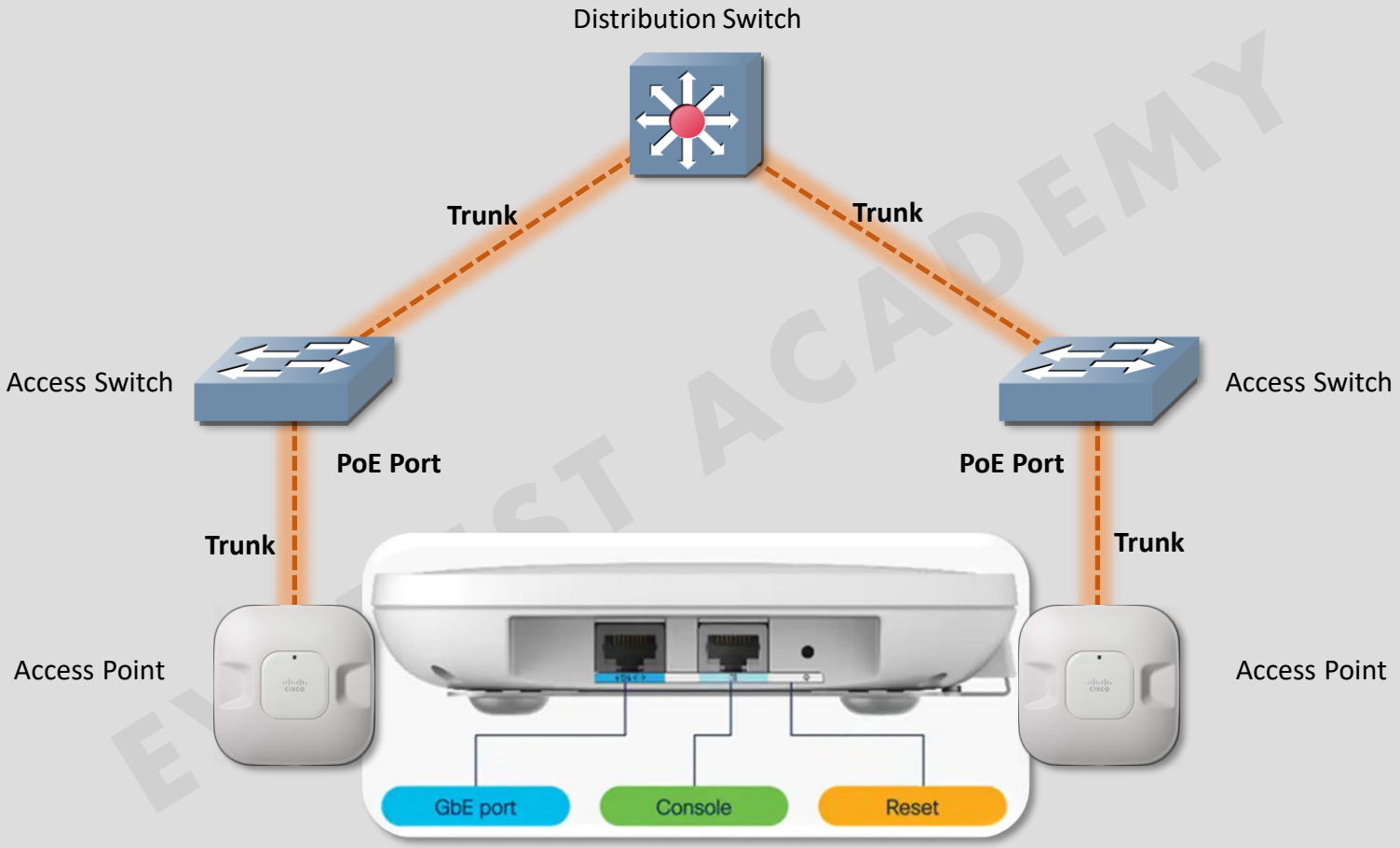
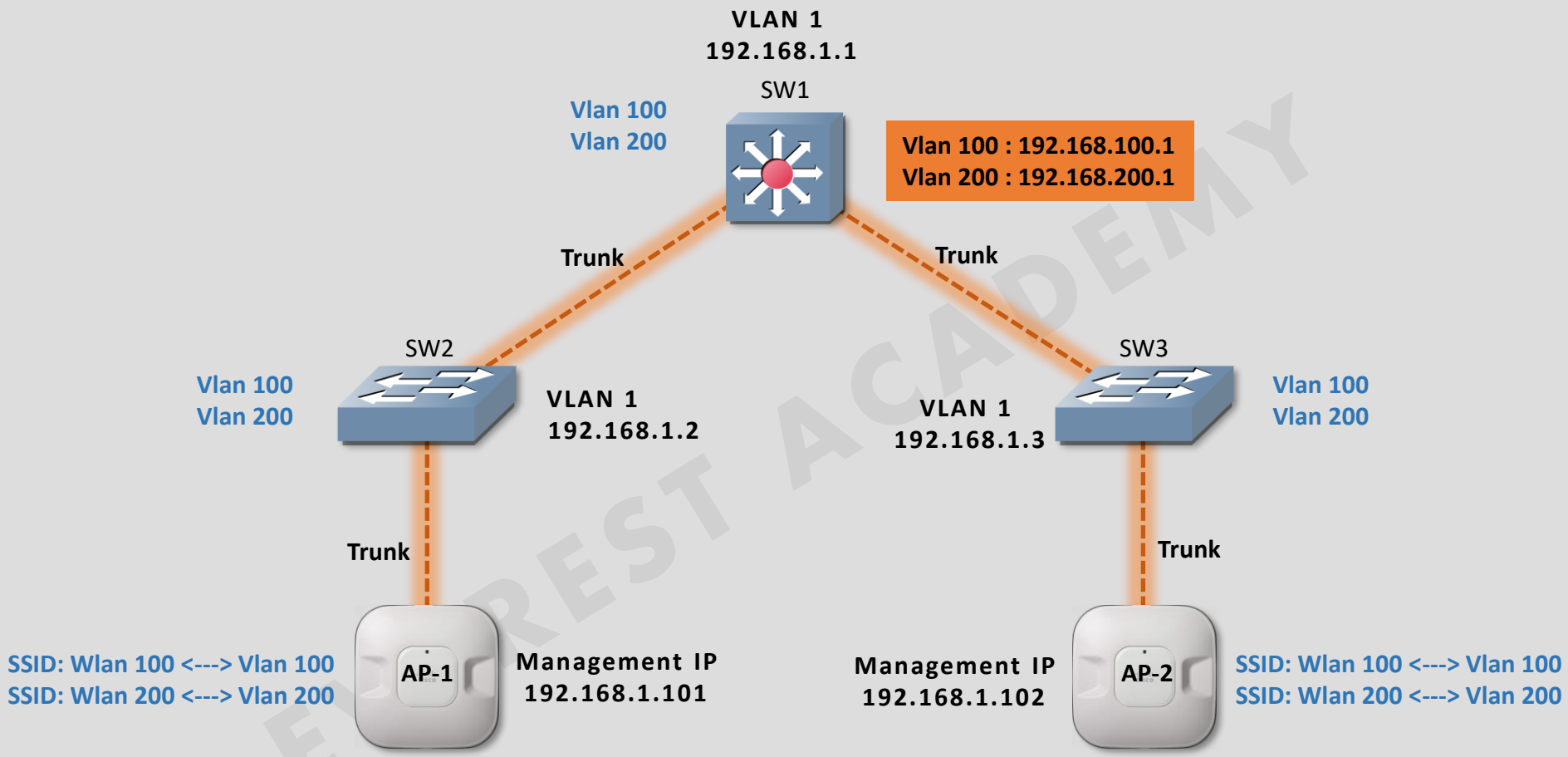
Cisco Wireless Architectures

- Autonomous AP Architecture.
- Cloud-based AP Architecture.
- Split-MAC Architectures.

