Global support and services
- Consumption choice: GL4A, NaaS
- Financing: HPEFS

Switch Labs

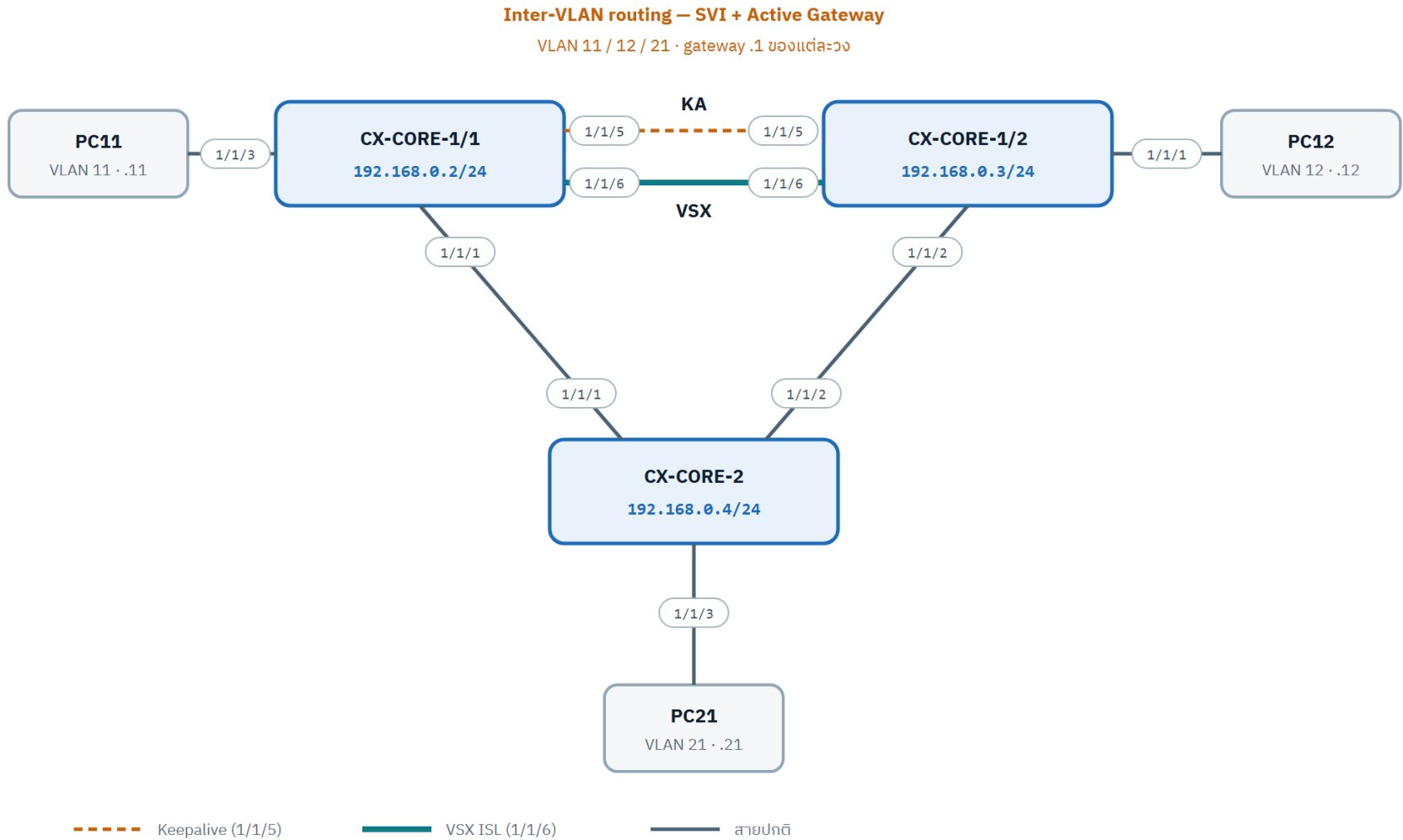
Aruba Campus Network Training — Lab Topology

RMUTT × Commserv Siam · 26 ส.ค. 2569 · RAP จบที่ Aruba 9004-LTE · Campus AP จบที่ Controller VM ของชุดตัวเอง · 7 ชุดนักศึกษา + 1 ชุดผู้สอน



Switch Lab uu PNETLAB

RMUTT x Commserv Siam · 26 ส.ค. 2569 · VSX pair + Active Gateway · PC คณะ VLAN เพื่อทดสอบ inter-VLAN routing



การใช้งาน PNETLAB

URL <http://10.69.11.10/>
ผู้ใช้ pod1 - pod7 (ตามชุดตัวเอง)
รหัสผ่าน P@ssw0rd

ทุกคนในชุดใช้สิทธิ์กันเดียวกัน — ตกลงกันก่อนว่าใครกดอะไร

ค่าที่ใช้ในผังนี้

รายการ	ค่า
CX-CORE-1/1 · CX-CORE-1/2	192.168.0.2 · 192.168.0.3
CX-CORE-2	192.168.0.4
PC11 — VLAN 11	192.168.11.11 · gw .1
PC12 — VLAN 12	192.168.12.12 · gw .1
PC21 — VLAN 21	192.168.21.21 · gw .1
VSX ISL / Keepalive	1/1/6 / 1/1/5
LAG ลง CX-CORE-2	1/1/1 และ 1/1/2

อ่านผังนี้อย่างไร

- สวิตช์สามตัวเป็น VM คนละชุดกับเพื่อน — พังได้ reset ใหม่ได้
- CX-CORE-1/1 กับ CX-CORE-1/2 จับคู่เป็น VSX
- SVI ของทั้งสาม VLAN อยู่บนคู่ VSX · CX-CORE-2 เป็น L2 อย่างเดียว
- PC อยู่คนละ VLAN — ping หากันได้ต้องผ่าน inter-VLAN routing

LAB 0 เข้า PNETLAB และเปิดเครื่องมือให้ครบ

ที่โต๊ะ: เข้าห้องแล็บของชุดตัวเองได้ เห็นสวิตช์ครบสามตัว และเข้า Controller VM ของชุดได้

1. เปิด <http://10.69.11.10/> แล้วล็อกอินด้วยผู้ใช้ของชุดตัวเอง — POD 1 ใช้ pod1 รหัส P@ssw0rd
2. เปิด lab ของชุดตัวเอง กด START แล้วรอให้ทั้งสามสวิตช์ขึ้น
3. คลิกที่สวิตช์เพื่อเปิด console — เริ่มที่ CX-CORE-1/1
4. เปิดอีกแท็บ เข้าเว็บ Controller VM ของชุดตัวเอง เช่น POD 1 » <https://192.168.10.221:4343>
5. จดไว้: สวิตช์ 192.168.0.2 / .3 / .4 · VLAN 11 / 12 / 21 (gateway .1 ของแต่ละวง) · Controller 192.168.10.22n

ตรวจสอบ

```
show version
show interface brief
```

ระวัง

ทุกคนในชุดใช้ล็อกอิน PNETLAB เดียวกัน — ถ้าสองคนกดพร้อมกันจะแย่ง console ตกลงกันก่อนว่าใครทำตัวไหน

LAB 1 ตั้งชื่อและ IP ให้สวิตช์ทั้งสามตัว (1/2)

PNETLAB (สวิตช์จำลอง) แยกออกว่ากำลังพิมพ์อยู่ที่สวิตช์ตัวไหน และ ping ถึงกันได้ทั้งสามตัว

1. ที่ CX-CORE-1/1 ตั้งชื่อและ IP บนพอร์ตที่ต่อหากัน (1/1/5 คือเส้น keepalive)

```
configure terminal
hostname CX-CORE-1-1
interface 1/1/5
  no shutdown
  ip address 192.168.0.2/24
```

2. ที่ CX-CORE-1/2 ทำแบบเดียวกันแต่เปลี่ยนเลข

```
hostname CX-CORE-1-2
interface 1/1/5
  no shutdown
  ip address 192.168.0.3/24
```

3. ที่ CX-CORE-2 ตั้งชื่อไว้ก่อน ส่วน IP 192.168.0.4 ใช้ตอนทำ LAB 4

```
hostname CX-CORE-2
```

ตรวจสอบผล

```
show interface brief
show ip interface brief
ping 192.168.0.3
```

ระวัง

ping ไม่ผ่านให้ดูก่อนว่าใส่ IP ผิดตัวหรือเปล่า — console ทั้งสามหน้าต่างเหมือนกันหมดจนกว่าจะตั้ง hostname

LAB 1 ตั้งชื่อและ IP ให้สวิตช์ทั้งสามตัว (2/2)

PNETLAB (สวิตช์จำลอง) แยกออกจากกำลังพิมพ์อยู่ที่สวิตช์ตัวไหน และ ping ถึงกันได้ทั้งสามตัว

4. ทดสอบว่าคู่ VSX คุยกันได้
ping 192.168.0.3
5. บันทึกทุกตัว
write memory

ตรวจสอบผล

```
show interface brief
show ip interface brief
ping 192.168.0.3
```

ระวัง

ping ไม่ผ่านให้ดูก่อนว่าใส่ IP ผิดตัวหรือเปล่า — console ทั้งสามหน้าต่างเหมือนกันหมดจนกว่าจะตั้ง hostname

LAB 2 VLAN ของแต่ละ PC (1/2)

PNETLAB (สวิตช์จำลอง) ให้ PC ทั้งสามเครื่องอยู่คนละ VLAN คนละวง — ชั้นแรกของการทดสอบ inter-VLAN routing

1. สร้าง VLAN ทั้งสามวงบนคู่ VSX — ทำเหมือนกันทั้ง CX-CORE-1/1 และ CX-CORE-1/2

```
configure terminal
vlan 11
    name PC11
vlan 12
    name PC12
vlan 21
    name PC21
```

2. ที่ CX-CORE-1/1 ตั้งพอร์ตที่ PC11 เสียบให้เป็น VLAN 11

```
interface 1/1/3
    no shutdown
    no routing
    vlan access 11
```

ตรวจสอบ

```
show vlan
show interface brief
show mac-address-table
```

ระวัง

ตอนนี้ PC ยังคุยข้ามกันไม่ได้เลย เพราะยังไม่มี SVI ให้ routing และยังไม่มี LAG เป็นเรื่องปกติ — จะเห็นความต่างชัดหลังทำ LAB 4

LAB 2 VLAN ของแต่ละ PC (2/2)

PNETLAB (สวิตช์จำลอง) ให้ PC ทั้งสามเครื่องอยู่คนละ VLAN คนละวง — ชั้นแรกของการทดสอบ inter-VLAN routing

3. ที่ CX-CORE-1/2 ตั้งพอร์ตที่ PC12 เลียบให้เป็น VLAN 12

```
interface 1/1/1
no shutdown
no routing
vlan access 12
```

4. ที่ CX-CORE-2 สร้าง VLAN 21 แล้วตั้งพอร์ตที่ PC21 เลียบ

```
configure terminal
vlan 21
name PC21
interface 1/1/3
no shutdown
no routing
vlan access 21
```

5. ตั้ง IP ให้ PC — PC11 192.168.11.11 · PC12 192.168.12.12 · PC21 192.168.21.21 gateway ของแต่ละเครื่องคือ

.1 ของวงตัวเอง แล้วบันทึก config สวิตช์

```
write memory
```

ตรวจสอบผล

```
show vlan
show interface brief
show mac-address-table
```

ระวัง

ตอนนี้ PC ยังคุยข้ามกันไม่ได้เลย เพราะยังไม่มี SVI ให้ routing และยังไม่มี LAG เป็นเรื่องปกติ — จะเห็นความต่างชัดหลังทำ LAB 4

LAB 3 จับคู่ VSX (1/2)

PNETLAB (สวิตช์จำลอง) ทำให้ CX-CORE-1/1 กับ CX-CORE-1/2 เป็นคู่ VSX ที่มองจากข้างล่างเหมือนสวิตช์ตัวเดียว

1. สร้าง ISL เป็น LAG บนพอร์ต 1/1/6 — ทำเหมือนกันทั้งสองตัว

```
configure terminal
interface lag 256
  no shutdown
  description VSX-ISL
  no routing
  vlan trunk native 1
  vlan trunk allowed all
  lacp mode active
interface 1/1/6
  no shutdown
  lag 256
```

ตรวจสอบผล

```
show vsx status
show vsx brief
show lacp interfaces
```

ระวัง

system-mac ต้องเป็นค่าเดียวกันทั้งคู่ ถ้าใส่ไม่ตรงกัน VSX จะไม่ขึ้น · ISL ใช้ 1/1/6 ส่วน keepalive ใช้ 1/1/5 อย่าสลับกัน

LAB 3 จับคู่ VSX (2/2)

PNETLAB (สวิตช์จำลอง) ทำให้ CX-CORE-1/1 กับ CX-CORE-1/2 เป็นคู่ VSX ที่มองจากข้างล่างเหมือนสวิตช์ตัวเดียว

2. ที่ CX-CORE-1/1 ตั้งเป็น primary — keepalive รังบน 1/1/5 ที่ใส่ IP ไว้ใน LAB 1

```
vsx
system-mac 02:00:00:00:01:00
inter-switch-link lag 256
role primary
keepalive peer 192.168.0.3 source 192.168.0.2
```

3. ที่ CX-CORE-1/2 ตั้งเป็น secondary — system-mac ต้องตรงกัน

```
vsx
system-mac 02:00:00:00:01:00
inter-switch-link lag 256
role secondary
keepalive peer 192.168.0.2 source 192.168.0.3
```

4. บันทึกทั้งสองตัว

```
write memory
```

ตรวจสอบผล

```
show vsx status
show vsx brief
show lacp interfaces
```

ระวัง

system-mac ต้องเป็นค่าเดียวกันทั้งคู่ ถ้าใส่ไม่ตรงกัน VSX จะไม่ขึ้น · ISL ใช้ 1/1/6 ส่วน keepalive ใช้ 1/1/5 อย่าสลับกัน

LAB 4 Active Gateway, LAG และ Inter-VLAN routing (1/4)

PNETLAB (สวิตช์จำลอง) ให้แต่ละ VLAN มี gateway อยู่บนคู่ VSX แล้วทำให้ PC ทั้งสามเครื่อง ping ข้าม VLAN หากันได้

1. ที่ CX-CORE-1/1 สร้าง SVI ของทั้งสาม VLAN พร้อม active gateway — ตัวนี้ใช้เลขลงท้าย .2

```
configure terminal
interface vlan 11
  ip address 192.168.11.2/24
  active-gateway ip 192.168.11.1 mac 02:00:00:00:00:11
interface vlan 12
  ip address 192.168.12.2/24
  active-gateway ip 192.168.12.1 mac 02:00:00:00:00:12
interface vlan 21
  ip address 192.168.21.2/24
  active-gateway ip 192.168.21.1 mac 02:00:00:00:00:21
```

2. ที่ CX-CORE-1/2 ทำ SVI ทั้งสามวงแบบเดียวกัน เปลี่ยนเฉพาะเลขลงท้ายเป็น .3 — ส่วน active-gateway ทั้ง ip และ mac ต้องเหมือนกับ CX-CORE-1/1 ทุกตัว ไม่งั้น gateway จะย้ายข้างไม่ได้ตอน failover

ตรวจสอบ

```
show ip route
show ip interface brief
show vsx status
show lacp interfaces
```

ระวัง

ping ข้าม VLAN ไม่ผ่านให้ไล่ตามลำดับ — PC ping gateway ตัวเองได้ไหม → show ip route เห็นวงปลายทางไหม → VLAN นั้นอยู่ใน vlan trunk allowed ของ LAG หรือยัง

LAB 4 Active Gateway, LAG และ Inter-VLAN routing (2/4)

PNETLAB (สวิตช์จำลอง) ให้แต่ละ VLAN มี gateway อยู่บนคู่ VSX แล้วทำให้ PC ทั้งสามเครื่อง ping ข้าม VLAN หากันได้

3. ที่คู่ VSX สร้าง multi-chassis LAG ลง CX-CORE-2 ให้ VLAN 21 ผ่านได้ — CX-CORE-1/1 ใช้พอร์ต 1/1/1 · CX-CORE-1/2 ใช้ 1/1/2

```
interface lag 1 multi-chassis
  no shutdown
  no routing
  vlan trunk native 1
  vlan trunk allowed 11,12,21
  lacp mode active
interface 1/1/1
  no shutdown
  lag 1
```

ตรวจสอบผล

```
show ip route
show ip interface brief
show vsx status
show lacp interfaces
```

ระวัง

ping ข้าม VLAN ไม่ผ่านให้ไล่ตามลำดับ — PC ping gateway ตัวเองได้ไหม → show ip route เห็นวงปลายทางไหม → VLAN นั้นอยู่ใน vlan trunk allowed ของ LAG หรือยัง

LAB 4 Active Gateway, LAG และ Inter-VLAN routing (3/4)

PNETLAB (สวิตช์จำลอง) ให้แต่ละ VLAN มี gateway อยู่บนคู่ VSX แล้วทำให้ PC ทั้งสามเครื่อง ping ข้าม VLAN หากันได้

4. ที่ CX-CORE-2 สร้าง LAG ธรรมดาแล้วใส่ทั้งสองพอร์ตเข้าไป

```
interface lag 1
  no shutdown
  no routing
  vlan trunk native 1
  vlan trunk allowed 11,12,21
  lacp mode active
interface 1/1/1-1/1/2
  no shutdown
  lag 1
write memory
```

5. ทดสอบ inter-VLAN routing: ping จาก PC21 (VLAN 21) ไป PC11 (VLAN 11) และ PC12 (VLAN 12) ต้องผ่าน และ ping gateway ของตัวเองต้องผ่านก่อนเสมอ

ตรวจสอบผล

```
show ip route
show ip interface brief
show vsx status
show lacp interfaces
```

ระวัง

ping ข้าม VLAN ไม่ผ่านให้ไล่ตามลำดับ — PC ping gateway ตัวเองได้ไหม → show ip route เห็นวงปลายทางไหม → VLAN นั้นอยู่ใน vlan trunk allowed ของ LAG หรือยัง

LAB 4 Active Gateway, LAG และ Inter-VLAN routing (4/4)

PNETLAB (สวิตช์จำลอง) ให้แต่ละ VLAN มี gateway อยู่บนคู่ VSX แล้วทำให้ PC ทั้งสามเครื่อง ping ข้าม VLAN หากันได้

6. ทดสอบ failover: shutdown พอร์ต 1/1/1 ที่ CX-CORE-1/1 แล้ว ping ต้องยังผ่าน — gateway ย้ายไปอยู่อีกตัวโดยที่ PC ไม่รู้ตัว

```
interface 1/1/1
shutdown
no shutdown
```

ตรวจสอบผล

```
show ip route
show ip interface brief
show vsx status
show lacp interfaces
```

ระวัง

ping ข้าม VLAN ไม่ผ่านให้ไล่ตามลำดับ — PC ping gateway ตัวเองได้ไหม → show ip route เห็นวงปลายทางไหม → VLAN นั้นอยู่ใน vlan trunk allowed ของ LAG หรือยัง

ArubaOS-CX switch CLI contexts

Operator (>)

- Enables execution of commands to view—but not change—the configuration
- Switch prompt:
 - switch>

Manager (#)

- From manager context (#), execute commands that do not require saving changes to configuration
- Switch prompt:
 - switch#

Global configuration (config)#

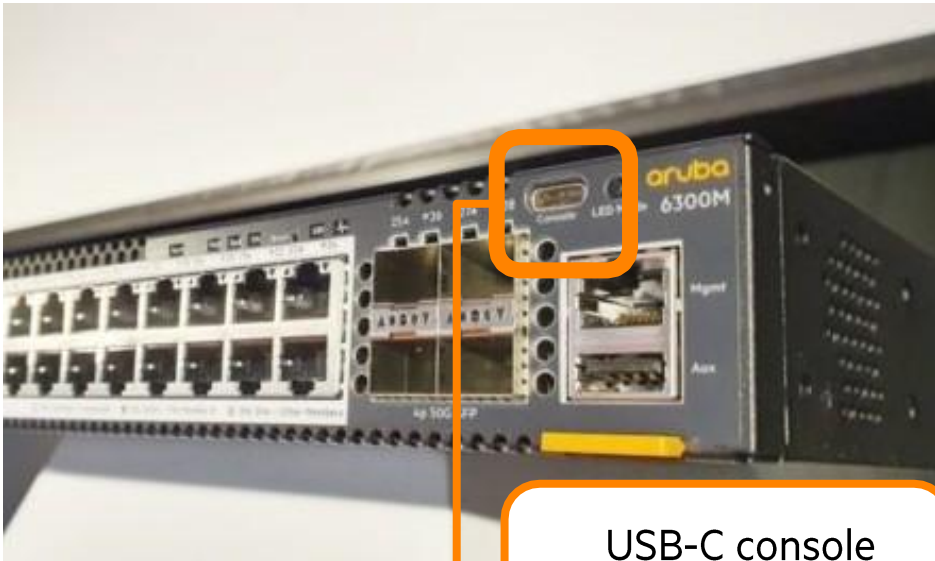
- From global configuration context (config), execute commands that change configuration of switch
- Switch prompt:
 - switch(config)#

Other configuration

- switch(config-if)#
- switch(config-router)#
- switch(config-vlan-100)#

Note: If you log into a device with the admin role you are immediately put into enable context. Type 'exit' at enable to disconnect (not be put into operator mode).

