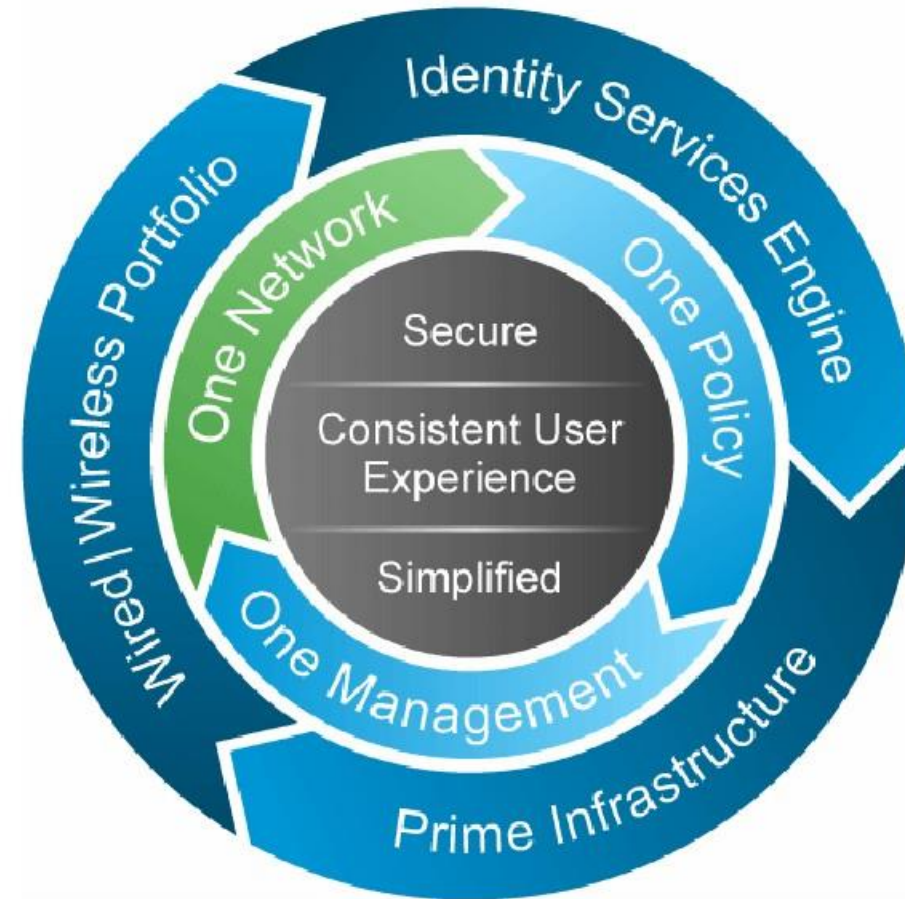


# 经典思科网络技术AireOS简介和基本操作内容

- 思科无线部署基本概念
  - 思科融合无线一体化解决方案
  - AireOS基本概念介绍
  - 控制器端口，接口和映射关系
- 思科无线部署操作实现
  - 基本配置流程图
  - 初始化WLC
  - AP初始化
  - WLC特性配置
  - 客户访问
  - 漫游特性

# Cisco Unified Access Architecture

- One Network
  - One infrastructure for wired and wireless
- One Policy
  - One place to define policy
- One Management
  - One pane of glass



# One Network Overview

## One Network (5 deployment options)

- Cloud managed UA portfolio—Meraki AP, switches, security appliances
- Premise managed UA portfolio
  - Autonomous – IOS
  - Converged—IOS-XE
  - Centralized
    - AireOS (Cisco Unified Wireless Network)
    - IOS-XE (using 5760)
  - Flex Connect – AireOS (CUWN)

# Wireless Controllers as a Function

The WLAN Controller has become a function, just like routing, and can be hosted by any network component