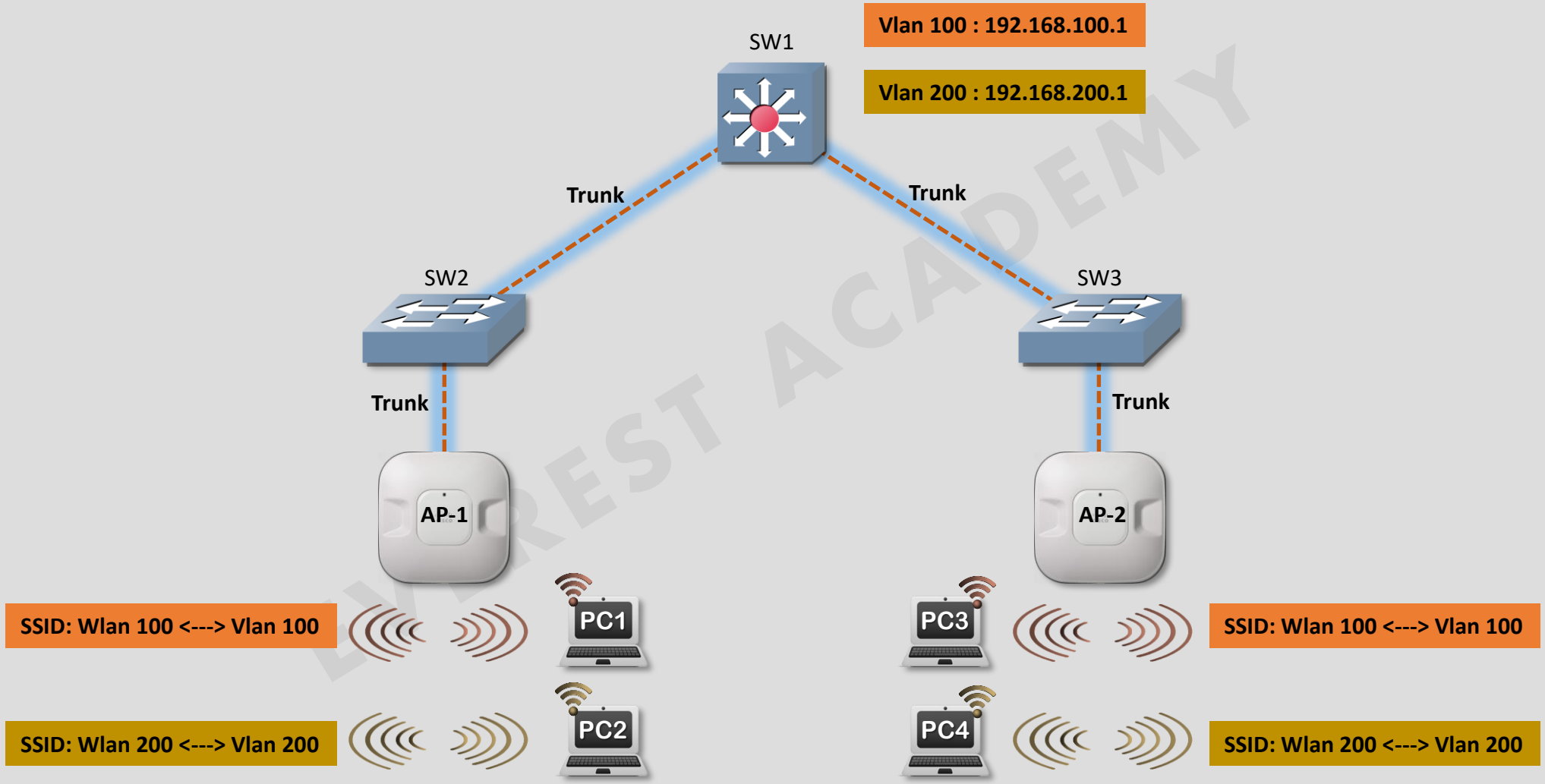
Autonomous AP Architecture



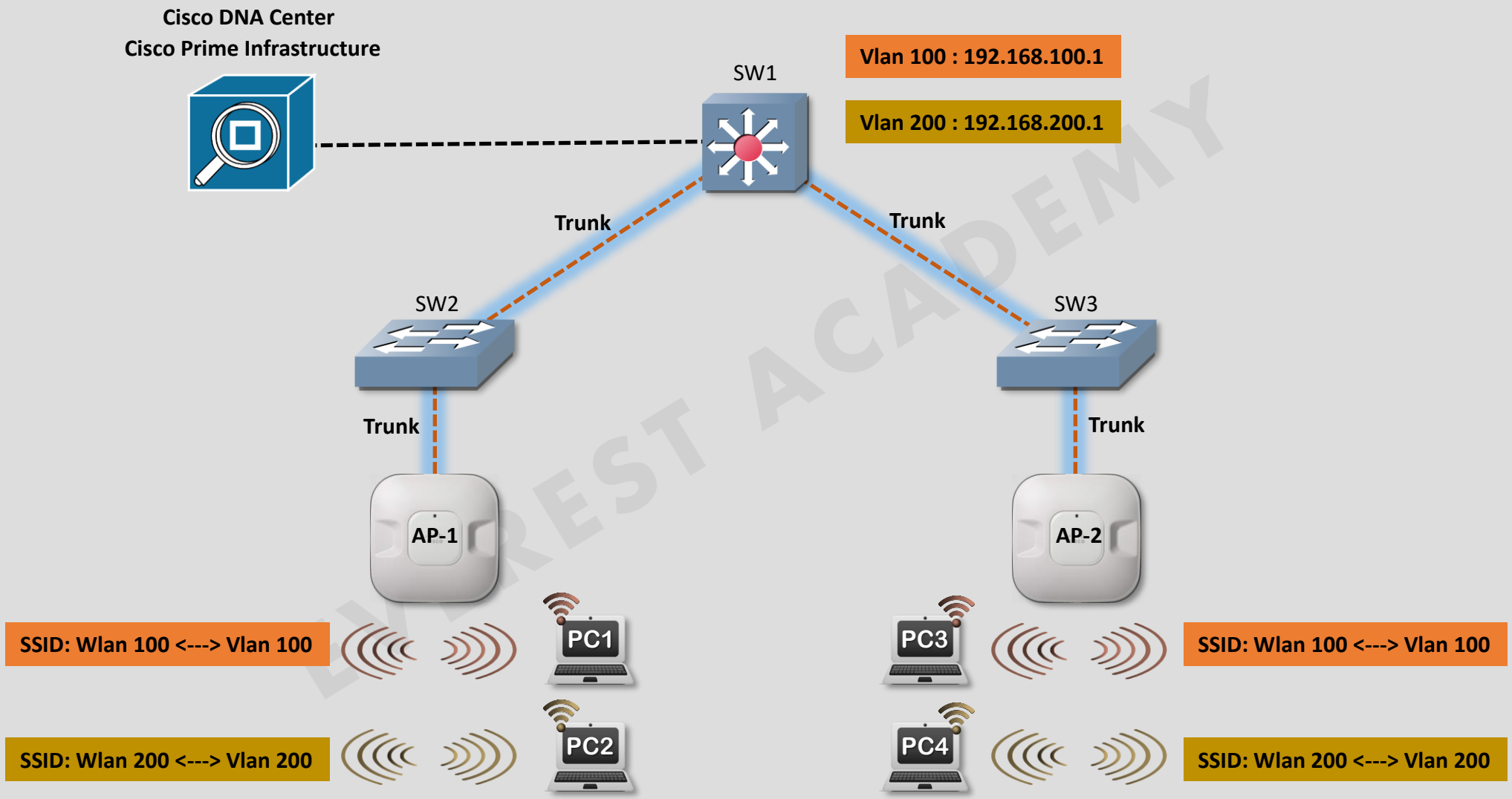
Autonomous AP Architecture



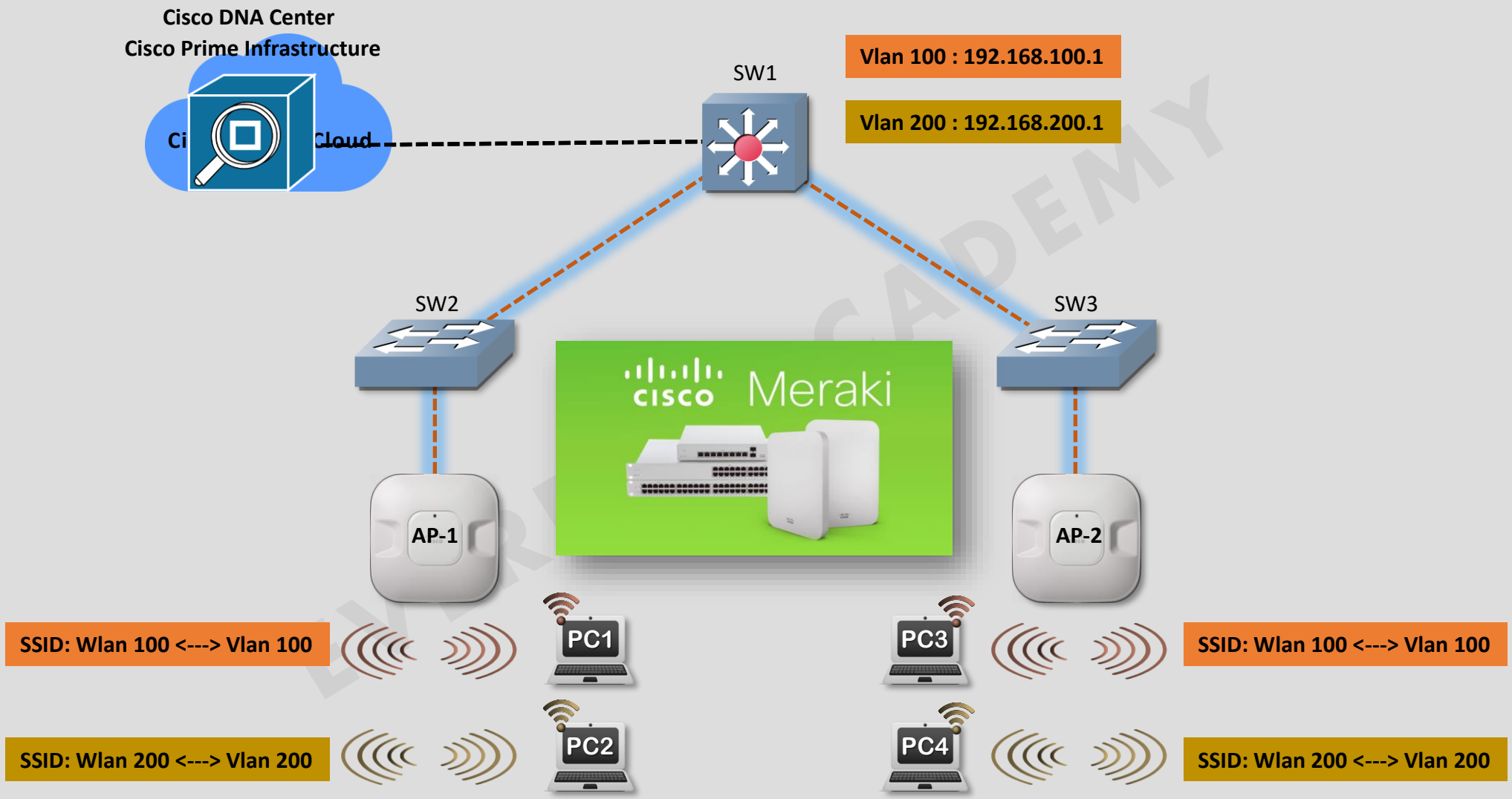
Autonomous AP Architecture



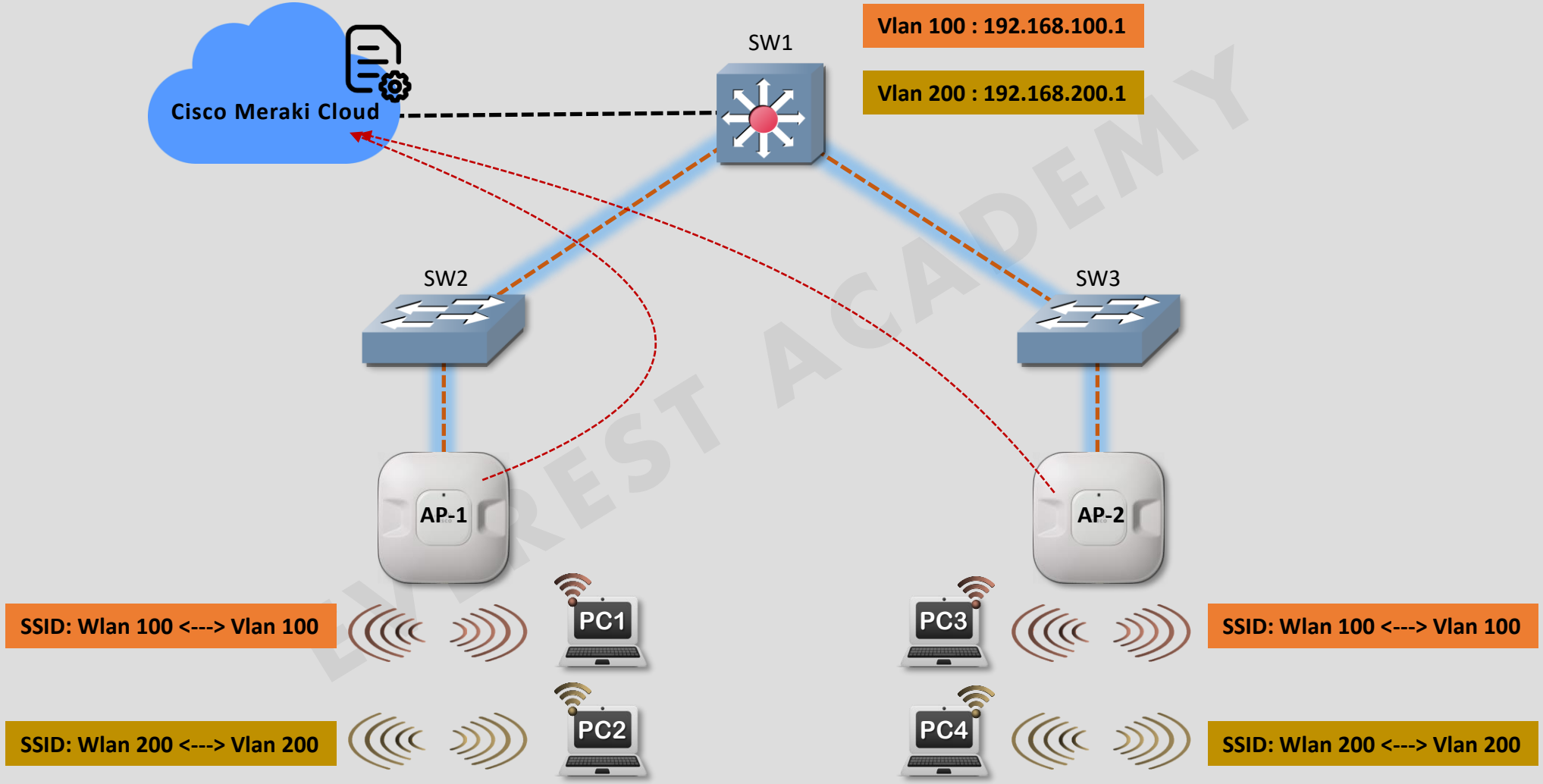
Autonomous AP Architecture



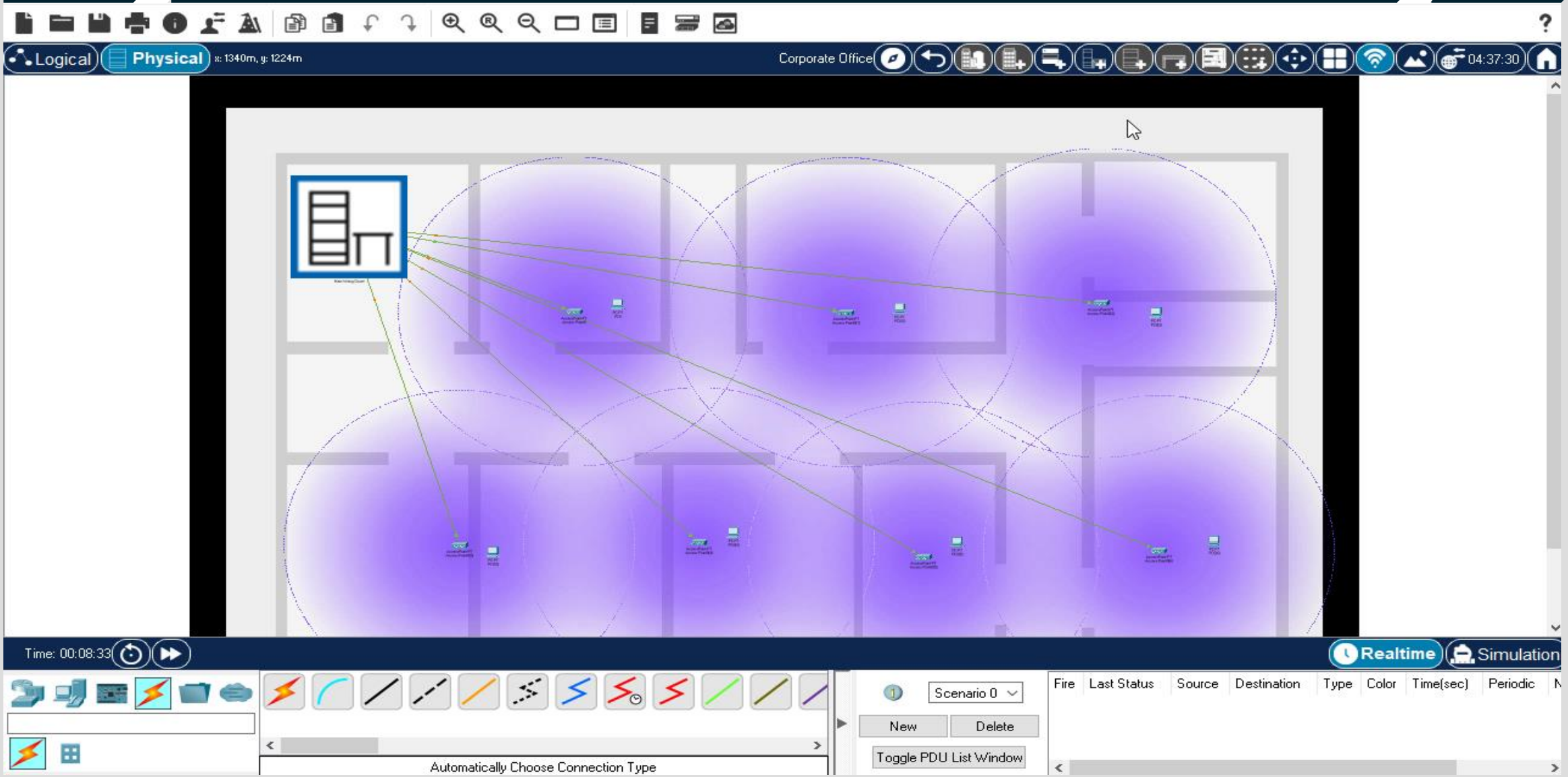
Cloud-based AP Architecture



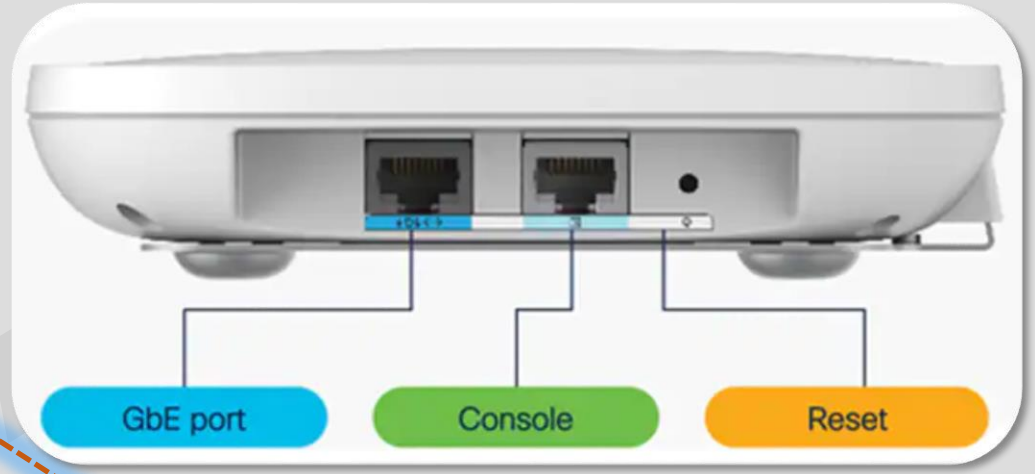
Cloud-based AP Architecture