Connecting to Console Port



USB-C console
No RJ45 console
(CX6300)



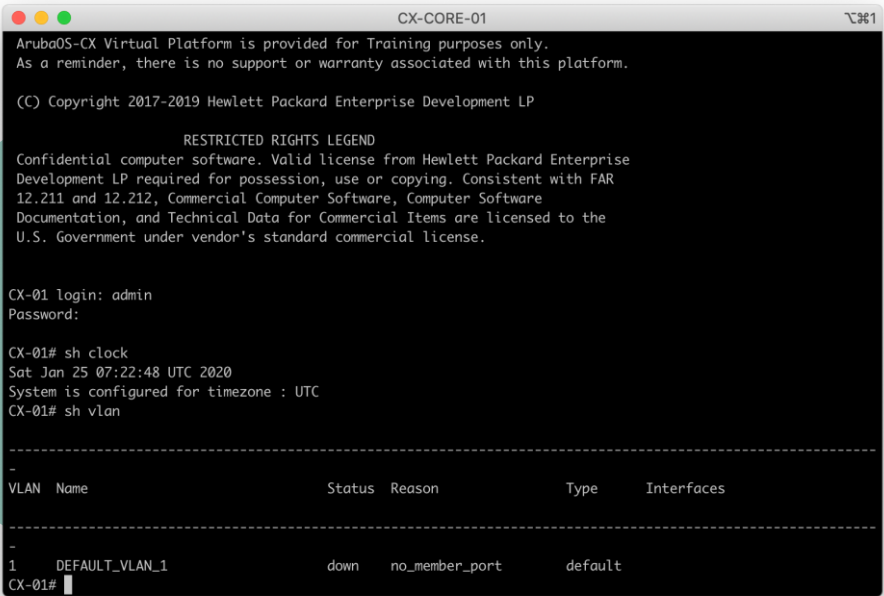
CX Switch

Direct serial connection to console port

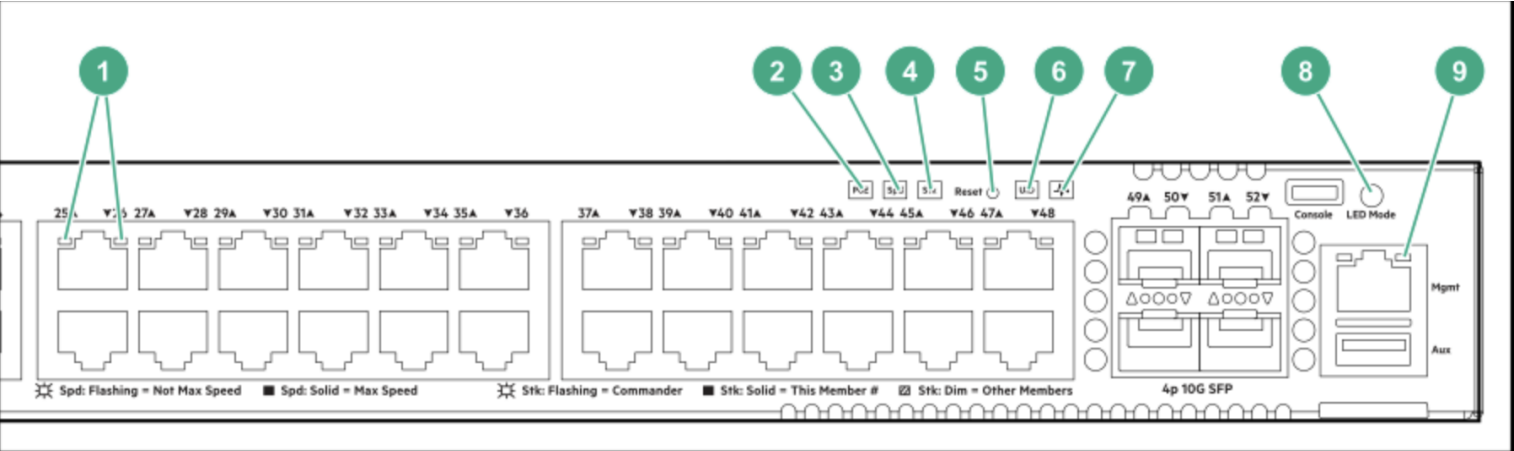
CX Switch	Serial Console Type
8400, 8325-48Y8C	RJ45 and Micro USB-B
8320, 8325-32C	RJ45
6400	RJ45 and USB-C
6300	USB-C
6200 (12 port)	USB-C, RJ45

Terminal software settings

- Speed: 115200 bps
- Data bits: 8
- Stop bits: 1
- Parity: None
- Flow control: None



Switch LEDs



Label	Description
1	Switch port LEDs
2	PoE LED (only support POE)
3	Speed mode selected LED
4	Stk LED
5	Reset button
6	UID (Unit Identification)
7	Global Status LED
8	Mode select button
9	OOBM port LED

User Accounts

- admin is the default user with **no password**
- Administrators
 - Users with administrator rights can execute any command.
 - Default setting will have admin user account without password, and you are required to enter a **new password after login**
- Operators
 - Users with operator rights can execute commands in the operator context (>) only
- Auditors
 - Users with auditor rights can execute commands in the auditor context (**auditor>**) only
 - Limited view of show command

Lab 1.1 – Initialize Admin Account and Change Hostname

```
switch login: admin  
Password:
```

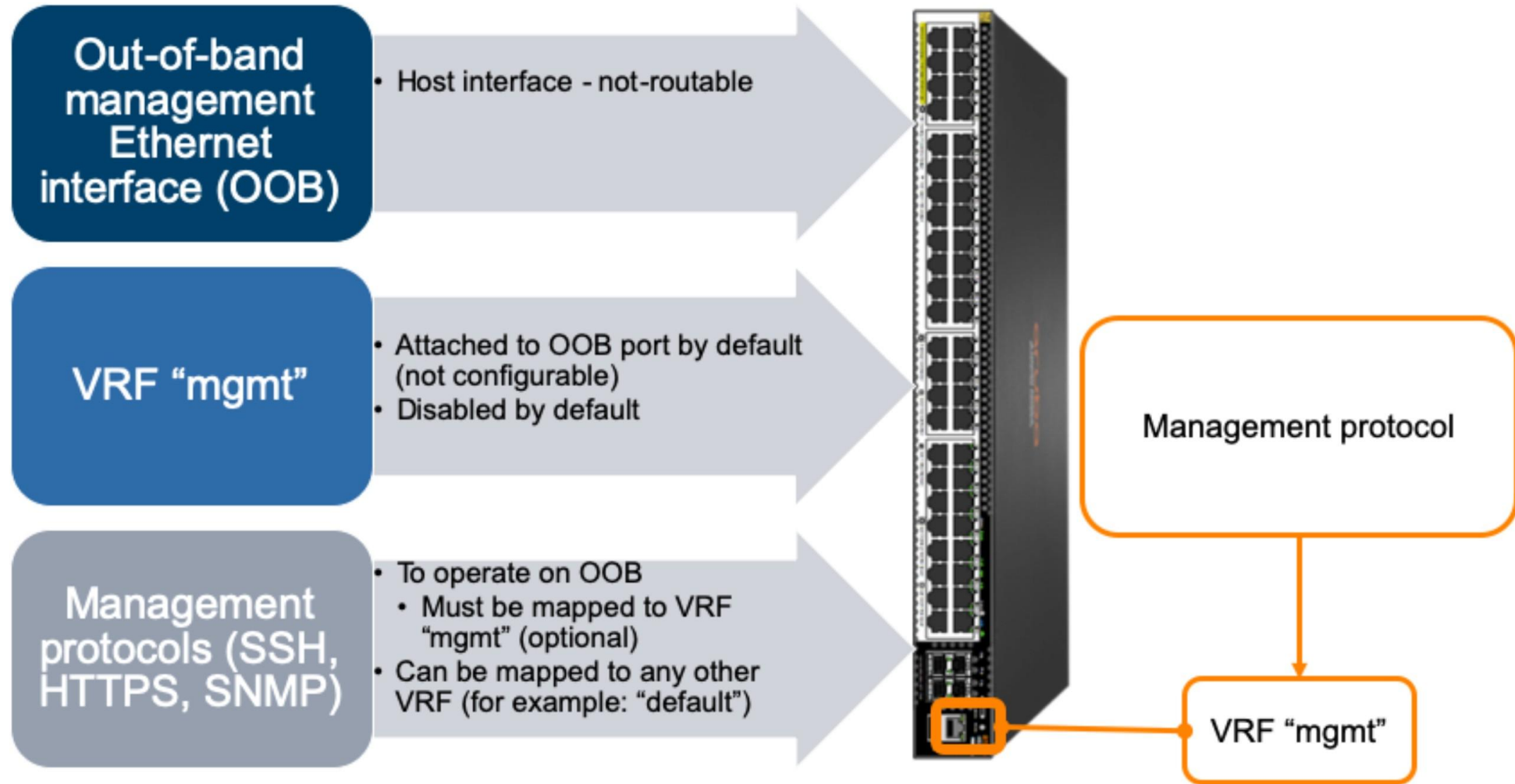
```
Please configure the 'admin' user account  
password. Enter new Password: ****  
Confirm new password: ****
```

1. Default setting will have admin user account without password, and you are required to enter a new password after login
2. Enter any password string you want, we will change to the new one in the next lab

```
Switch# config terminal  
Switch(config)# hostname CX-CORE-01  
CX-CORE-01(config)#
```

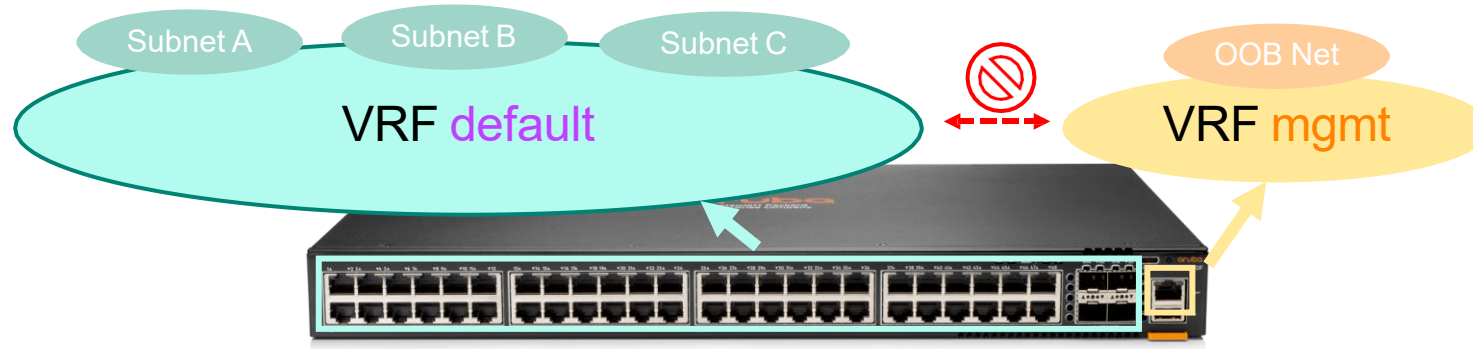
1. Change switch name to CX-CORE-01

Out of band Management



VRF-lite in ArubaOS-CX

- VRF technology is an integral part of the operating system
- There is two default VRF called default and mgmt
 - The management interface belongs to the **mgmt**
 - All data L3 interfaces belong to the **default**



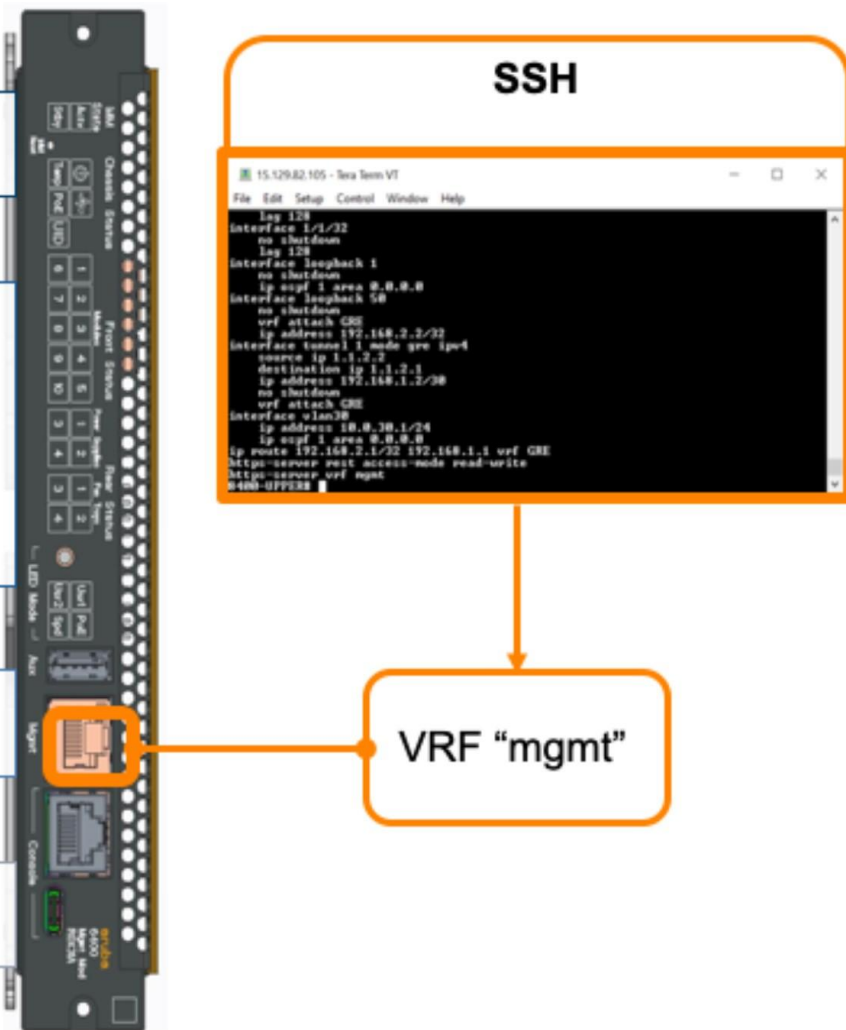
have a password

Must be attached to a VRF

- “mgmt” for OOB management
- “default”
- Any other

for multiple VRFs

supported	
-----------	--



HTTPS Server - WebUI

Requires the admin user to have a password

Must be attached to a VRF

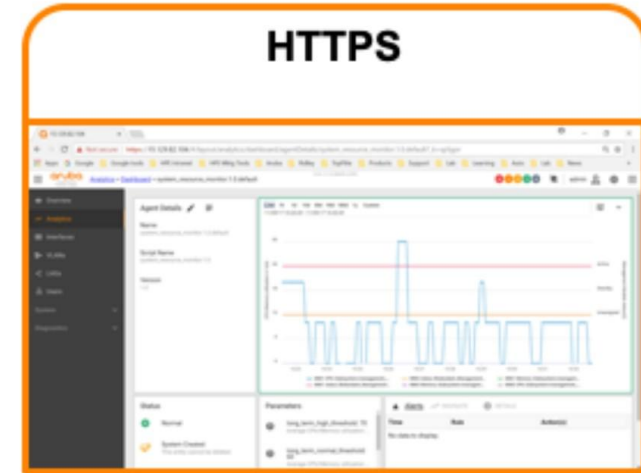
- “mgmt” for OOB management
- “default”
- Any other

Can be assigned simultaneously to multiple VRFs

API is accessible in read-only or read-write

Web-UI is disabled by default

Note: HTTP server is not supported



VRF “mgmt”

REST Interface

Requires admin user to have a password

REST reached via HTTPS

Access can be read-write or read-only (default read-only)



REST

ArubaOS-CX REST API

RESTful interface for ArubaOS-CX switch software

AAA_Server_Group	Show/Hide	Lock Operations	Expand Operations
AAA_Server_Group_Profile	Show/Hide	Lock Operations	Expand Operations
ACL	Show/Hide	Lock Operations	Expand Operations
ACL_Entry	Show/Hide	Lock Operations	Expand Operations
Aggregate_address	Show/Hide	Lock Operations	Expand Operations
SGP_Path_Filter	Show/Hide	Lock Operations	Expand Operations
SGP_Path_Filter_Entry	Show/Hide	Lock Operations	Expand Operations
SGP_Community_Filter	Show/Hide	Lock Operations	Expand Operations
SGP_Community_Filter_Entry	Show/Hide	Lock Operations	Expand Operations
SGP_Neighbor	Show/Hide	Lock Operations	Expand Operations
SGP_Route	Show/Hide	Lock Operations	Expand Operations
SGP_Router	Show/Hide	Lock Operations	Expand Operations

VRF "mgmt"

Lab 1.3 - Enable Remote Management Access

```
CX-CORE-01# configure terminal
CX-CORE-01(config)# https-server vrf mgmt
CX-CORE-01(config)# ssh server vrf mgmt
CX-CORE-01(config)# https-server rest access-mode read-only
CX-CORE-01(config)# interface mgmt
CX-CORE-01(config-if-mgmt)# ip static 10.1.10.101-103/24
CX-CORE-01(config-if-mgmt)# default-gateway 10.1.10.1
CX-CORE-01(config-if-mgmt)# nameserver 8.8.8.8
CX-CORE-01(config-if-mgmt)# no shutdown
```

- 1. Bind the https and ssh server with VRF “mgmt.”
- 2. Assign IP address, Gateway and DNS to the management interface

- 1. Open the browser and see if you can access CX switches
- 2. SSH CX switches and make sure you have the access
- 3. Ping to the switch IP address on mgmt VRF

MGMT IP Address
Group1 - CX-CORE = 10.1.10.101-103/24
Group2 - CX-CORE = 10.1.10.104-106/24
Group3 - CX-CORE = 10.1.10.107-109/24
Group4 - CX-CORE = 10.1.10.110-112/24
Group5 - CX-CORE = 10.1.10.113-115/24
Group6 - CX-CORE = 10.1.10.116-118/24
Group7 - CX-CORE = 10.1.10.119-121/24

ping 10.1.10.101
PING 10.1.10.101 (10.1.10.101) 100(128) bytes of data.