Router



Switch



Cloud



Virtual



Appliance



Access Point



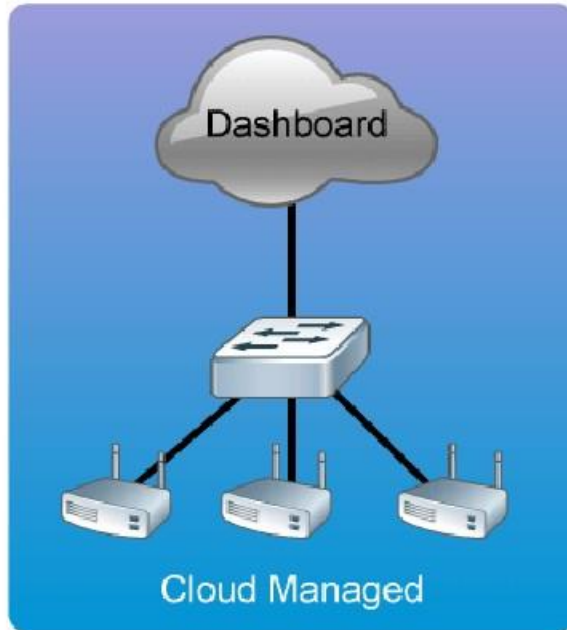
## Basic WLC Function

- AP configuration management
- AP image management
- Holistic RF management

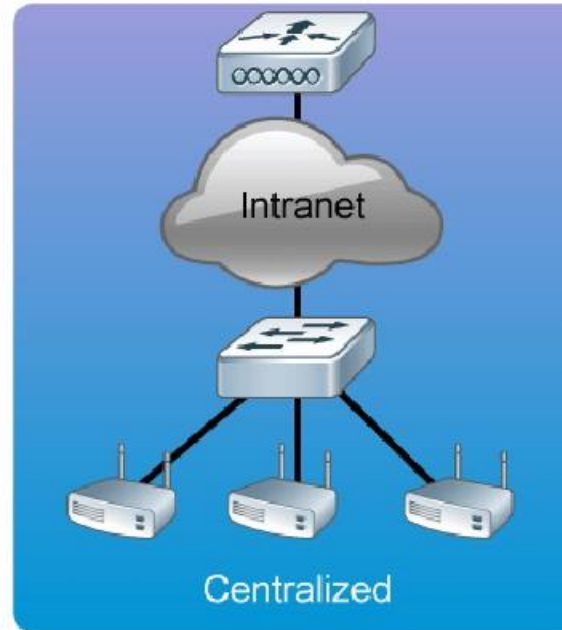
## Advanced WLC Function

- AVC
- SSO
- Profiling
- Policy

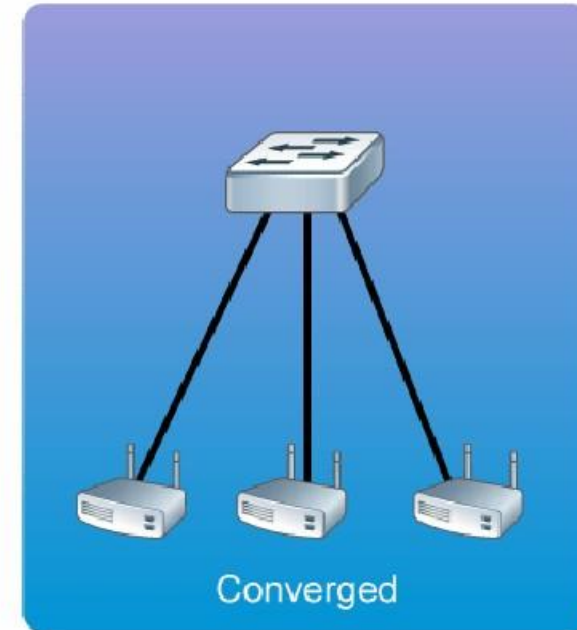
## Wireless Controllers as a Function (Cont.)



Controller:  
Dashboard



Controllers:  
8510/5760/5508/  
WiSM2/2504/  
vWLC



Controllers:  
Integrated 3850/3650  
WLC 5760

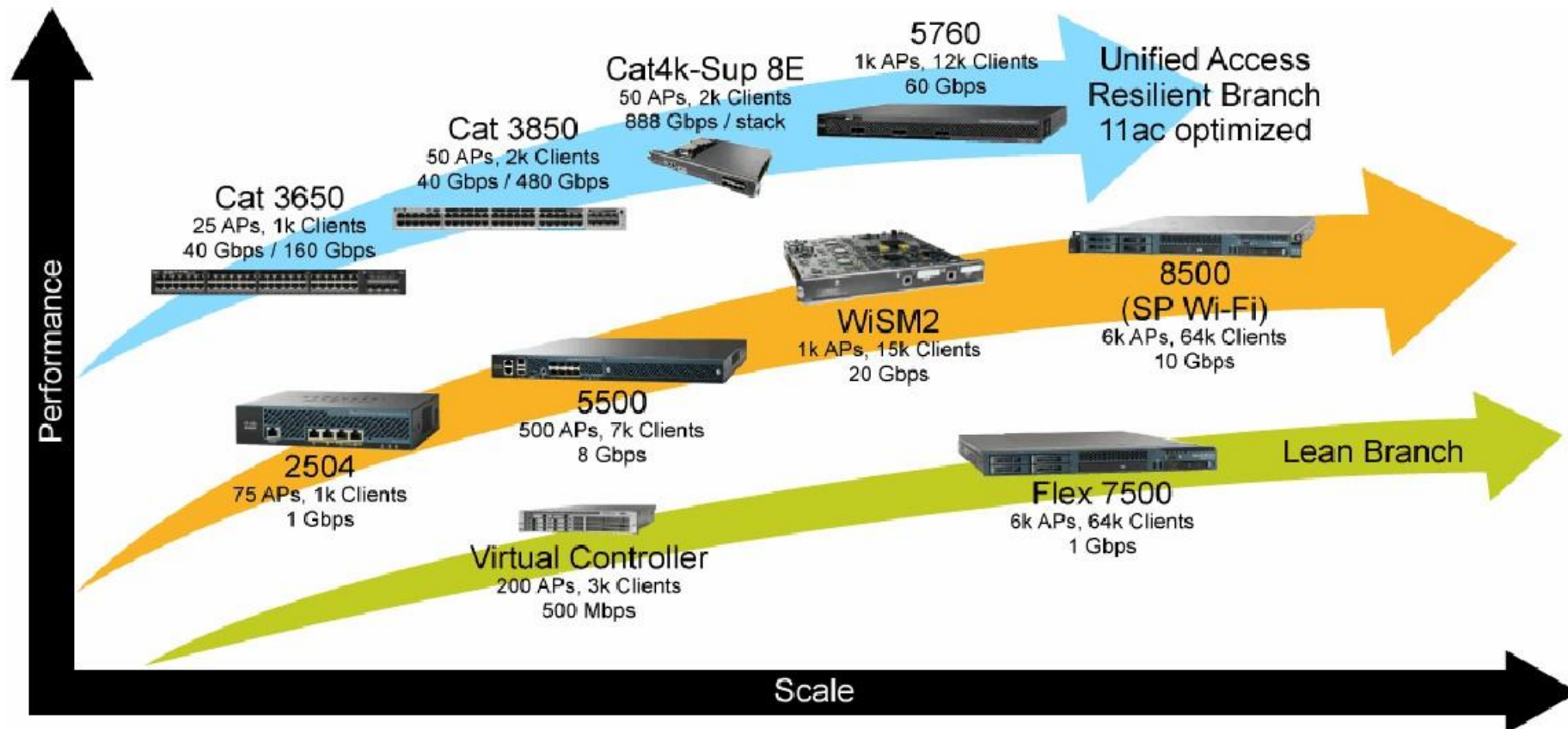
# AireOS Controllers

- Support the following deployment modes:
  - FlexConnect
  - Centralized
  - Mesh
  - OfficeExtend
- Support most wireless features and functions the product line
- GUI and CLI interfaces
- Some controllers (Flex 7500 and vWLC) do not support all deployment modes or features