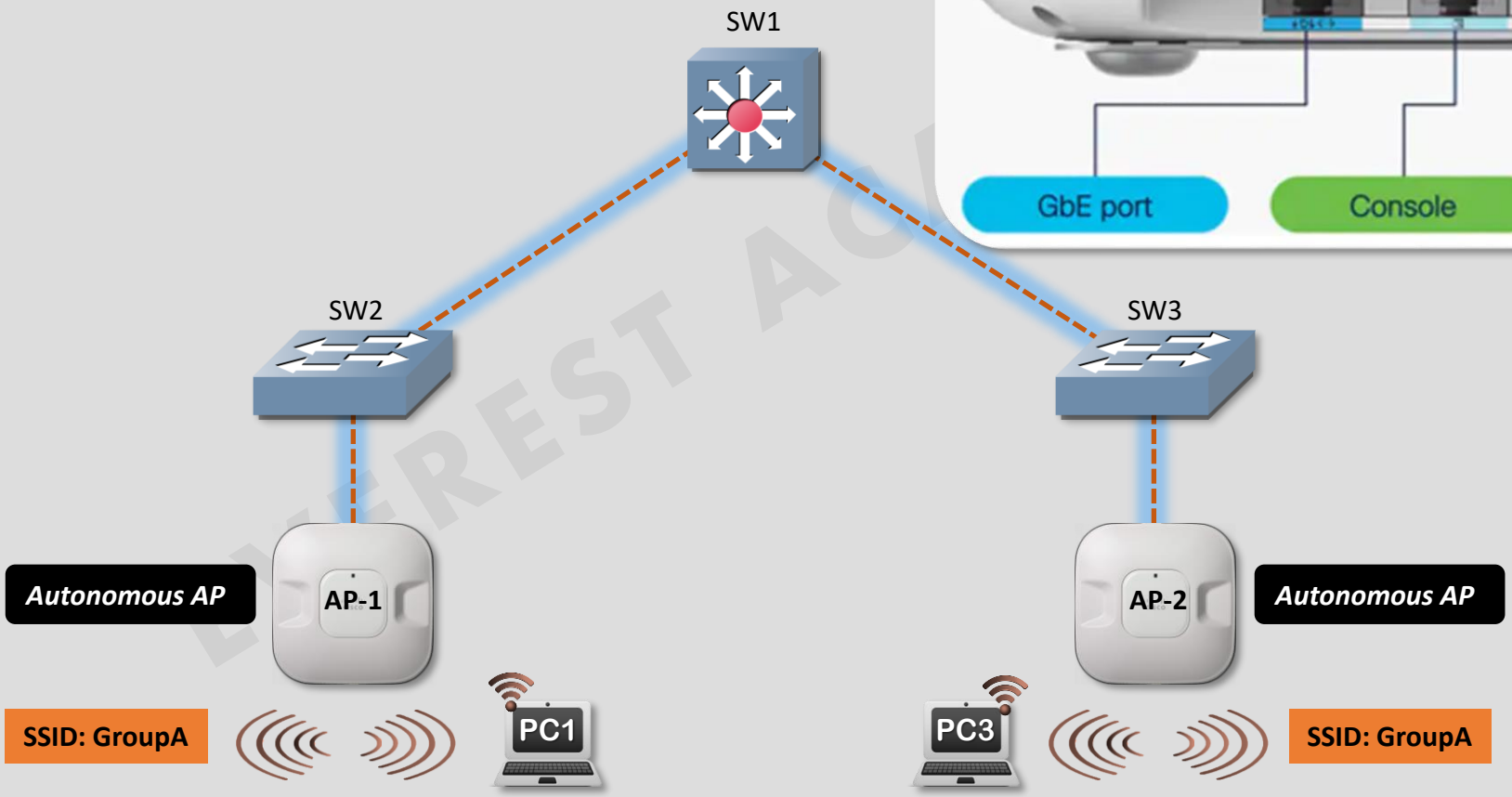


LAB - Autonomous Access Points

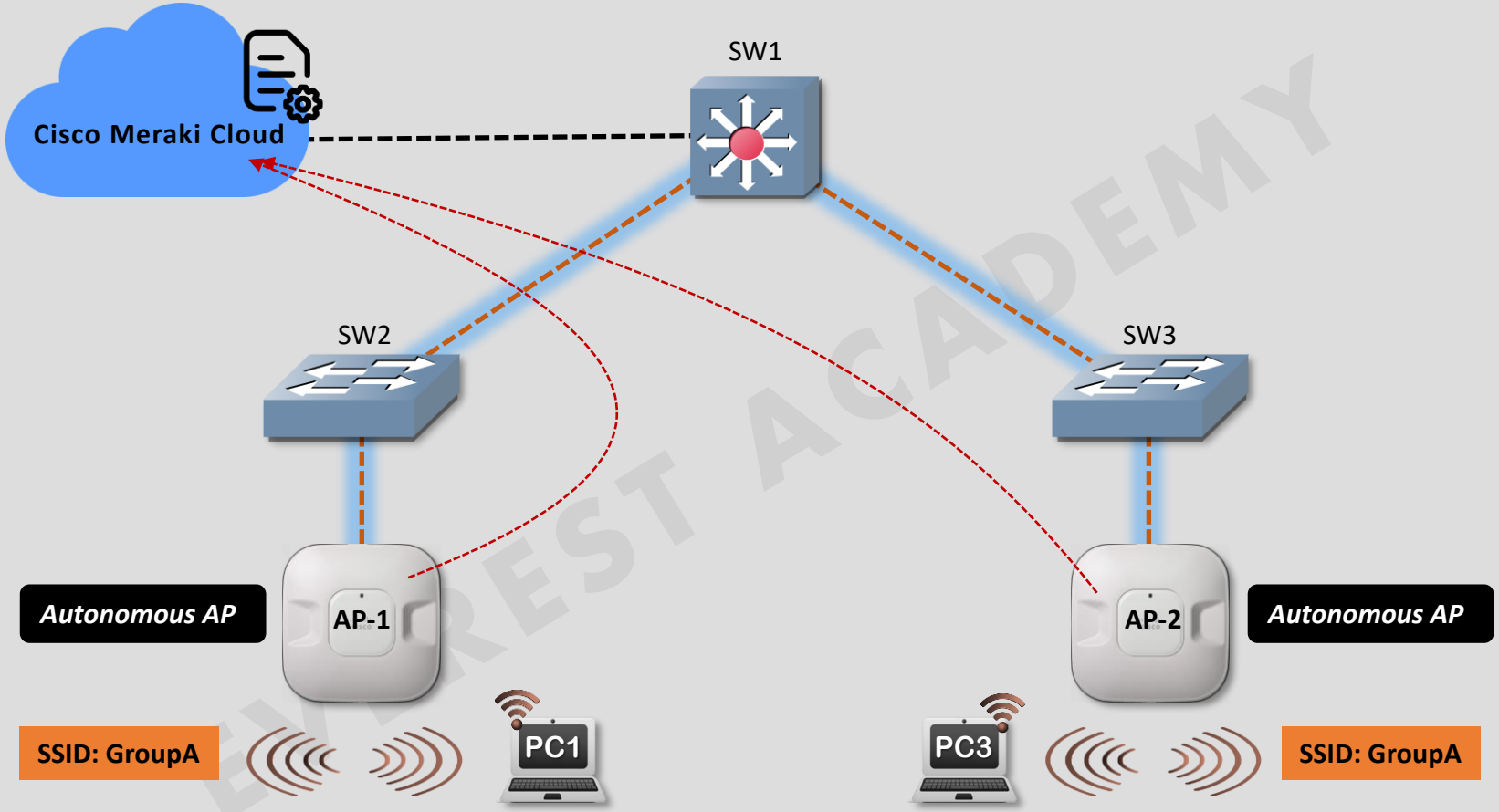


Autonomous AP Architecture

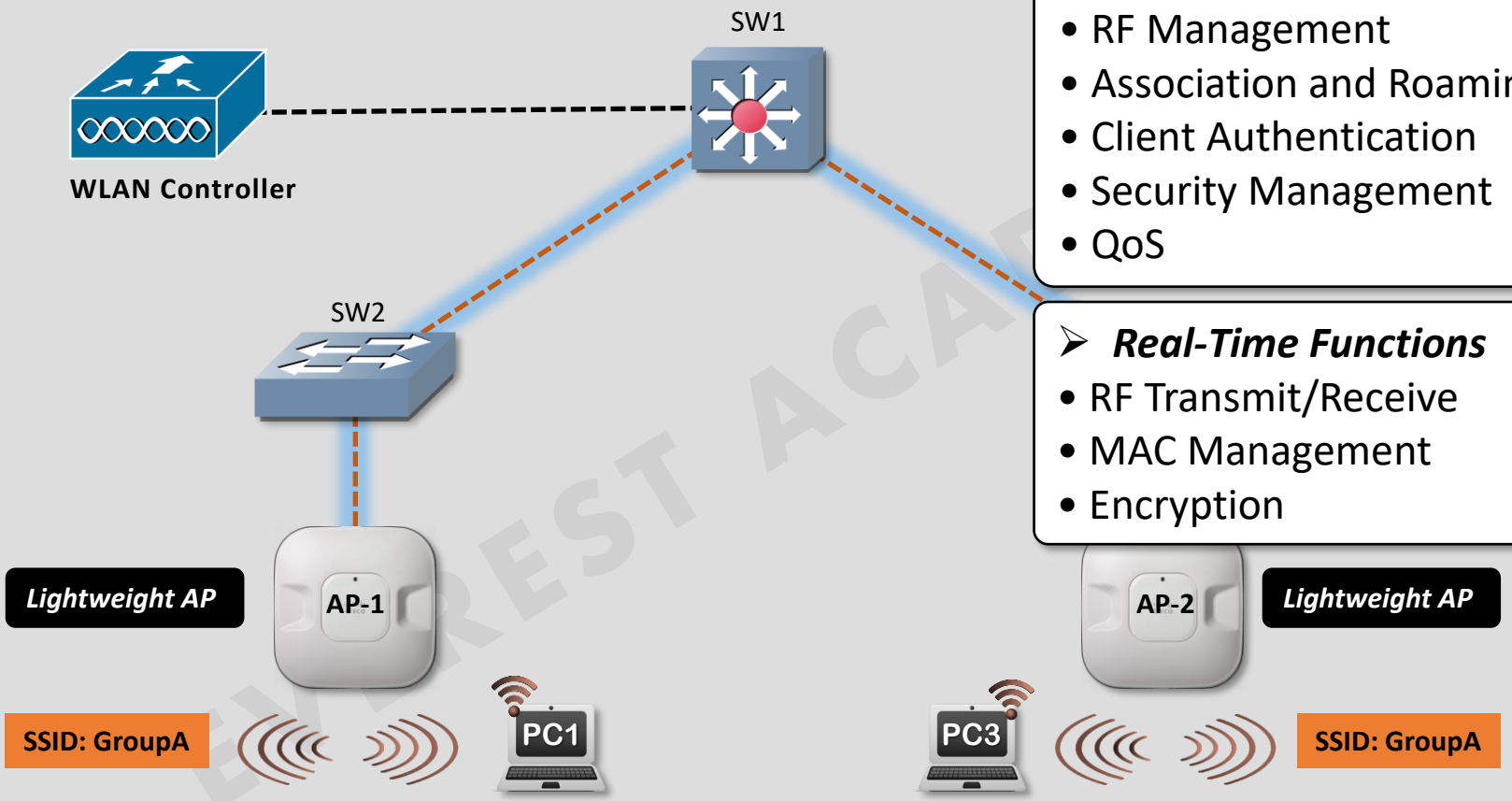




Cloud-based AP Architecture



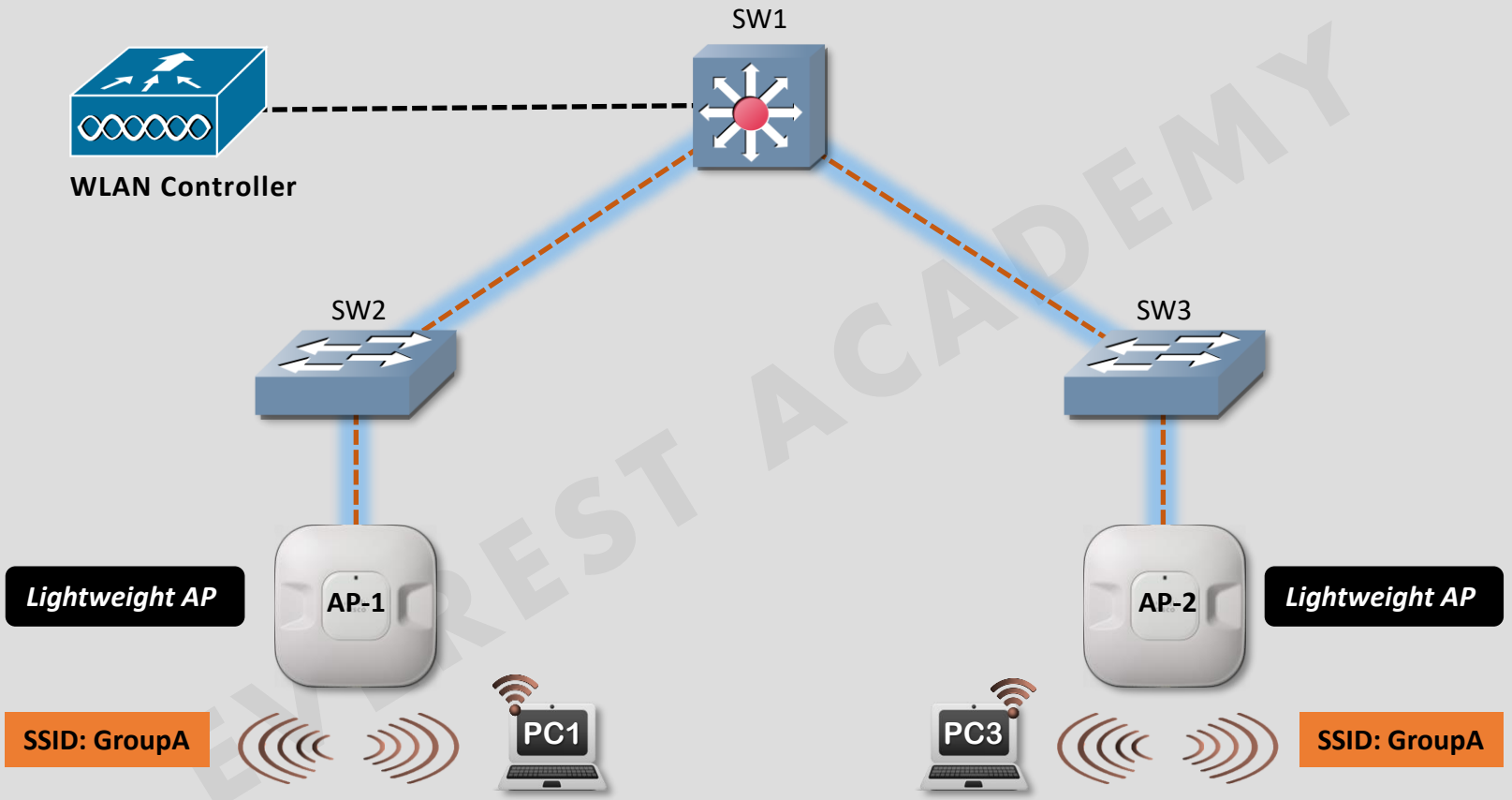
Split-MAC Architecture



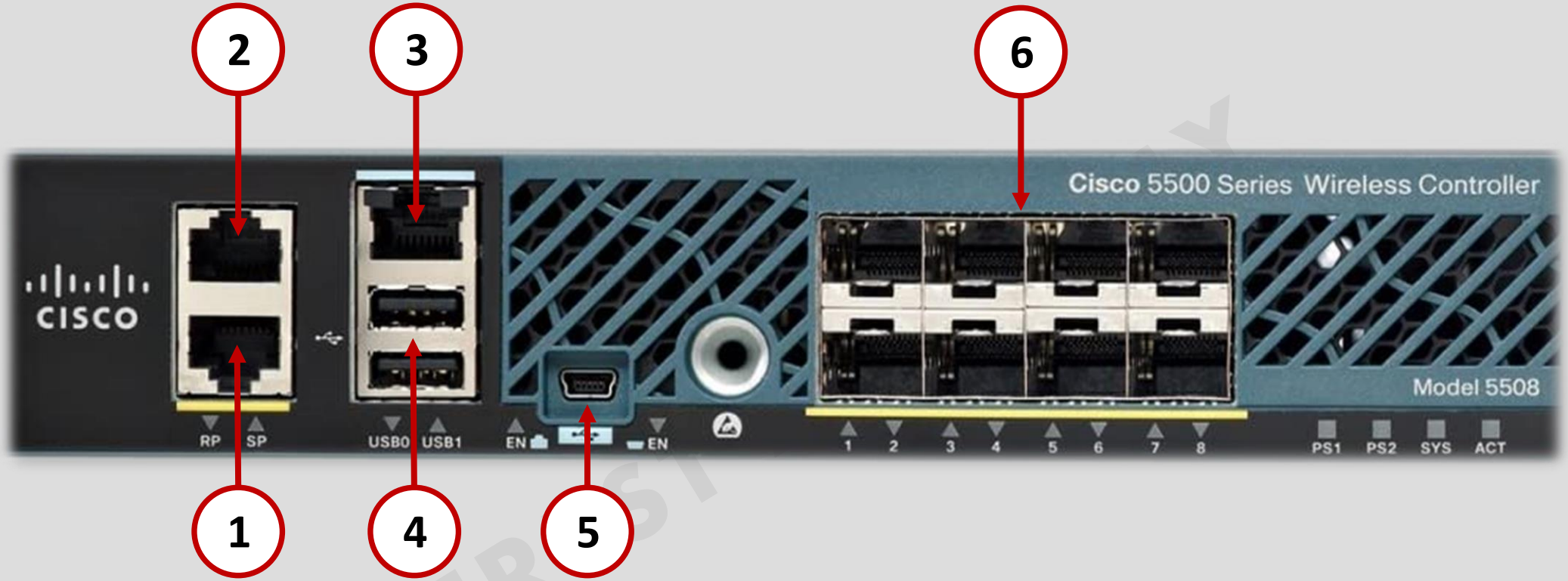
- ***Management Functions***
  - RF Management
  - Association and Roaming Management
  - Client Authentication