108	bytes	from	10.1.10.101:	icmp_seq=1	ttl=128	time=1.04 ms
108	bytes	from	10.1.10.101:	icmp_seq=2	ttl=128	time=0.454 ms
108	bytes	from	10.1.10.101:	icmp_seq=3	ttl=128	time=0.763 ms
108	bytes	from	10.1.10.101:	icmp_seq=4	ttl=128	time=0.681 ms
108	bytes	from	10.1.10.101:	icmp_seq=5	ttl=128	time=0.604 ms

Lab 1.4 – Configure Clock, Timezone, DNS and SNMP

- Some of the basic configuration like DNS and Logging supports VRF binding

```
CX-CORE-01 # configure terminal
CX-CORE-01(config)# clock timezone Asia/Bangkok
CX-CORE-01(config)# ip dns server-address 8.8.8.8 vrf mgmt
CX-CORE-01(config)# ntp server 0.th.pool.ntp.org
CX-CORE-01(config)# ntp vrf mgmt
CX-CORE-01(config)# ntp enable
CX-CORE-01(config)# snmp-server system-description CX-CORE-01
CX-CORE-01(config)# snmp-server system-contact Administrator
CX-CORE-01(config)# snmp-server system-location CX_LAB
CX-CORE-01(config)# snmp-server community cx_snmp
CX-CORE-01(config)# snmp-server vrf mgmt
CX-CORE-01(config)# snmp-server host x.x.x.x trap version v2c community cx_snmp
CX-CORE-01(config)# logging x.x.x.x vrf mgmt
```

- SNMP trap and log server are dummy IP address. It is intended for student to practice how to config these two settings.

```
CX-CORE-01# sh ntp associations
```

ID	NAME	REMOTE	REF-ID	ST	LAST	POLL	REACH
* 1	0.th.pool.ntp.org	202.12.97.45	.PPS.	1	7	64	377

```
CX-CORE-01# show clock
Tue Jan 28 13:50:39 ICT 2020
System is configured for timezone : Asia/Bangkok
```

- Verify date, time and timezone

Configuration Management

- “**write memory**” to save running configuration into the Startup configuration
- **Types of checkpoints**
 - **System generated checkpoints:** Checkpoints that the system automatically generates whenever a configuration change is detected.
 - **User generated checkpoints:** Checkpoints that the user manually generates
- Total limit of checkpoint is **64** including the startup configuration; **32** each type
- After the limit the system will overwrite the oldest checkpoint
- For each additional configuration change, the **300** second timeout counter is reset. Once the timeout limit is reached with no additional configuration changes detected, the system will automatically generate a new checkpoint
- This system generated checkpoints are listed with a time stamp format CPC<**YYYYMMDDHHMMSS**>
- The checkpoints can be applied using the “**checkpoint rollback**” or “**copy checkpoint**” command
- **Difference** between two configuration can be viewed between two different checkpoints or between any checkpoint and the startup/running configuration

Lab 1.5 – Creating Configuration Checkpoint

```
CX-CORE-01 # copy running-config checkpoint initial_config
Large configuration changes will take time to process, please be patient.
```

```
CX-CORE-01# show checkpoint
CPC20200128072408
CPC20200128075706
initial_config
```

- Use this command to show all saved configuration checkpoint

```
CX-CORE-01# show checkpoint initial_config
. . .
. . .
```

- Use this command to show initial_config checkpoint

Lab 1.7 – Checkpoint Rollback

Use the **same CX switch in lab 1.6** to do this lab

```
CX-CORE-01# sh session-timeout
session-timeout: 0 minute
```

```
CX-CORE-01# sh banner motd
#####
TEST BANNER
#####
```

```
CX-CORE-01# sh snmp community
-----
SNMP communities
-----
public
```

1. Record the show output result and verify the difference after perform a configuration rollback

2. After that, issue a rollback command. You have two way to rollback your configuration to any checkpoint
3. Verify the show out result after rollback your configuration. What is the difference?

```
CX-CORE-01# copy checkpoint initial_config running-config
Configuration changes will take time to process, please be patient.
```

Option 1

```
CX-CORE-01# checkpoint rollback initial_config
Configuration changes will take time to process, please be patient.
```

Option 2

Knowledge Check #1

Which console interfaces and default baud rates are supported on the HPE Aruba CX 6200F 12-port model? (Select two.)

- a. USB-A, baud rate = 115200
- b. USB-C, baud rate = 9600
- c. RJ-45, baud rate = 115200
- d. USB-C, baud rate = 115200
- e. RJ-45, baud rate = 112500

Knowledge Check #2

Does the HPE Aruba 6200F model support only two VRF?

- a. True.
- b. False.

Knowledge Check #3

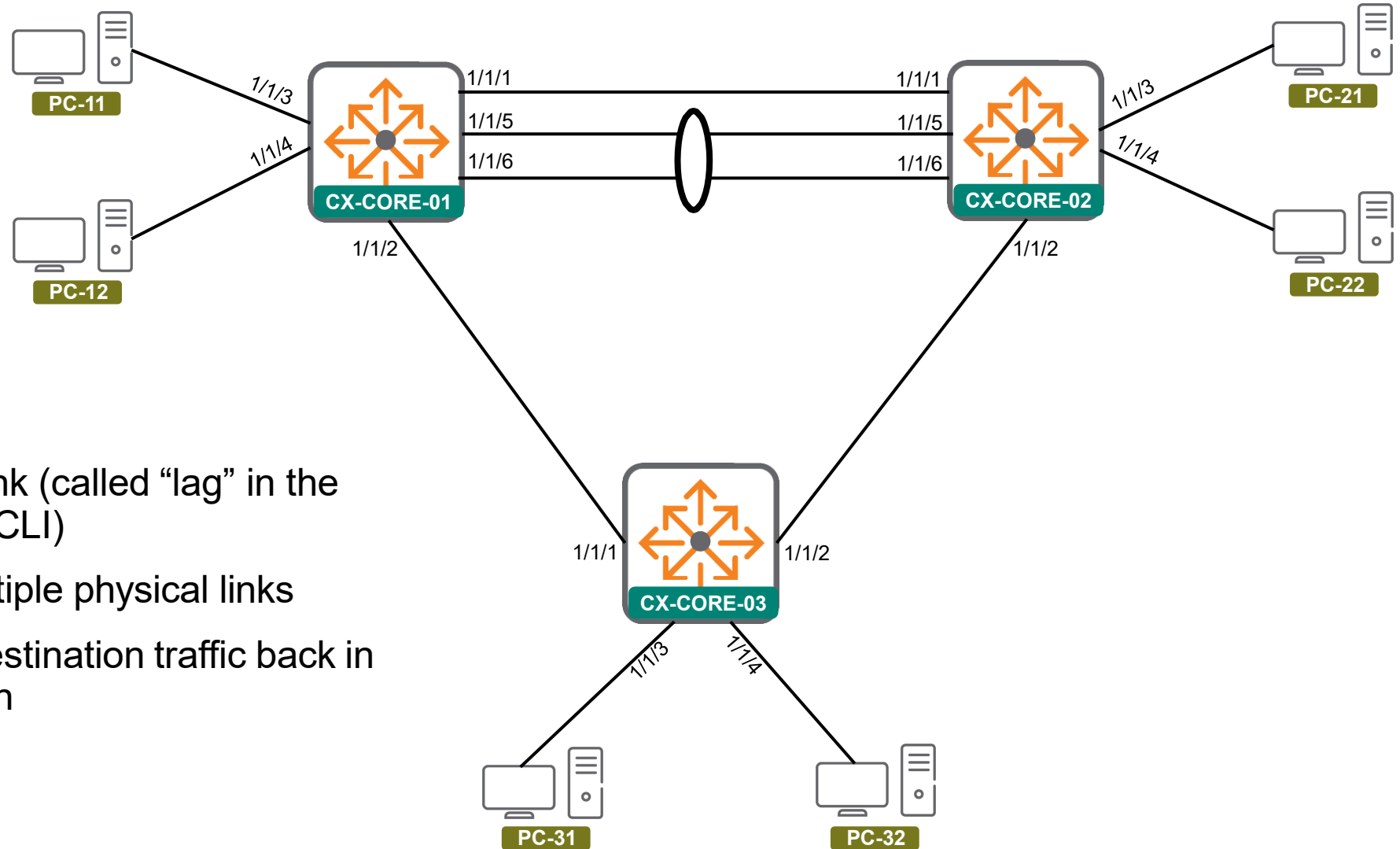
The REST API on Aruba CX supports both read and write operations (GET, POST, PUT, DELETE)?

- a. True.
- b. False.

Lab 2

Layer 2 Switching and Features

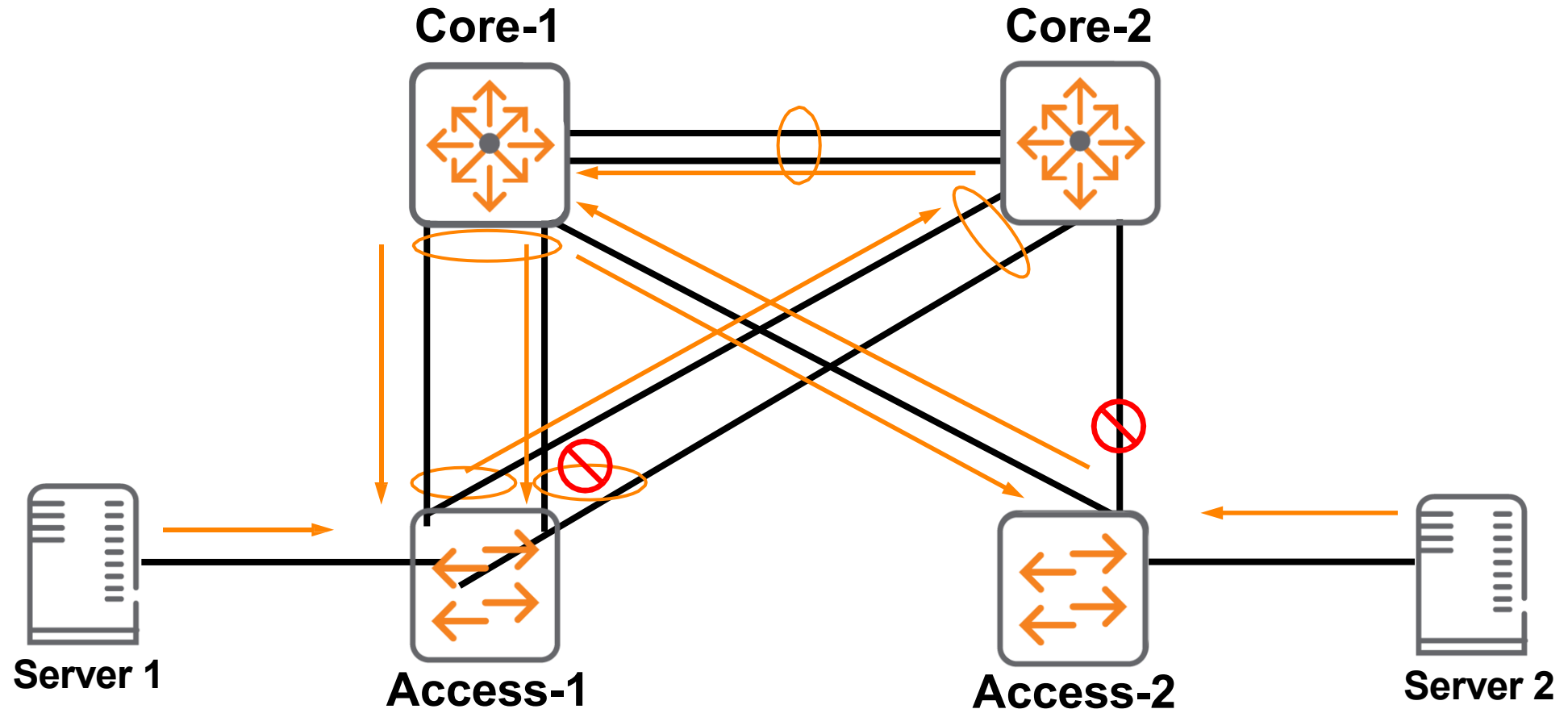
Link Aggregation



- Acts as one logical link (called “lag” in the ArubaOS-CX switch CLI)
- Carries traffic on multiple physical links
- Never floods multi-destination traffic back in the same aggregation

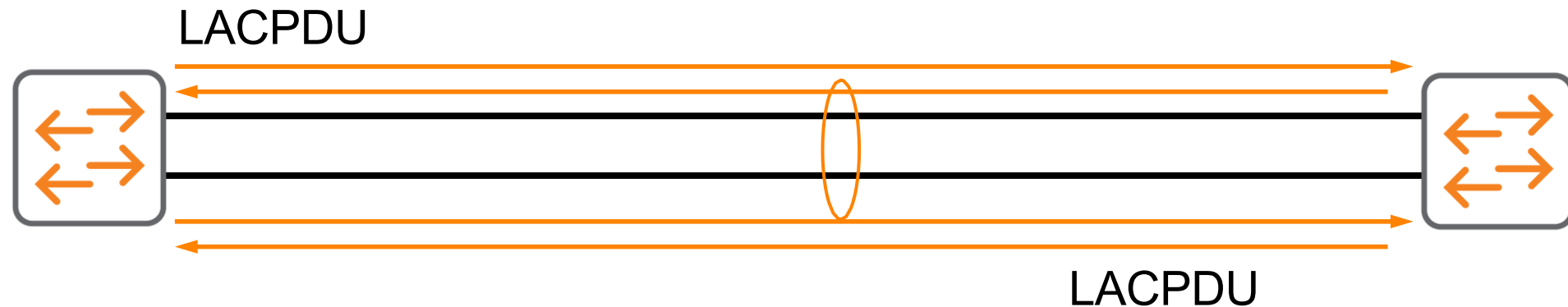
Potential issue with manual link aggregation

- What if you accidentally configure the wrong ports in a link aggregation?



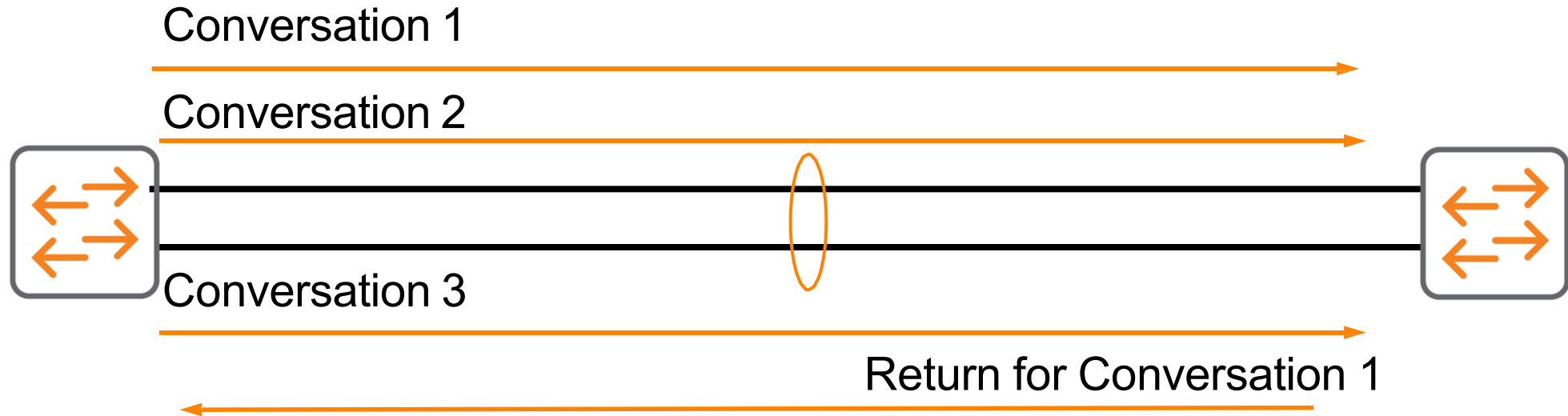
LACP

- Uses messages to establish the link aggregation
- Ensures that all links are connected to the same peer (system ID) and link aggregation (operational key)
- Ensures compatibility for other settings
- Manages adding and removing links