# Appliance Based Wireless Controllers Products

## Wireless Controllers Product Portfolio



# 入门级别无线控制器

## 2500 Series – AireOS Controller

- Support up to 75 access points and 1000 clients
- 1 Gbps throughput, four 1 Gigabit Ethernet ports (two support PoE)
- Standalone, small form-factor appliance



## Cisco 3504 Wireless Controller

- Get ready for the 802.11ac Wave 2 world.
- Supports 150 APs, 3000 clients
- Redundant 1 Gigabit Ethernet, Cisco Multigigabit Ethernet, or 10 GE connectivity
- 4 Gbps throughput





# 旗舰级别无线控制器

## 5500 Series—AireOS Controller

- Support for up to 500 access points and 7000 clients
- 8-Gbps throughput, eight 1 Gigabit Ethernet ports, with LAG support
- Standalone, rack-mountable appliance



## Cisco 5520 Wireless Controller

- Support up to 1500 access points and 20,000 clients
- Optimize 802.11ac Wave 2 next-generation networks with 20 Gb throughput



# 大型机构远程站点部署

## Flex 7500 Series—AireOS Controller

- Deployment extends wireless services to distributed branches
  - Supports up to 6000 branch offices
  - Supports up to 100 access points per branch
- 6000 access points and 64,000 clients
- Designed specifically for wireless branches with local survivability features



## Cisco 8540 Wireless Controller

- Optimize 802.11ac Wave 2 next-generation networks with 40 Gb throughput
- Support up to 6000 access points and 64,000 clients
- Support centralized, distributed, and mesh deployments



## WiSM2 (Catalyst 6500 Module)—AireOS Controller

- Designed for mid-sized and large single-site enterprises
- Support for up to 1000 access points and 15,000 clients
- 20-Gbps throughput
- Integrated switch blade for Cisco Catalyst 6500 Series chassis
- Supports up to seven Cisco WiSM2 blades per chassis for added scalability