  - Security Management
  - QoS

- ***Real-Time Functions***
  - RF Transmit/Receive
  - MAC Management
  - Encryption

Control and Provisioning of Wireless Access Points (CAPWAP) Protocol

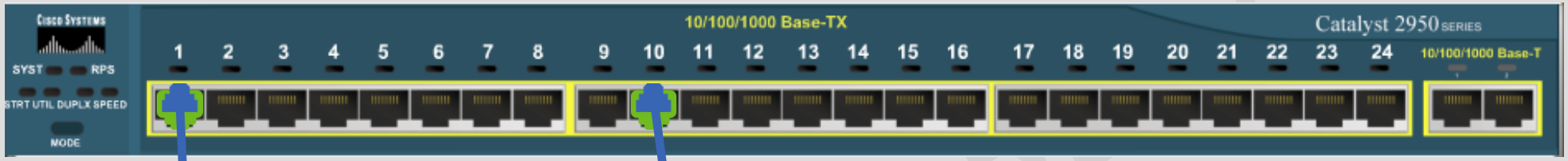


WLC Interfaces



1	Redundant port (RJ-45)
2	Service port (RJ-45)
3	Console port (RJ-45)
4	USB ports 0 and 1 (Type A)
5	Console port (Mini USB Type B)
6	SFP distribution system ports 1–8