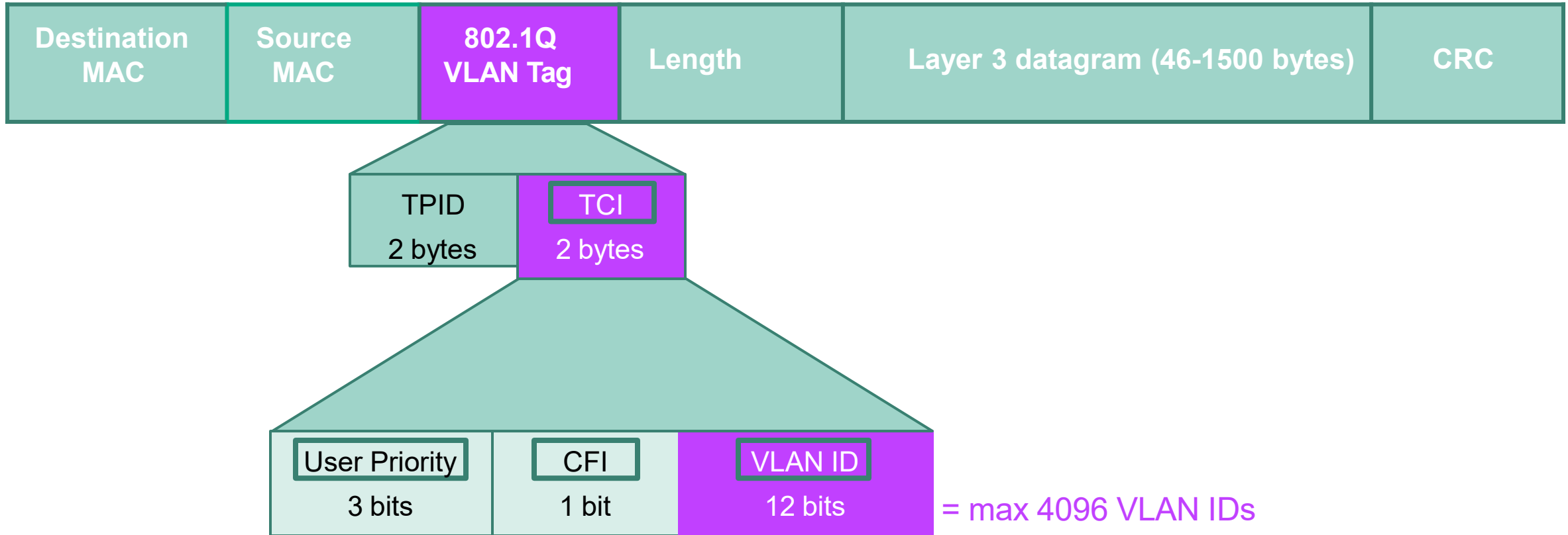


Load-sharing traffic over a link aggregation

- The link aggregation uses a hash to select a link for each *conversation*:
 - Conversation defined by the load-sharing mode
 - MAC source and destination address (L2-based)
 - IP source and destination address (L3-based) = Default option
 - Source and destination UDP/TCP ports (L4-based) = Only 8400 series switches support L4 hashing
 - Link for a conversation stays constant
 - Traffic tends to be balanced more evenly as conversations increase



Ethernet Frame Structure



Knowledge Check

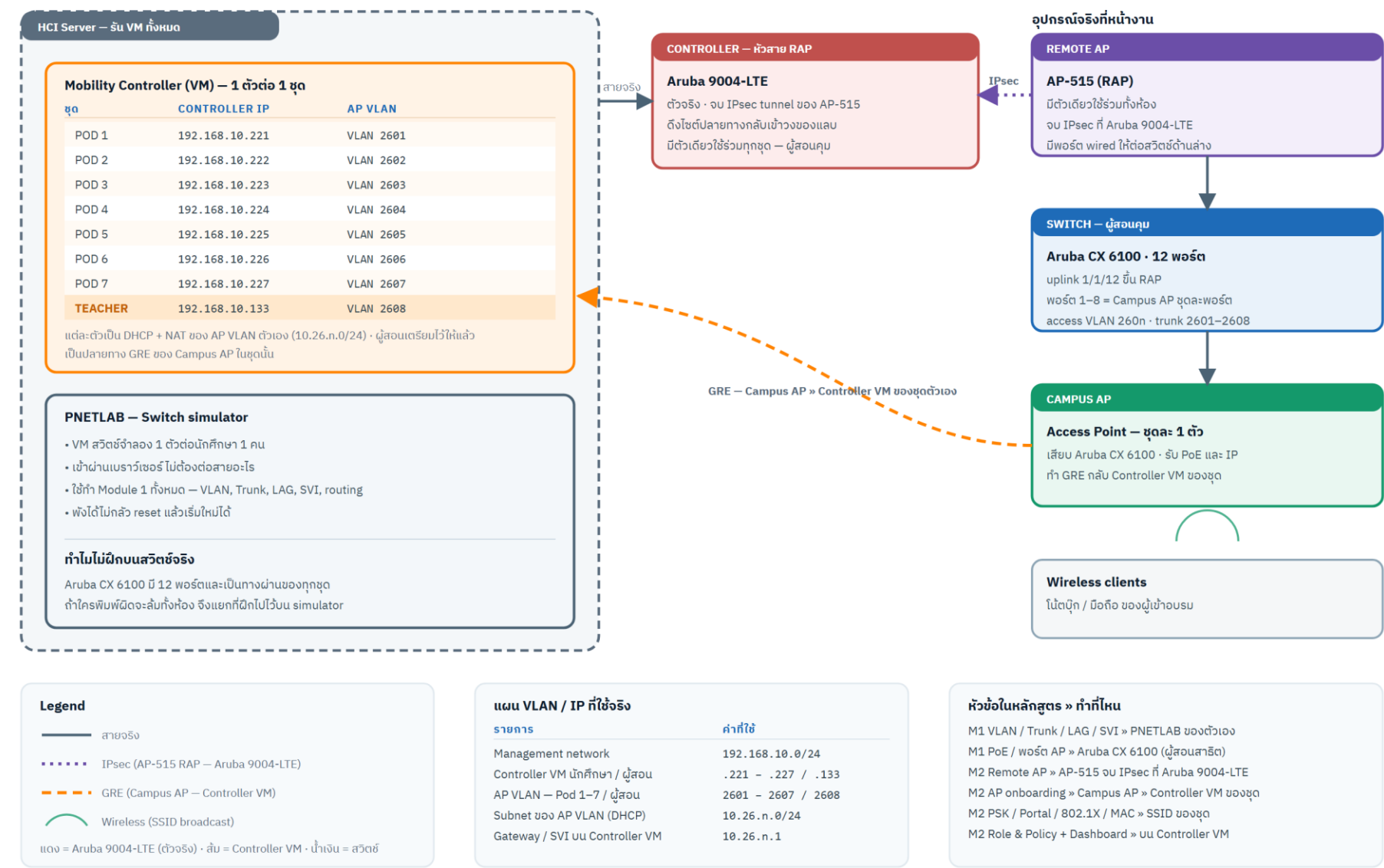
What feature allows combining multiple physical links into a single logical interface?

- a. VLAN
- b. STP
- c. LACP (Link Aggregation Control Protocol)
- d. LLDP

WLAN Labs

Aruba Campus Network Training — Lab Topology

RMUTT x Commserv Siam · 26 ส.ค. 2569 · RAP จบที่ Aruba 9004-LTE · Campus AP จบที่ Controller VM ของชุดตัวเอง · 7 ชุดนักศึกษา + 1 ชุดผู้สอน



LAB 5 เข้า Controller VM และอ่านค่าที่เตรียมไว้

Controller VM ของชุดตัวเอง เข้าใช้ controller ของชุดตัวเองได้ และรู้ว่าอะไรถูกตั้งไว้ให้แล้วบ้าง

1. เข้าเว็บ controller ของชุดตัวเอง (POD 1 = <https://192.168.10.221:4343>) ผู้ใช้ admin
2. ดู license AP และ PEF ที่ Configuration → License — ผู้สอนใส่ไว้แล้ว
3. ดูเวลาและ timezone ที่ Configuration → System → General ต้องเป็น Asia/Bangkok
4. ดู country code ต้องเป็น TH ไม่งั้น AP จะไม่ยอมกระจายสัญญาณ

ตรวจสอบ

```
show switchinfo  
show license  
show clock
```

ระวัง

เวลาผิดพลาดให้ certificate ของ AP ไม่ผ่านแล้ว AP จะไม่ขึ้น — ถ้าเจอ AP ไม่ขึ้นทั้งชุด ให้ดูเวลาก่อน

LAB 6 VLAN, SVI, DHCP และ NAT บน Controller

Controller VM ของชุดตัวเอง ทำให้ controller เป็น gateway และ DHCP server ของ AP VLAN ของตัวเอง แล้ว NAT ออกเน็ต

1. เปิดหัวข้อ Config ด้านบน เลือกแท็บชุดตัวเอง กดคัดลอก แล้ววางลง CLI ของ controller
2. อ่านทีละท่อนว่าแต่ละบล็อกทำอะไร — VLAN กับ SVI ที่มี ip nat inside → ช่วง IP ที่กันไม่ให้แจก → DHCP pool → service dhcp
3. บันทึก
write memory

ตรวจสอบ

```
show ip interface brief  
show ip dhcp binding  
show ip dhcp statistics
```

ระวัง

service dhcp ไม่เปิด pool จะไม่ทำงานแม้ config ถูกหมด ·
เพลอวางของชุดอื่นให้ลบด้วย no interface vlan และ no ip
dhcp pool ก่อนวางใหม่

LAB 7 Campus AP onboarding

Controller VM ของชุดตัวเอง + AP เอา Campus AP ของชุดตัวเอง (1 ตัว) ขึ้นมาอยู่กับ controller ของชุด และแยกเป็น AP group

1. AP ของชุดตัวเองเสียบอยู่ที่ CX 6100 พอร์ตของชุดนั้นแล้ว (POD 1 = 1/1/1) — รับ PoE และ IP จาก DHCP บน controller
2. ถ้า AP เคยใช้ที่อื่นมาก่อน ให้ reset โดยกดปุ่ม reset ค้างเกิน 10 วินาทีตอนเปิดเครื่อง
3. ชี้ AP มาที่ controller ของชุดตัวเอง (convert to campus mode)
4. อนุมัติ AP ที่ Configuration → Access Points → Allowlist → Approve
5. สร้าง AP group ของชุดตัวเอง แล้วย้าย AP เข้ากลุ่ม

ตรวจสอบ

```
show ap database  
show ap active  
show ip dhcp binding
```

ระวัง

AP ไม่ขึ้นให้ไล่จากล่างขึ้นบน — พอร์ตบน CX 6100 ไขของชุดเราใหม่ → ได้ IP ใหม่ → เห็นใน show ap database ใหม่

LAB 8 WLAN — PSK และ MAC Authentication

Controller VM ของชุดตัวเอง สร้าง SSID แรกด้วย PSK แล้วเพิ่มการตรวจ MAC จากฐานข้อมูลในตัว controller

1. สร้าง WLAN ที่ Configuration → WLANs → + ตั้งชื่อ SSID เป็นของชุดตัวเอง เช่น POD1-IOT
2. เลือก AP group ของตัวเอง · VLAN 2601 · Forwarding mode Tunnel
3. ตั้ง security เป็น Personal (PSK) แล้วทดสอบด้วยโน้ตบุ๊ก
4. เพิ่ม MAC ของเครื่องทดสอบเป็น local user ที่ Configuration → Authentication → Internal Server → Users โดยใช้ MAC เป็นทั้ง username และ password
5. เปิด MAC authentication บน WLAN เดิม แล้วทดสอบใหม่

ตรวจสอบผล

```
show user-table  
show ap association
```

ระวัง

ใส่ MAC ผิดฟอร์แมตคือปัญหาที่เจอบ่อย — ดู MAC จริงจาก show user-table ของเครื่องที่เพิ่งต่อ แล้วคัดลอกไปใส่

LAB 9 WLAN — Captive portal สำหรับ Guest

Controller VM ของชุดตัวเอง สร้าง SSID สำหรับผู้มาเยือน ที่ต้องล็อกอินผ่านหน้าเว็บก่อนใช้งาน

1. สร้าง WLAN ใหม่ ชื่อ POD1-GUEST · VLAN 2601 · AP group ของตัวเอง
2. เลือก security เป็น Captive portal (Guest)
3. สร้าง guest user ใน Internal Server
4. ต่อด้วยมือถือ — ต้องหน้าจอ login ก่อนถึงจะออกเน็ตได้

ตรวจสอบผล

```
show user-table  
show rights
```

ระวัง

ไม่หน้าจอ login ให้ดูว่าเครื่องได้ IP กับ DNS จริงหรือยัง —
captive portal ต้องให้ DNS ผ่านก่อน

LAB 10 WLAN — 802.1X ด้วย Internal Server

Controller VM ของชุดตัวเอง สร้าง SSID ที่ผู้ใช้งานใส่ username และ password ของตัวเอง โดยตรงกับฐานข้อมูลในตัว controller

1. สร้าง WLAN ใหม่ ชื่อ POD1-EMP · VLAN 2601 · AP group ของตัวเอง
2. เลือก security เป็น Enterprise (802.1X) แล้วเลือก auth server เป็น Internal
3. สร้าง user ที่ Configuration → Authentication → Internal Server → Users
4. ต่อด้วยโน้ตบุ๊ก ใส่ username และ password ที่สร้างไว้

ตรวจสอบผล

```
show user-table  
show aaa authentication-server internal
```

ระวัง

งานนี้ไม่มี ClearPass — 802.1X ทำได้เฉพาะฝั่ง WLAN ที่ controller ตรวจสอบ ฝั่ง wired ไม่มี RADIUS ให้ใช้

LAB 11 Role, Policy และ Dashboard

Controller VM ของชุดตัวเอง จำกัดสิทธิ์ผู้ใช้ด้วย role แล้วดูผลบน dashboard

1. สร้าง network alias ของวงที่จะห้าม ที่ Configuration → Roles & Policies → Aliases
2. สร้าง policy ที่ deny ปลายทางเป็น alias นั้น แล้ว permit ที่เหลือ
3. สร้าง role ใหม่ แล้วผูก policy เข้าไป
4. ผูก role ให้ user ที่สร้างไว้ใน LAB 10 แล้วต่อใหม่
5. ดูผลที่ Dashboard → Clients และดู AppRF ว่าเห็น traffic อะไรบ้าง

ตรวจสอบผล

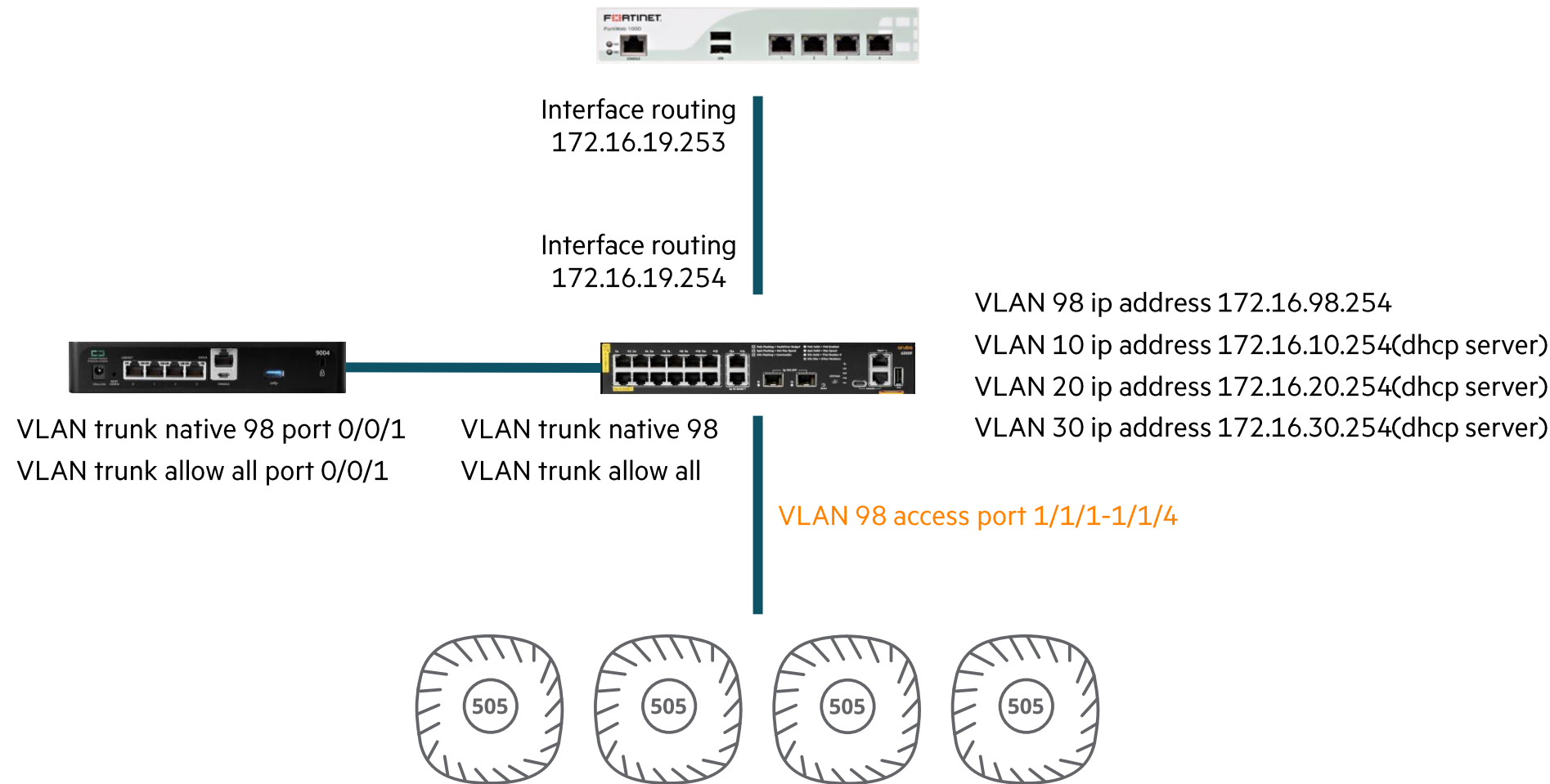
```
show user-table  
show rights  
show datapath session table
```

ระวัง

role ที่ผูกกับ user มีผลตอนต่อใหม่เท่านั้น — ตัดการเชื่อมต่อแล้วต่อใหม่ก่อนสรุปว่า policy ไม่ทำงาน

A. Diagram

Diagram



B.Console Cable

C.Initial Mobility Controller(MC)

- **Initial Controller**
- **Generate trail license AP & PEF**
- **Add License AP & PEF**
- **Set Time**
- **Configure CPSec**

Enter initial command : Full-setup

```
Auto-provisioning is in progress. It requires DHCP and Activate servers
Choose one of the following options to override or debug auto-provisioning...
'enable-debug'      : Enable auto-provisioning debug logs
'disable-debug'     : Disable auto-provisioning debug logs
'mini-setup'        : Start mini setup dialog. Provides minimal customization and requires DHCP server
'full-setup'        : Start full setup dialog. Provides full customization
'static-activate'   : Provides customization for static or PPPoE ip assignment. Uses activate for conductor information

Enter Option (partial string is acceptable): full-setup

Are you sure that you want to stop auto-provisioning and start full setup dialog? (yes/no): yes
```

Auto-provisioning is in progress. It requires DHCP and Activate servers
Choose one of the following options to override or debug auto-provisioning....