# Virtual Wireless LAN Controller (vWLC)



Unified Computing System



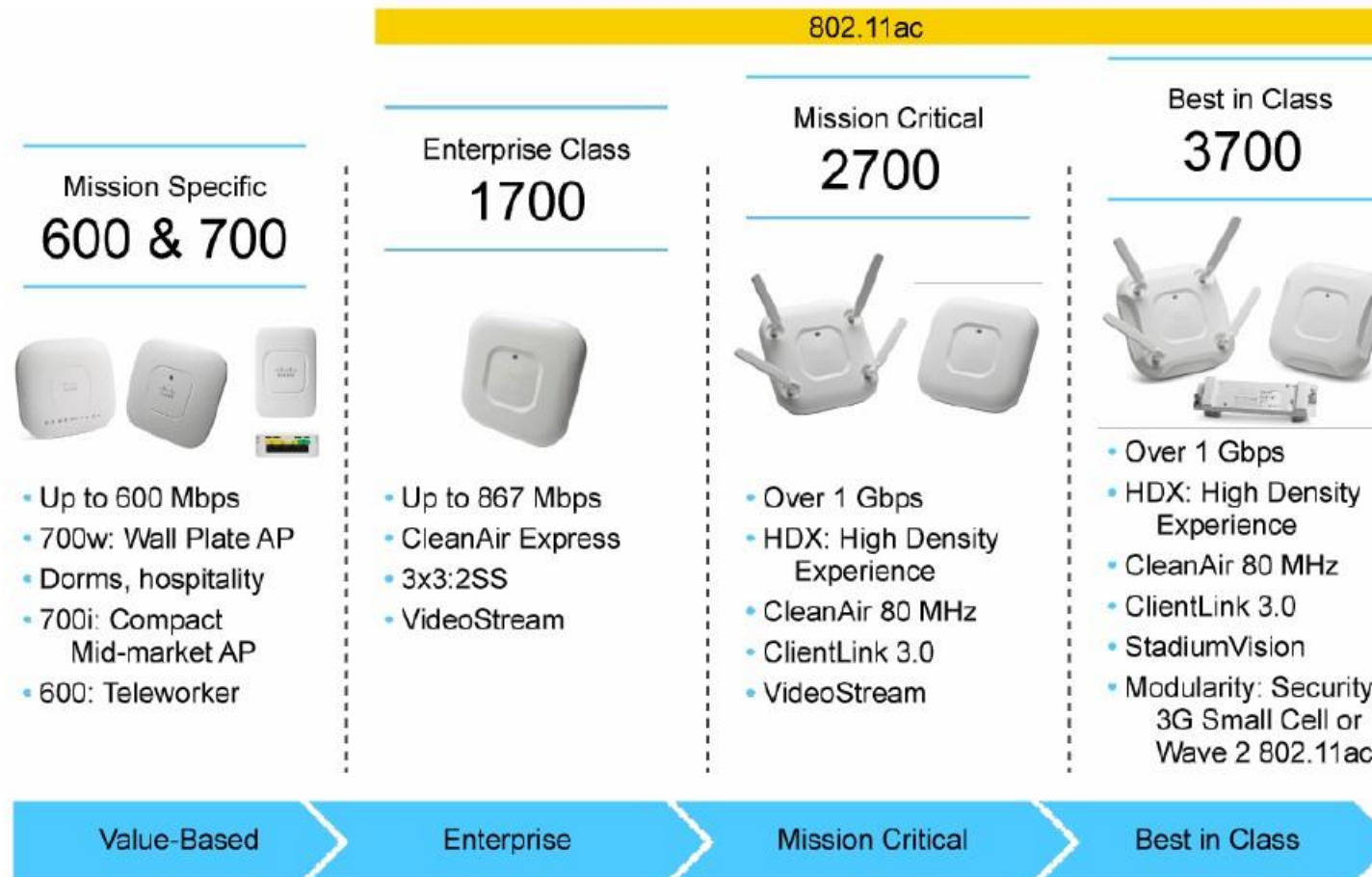
UCS- E-Series for ISR-G2



SRE for ISR-G2

# Cisco Aironet Access Points

## Cisco Aironet Indoor Access Points

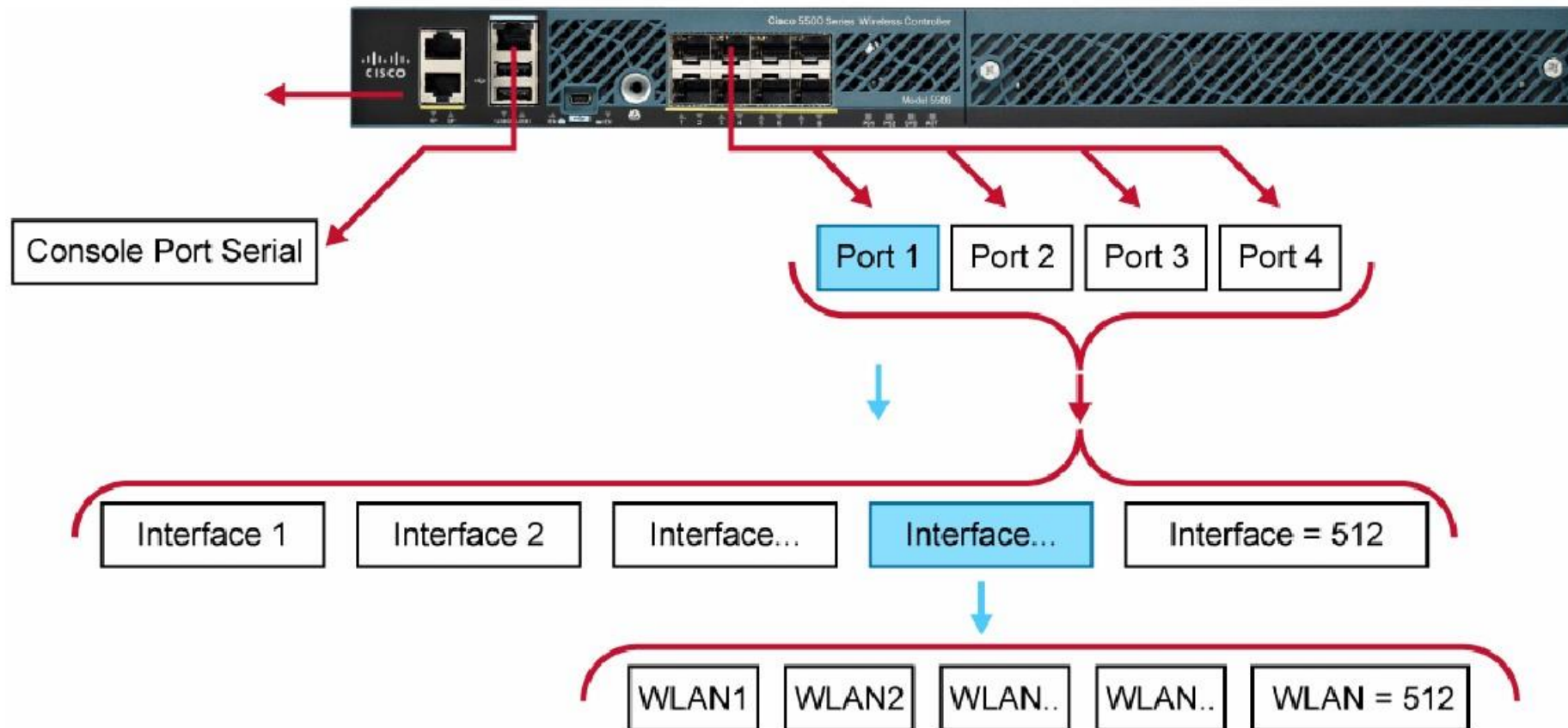




控制器端口，接口和映射关系

# Controller Ports, Interfaces, and Mapping

## WLC Terminology



物理端口

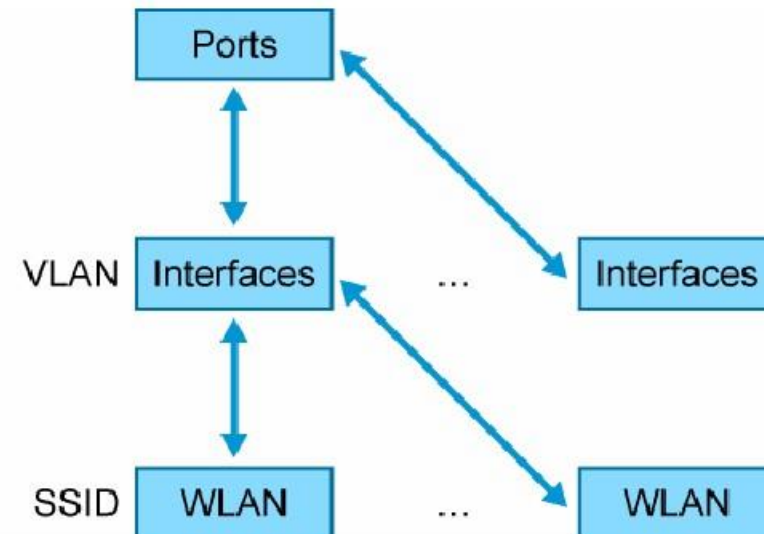
## Ports

Cisco wireless controllers use ports for the following features:

- Controlling of associated Cisco wireless APs
- Distribution system to enterprise network
  - Can assign multiple interfaces to a port
  - Data must be tagged to support multiple VLANs on the same trunk

The BSSID in the encapsulated frame header identifies the WLAN and the AP.