WLC Interfaces

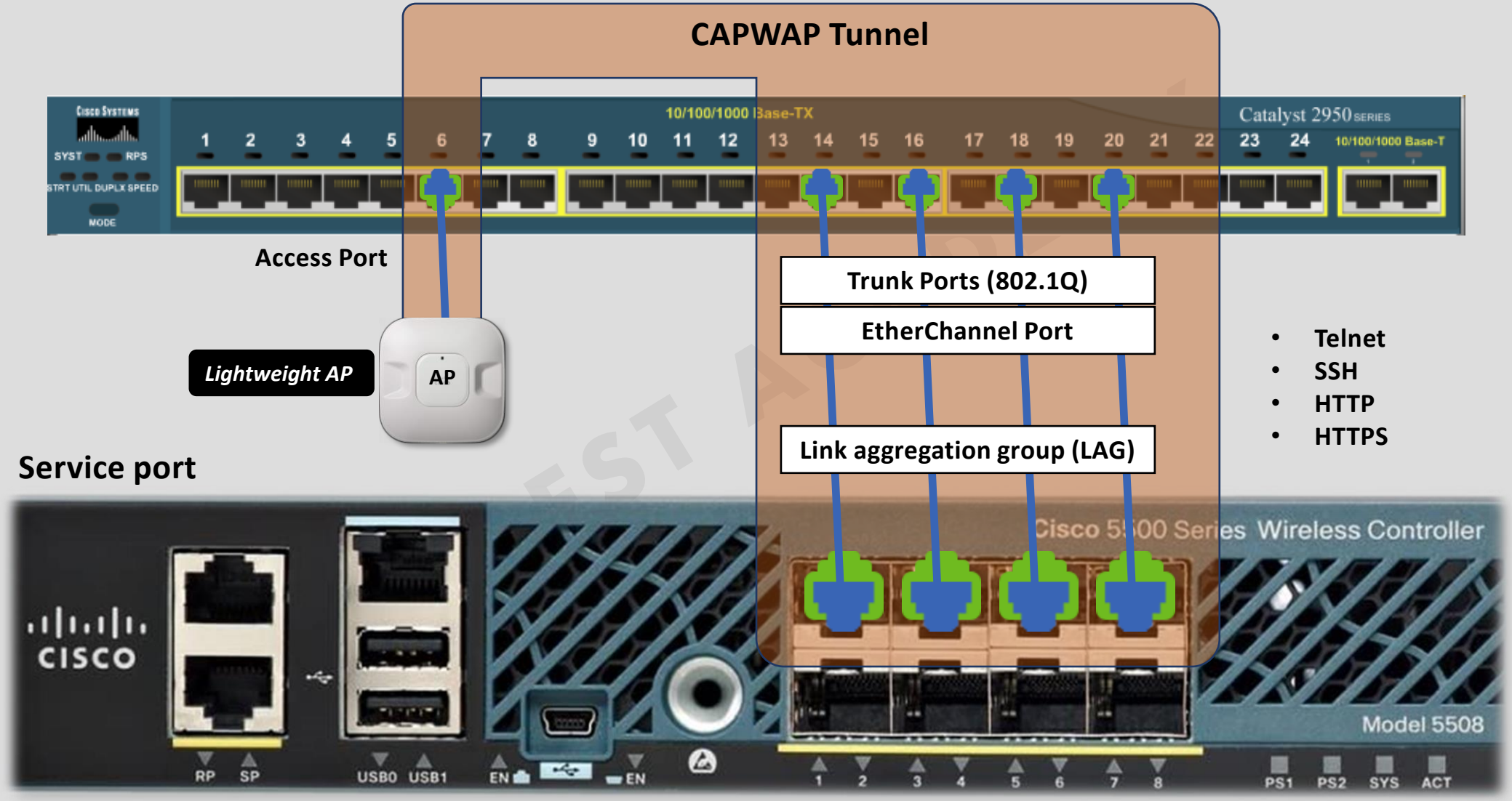


Access Port

- Telnet
- SSH
- HTTP
- HTTPS

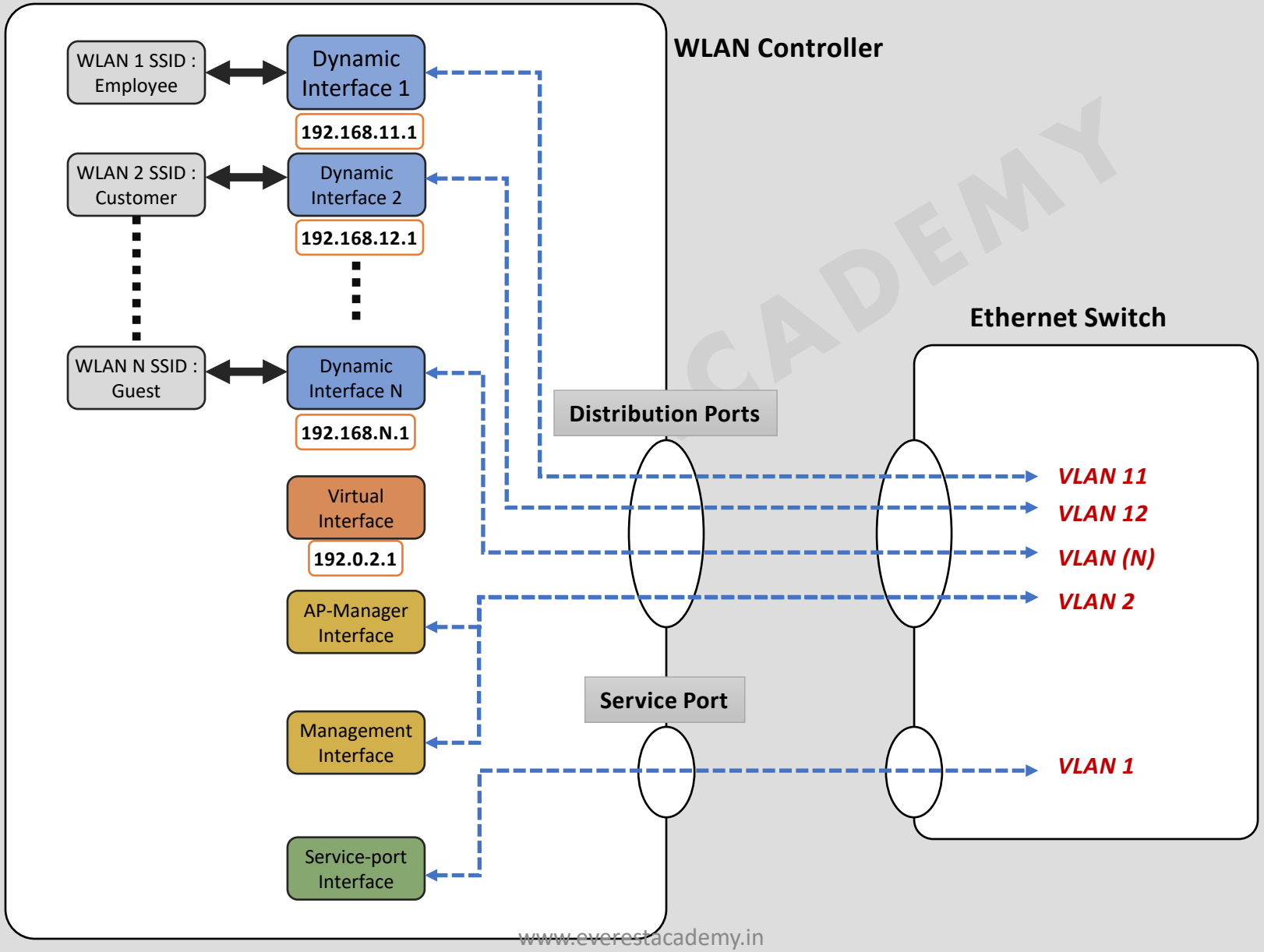
Service port

WLC Interfaces

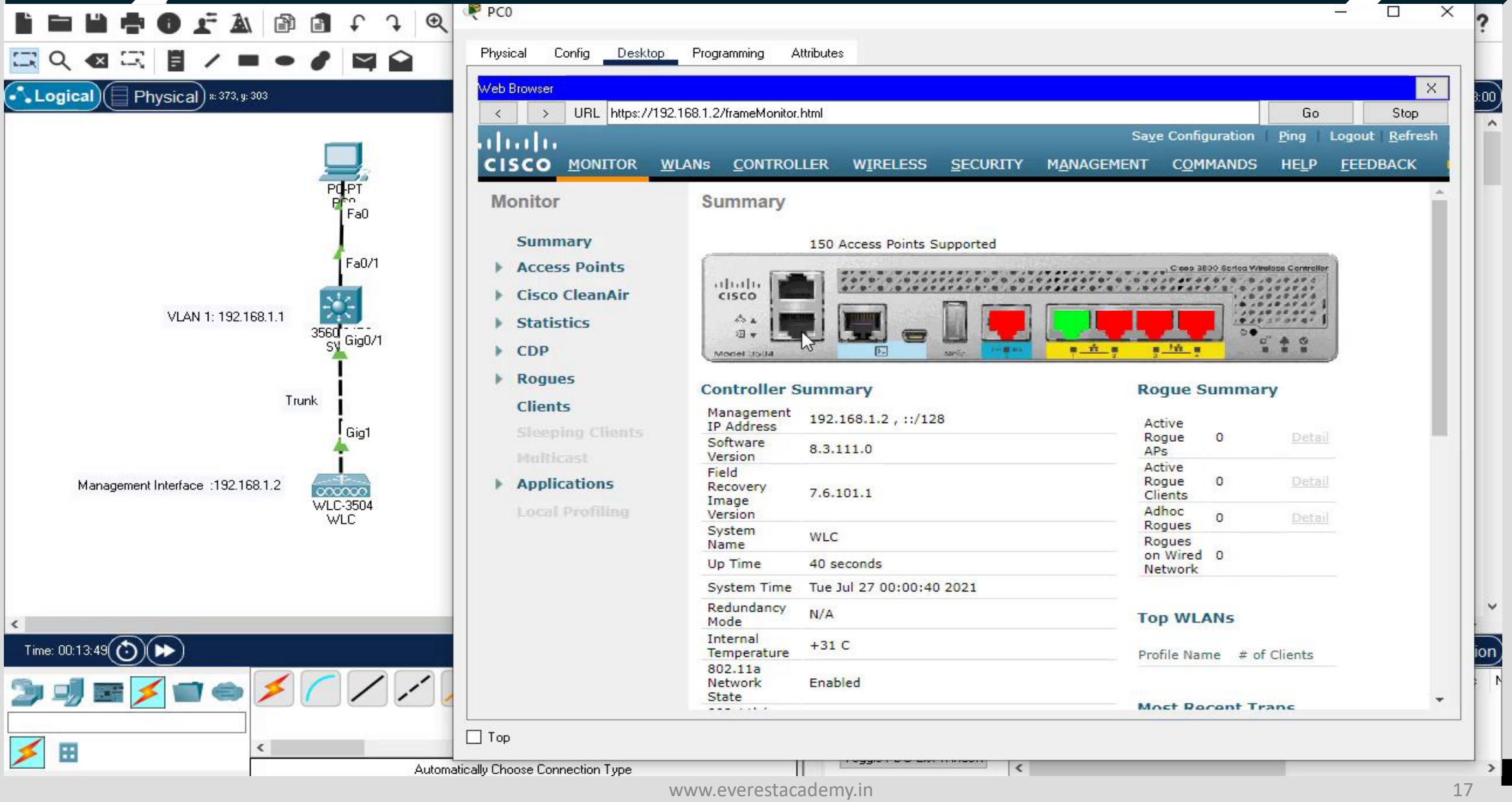


- Telnet
- SSH
- HTTP
- HTTPS

WLC Interfaces



WLC -LAB


Logical
Physical
x: 373, y: 303
PC-PT
Fa0
Fa0/1
VLAN 1: 192.168.1.1
Gig0/1
Trunk
Gig1
Management Interface :192.168.1.2
WLC-3504
WLC
Time: 00:13:49
Automatically Choose Connection Type
PC0
Physical
Config
Desktop
Programming
Attributes
Web Browser
URL
https://192.168.1.2/frameMonitor.html
Go
Stop
Save Configuration
Ping
Logout
Refresh
CISCO
MONITOR
WLANs
CONTROLLER
WIRELESS
SECURITY
MANAGEMENT
COMMANDS
HELP
FEEDBACK
Monitor
Summary
Access Points
Cisco CleanAir
Statistics
CDP
Rogues
Clients
Sleeping Clients
Multicast
Applications
Local Profiling
Summary
150 Access Points Supported
Controller Summary
Management IP Address
192.168.1.2 , ::/128
Software Version
8.3.111.0
Field Recovery Image Version
7.6.101.1
System Name
WLC
Up Time
40 seconds
System Time
Tue Jul 27 00:00:40 2021
Redundancy Mode
N/A
Internal Temperature
+31 C
802.11a Network State
Enabled
Rogue Summary
Active Rogue APs
0
Detail
Active Rogue Clients
0
Detail
Adhoc Rogues
0
Detail
Rogues on Wired Network
0
Top WLANs
Profile Name
# of Clients
Most Recent Traps
Top

WLC –LAB EVE NG

EVE | Topology

Cisco-5000.0001.0001

Not secure | 192.168.1.100/screens/frameset.html

Apps | Getting Started | Latest Headlines | Google Image Resu... | Reading list

Save Configuration | Ping | Logout | Refresh

MONITOR | WLANs | CONTROLLER | WIRELESS | SECURITY | MANAGEMENT | COMMANDS | HELP | FEEDBACK | Home

Monitor

- Summary
- Access Points
- Cisco CleanAir
- Statistics
- CDP
- Rogues
- Clients
- Sleeping Clients
- Multicast
- Applications
- Local Profiling
- Cloud Services

Summary

200 Access Points Supported

Cisco Virtual Wireless Controller

Controller Summary

Management IP Address	192.168.1.100 , ::/128
Service Port IP Address	192.168.2.100 , ::/128
Software Version	8.7.102.0
Emergency Image Version	8.7.102.0
System Name	Cisco-5000.0001.0001
Up Time	0 days, 0 hours, 6 minutes
System Time	Tue Jul 27 22:07:43 2021
Redundancy Mode	N/A
802.11a Network State	Enabled
802.11b/g Network State	Enabled
Local Mobility Group	Group1
CPU Usage	36%
Memory	62%

Rogue Summary

Active Rogue APs	0	Detail
Active Rogue Clients	0	Detail
Adhoc Rogues	0	Detail
Rogues on Wired Network	0	

Session Timeout

Top WLANs

Profile Name	# of Clients

Most Recent Traps

Interface: management IPv6 address status =REACHABLE, IPv6 Address =fe80::5200:ff:fe01:1

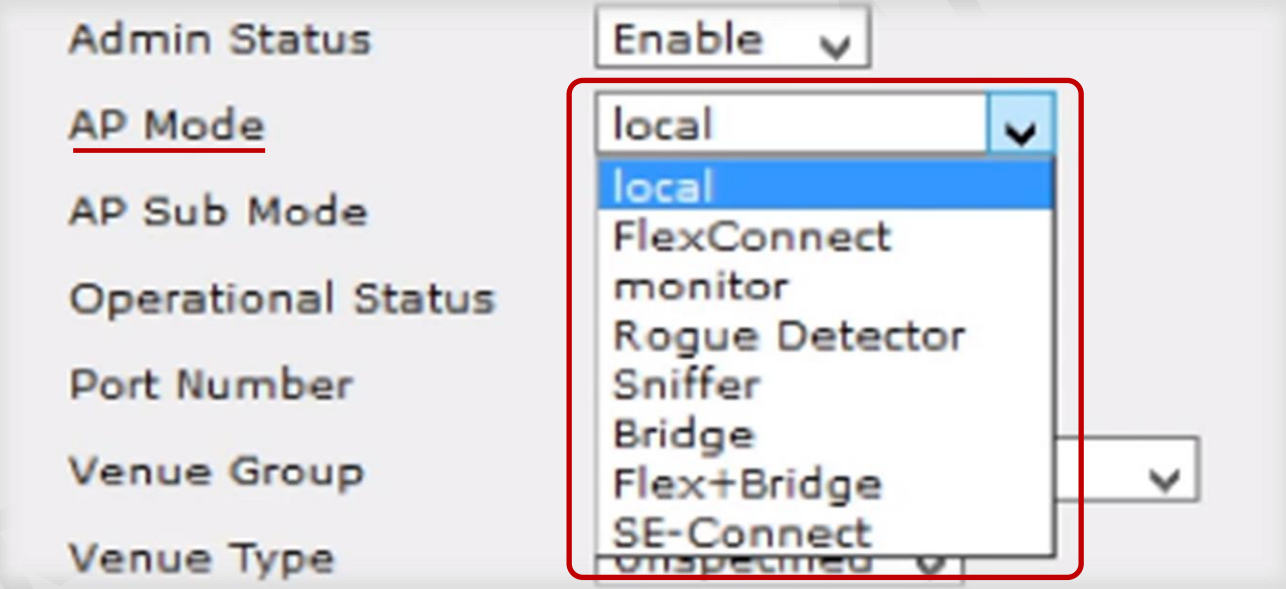
Cold Start:

Link Up: Slot: 0 Port: 1 Admin Status: Enable Oper Status: Link Up

A RF group member has been added on 802.11a network on controller with IP 192.168.3.100(MAC

Cisco Wireless AP Modes

- Local Mode
- FlexConnect Mode
- Sniffer Mode
- SE-Connect Mode
- Rogue Detector Mode
- Monitor Mode
- Bridge Mode
- Flex + Bridge Mode

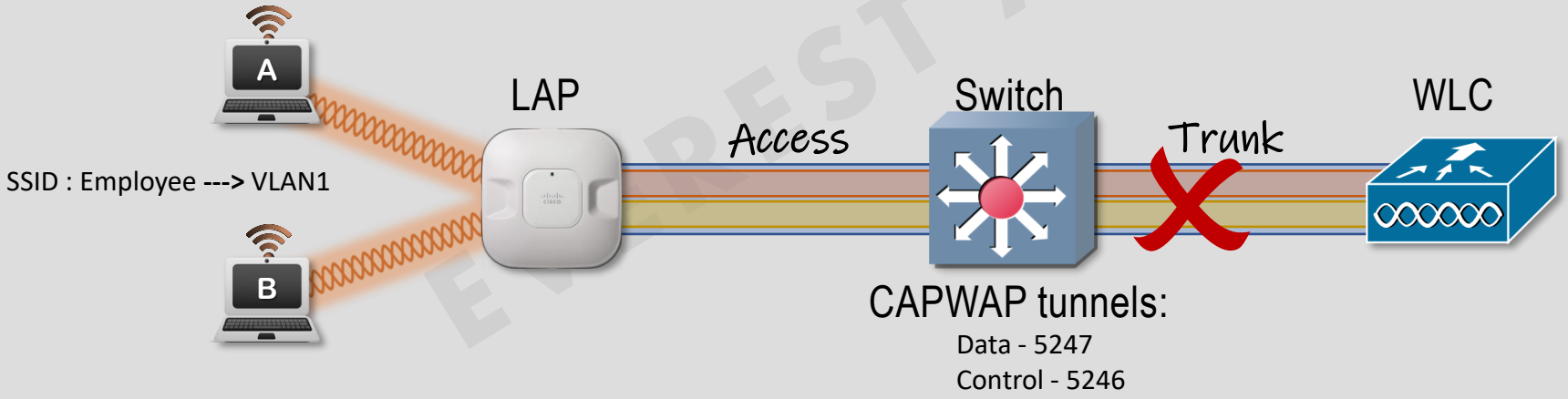


- An AP is considered to be a **rogue AP** if it is both unauthorized and plugged into the **wired side** of the network.
- An AP is considered to be an **interfering AP** if it is seen in the RF environment but is not connected to the wired network. However, an interfering AP may be reclassified as a rogue AP.

Cisco Wireless AP Modes

Local Mode

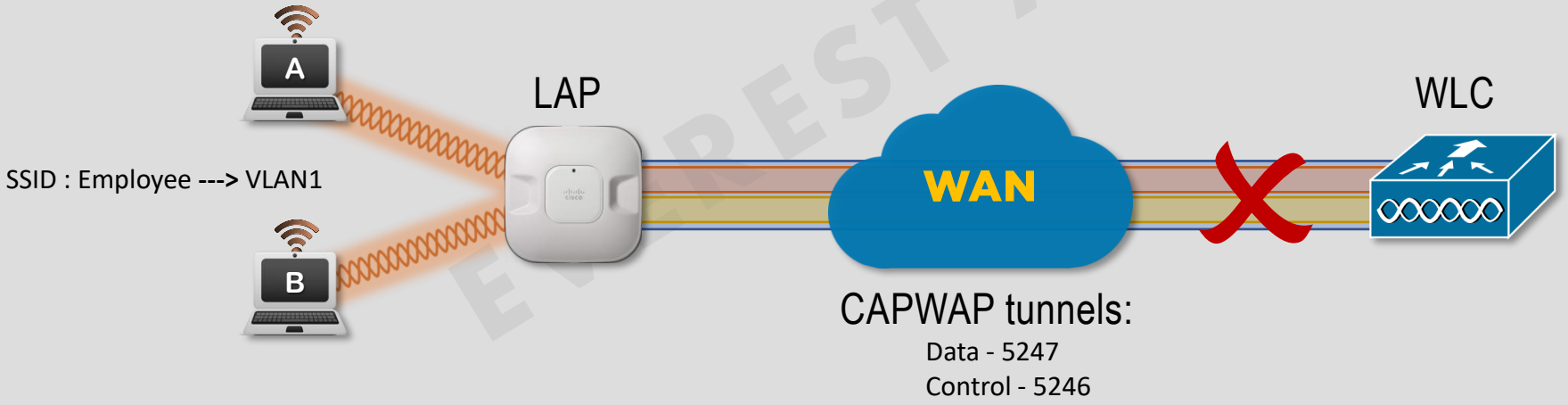
- This is the **default** mode that offers one or more functioning **BSSs** on a specific channel.
- All traffic will be carried back to the wireless controller through **CAPWAP tunnels**.
- When the AP isn't busy transmitting traffic, it'll keep itself busy by scanning the other channels for **interference**, measuring the **noise level**, and checking for **rogue devices.**
- The AP can not function if it looses connection with the controller.



Cisco Wireless AP Modes

FlexConnect Mode

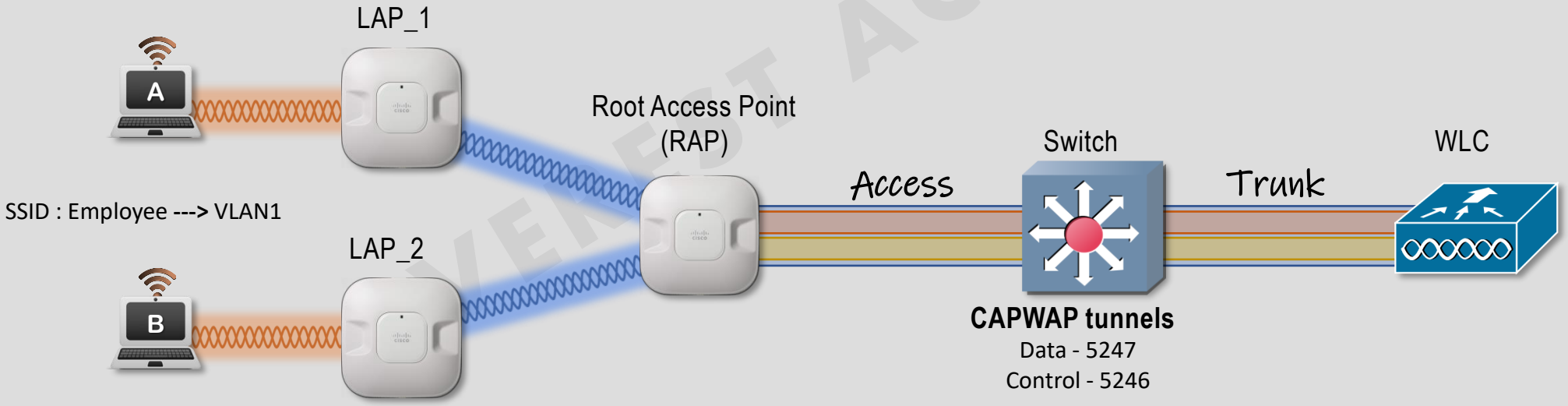
- FlexConnect is a wireless solution for branch office and remote office deployments.
- FlexConnect allows APs to locally switch traffic rather than send it to the controller.
- It basically causes the AP to behave like an autonomous AP, but be managed by the WLC.
- In this mode, the AP can still function even if it looses connection with the controller.