- 'enable-debug' : Enable auto-provisioning debug logs
- 'disable-debug' : Disable auto-provisioning debug logs
- 'mini-setup' : Start mini setup dialog. Provides minimal customization and requires DHCP server
- ' **full - setup** ' : Start full setup dialog. Provides full customization
- 'static-activate' : Provides customization for static or PPPoE ip assignment. Uses activate for conductor information

Enter Option (partial string is acceptable): **full-setup**

Are you sure that you want to stop auto-provisioning and start full setup dialog? (yes/no): **yes**

Initial MC-0X

Commands: <Enter> Submit input or use [default value], <ctrl-I> Help
<ctrl-B> Back, <ctrl-F> Forward, <ctrl-A> Line begin, <ctrl-E> Line end
<ctrl-D> Delete, <BackSpace> Delete back, <ctrl-K> Delete to end of line
<ctrl-P> Previous question <ctrl-X> Restart beginning <ctrl-R> Reload box

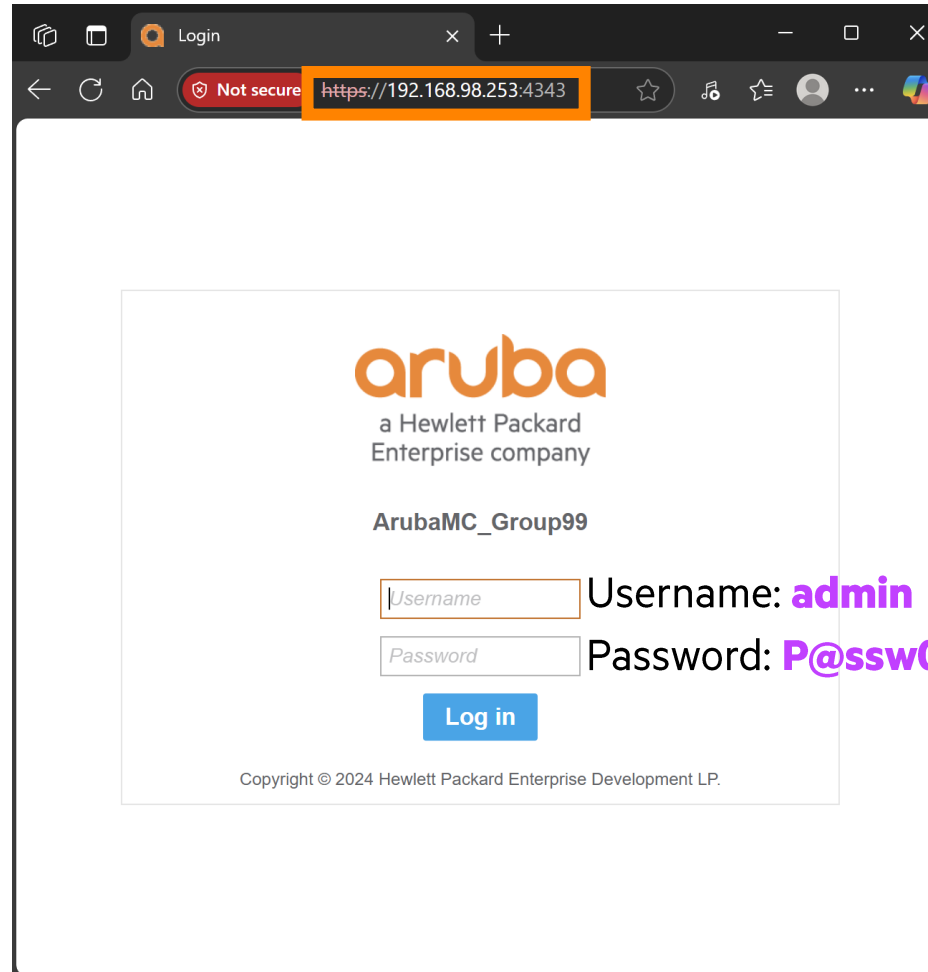
```
Enter System name [Aruba7210_01_B1_F8]: ArubaMC_Group99
Enter Switch Role (conductor|standalone|md) [md]: standalone
Enter Controller VLAN ID [1]: 98
Enter Controller VLAN port [GE 0/0/0]:
Enter Controller VLAN port mode (access|trunk) [access]: trunk
Enter Native VLAN ID [1]: 98
Do you wish to configure IPV4 address on vlan (yes|no) [yes]: yes
Enter VLAN interface IP address [172.16.0.254]: 192.168.98.253
Enter VLAN interface subnet mask [255.255.255.0]: 255.255.255.0
Enter IP Default gateway [none]: 192.168.98.254
Enter DNS IP address [none]: 8.8.8.8
Do you wish to configure IPV6 address on vlan (yes|no) [yes]: no
Enter Country code (ISO-3166), <ctrl-I> for supported list: TH
You have chosen Country code TH for Thailand (yes|no)?: yes
Enter the controller's IANA Time zone [America/Los_Angeles]: Asia/Bangkok
Enter Time in UTC [07:01:44]: 14:04:00
Enter Date (MM/DD/YYYY) [6/14/2025]:
Enter Password for admin login (up to 32 chars): *****
Re-type Password for admin login: *****
```

Commands: <Enter> Submit input or use [default value], <ctrl-I> Help
<ctrl-B> Back, <ctrl-F> Forward, <ctrl-A> Line begin, <ctrl-E> Line end
<ctrl-D> Delete, <BackSpace> Delete back, <ctrl-K> Delete to end of line
<ctrl-P> Previous question <ctrl-X> Restart beginning <ctrl-R> Reload box

```
Enter System name [Aruba7210_01_B1_F8]: ArubaMC_GroupXX
Enter Switch Role (conductor|standalone|md) [md]: standalone
Enter Controller VLAN ID [1]: 98
Enter Controller VLAN port [GE 0/0/0]: [Enter]
Enter Controller VLAN port mode (access|trunk) [access]: trunk
Enter Native VLAN ID [1]: 98
Do you wish to configure IPV4 address on vlan (yes|no) [yes]: yes
Enter VLAN interface IP address [172.16.0.254]: 172.16.98.1-7 //เรียงตาม group
Enter VLAN interface subnet mask [255.255.255.0]: 255.255.255.0
Enter IP Default gateway [none]: 172.16.98.254
Enter DNS IP address [none]: 8.8.8.8
Do you wish to configure IPV6 address on vlan (yes|no) [yes]: no
Enter Country code (ISO-3166), <ctrl-I> for supported list: TH
You have chosen Country code TH for Thailand (yes|no)?: yes
Enter the controller's IANA Time zone [America/Los Angeles]: Asia/Bangkok
Enter Time in UTC [07:01:44]: 14:04:00 //Current Time HH:MM:SS
Enter Date (MM/DD/YYYY) [6/14/2025]: [Enter] // Check Date Current
Enter Password for admin login (up to 32 chars): P@ssw0rd
Re-type Password for admin login: P@ssw0rd
```

Add License

Enter Web Browser URL >> **https://172.16.98.(1-7):4343**

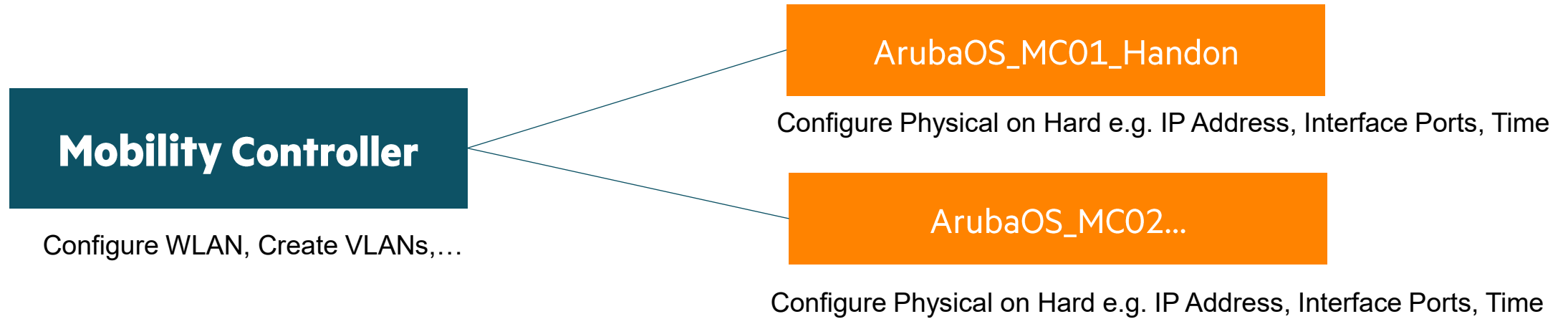


The screenshot shows a web browser window with the title "Login". The address bar displays "https://192.168.98.253:4343" with a "Not secure" warning. The main content area features the Aruba logo, the text "a Hewlett Packard Enterprise company", and the identifier "ArubaMC_Group99". Below this are input fields for "Username" and "Password", a "Log in" button, and a copyright notice at the bottom: "Copyright © 2024 Hewlett Packard Enterprise Development L.P.".

Username: **admin**

Password: **P@ssw0rd**

Hierarchy



Add License

aruba MOBILITY CONTROLLER ArubaMC_Group99

ACCESS POINTS 0 0 CLIENTS 0 0 ALERTS 0

admin

1 Mobility Controller

Dashboard

2 Configuration

WLANs

Roles & Policies

Access Points

AP Groups

Authentication

Services

Interfaces

System

Tasks

3 License

Redundancy

Connect to external license server: ☐

Usage

Usage Summary	Usage by This Controller		Usage by Other Controller			
	AP Access Points	PEF Policy Enforcement Firewall	RF Protect Wireless Intrusion Protection	ACR Advanced Cryptography	WebCC Web Content Classification	VIA Virtual Intranet Access
Feature Enabled	☒	☐	☐	☐	☐	☒
Scope	Per-AP	Per-AP	Per-AP	Per-Session	Per-AP	Per-Session
Licenses Installed	0	0	0	0	0	0
Expired Licenses	0	0	0	0	0	0
Active Licenses	0	0	0	0	0	0
Licenses Used	0	0	0	0	0	0
Licenses Remaining Available	0	0	0	0	0	0

4 > Inventory

Set Time

1

Mobility Controller

Dashboard

Configuration

WLANs

Roles & Policies

Access Points

AP Groups

Authentication

ArubaMC_Group99

2

Admin AirWave CPSec Certificates SNMP Logging Profiles

Basic Info

Password for user admin:

Retype password:

> Domain Name System

CPSec with auto cert provisioning

The screenshot displays the Aruba Mobility Controller web interface. The interface is divided into a left sidebar and a main content area. The sidebar contains a menu with the following items: Dashboard, Configuration, WLANs, Roles & Policies, Access Points, AP Groups, Authentication, Services, Interfaces, System, Tasks, License, and Redundancy. The main content area has a top navigation bar with tabs: General, Admin, AirWave, CPsec, Certificates, SNMP, Logging, and Profiles. The CPsec tab is selected. Below the tabs, the 'Control Plane Security' section is expanded, showing three toggle switches: 'Enable CPsec' (checked), 'Enable auto cert provisioning' (checked), and 'Only accept APs from specified ranges' (unchecked). A link for 'Cluster for Allowlist Propagation' is also visible. Numbered callouts are placed over the interface: 1 points to the 'Mobility Controller' header, 2 points to the 'Configuration' menu item, 3 points to the 'System' menu item, 4 points to the 'CPsec' tab, 5 points to the 'Enable auto cert provisioning' toggle, and 6 points to the 'Pending Changes' button in the top right corner.

1 Mobility Controller

2 Configuration

3 System

4 CPsec

5 Enable auto cert provisioning

6 Pending Changes

D.Configure VLANs

- **Create VLANs**
- **Configure VLAN Interface**
- **Assign VLANs on port**

Create VLANs

The screenshot displays the Aruba Mobility Controller web interface. At the top, the header includes the Aruba logo, the system name 'ArubaMC_Group99', and status indicators for Access Points (0), Clients (0), and Alerts (0). The user is logged in as 'admin'. The left sidebar shows a menu with 'Configuration' and 'Interfaces' highlighted. The main content area shows the 'VLANs' tab selected, with a table listing existing VLANs and a '+ 5' button to add a new one.

MOBILITY CONTROLLER
ArubaMC_Group99

ACCESS POINTS 0 0
CLIENTS 0 0 0
ALERTS 0

Mobility Controller

Dashboard
Configuration
WLANs
Roles & Policies
Access Points
AP Groups
Authentication
Services
Interfaces
System
Tasks
License
Redundancy

Ports **VLANs** IP Routes GRE Tunnels Pool Management OSPF Multicast

VLANs

NAME	ID(S)
--	1

+ 5

Configure VLAN Interface

Mobility Controller > **ArubaMC_Group99**

Dashboard

Configuration

- WLANs
- Roles & Policies
- Access Points
- AP Groups
- Authentication
- Services
- Interfaces**
- System
- Tasks
- Redundancy
- IoT

Diagnostics

Maintenance

Ports **VLANs** Routes IPv6 Neighbors GRE Tunnels Pool Management

VLANs

NAME	ID(S)	
Client	10,20,30	
--	1,98	

VLANs > Client

ID	IPV4 AD...	IPV6 AD...	ENABLE ...	PORT M...	ADMIN ...	OPERATI...	PD CLIE...	DHCP SE...
10	--	--	--	0/0/0	--	--	Disabled	None
20	--	--	--	0/0/0	--	--	Disabled	None
30	--	--	--	0/0/0	--	--	Disabled	None

Assign VLANs on port

Mobility Controller > ArubaMC_Group99

Dashboard
Configuration
WLANs
Roles & Policies
Access Points
AP Groups
Authentication
Services
Interfaces
System
Tasks
Redundancy
IoT
Diagnostics
Maintenance

Ports VLANs IP Routes IPv6 Neighbors GRE Tunnels Pool Management

Port Channel

NAME	MEMBERS	PROTOCOL	TRUSTED	POLICY	MODE	NATIVE VLAN	TRUNK VLANS
+							

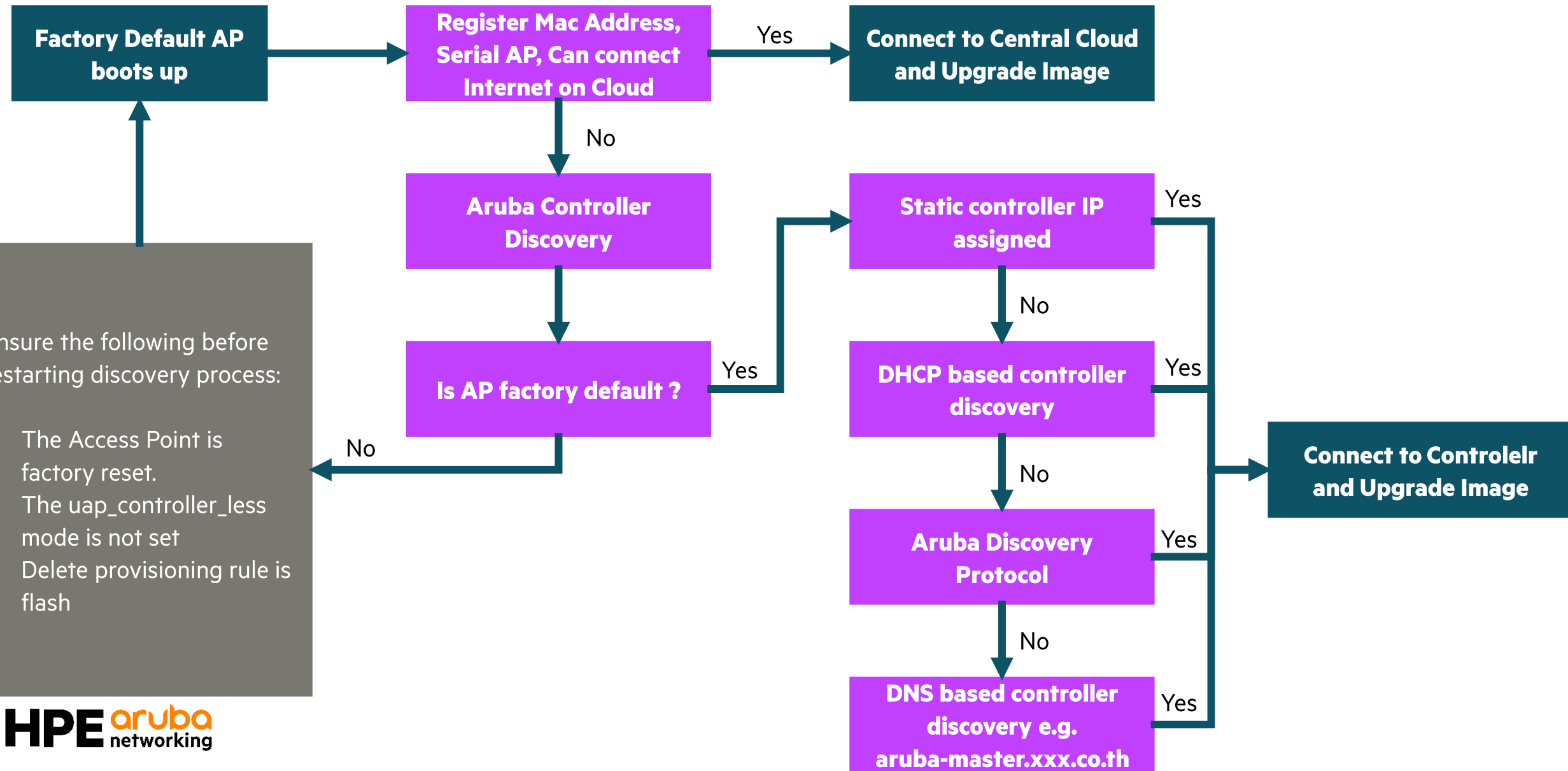
Ports

PORT	ADMI...	TRUST...	POLICY	MODE	NATIV...	ACCES...	TRUN...	SPAN...	MONI...	DESC...
GE-0/...	Enabl...	✓	Not-d...	trunk	98	1	1-4094	✓	--	--
GE-0/...	Enabled	✓	Not-d...	access	1	1	1-4094	✓	--	--
GE-0/...	Enabled	✓	Not-d...	access	1	1	1-4094	✓	--	--
GE-0/...	Enabled	✓	Not-d...	access	1	1	1-4094	✓	--	--