This is translated into VLAN tags on the distribution port.



## Interfaces

### Interfaces

- Cisco wireless interface configuration allows the association of a VLAN name to a VLAN ID, which is then mapped to a physical port and WLAN
  - Must assign each interface to a port for distribution into the enterprise
  - Cannot assign multiple ports to an interface
  - Can assign multiple WLANs to an interface
- The VLAN ID will represent either untagged traffic (value 0) or IEEE 802.1Q tagged traffic (value 1-4095).
  - Can assign multiple interfaces to a port
- Various interfaces include the following:
  - Static – Management (default AP Mgr.), Service port, Virtual
  - Dynamic – User defined

## Management Interface

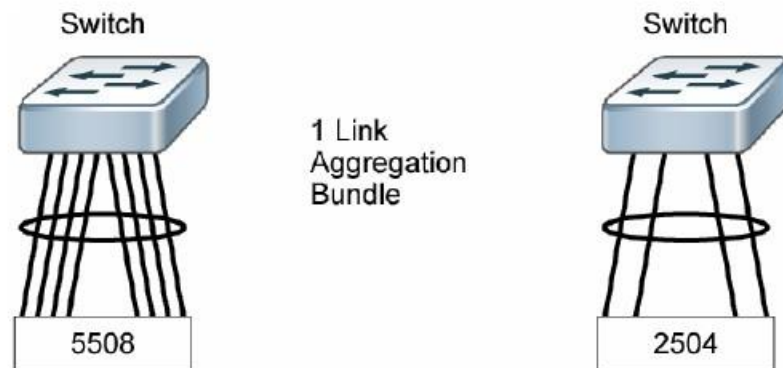
Cisco wireless uses the management interface as:

- Default interface for in-band management of the Cisco wireless controller
- Connectivity to enterprise services such as AAA
- Communications between the controller and access points

## 链路聚合 Link Aggregation

Link Aggregation—Simplifies redundancy setup on the controller because you do not need to configure primary and secondary ports for each interface.

- If any of the controller ports fail, traffic automatically migrates to one of the other ports
- As long as at least one controller port is functioning, the system continues to operate, access points remain connected to the network, and wireless clients continue to send packets.





服务接口

## Service Interface

Associated only with the physical service port on the Cisco wireless controller front panel 10/100/1000 BASE-T Ethernet port dedicated to out-of-band management.

- The service port is not autosensing.

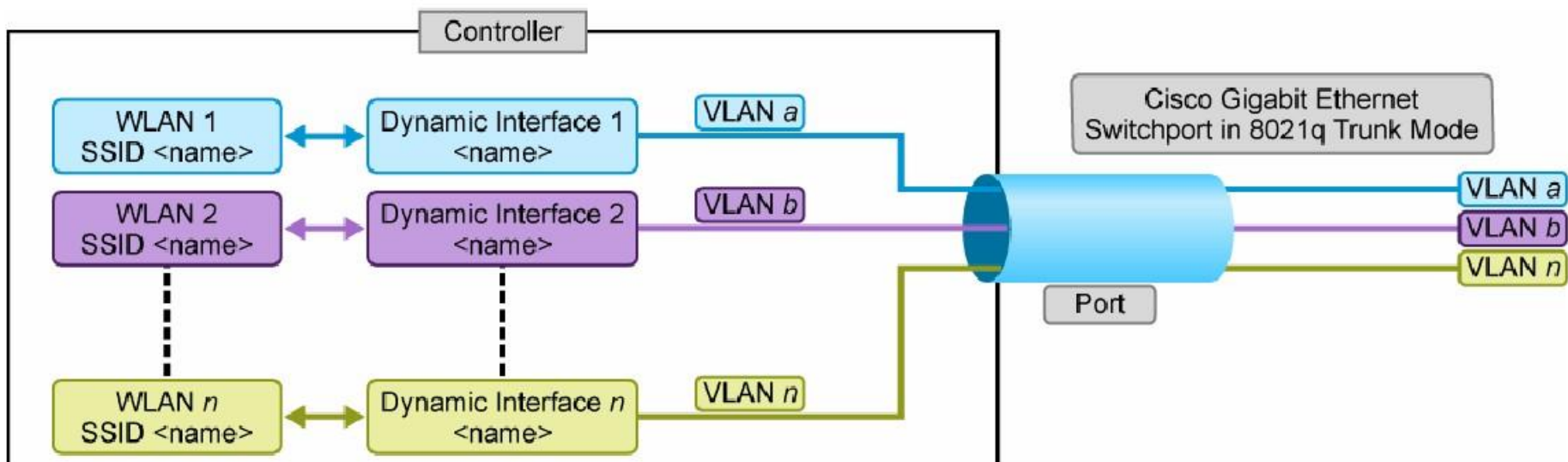
## Virtual Interface

Virtual interface is used when supporting the following features:

- Mobility management
  - Mobile client uses the same virtual IP address across multiple controllers
- DHCP relay
  - Client uses the virtual IP address as DHCP server address
- Layer 3 security
  - Web authentication uses the virtual interface as the gateway IP address

## Dynamic Interface

- Dynamic interfaces are also called VLAN interfaces
- These interfaces are manually configured by the administrator
- Can act as a DHCP relay for wireless clients
- Multiple WLANs SSIDs can map to a single Dynamic Interface