Cisco Wireless AP Modes

➢ Bridge Mode

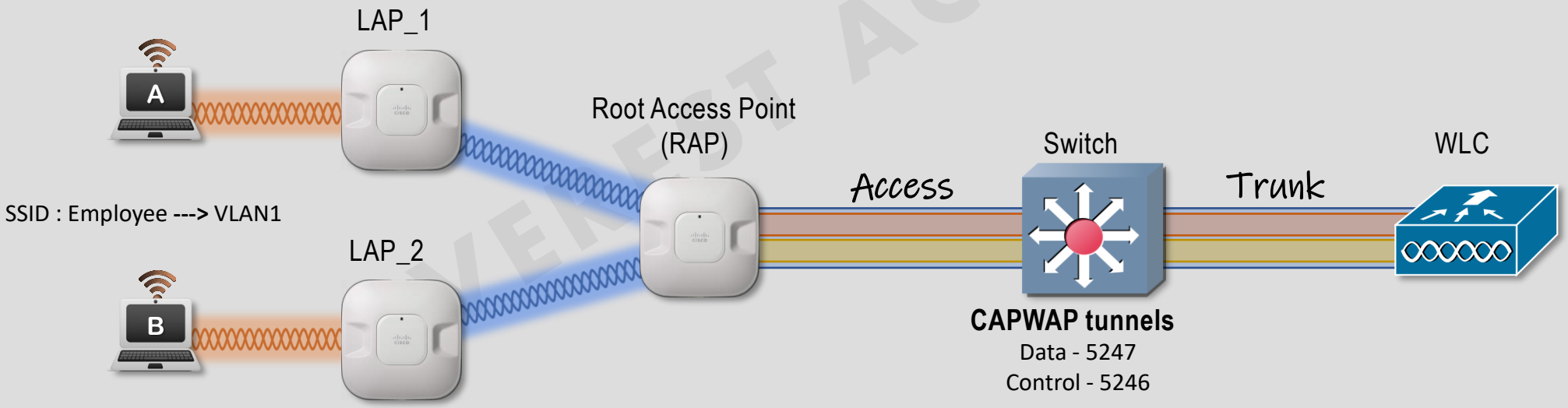
- This mode is also known as a mesh and allows an AP to connect to another AP to form **a point-to-point or point-to-multipoint** connection.
- This helps when connecting areas together wirelessly if you can't run a **cable** between the sites .
- The access point at the top of the mesh network is called **the Root Access Point (RAP).**
- When traffic reaches the RAP, it's sent to the **controller** through a **CAPWAP tunnel** just like with **local mode**.



Cisco Wireless AP Modes

➢ Flex + Bridge Mode

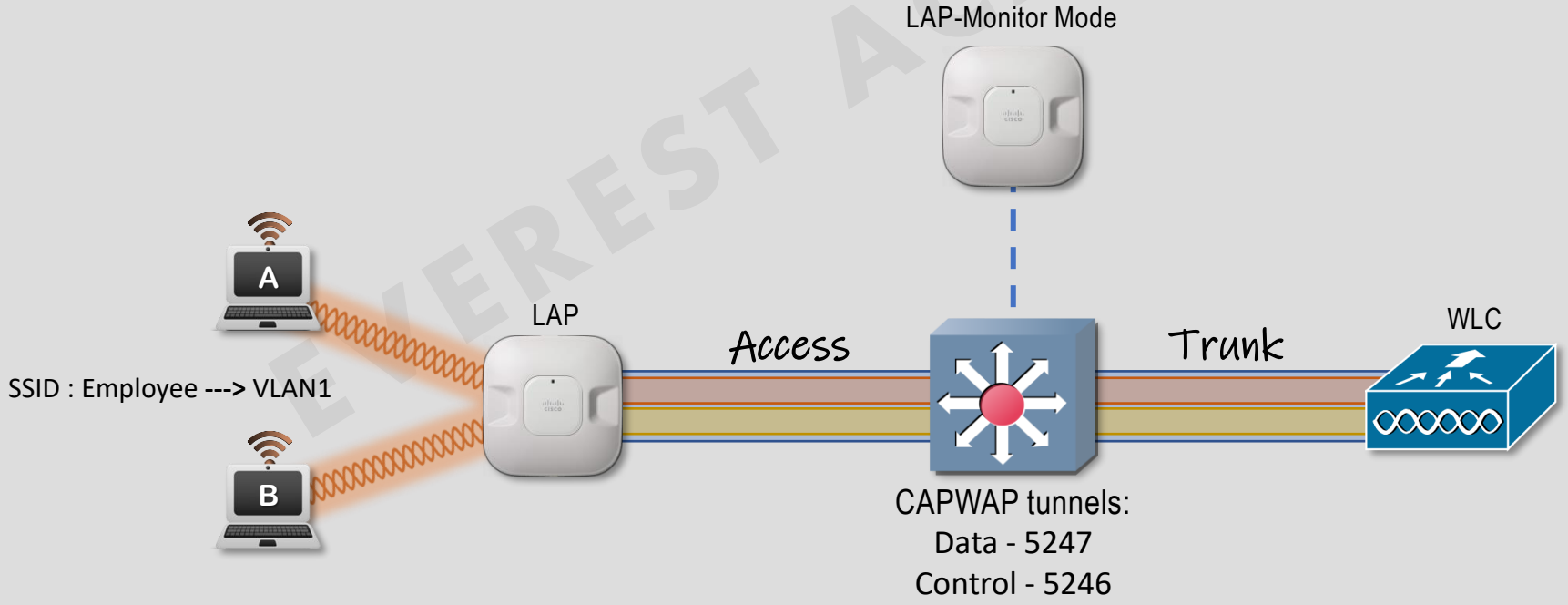
- This mode adds **FlexConnect** to the mesh network In it, traffic is **locally switched** from the RAP when it reenters the network.



Cisco Wireless AP Modes

Monitor Mode

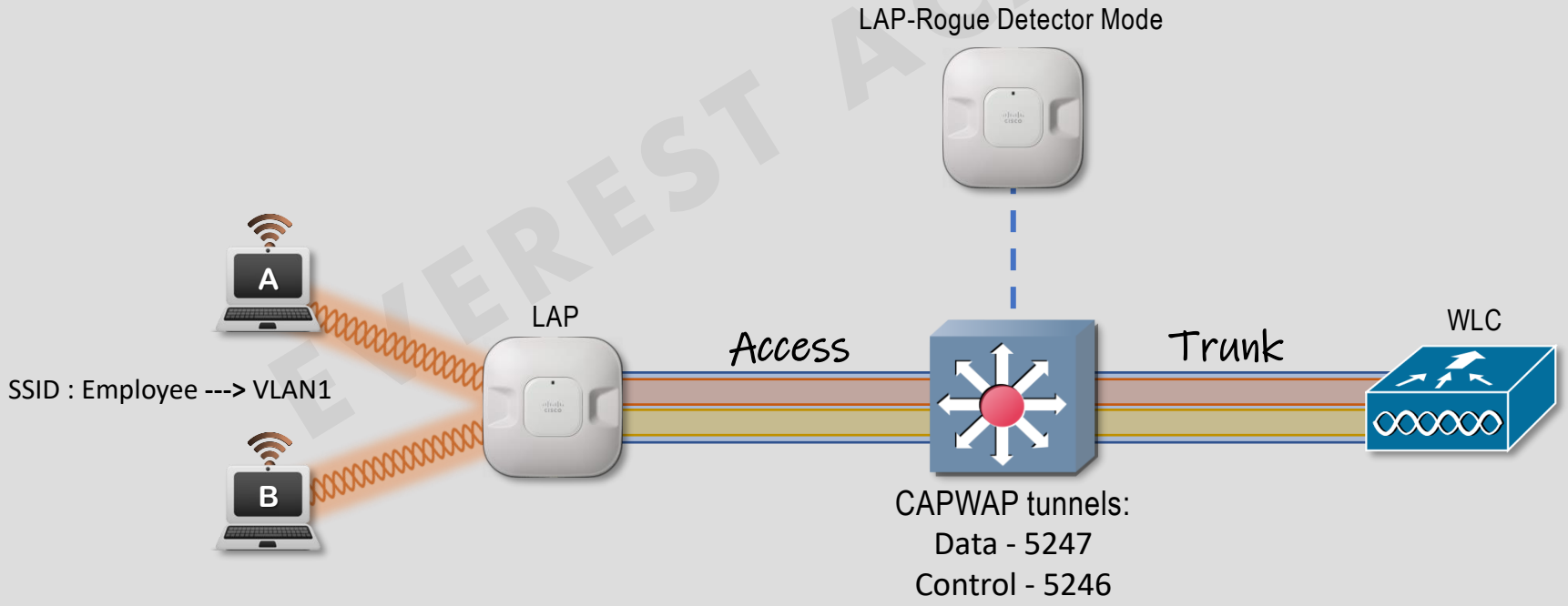
- The AP does not transmit at all, but its receiver is enabled to act as a **dedicated sensor**.
- Just like with **local mode**, it will check the **noise**, check for **interference**, check for **rogue devices** and determines the **position** of stations through **location-based services**.



Cisco Wireless AP Modes

➢ Rogue Detector Mode

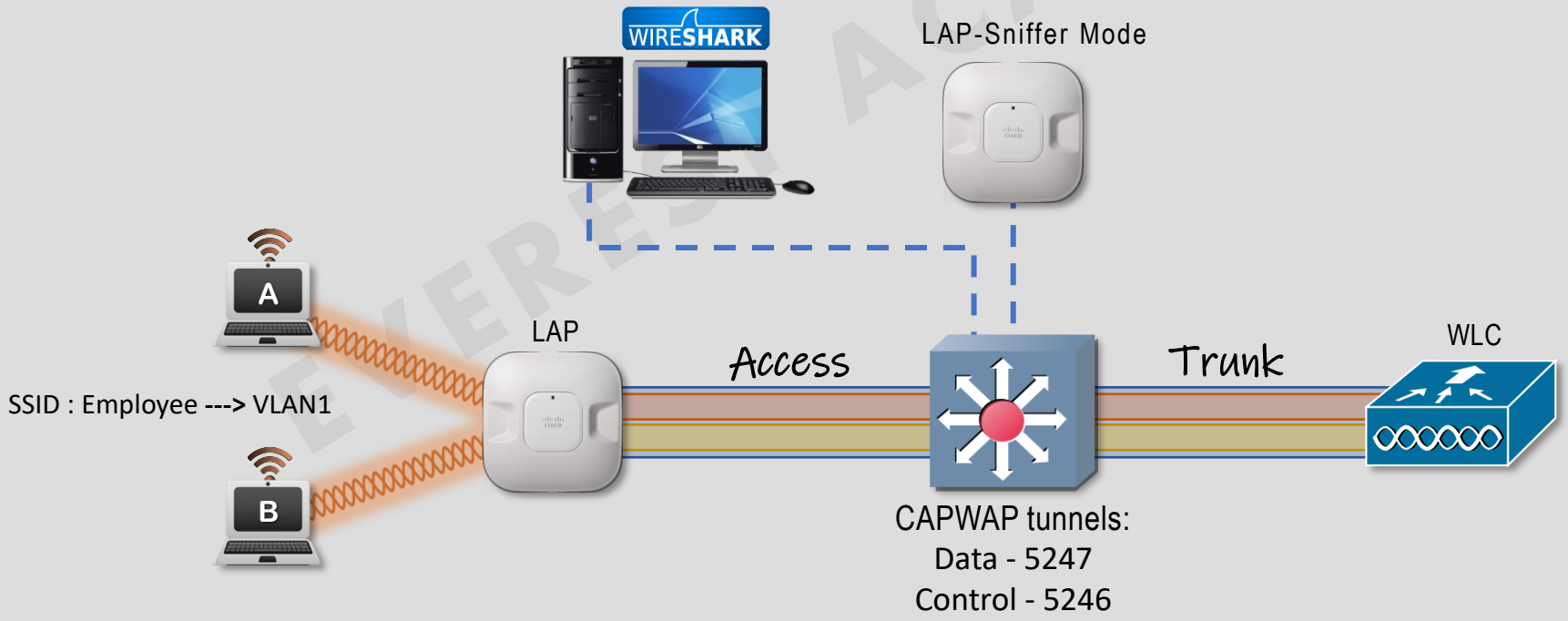
- This is another mode that doesn't send wireless traffic but dedicates itself to tracking access points that aren't joined to the WLC but are still possibly in your network.
- Once the WLC detects a rogue AP, it can either notify the Admin.



Cisco Wireless AP Modes

Sniffer Mode

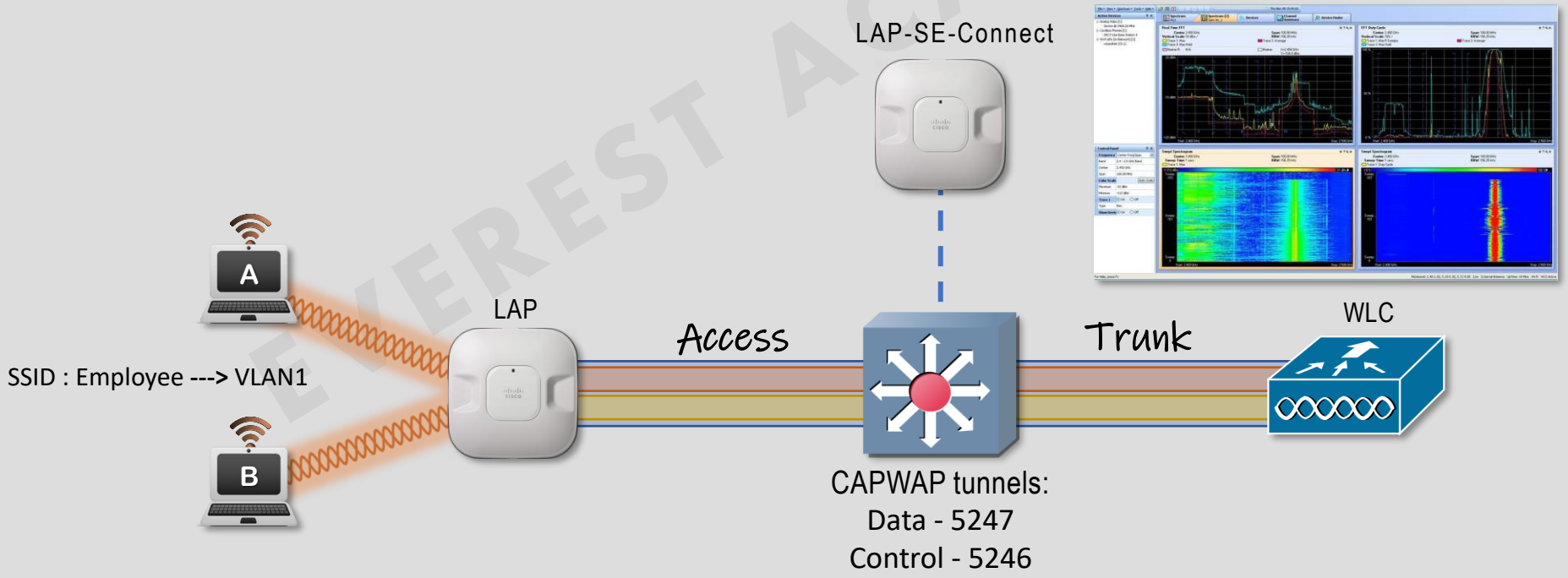
- This mode is great when you're troubleshooting an issue with the wireless network and need to do a packet capture.
- It doesn't serve traffic, but it does start a packet capture that can be sent to a PC running network analyzer software such as **WireShark**.