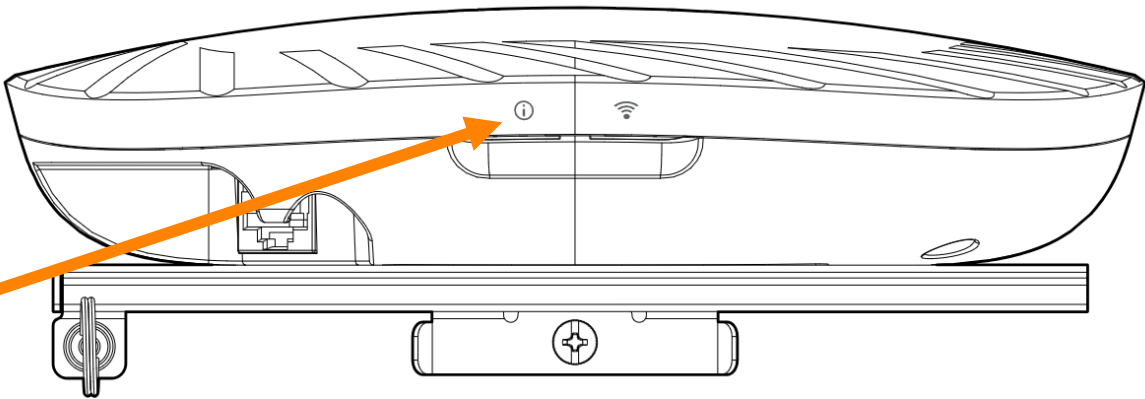
E.Initial Access Point(AP)

- **Understand Flow Unified**
- **LED Status**
- **Reset Setup**
- **AP convert to Controller**

Understand Flow Unified AP



LED Status

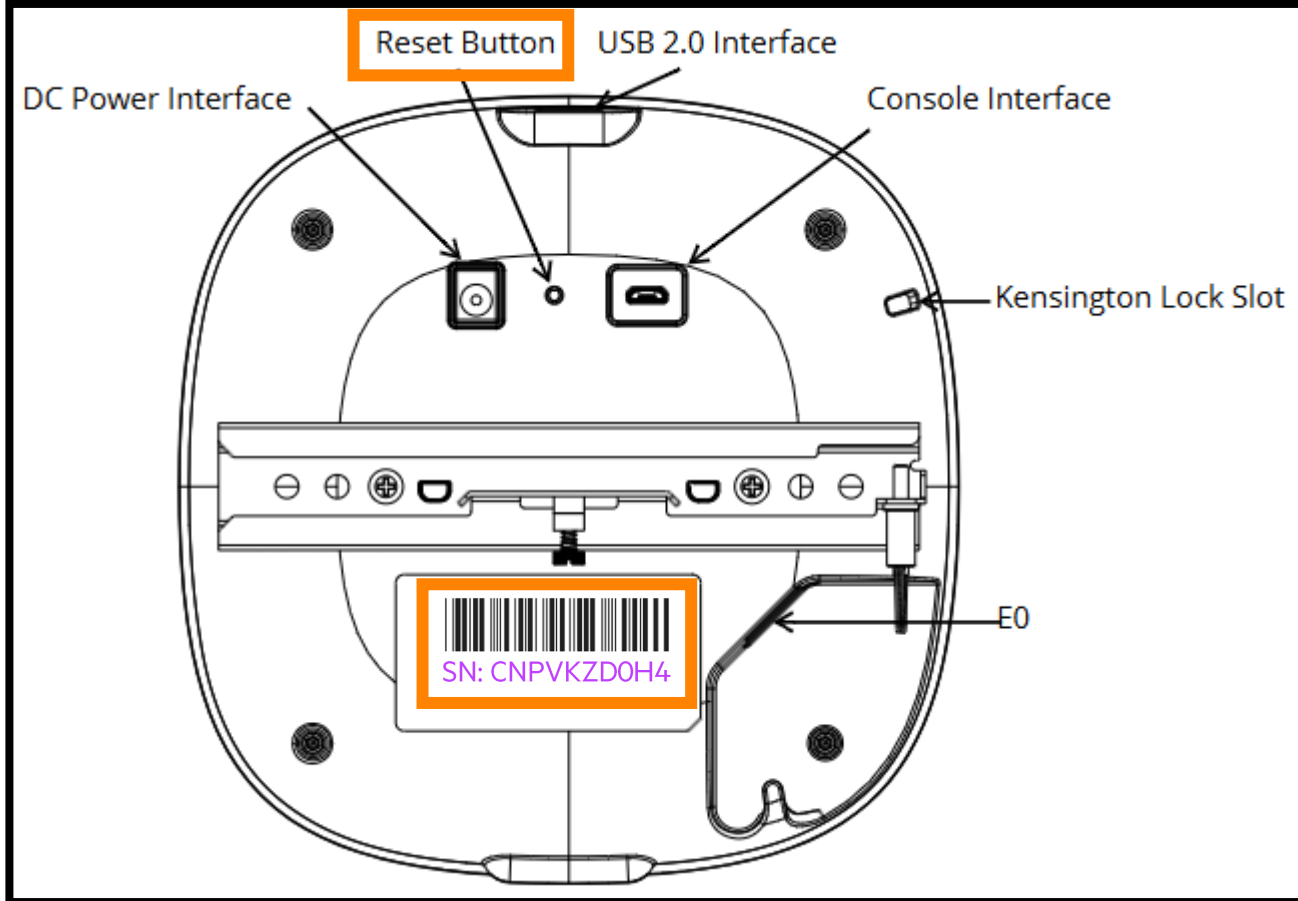


System Status LED ⓘ

Color/State	Meaning
Off	Device Powered off
Green - solid	Device ready, fully functional, no network restrictions
Green - blinking ¹	Device booting, not ready
Green - flash on ²	Device ready, fully functional, uplink negotiated in sub-optimal speed (<1Gbps)
Green - flash off ³	Device in deep-sleep mode
Amber - solid	Device ready, restricted power mode (IPM restrictions applied), no network restrictions
Amber - flashing off	Device ready, restricted power mode (IPM restrictions applied), uplink negotiated in sub-optimal speed (<1Gbps)
Red	System error conditions – Immediate action required

- 1. Blinking: one second on, one second off, 2 seconds cycle.
- 2. Flashing off: mostly on, fraction of a second off, 2 seconds cycle.
- 3. Flashing on: mostly off, fraction of a second on, 2 seconds cycle.

Reset Setup



Opt-1 Reset the AP during normal operation

press and hold down the reset button using a small, narrow object such as a paper clip for more than 10 seconds during normal operation.

Opt-2 Reset the AP while powering up

1. Press and hold down the reset button using a small, narrow object such as a paper clip while the access point is not powered on (either via DC power or PoE).
2. Connect the power supply (DC or PoE) to the access point while the reset button is being held down.
3. Release the reset button on the access point after 15 seconds.

Next Step

Access Point broadcast SSID : SetMeUp-XX:XX:XX

 SetMeUp-C2:69:D4

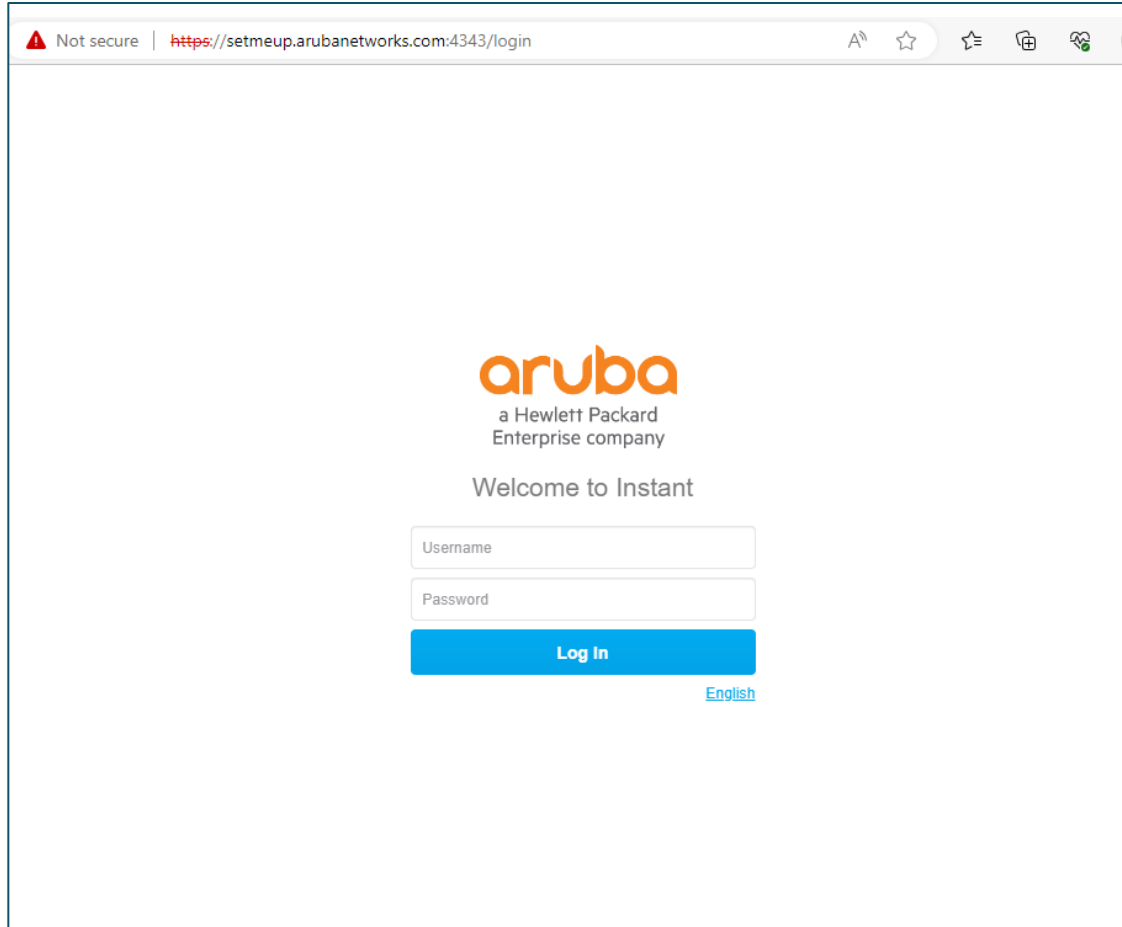
Default User/Pass

Username : **admin** Password : **CNPVKZD0H4** //S/N (Uppercase)

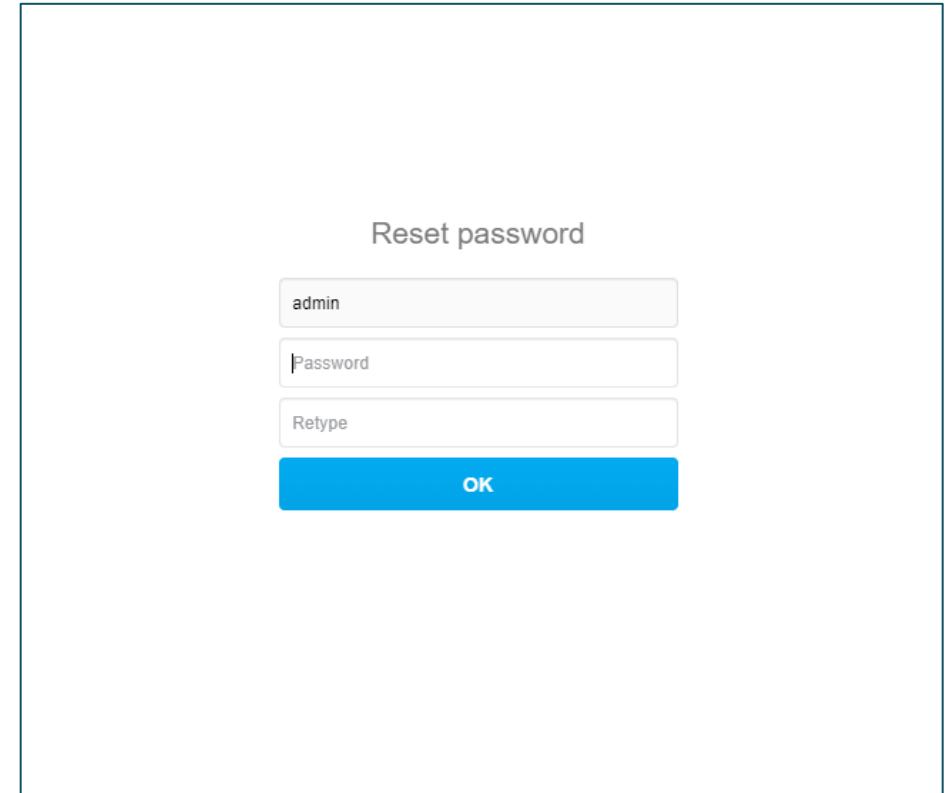
Login GUI and Changes password

Default User/Pass

Username : **admin** Password : **CNPVKZD0H4** //S/N (Uppercase)



A screenshot of a web browser showing the Aruba Instant login page. The browser's address bar displays "https://setmeup.arubanetworks.com:4343/login". The page features the Aruba logo (a Hewlett Packard Enterprise company) and the text "Welcome to Instant". Below this, there are two input fields: "Username" and "Password", followed by a blue "Log In" button. A small "English" link is visible at the bottom right of the login area.



A screenshot of the "Reset password" page. It contains three input fields: the first is pre-filled with "admin", the second is labeled "Password", and the third is labeled "Retype". Below these fields is a blue "OK" button.

Enter new **Password: P@ssw0rd** and **Retype password: P@ssw0rd**

Select Country Code

Select : **TH-Thailand**

Overview

Info

Networks

Access Points

Clients

Name

SetMeUp-C2:69:D4

Country code

Management

Uplink type

Welcome to Instant

Please specify the Country Code

TH - Thailand

1

RO - Romania

RS - Serbia

RU - Russia

RW - Rwanda

SA - Saudi Arabia

SE - Sweden

SG - Singapore

SH - Saint Helena

SI - Slovenia

SJ - Svalbard and Jan Mayen

SK - Slovak Republic

SM - San Marino

SN - Senegal

SR - Suriname

SS - South Sudan

SV - El Salvador

SX - Sint Maarten

TC - Turks And Caicos Islands

TF - French Southern Territories

TH - Thailand

please try [Upgrading your AP](#) to the latest version and try

ision, please contact technical support for mor

Dashboards-> Overview

aruba

VIRTUAL CONTROLLER

SetMeUp-C2:69:D4

Search

Alerts

Help

Profile

Dashboard

Overview

Networks

Access Points

Clients

Mesh Devices

Configuration

Maintenance

Support

Overview

Networks

Access Points

Clients

Mesh Devices

Active

Inactive

Up

Down

Wireless

Wired

1

0

1

0

1

0

Dashboard

IDS

AirGroup

0 Alerts

Clients

2

1

0

12:28

12:29

12:30

12:31

12:32

Throughput (bps)

1M

10K

100

0

100

10K

1M

12:28

12:29

12:30

12:31

12:32

Out

In

RF Dashboard

Clients

Signal

Speed

Access Points

Utilization

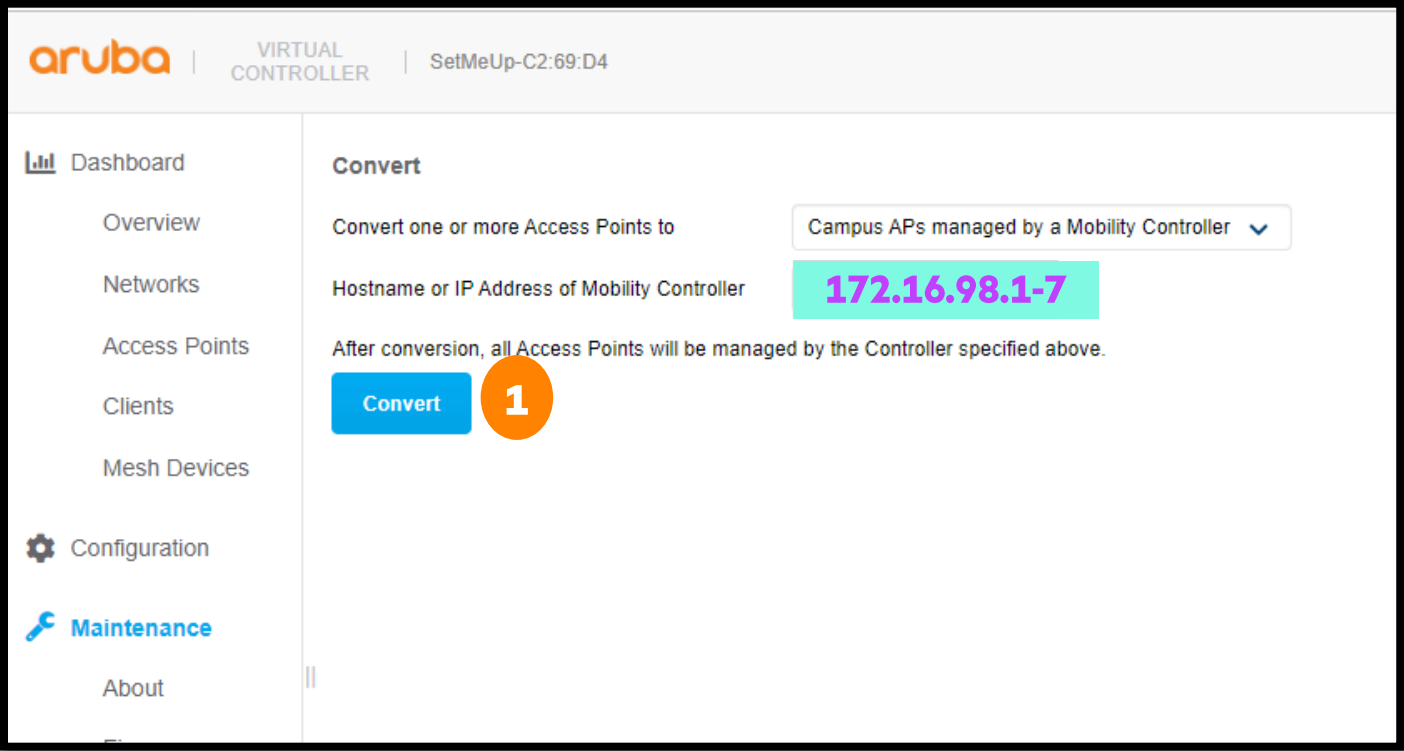
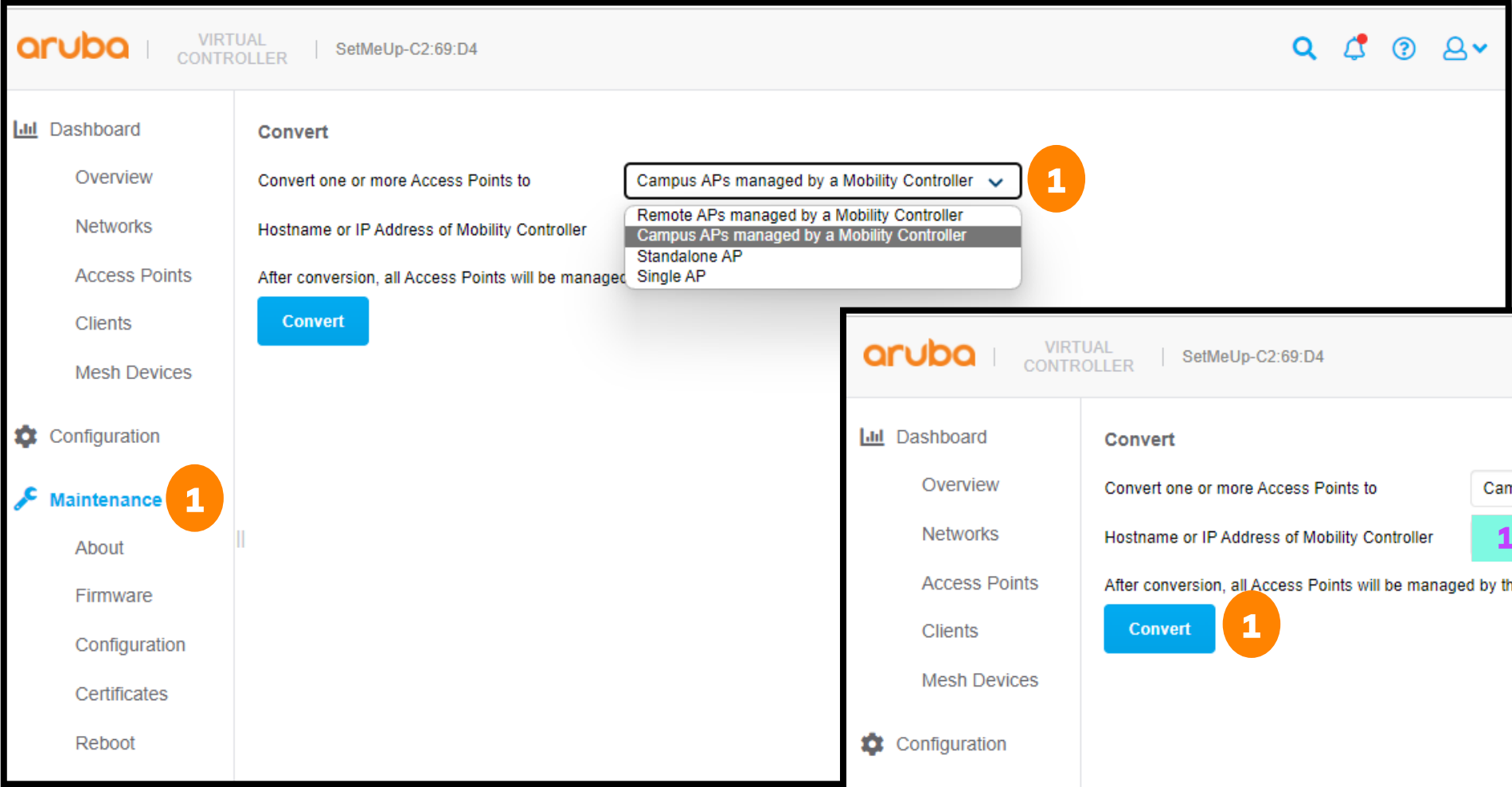
Noise