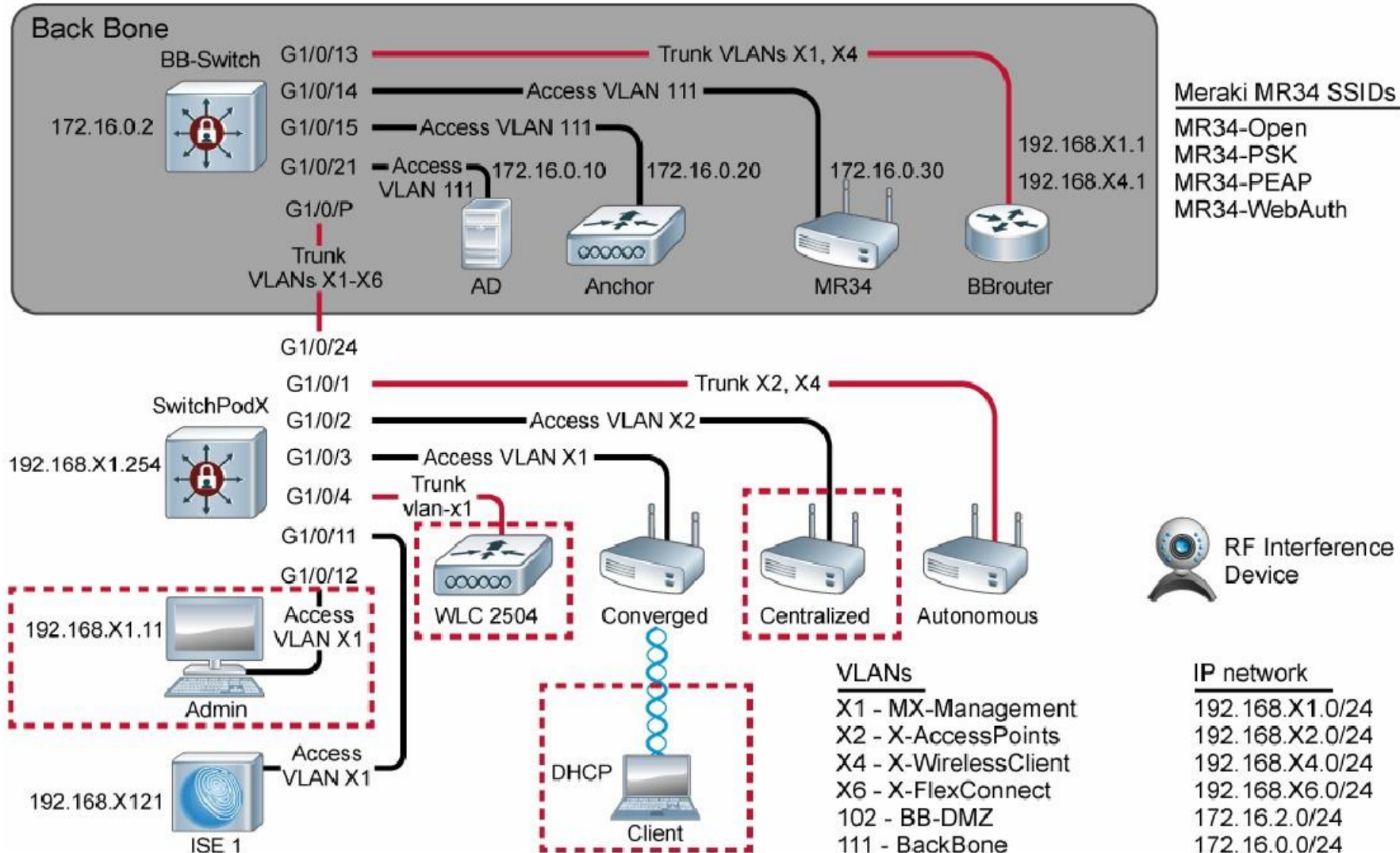


## Prime Infrastructure 2.2 and the WLC

- WLCs can be configured and monitored from Prime Infrastructure
- AireOS 8.x WLCs can only be managed by PI 2.2 or higher
- Prime Infrastructure can use WLC templates to add or modify WLCs
- Prime Infrastructure gives comprehensive management and monitoring of the following:
  - WLCs
  - APs
  - Client Devices