Cisco Wireless AP Modes

➢ SE-Connect Mode

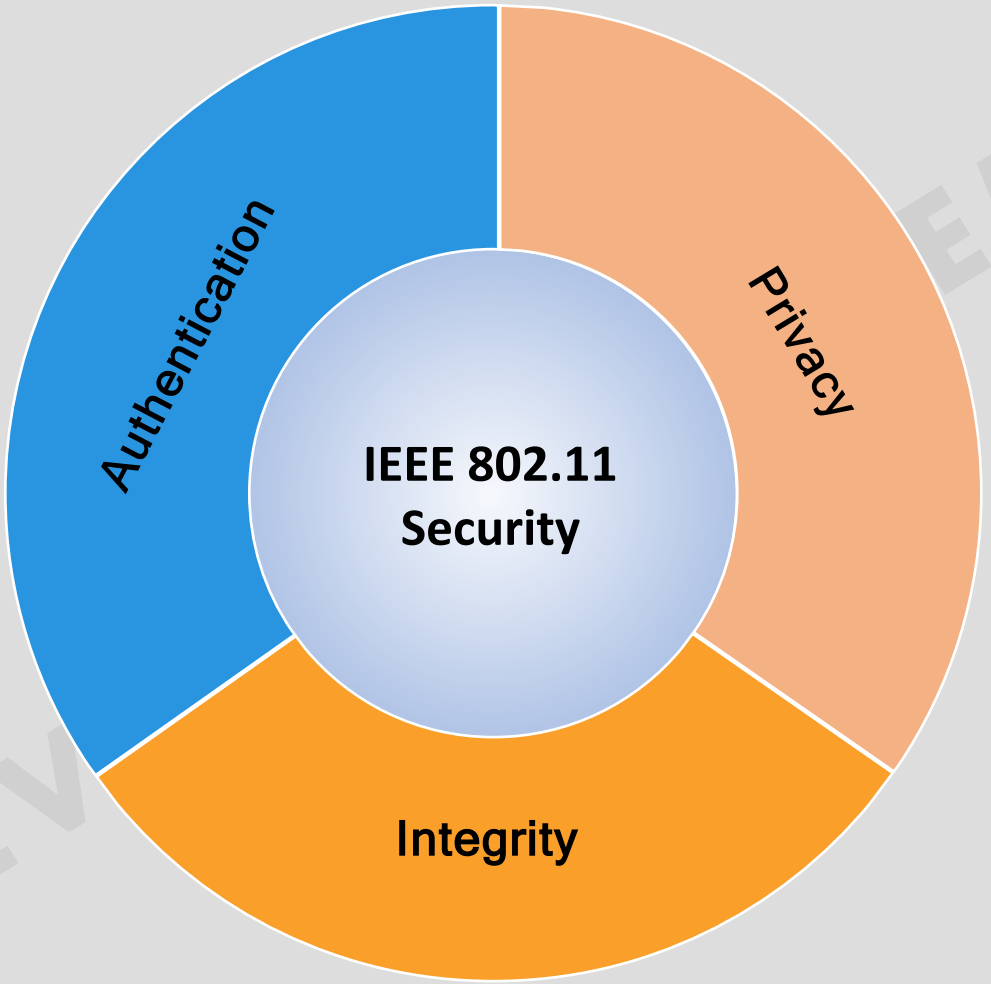
- The AP dedicates its radios to **spectrum analysis** on all wireless channels.
- You can remotely connect a PC running software such as **Cisco Spectrum Expert** to the AP to collect and analyze the spectrum analysis data to discover sources of interference.



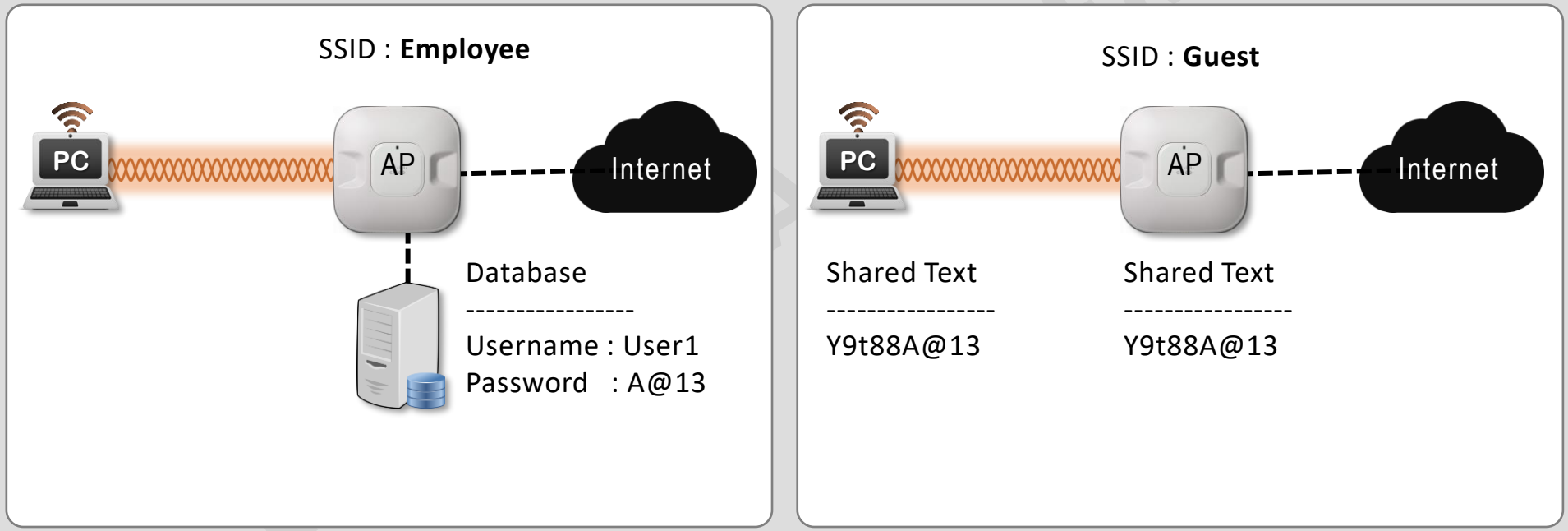
WLAN Security

- Identifying the endpoints of a wireless connection.
- Identifying the end user.
- Protecting the wireless data from eavesdroppers.
- Protecting the wireless data from tampering.

WLAN Security



Authentication



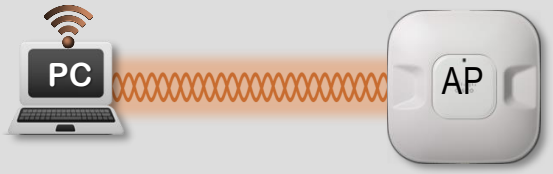
Authentication

Authenticating a Wireless Client

Who are you?

I am PC.

Ok.



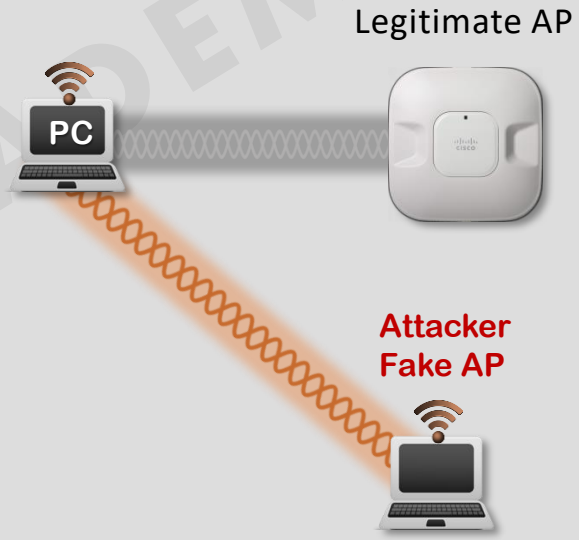
Authenticating a Wireless AP

Who are you?

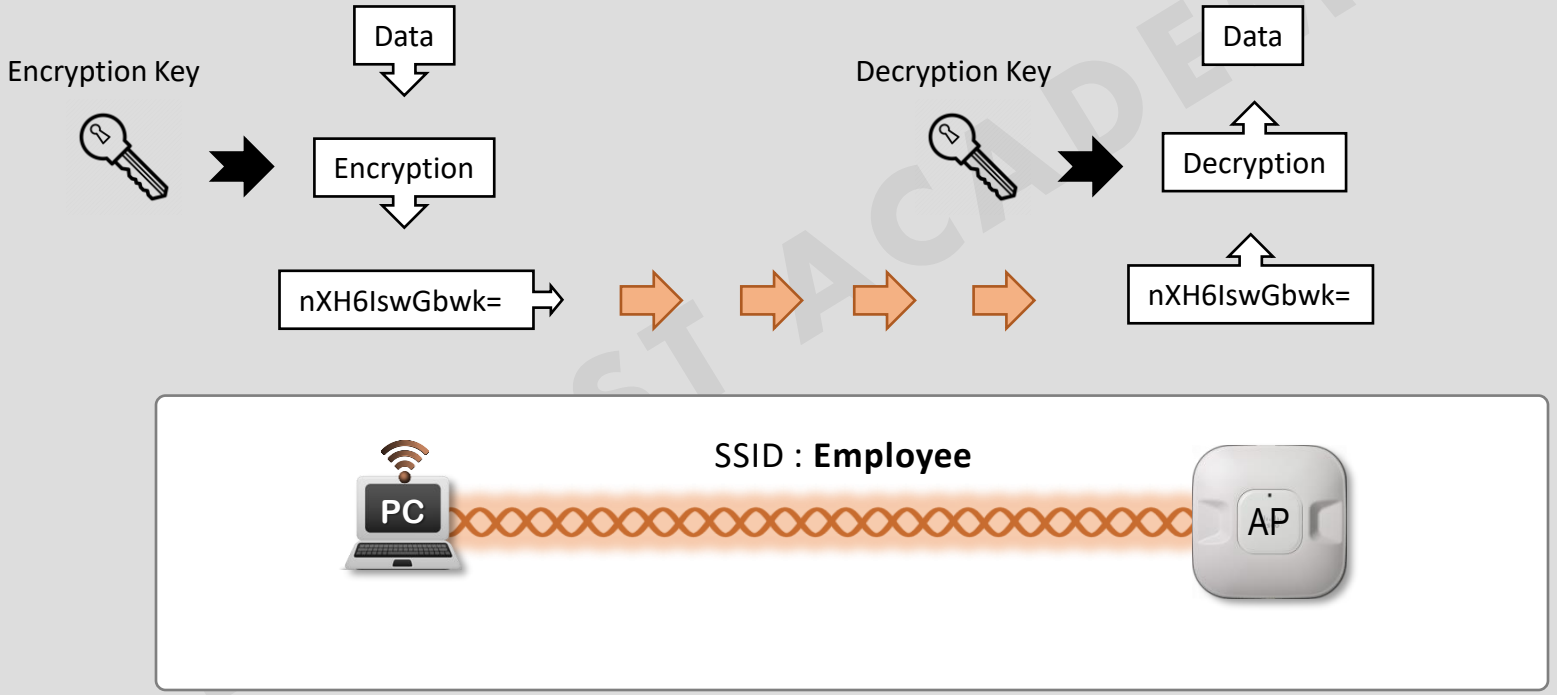
I am AP, These are my management frames.

Ok.

Man-in-the-Middle (MITM) Attack

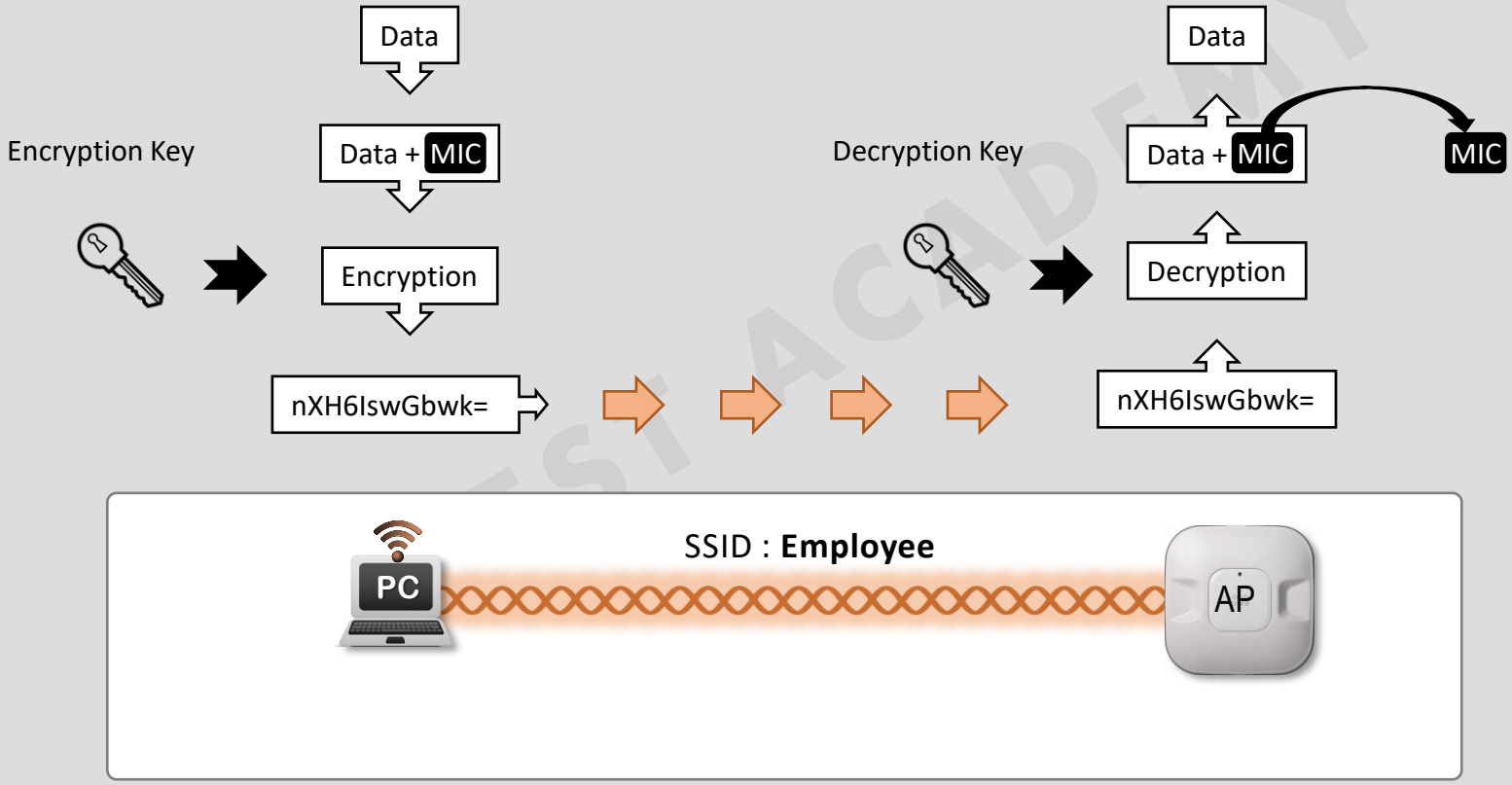


Message Privacy



Message Integrity

Message Integrity Check (MIC)