Errors

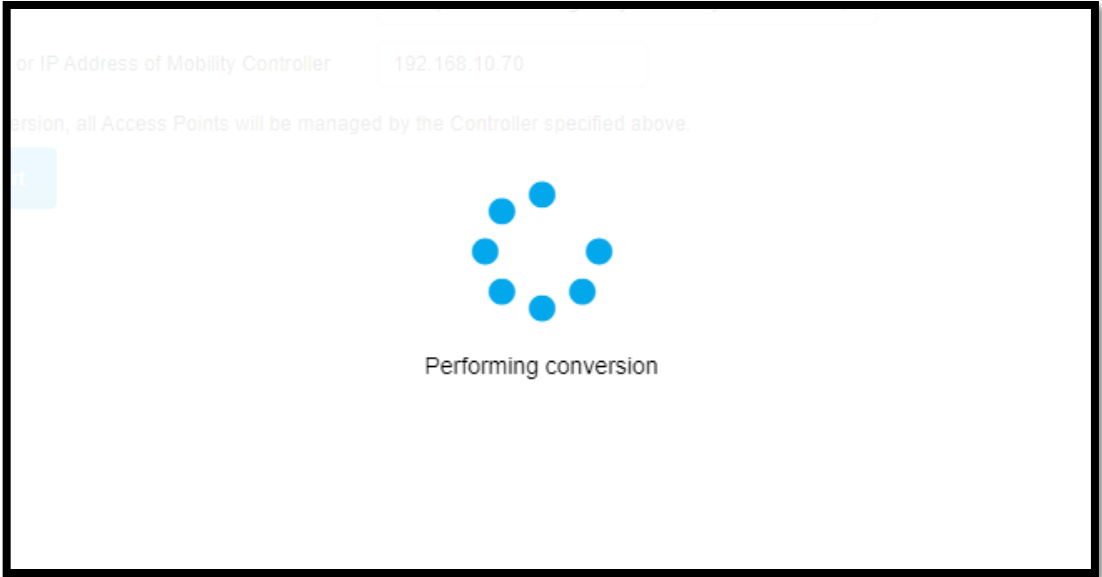
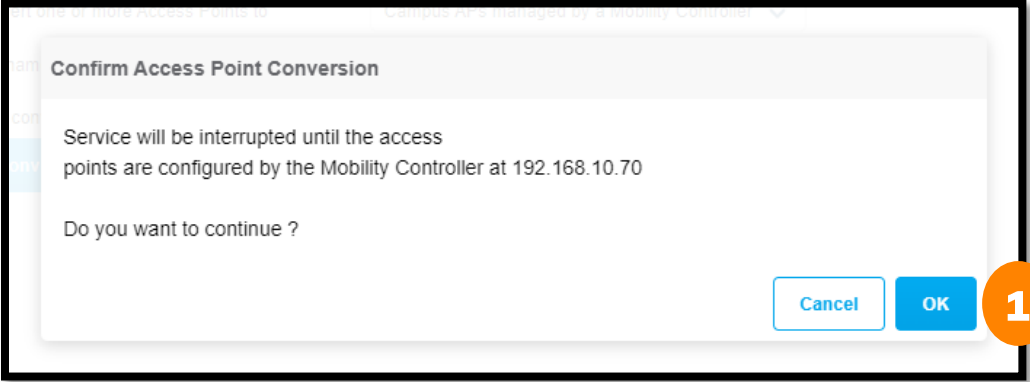
All Clients

9c:8c:d8:c2:6...

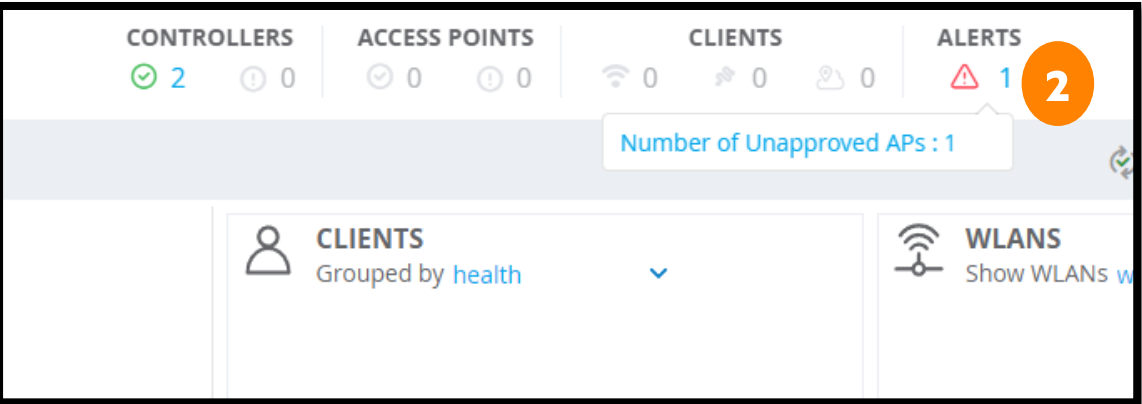
Convert Access Point Campus mode



Convert Access Point Campus mode (Cont.)



Approve device on Mobility Controller(MC)
In-Case: enable auto cert provisioning not yet.



Top bar show one **ALERTS** **“Number of Unapproved APs : 1”**

The dashboard provides a high-level overview of the network status. It features four main sections: CONTROLLERS, ACCESS POINTS, CLIENTS, and ALERTS. Each section displays a status icon (green checkmark for success, yellow warning for issues) and a count. A tooltip for the Alerts section indicates 'Number of Unapproved APs : 1'.

CONTROLLERS	ACCESS POINTS	CLIENTS	ALERTS
2	0	0	1

Number of Unapproved APs : 1

Campus APs Remote APs Mesh APs **Allowlist** Provisioning Rules

Campus AP Allowlist		Remote AP Allowlist						
	MAC ADDRESS	NAME	AP GROUP	DESCRIPTION	STATUS	REVOKE TEXT	APPROVED	UPDATED
2	☒	9c:8c:d8:c2:69:d4	--	--	Accepted	--	No	Mon Jul 10 12:40

+ 3

Delete Revoke Approve

50 ▾ < 1 >

F. Create AP Group

- Provision AP Change to Group

Create Group AP

aruba

MOBILITY
CONTROLLER
ArubaMC_Group99

ACCESS POINTS

✓ 1

⌚ 0

CLIENTS

📶 0

🔊 0

👤 0

ALERTS

⚠ 0

?

admin ▾

Mobility Controller

Dashboard

Configuration

WLANs

Roles & Policies

Access Points

AP Groups

Authentication

Services

Interfaces

System

Tasks

License

Redundancy

AP Groups 2

NAME	APs
default	1
NoAuthApGroup	--

+

New AP Group

Name:

Group-99

Cancel

Submit

HPE

aruba
networking

Change AP to New Group

Mobility Controller > 1

Dashboard

Configuration 2

WLANs

Roles & Policies

Access Points 3

AP Groups

Authentication

Services

Interfaces

System

Tasks

License

Redundancy

Campus APs Remote APs Mesh APs Allowlist Provisioning Rules

Campus APs 1

☒	AP NAME	AP GROUP	IPV4 ADD...	IPV6 ADD...	SWITCH IP	MAC ADD...	SERIAL #	T
☒	7c:57:3c:c...	default	192.168.9...	--	192.168.9...	7c:57:3c:c...	CNPBK51...	3

5 Provision

Flags:
U = Unprovisioned, N = Duplicate name, G = No such group, L = Unice...
Mismatch, X = Maintenance Mode, P = PPPoE AP, B = Built-in AP, s = LA...
RAP, c = CERT-based RAP, 1 = 802.1x authenticated AP use EAP-PEAP, 1...
u = Custom-Cert RAP, S = Standby-mode AP, J = USB cert at AP, f = No S...
Mesh Recovery, z = Datazone AP, e = Custom EST cert, p = In deep-sleep...
ShutDown, F = AP failed 802.1x authentication

7c:57:3c:c3:e0:e4

MAC address: 7c:57:3c:c3:e0:e4

LLDP neighbor chassis ID / port ID: 6200 / 1/1/3

Name: 7c:57:3c:c3:e0:e4

AP group: Group-99 6 Select New Group

Controller discovery: ☒ Use AP discovery protocol (ADP) ☐ Static

Controller discovery preference: ☒ IPv4 ☐ IPv6

IP: ☒ DHCP ☐ Static

Deployment: ☒ Campus ☐ Remote ☐ Mesh ☐ Remote mesh portal

Wi-Fi uplink: ☐ Wi-Fi uplink

advanced options

Cancel Submit 6

Access Points will be Rebooted

CAUTION: Applying this configuration change will interrupt service while the affected Access Points are rebooted.

Do you want to continue ?

Cancel Continue & Reboot 7

A. Configure WLAN PSK+MAC

- Add local user

Configure WLAN PSK

aruba

MOBILITY
CONTROLLER
ArubaMC_Group99

ACCESS POINTS

✓ 1

⌚ 0

CLIENTS

📶 0

👤 0

📍 0

ALERTS

⚠ 0

?

admin ▾

☰ Mobility Controller 1

Dashboard

Configuration 2

WLANs

Roles & Policies

Access Points

AP Groups

Authentication

Services

Interfaces

System

Tasks

WLANs 0

NAME (SSID)	AP GROUP	KEY MANAGEMENT	INFORMATION	
+ 3				



Configure WLAN PSK

aruba

MOBILITY CONTROLLER
ArubaMC_Group99

ACCESS POINTS

1

0

CLIENTS

1

0

0

ALERTS

0

admin

Mobility Controller

Search

Dashboard

Overview

Infrastructure

Traffic Analysis

Security

Services

Configuration

Diagnostics

Maintenance

Client

WLAN

265 kB

Radios

Wireless Clients 1

NAME	IP ADDRESS	HEALTH	BAND	ROLE	SNR	USAGE	WLAN	CONNECTED...
192.168.20.1	192.168.20.1	Good	5 GHz	authenticated	54 dB	104 kB	PSK-G99	7c:57:3c:c3:e0:e4

DETAILS

Name
192.168.20.1

IP address
192.168.20.1

MAC address
a4:d9:31:b8:57:75

Health score
92%

Speed
842 Mbps

Max speed
866 Mbps

Frames in the last minute
121

SIGNAL

Show information about signal quality

100

75

50

25

0

20:21

20:22

Now

USAGE

Show information about throughput

10k

0

10k

20k

20:22

Now

Transmitted

Received

2

Copy mac address

Add mac address to local user

aruba

MOBILITY CONTROLLER
ArubaMC_Group99

ACCESS POINTS

10

CLIENTS

100

ALERTS

0

admin

Mobility Controller

Dashboard

Configuration

WLANs

Roles & Policies

Access Points

AP Groups

Authentication

Services

Interfaces

System

Tasks

License

Redundancy

Diagnostics

Maintenance

Auth Servers

Profiles

L2 Authentication

L3 Authentication

User Rules

Advanced

Server Groups

2

NAME	SERVICES	FAIL THROUGH	LOAD BALANCE	SERVICES RULES	
default	1	--	--	1	
internal	1	--	--	1	

Server Group > internal

ServersOptionsServer Rules

NAME	TYPE	IP ADDRESS	TRIM FQDN	MATCH RULES	
Internal	--	--	--	0	

Server Group > internal > Internal

UsersOptionsImportExportServer Group Trim FQDNServer Group Match RulesGuest user page

USER NAME	ROLE	EMAIL	EXPIRATION	STATIC IP FOR RAPS	ENABLED	
-----------	------	-------	------------	--------------------	---------	--

Add mac address to local user

1 Past mac address to username, password, retype password

Internal Server > Add New User

User name:	a4d931b85775	Generate
Password:		Generate
Retype password:		
Role:	authenticated	2
E-mail:		
Static inner IP for RAPs:		
Enabled:	☒	
Expiration:	None	

Cancel Submit 3

Configure WLAN Add MAC Authentication

1. Mobility Controller

2. Configuration

3. WLANs

NAME (SSID)	AP GROUP	KEY MANAGEMENT	INFORMATION
PSK-G99	default	WPA2-Personal	--

Dashboard

Configuration

- WLANs
- Roles & Policies
- Access Points
- AP Groups
- Authentication
- Services
- Interfaces

PSK-G99

General VLANs Security Access Profiles

More Secure

Enterprise

Personal

Open

Less Secure

Key management: WPA3-Personal

Enable backward compatibility

Passphrase:

Retype:

MAC authentication: Enabled

Denylisting: ☐

4. Enable MAC authentications

Cancel Submit

Configure WLAN Add MAC Authentication

PSK-G99 General VLANs Security **Access** Profiles

Default role: denyall

MAC authentication role: guest

Show [roles](#)

Cancel Submit

Pending Changes

WLANs 1

NAME (SSID)	AP GROUP	KEY MANAGEMENT	INFORMATION
PSK-G99	default	WPA2-Personal	--

+

General VLANs Security **Access** Profiles

Default role: denyall

MAC authentication role: guest

Show [roles](#)

Pending Changes

☒ Pending Changes for 1 Group

☒ + Mobility Controller

Close Discard changes Deploy changes

Configure WLAN Add MAC Authentication

PSK-G99 General VLANs Security **Access** Profiles

Default role: denyall

MAC authentication role: guest

Show [roles](#)

Cancel Submit

Pending Changes

WLANs 1

NAME (SSID)	AP GROUP	KEY MANAGEMENT	INFORMATION
PSK-G99	default	WPA2-Personal	--

+

General VLANs Security **Access** Profiles

Default role: denyall

MAC authentication role: guest

Show [roles](#)

Pending Changes

☒ Pending Changes for 1 Group

☒ + Mobility Controller

Close Discard changes Deploy changes

B. Configure WLAN 802.1X

Configure WLAN 802.1X

The screenshot displays the Aruba Mobility Controller web interface. At the top, the Aruba logo is on the left, and the title 'MOBILITY CONTROLLER ArubaMC_Group99' is in the center. To the right of the title are three status sections: 'ACCESS POINTS' with a green checkmark and '1', 'CLIENTS' with a Wi-Fi icon and '0', and 'ALERTS' with a warning triangle and '0'. Further right is a help icon and a user dropdown menu showing 'admin'. Below the title bar is a navigation bar with a hamburger menu icon and the text 'Mobility Controller'. The left sidebar contains a 'Dashboard' link and a 'Configuration' link, which is highlighted with an orange box and a '2'. Under 'Configuration', there is a 'WLANs' link and a list of other configuration options: 'Roles & Policies', 'Access Points', 'AP Groups', 'Authentication', 'Services', 'Interfaces', 'System', and 'Tasks'. The main content area shows a table titled 'WLANs 0'. The table has four columns: 'NAME (SSID)', 'AP GROUP', 'KEY MANAGEMENT', and 'INFORMATION'. Below the table is a blue plus sign icon and a '3' in an orange circle, indicating a button to add a new WLAN.

aruba

MOBILITY CONTROLLER
ArubaMC_Group99

ACCESS POINTS
✓ 1 0

CLIENTS
0 0 0

ALERTS
0

admin

Mobility Controller

Dashboard

Configuration

WLANs

Roles & Policies

Access Points

AP Groups

Authentication

Services

Interfaces

System

Tasks

WLANs 0

NAME (SSID)	AP GROUP	KEY MANAGEMENT	INFORMATION
+ 3			

Configure WLAN 802.1X

New WLAN

General VLANs Security Access

Name (SSID): 802.1X-G99 **1**

Primary usage: ☒ Employee ☐ Guest

Select AP Groups **2**

Broadcast on: ☐ default ☒ Group-99

Forwarding mode: Tunnel

Cancel Back Next **3**

New WLAN

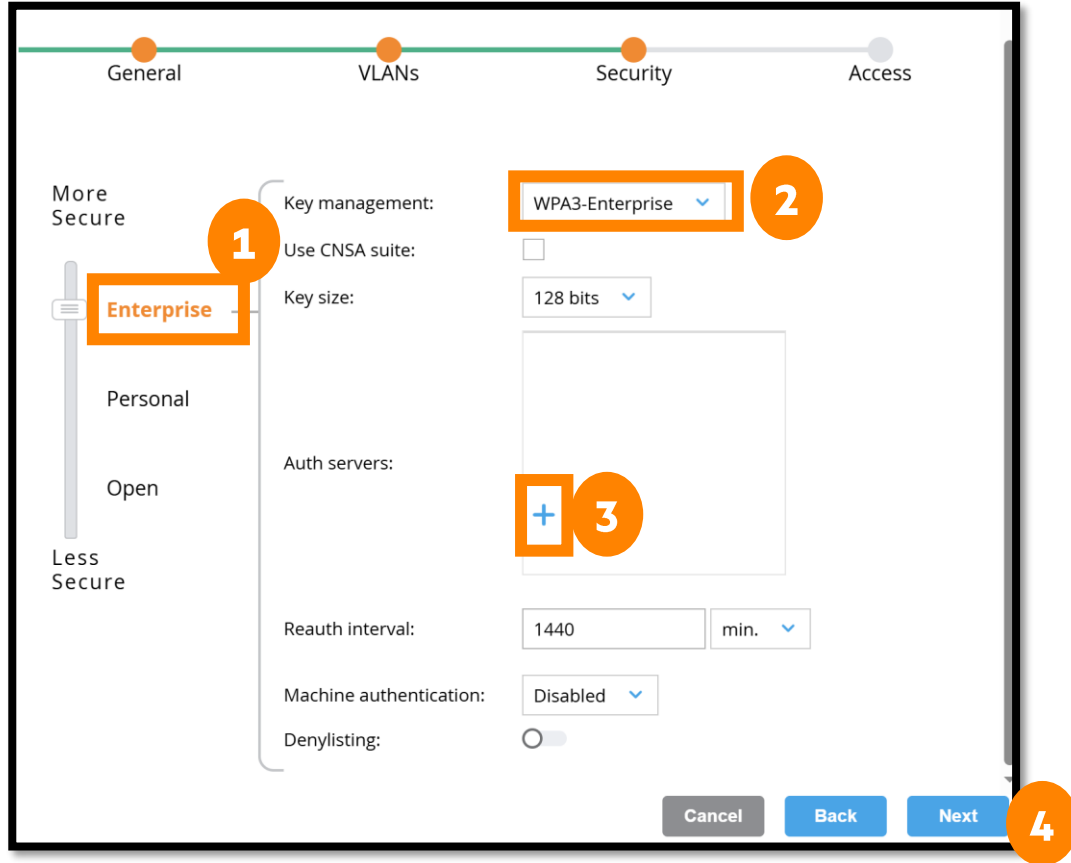
General VLANs Security Access

VLAN: 10 **4** Select vlan 10

[Show VLAN details](#)

Cancel Back Next **5**

Configure WLAN 802.1X



General VLANs Security Access

More Secure

Enterprise

Personal

Open

Less Secure

Key management: WPA3-Enterprise

Use CNSA suite: ☐

Key size: 128 bits

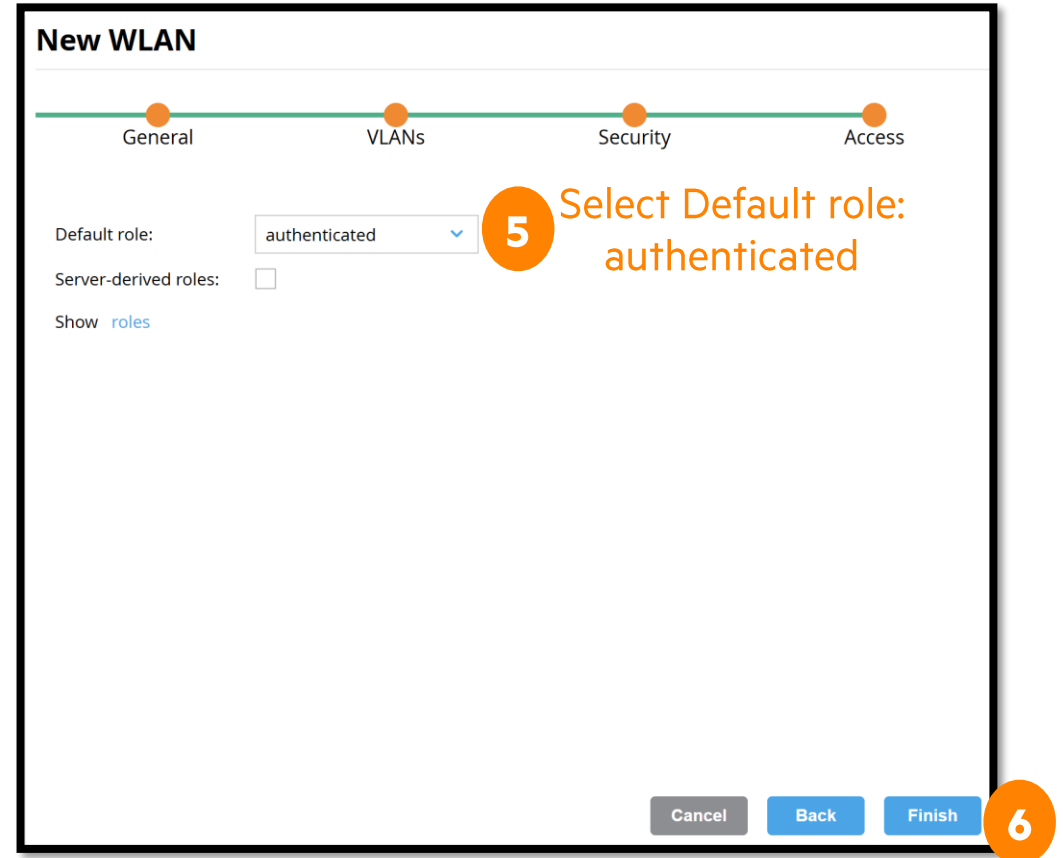
Auth servers: +

Reauth interval: 1440 min.

Machine authentication: Disabled

Denylisting: ☐

Cancel Back Next



New WLAN

General VLANs Security Access

Default role: authenticated

Server-derived roles: ☐

Show roles

Cancel Back Finish

Select Default role: authenticated

Configure add local user for 802.1X

Mobility Controller

Dashboard

Configuration (1)

WLANs

Roles & Policies

Access Points

AP Groups

Authentication (2)

Services

Interfaces

System

Tasks

License

Redundancy

Diagnostics

Maintenance

Auth Servers (3)

AAA Profiles L2 Authentication L3 Authentication

Server Groups 3

NAME	SERVICES	FAIL THROUGH	LOAD BALANCE	SERVER RULES
default	1	--	--	1
Internal	1	--	--	1
802.1X-G99_dot...	1	--	--	0

All Servers 1

NAME	TYPE	IP ADDRESS / HOST	SERVER GROUP
Internal	--	--	default internal 802....

Auth Servers AAA Profiles L2 Authentication L3 Authentication

Server > Internal **Users** Options Import Export Guest user page

USER NAME	ROLE	EMAIL	EXPIRATION	STATIC IP FO...	ENABLED
a4d931b857...	authenticated	--	--	0.0.0.0	Yes

Internal Server > Add New User (6)

User name: group99

Password:

Retype password:

Role: authenticated (7)

E-mail:

Static inner IP for RAPs:

Enabled: ☒

Expiration: None

Create User
User: group0X
Pass: P@sswOrd

Cancel Submit (8)

C. Configure WLAN Guest

- Add local user

Configure WLAN Guest

The screenshot displays the Aruba Mobility Controller web interface. At the top, the Aruba logo is on the left, and the title 'MOBILITY CONTROLLER ArubaMC_Group99' is in the center. To the right of the title are three status sections: 'ACCESS POINTS' with a green checkmark and '1', 'CLIENTS' with a Wi-Fi icon and '0', and 'ALERTS' with a warning triangle and '0'. Further right is a help icon and a user dropdown menu showing 'admin'. Below the title bar is a navigation bar with a hamburger menu icon and the text 'Mobility Controller'. A sidebar on the left contains a 'Dashboard' link and a 'Configuration' link, which is highlighted with an orange box and a '2'. Under 'Configuration', there is a 'WLANs' link and a list of other configuration options: 'Roles & Policies', 'Access Points', 'AP Groups', 'Authentication', 'Services', 'Interfaces', 'System', and 'Tasks'. The main content area shows a table titled 'WLANs 0'. The table has four columns: 'NAME (SSID)', 'AP GROUP', 'KEY MANAGEMENT', and 'INFORMATION'. Below the table is a blue plus sign icon and a '3' in an orange circle, indicating where to click to add a new WLAN.

aruba

MOBILITY CONTROLLER
ArubaMC_Group99

ACCESS POINTS
✓ 1 0

CLIENTS
0 0 0

ALERTS
0

admin

Mobility Controller

Dashboard

Configuration

WLANs

Roles & Policies

Access Points

AP Groups

Authentication

Services

Interfaces

System

Tasks

WLANs 0

NAME (SSID)	AP GROUP	KEY MANAGEMENT	INFORMATION
+			

Configure WLAN Guest

New WLAN

General VLANs Security Access

Name (SSID):

Primary usage: ☐ Employee ☒ Guest

Select AP Groups

Broadcast on: ☐ default ☒ Group-99

Forwarding mode:

Cancel Back Next

New WLAN

General VLANs Security Access

VLAN:

[Show VLAN details](#)

Cancel Back Next

D. Configure Role & Policy

- **Network aliases**

Network Aliases

Configure on node “Mobility Controller”-> Configuration-> Roles & Policies -> Aliases -> +

The screenshot displays the Aruba Mobility Conductor web interface. At the top, the header includes the Aruba logo, the text "MOBILITY CONDUCTOR ArubaOS_MM01_Ha...", and several status indicators: "CONTROLLERS" (2 green, 0 grey), "ACCESS POINTS" (0 green, 0 grey), "CLIENTS" (1 Wi-Fi icon, 0 user icon, 0 location pin icon), and "ALERTS" (0 warning icon). A user dropdown menu shows "admin".

The left sidebar contains a navigation menu with the following items: "Dashboard", "Configuration" (highlighted in orange), "WLANs", "Roles & Policies" (highlighted in orange), "Access Points", "AP Groups", "Authentication", "Services", "Interfaces", "Controllers", "System", and "Tasks".

The main content area is titled "Mobility Controller" and features a sub-navigation bar with "Roles", "Policies", "Applications", and "Aliases" (highlighted in orange). Below this, a section titled "Network Aliases" contains a table with the following data:

NAME	ITEMS	DESCRIPTION	IP VERSION	INVERT
mswitch	1	--	IPv4	--
controller	1	--	IPv4	--
vrrp_ip	1	--	IPv4	--
any	1	--	IPv4	--
user	1	--	IPv4	--
localip	1	--	IPv4	--
auth-google	2	--	IPv4	--

Below the table is a blue "+" icon for adding new aliases. A small grid icon is visible in the top right corner of the table area.

Network Aliases (cont.)

Enter Name "Local_Network" +

Destination Local_Network

IP version: 1

Name:

Description:

Invert: ☐

Items

TYPE	IP ADDRESS	NETMASK/RANGE/...	DOMAIN NAME
------	------------	-------------------	-------------

+ 2

Rule type : **Network**
IP Address : **192.168.0.0**
Network mask : **255.255.0.0**
OK -> Submit

Add New Destination

Rule type: 3

IP address:

Network mask:

4

Policies

Create Policies

Mobility Controller

Dashboard

Configuration

WLANs

Roles & Policies

Access Points

AP Groups

Authentication

Services

Interfaces

System

Tasks

License

Roles

Policies

Applications

Aliases

NAME	RULES COU...	TYPE	POLICY US...	DESCRIPTION
validuseret...	1	eth	--	--
global-sacl	0	session	guest, statef...	--
sdn-acl	0	session	--	--
sys-control	13	session	sys-ap-role, ...	--
sys-ap-acl	12	session	sys-ap-role	--
switch-logo...	1	session	switch-logon	--
sys-switch-acl	12	session	sys-switch-r...	--

+

New Policy

Policy type:

Session

Policy name:

Local_Network-Polic

Description:

Cancel

Submit

Policies (cont.)

Roles **Policies** Applications Aliases

Policies

NAME	RULES C...	TYPE	POLICY ...	DESCRIP...	
apprf-sys-ap-role-sacl	0	session	sys-ap-role	--	
apprf-sys-switch-role-sacl	0	session	sys-switc...	--	
apprf-guest-99-guest-log...	0	session	Guest-99...	--	
Local_Network-Policies	0	session	--	--	1
uplink-lb-cfg-racl	0	routing	--	--	
uplink-lb-sys-racl	0	routing	--	--	
master-boc-traffic	0	routing	--	--	

Policy > Local_Network-Policies Rules ⓘ Drag rows to re-order

IP VERSI...	SOURCE	DESTINA...	SERVICE/...	ACTION	DESCRIP...	
-------------	--------	------------	-------------	--------	------------	--

2

New Rule for Local_Network-Policies

Rule type: ☒ Access control **3** ☐ Application

Cancel

OK **4**

Local_Network-Policies > New forwarding Rule

IP version: IPv4 **5**
Source: Any
Destination: Alias
Destination alias: local_network
Service/app: Service
Services alias: svc-icmp
Action: Deny

TOS:
Time range: - None - Reset
802.1p priority:
Options:
☐ Log ☐ Mirror ☐ Denylist ☐ Disable scanning
Queue:
Description:

Cancel

Submit **6**

Create Policies Block ping

IP Version : **IPV4**

Source : **Any**

Destination : **Alias**

Destination alias : **Local_Network**

Service/app : **Service**

Service alias : **svc-icmp**

Action : **Deny**

Submit

Role

Create Role

Mobility Controller

Dashboard

Configuration

Roles & Policies

Access Points

AP Groups

Authentication

Services

Interfaces

System

Tasks

License

Roles

Policies

Applications

Aliases

Roles 15

NAME	RULES
logon	32 Rules
guest	11 Rules
ap-role	35 Rules
stateful-dot1x	0 Rules
guest-logon	27 Rules
sys-ap-role	25 Rules
sys-switch-role	25 Rules

+



New Role

Name:

engineer

Cancel

Submit

Role

Assign policies in Role engineer

Mobility Controller >

Dashboard

Configuration

WLANs

Roles & Policies

Access Points

AP Groups

Authentication

Services

Interfaces

System

Tasks

License

Redundancy

Diagnostics

Maintenance

Roles

ies

Applications

Aliases

Roles 16

NAME	RULES
denyall	1 Rules
default-via-role	3 Rules
default-vpn-role	4 Rules
authenticated	4 Rules
voice	45 Rules
Guest-99-guest-logon	26 Rules
engineer	0 Rules

+

engineer

Show Advanced View

Global Rules

IP VERSI...	SOURCE	DESTINA...	SERVICE/...	ACTION	DESCRIP...
-------------	--------	------------	-------------	--------	------------

+

engineer

Policies

Bandwidth

Captive Portal

Show Basic View

NAME	RULES COU...	TYPE	POLICY US...	DESCRIPTI...
global-sacl	0	session	guest, state...	--
apprf-engin...	0	session	engineer	--
engineer	0	session	engineer	--

+

Role

Assign policies > local_network(first), allowall(second)

New Policy

☒ Add an existing policy **1** ☐ Create a new policy

Policy type: Session

Policy name: Local_Network-Policies **2**

Description:

Position:

3 Cancel Submit

first
→

engineer	Policies	Bandwidth	Captive Portal	Show Basic View
NAME	RULES COU...	TYPE	POLICY US...	DESCRIPTI...
global-sacl	0	session	guest, state...	--
apprf-engin...	0	session	engineer	--
engineer	0	session	engineer	--
Local_Netw...	1	session	--	--

4

5

second
↓

New Policy

☒ Add an existing policy **6** ☐ Create a new policy

Policy type: Session

Policy name: allowall **7**

Description:

Position:

8 Cancel Submit

save
→

Pending Changes **10**

Roles Policies Applications Aliases

Roles 16

NAME	RULES
denyall	1 Rules
default-via-role	3 Rules
default-vpn-role	4 Rules
authenticated	4 Rules
voice	45 Rules
Guest-99-guest-logon	26 Rules
engineer	3 Rules

9

engineer	Policies	Bandwidth	Captive Portal	Show Basic View
NAME	RULES COU...	TYPE	POLICY US...	DESCRIPTI...
apprf-engin...	0	session	engineer	--
engineer	0	session	engineer	--
Local_Netw...	1	session	engineer	--
allowall	2	session	default-iap...	--

Role

Assign role engineer to user local

Mobility Controller

Dashboard

Configuration

WLANs

Roles & Policies

Access Points

AP Groups

Authentication

Services

Interfaces

System

Tasks

License

Redundancy

Diagnostics

Maintenance

Auth Servers

AAA Profiles

L2 Authentication

Server Groups

NAME	SERVERS	FAIL THRO...	LOAD BAL...	SERVER RU...
default	1	--	--	1
internal	1	--	--	1
802.1X-G99...	1	--	--	0

All Servers 1

NAME	TYPE	IP ADDRESS / ...	SERVER GROUP
Internal	--	--	default intern...

Server > Internal

Users

Options

Import

Guest user page

USER NA...	ROLE	EMAIL	EXPIRATI...	STATIC IP...	ENABLED
a4d931h	authenti...	--	--	0.0.0.0	Yes
group99	authenti...	--	--	0.0.0.0	Yes
guest99	guest	--	--	0.0.0.0	Yes



Edit User group99

User name:group99

Password:*****Generate

Role:engineer

E-mail:

Static inner IP for RAPS:0.0.0.0

Enabled:☒

Expiration:None

CancelSubmit

Change to Role engineer

Role

Test connect WiFi > 802.1X-G99

ACCESS POINTS

1

0

CLIENTS

1

0

0

ALERTS

0

admin

Search

1

3

82.1 kB

2

Wireless Clients 1

NAME	IP ADDR...	HEALTH	BAND	ROLE
group99	192.168.10.2	Unkno...	5 GHz	engineer

Test ping gateway user

Command Prompt

Microsoft Windows [Version 10.0.19045.5965]
(c) Microsoft Corporation. All rights reserved.

C:\Users\sakkr>ping 192.168.10.254

Pinging 192.168.10.254 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.10.254:
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Users\sakkr>ping 192.168.10.253

Pinging 192.168.10.253 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.10.253:
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

CUSTOMER FIRST
CUSTOMER LAST

The image features the text "CUSTOMER FIRST" on the top line and "CUSTOMER LAST" on the bottom line. The letters are large, bold, and white. Each letter is filled with a different photograph of people at what appears to be a conference or event. The photos show various individuals, some smiling, some looking at devices, and others in group settings. The overall theme is customer-centricity.