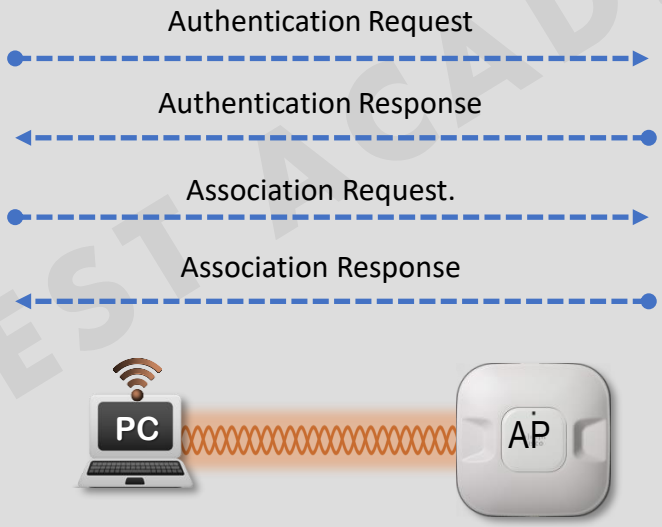


Wireless Client Authentication Methods

Open (Original 802.11 standard)		Open Authentication
WEP (Original 802.11 standard)		Wired Equivalent Privacy (deprecated)
802.1x/EAP (Extensible Authentication Protocol)	LEAP	Lightweight EAP
	EAP-FAST	EAP Flexible Authentication by Secure Tunneling
	PEAP	Protected EAP
	EAP-TLS	EAP Transport Layer Security

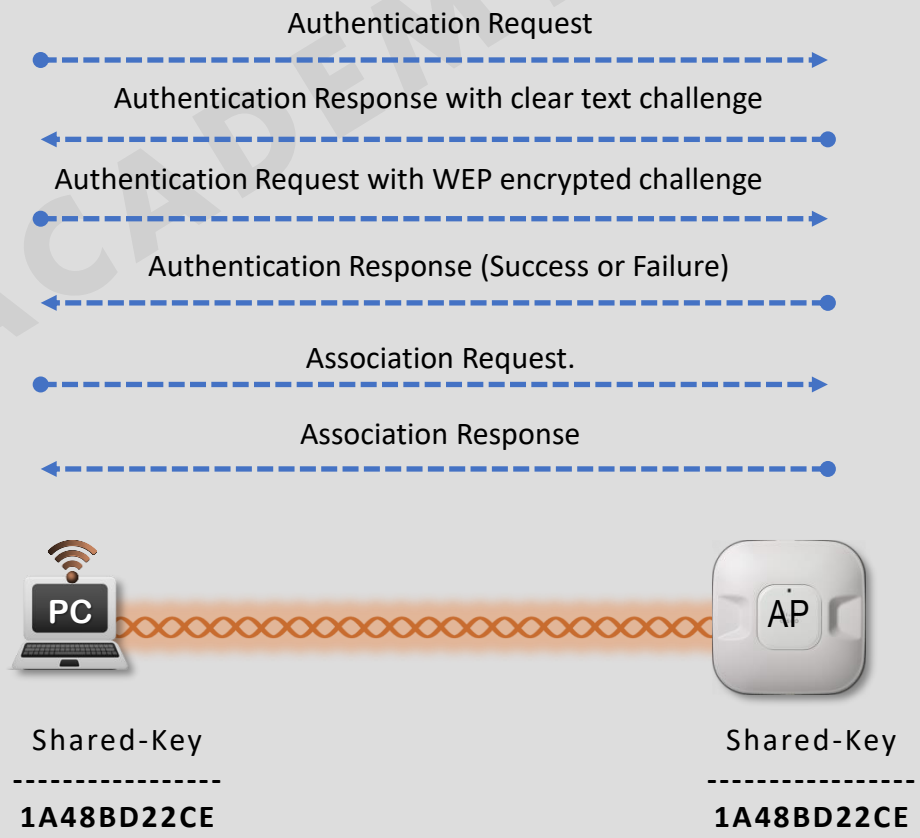
Wireless Client Authentication Methods

- Open Authentication.



Wired Equivalent Privacy (WEP) - deprecated

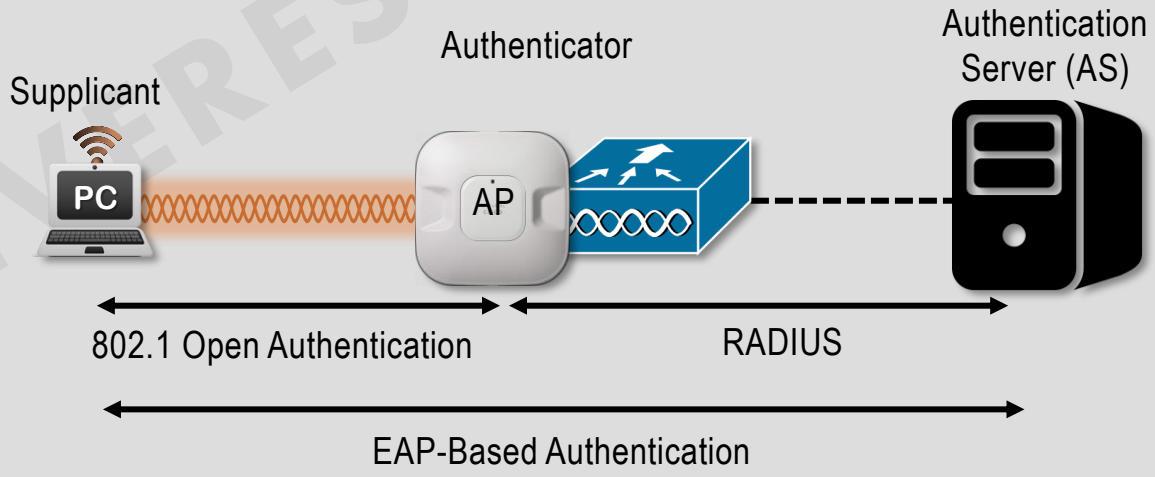
- Wired Equivalent Privacy (WEP) ---> shared-key security method.
- WEP uses the **RC4** cipher.
- WEP was defined in the original 802.11 standard in 1999,
- Every wireless adapter was built with encryption hardware specific to WEP.
- In 2001, a number of weaknesses were discovered and revealed, so work began to find better wireless security methods.
- By 2004, the 802.11i amendment was ratified and WEP was officially deprecated.



802.1X/EAP

- **Extensible Authentication Protocol (EAP).**
- **IEEE 802.1x port-based access control standard.**
- **802.1x Client Authentication Roles:**
  - **Supplicant.**
  - **Authenticator.**
  - **Authentication server (AS).**

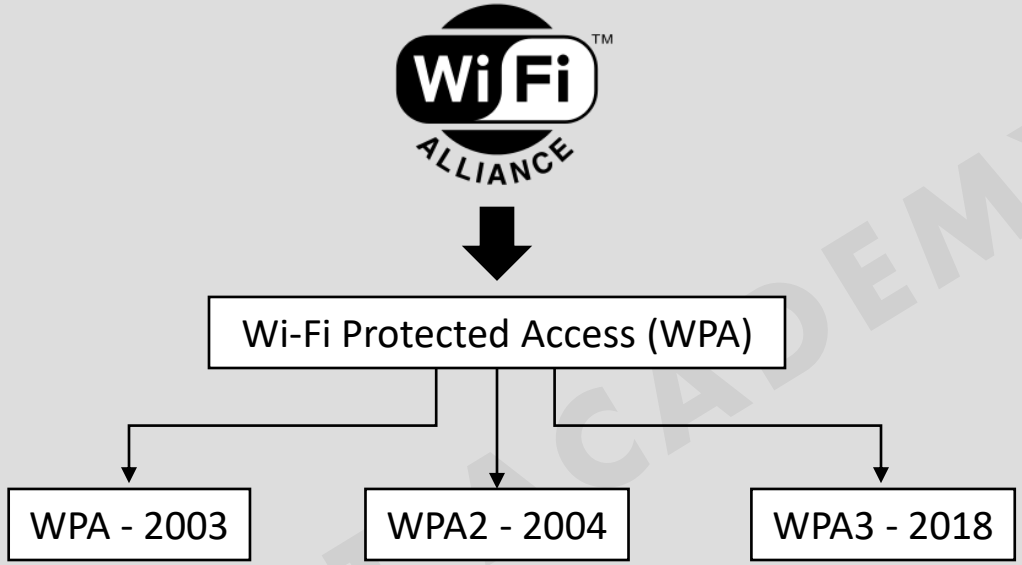
802.1x/EAP (Extensible Authentication Protocol)	
LEAP	Lightweight EAP
EAP-FAST	EAP Flexible Authentication by Secure Tunneling
PEAP	Protected EAP
EAP-TLS	EAP Transport Layer Security



Wireless Privacy and Integrity Methods

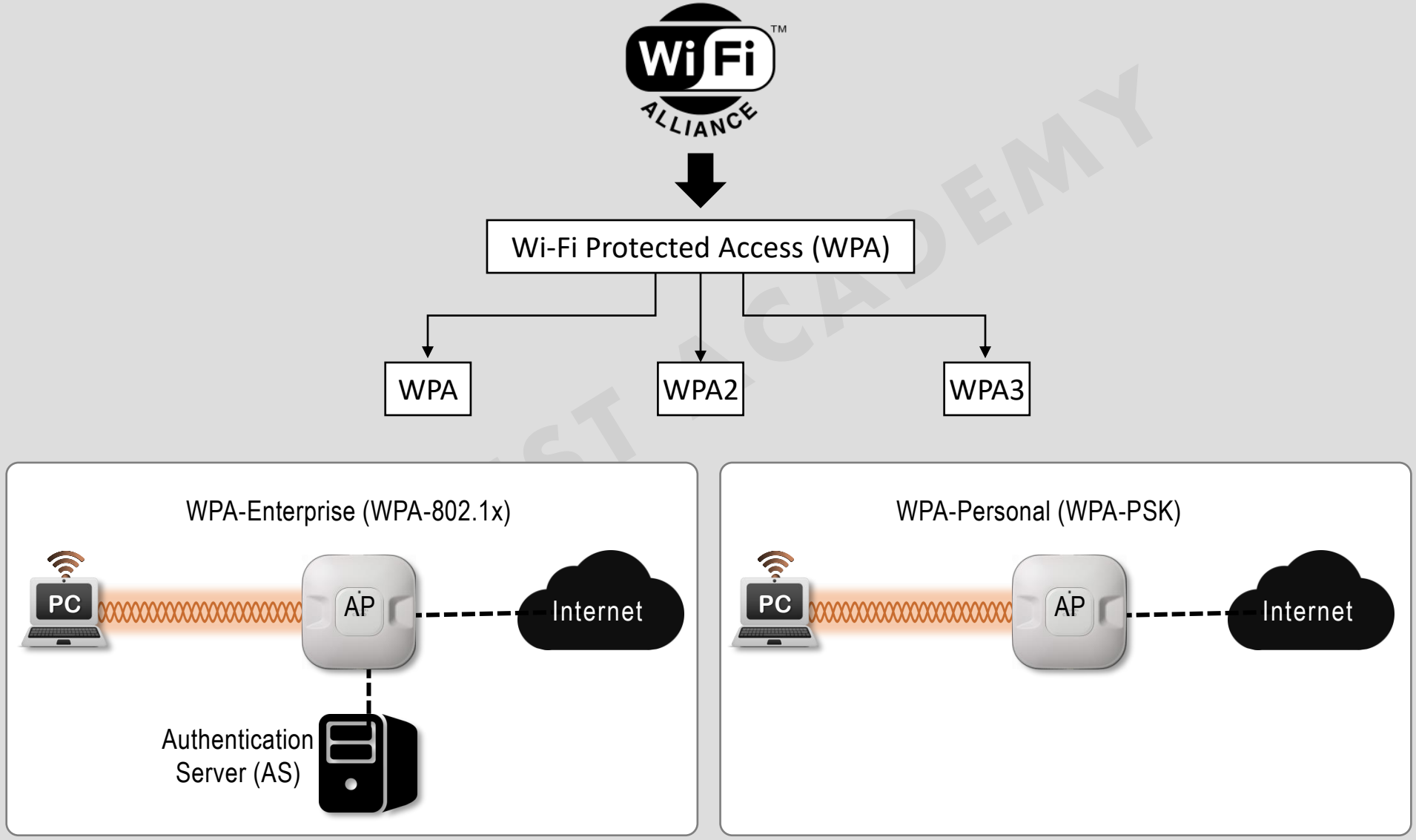
- Wired Equivalent Privacy (WEP).
  - RC4.
  - CRC-32 (Cyclic Redundancy Check).
- Temporal Key Integrity Protocol (**TKIP**).
  - RC4.
  - MIC (message integrity code).
- Counter Mode CBC-MAC Protocol (**CCMP**).
  - AES (Advanced Encryption Standard).
  - CBC-MAC (Cipher Block Chaining Message Authentication Code).
- Galois/Counter Mode Protocol (**GCMP**).
  - AES.
  - GMAC (Galois Message Authentication Code).

Wi-Fi Alliance (WPA, WPA2, and WPA3)



- WPA was based on parts of **802.11i** and implements **802.1x** authentication and **TKIP**.
- WPA2 implements **802.11i** and **AES** with **CCMP**, rather than the deprecated TKIP from WPA.
- WPA3 implements **AES** with **GCMP** and uses Protected Management Frames (**PMF**) to secure important 802.11 **management frames** between APs and clients and implements Simultaneous Authentication of Equals (SAE) for authentication.

Wi-Fi Alliance (WPA, WPA2, and WPA3)



Wi-Fi Alliance (WPA, WPA2, and WPA3)

WPA-Personal (WPA-PSK) Mode			
	WPA	WPA2	WPA3
Authentication	PSK	PSK	SAE
Encryption	TKIP/MIC	AES-CCMP	AES-CCMP

WPA-Enterprise (WPA-802.1x) Mode			
	WPA	WPA2	WPA3
Authentication	IEEE 802.1x/EAP	IEEE 802.1x/EAP	IEEE 802.1x/EAP
Encryption	TKIP/MIC	AES-CCMP	AES-GMAC