# Initialize a Centralized WLAN Deployment

WFUND Lab Topology





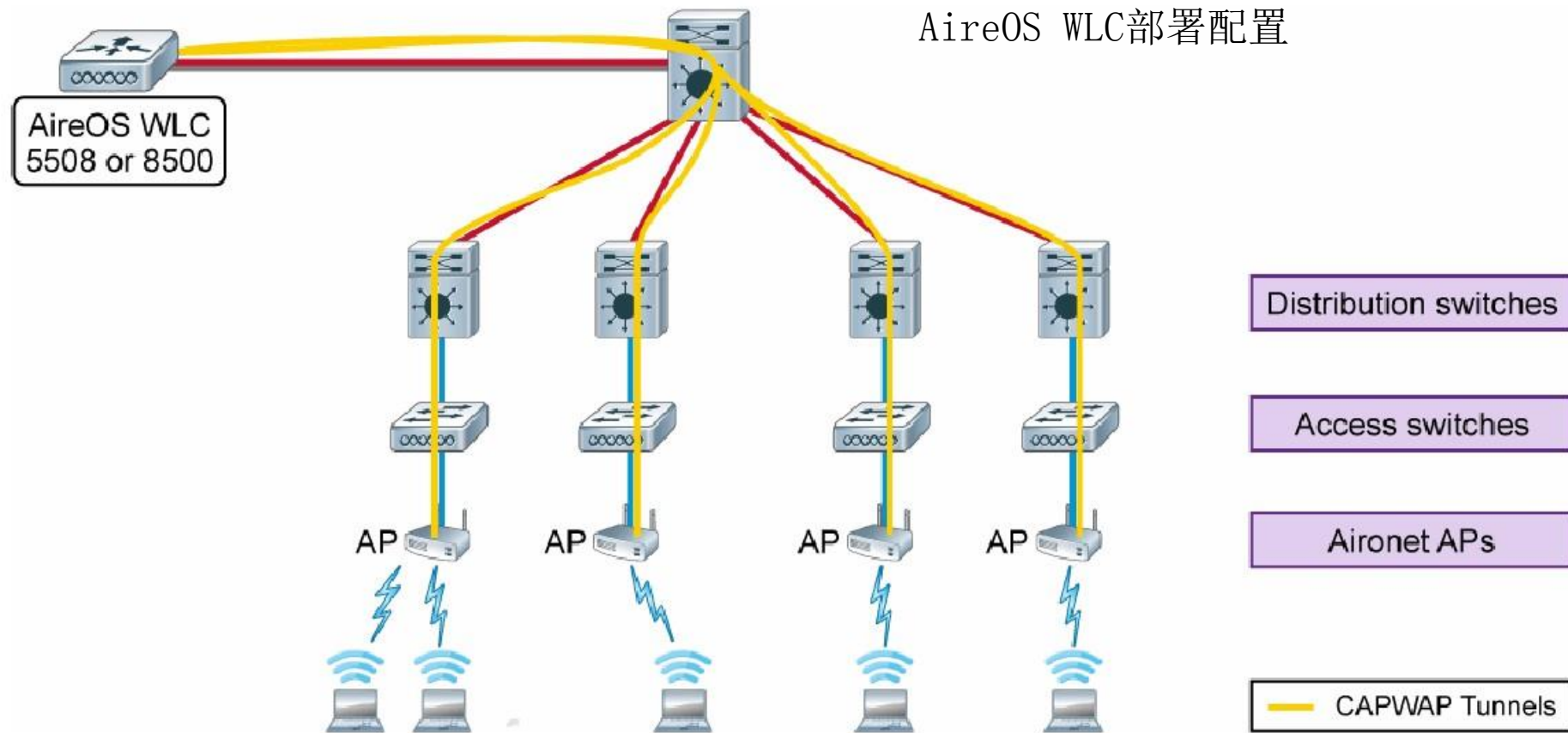


初始化集中的WLC

# Initialize a Centralized WLC

Implement Centralized Wireless Access

# Centralized WLC Deployment and Configuration— Centralized with AireOS WLC



WLC命令行接口

## WLC Command Line Interface

Available from:

- Telnet
- SSH
- Console Port
  - RJ-45 port on all current models
  - WLC 5500 series has USB option
  - Default port configuration
    - 9600 baud, 8 data bits, 1 stop bit, no parity, no hardware flow control

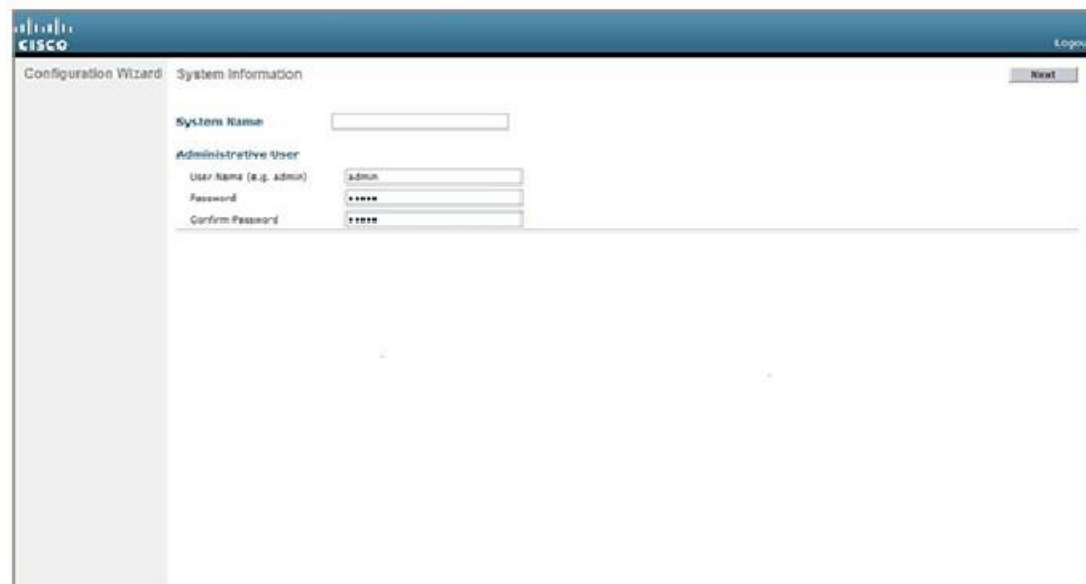
## WLC AireOS CLI Setup Wizard

- Connect PC to serial console port using VT-100 emulation (Set parameters to 9600 baud, 8 bits, 1 stop bit, no parity, and no hardware flow control)
- Power on the WLC and start the configuration wizard

## WLC AireOS GUI Setup Wizard

### WLC 5500

- Connect PC to Service Port
- Open compatible web browser and connect to http://192.168.1.1
- Configuration Wizard starts



The screenshot shows the Cisco Configuration Wizard interface for System Information. The page includes a header with the Cisco logo and a 'Logout' link. The main content area is titled 'System Information' and contains the following fields:

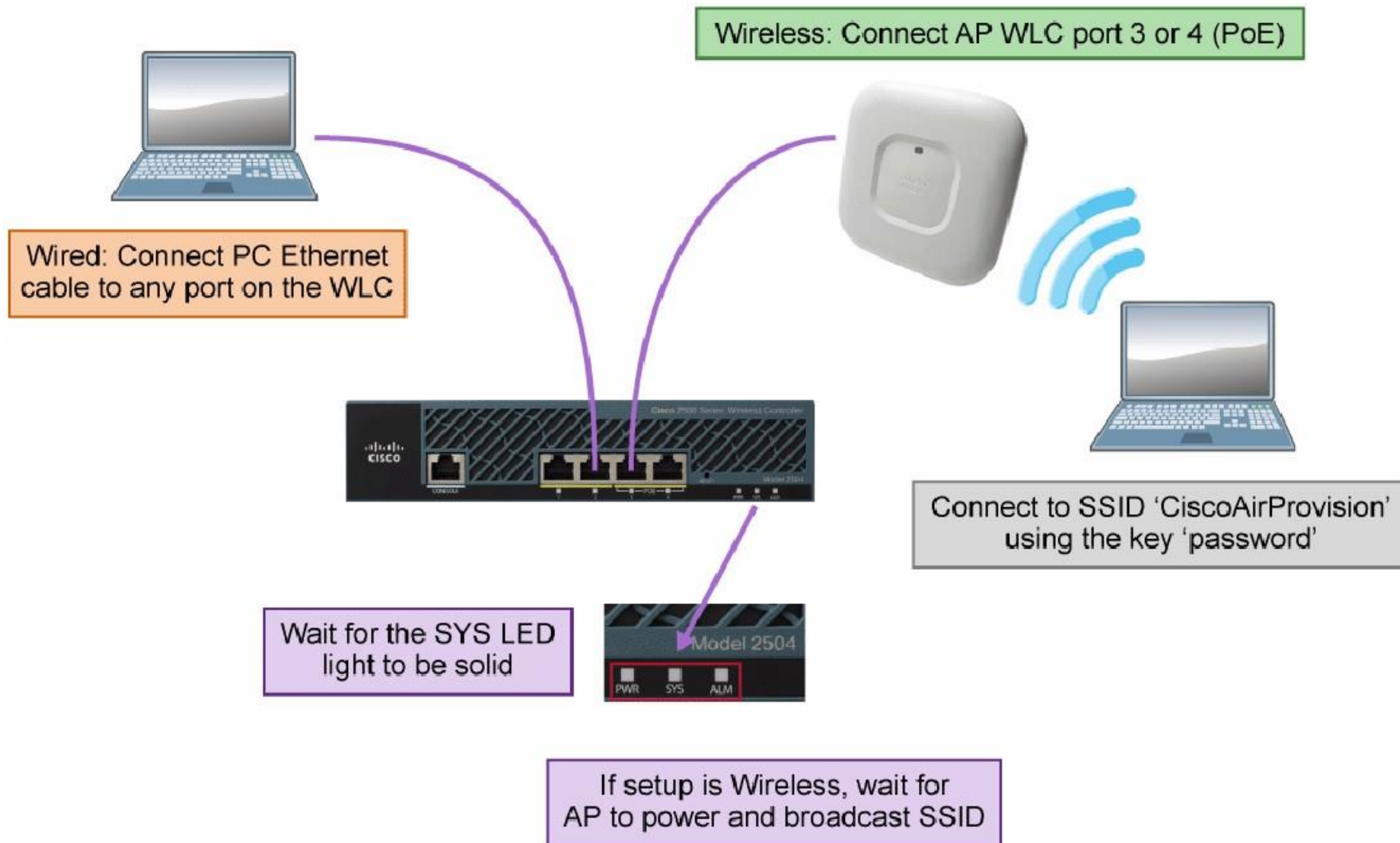
- System Name:** An empty text input field.
- Administrative User:** A section containing three fields:
  - User Name (e.g. admin):** A text input field with 'admin' entered.
  - Password:** A password input field with masked characters (dots).
  - Confirm Password:** A password input field with masked characters (dots).

A 'Next' button is located in the top right corner of the form area.



精简设置

# WLAN Express Setup (WES)



Example: WLC 2504

# WLAN Express Setup (WES) (Cont.)



## WLAN Express Setup (WES) (Cont.)

### WES Default Parameter Changes:

- Session Timeout disabled
- Aironet IE not checked
- Profiling is enabled
- Guest ACL applied to Guest SSID
- CleanAir and EDRRM are enabled
- 5 GHz channel bonding is enabled (40 MHz)
- AVC is enabled
- Wireless Management and Web Access (HTTP/HTTPS)
- Virtual IP Address is 192.0.2.1
- RF Group name is “default”

登录界面

## WLC Landing Page Option

Login Screen—HTTP or HTTPS



# WLC Landing Page Option (Cont.)

## Default landing page—Dashboard

Switch from Table to Pie Chart

Elements are clickable links to interface or item

The dashboard displays the following metrics and tables:

- Wireless Networks:** 2
- Access Points:** 2
- Active Client Devices:** 2 2.4GHz, 1 5GHz
- Rogues:** 64 APs, 1 Clients
- Interferers:** 2 2.4GHz, 0 5GHz

**Top Access Points**

Description	Volume	Clients
1 AP-3702-mDNS	45.58 KB	1
2 AP702	7.33 KB	1

**Top Applications**

Description	Volume	% Usage
1 itunes	37.40 MB	96.3%
2 ssl	1.32 MB	3.4%
3 facebook	43.07 KB	0.1%
4 dns	42.27 KB	0.1%
5 http	41.71 KB	0.1%
6 netbios-ns	3.05 KB	0.0%
7 netbios	923.00 B	0.0%
8 icmp	418.00 B	0.0%
9 isatap-ipv6-tunneled	240.00 B	0.0%

**Top Operating Systems**

Description	Clients	% Clients
1 Apple-Device	1	33.3%
2 Apple-iPad	1	33.3%
3 Microsoft-Workstation	1	33.3%

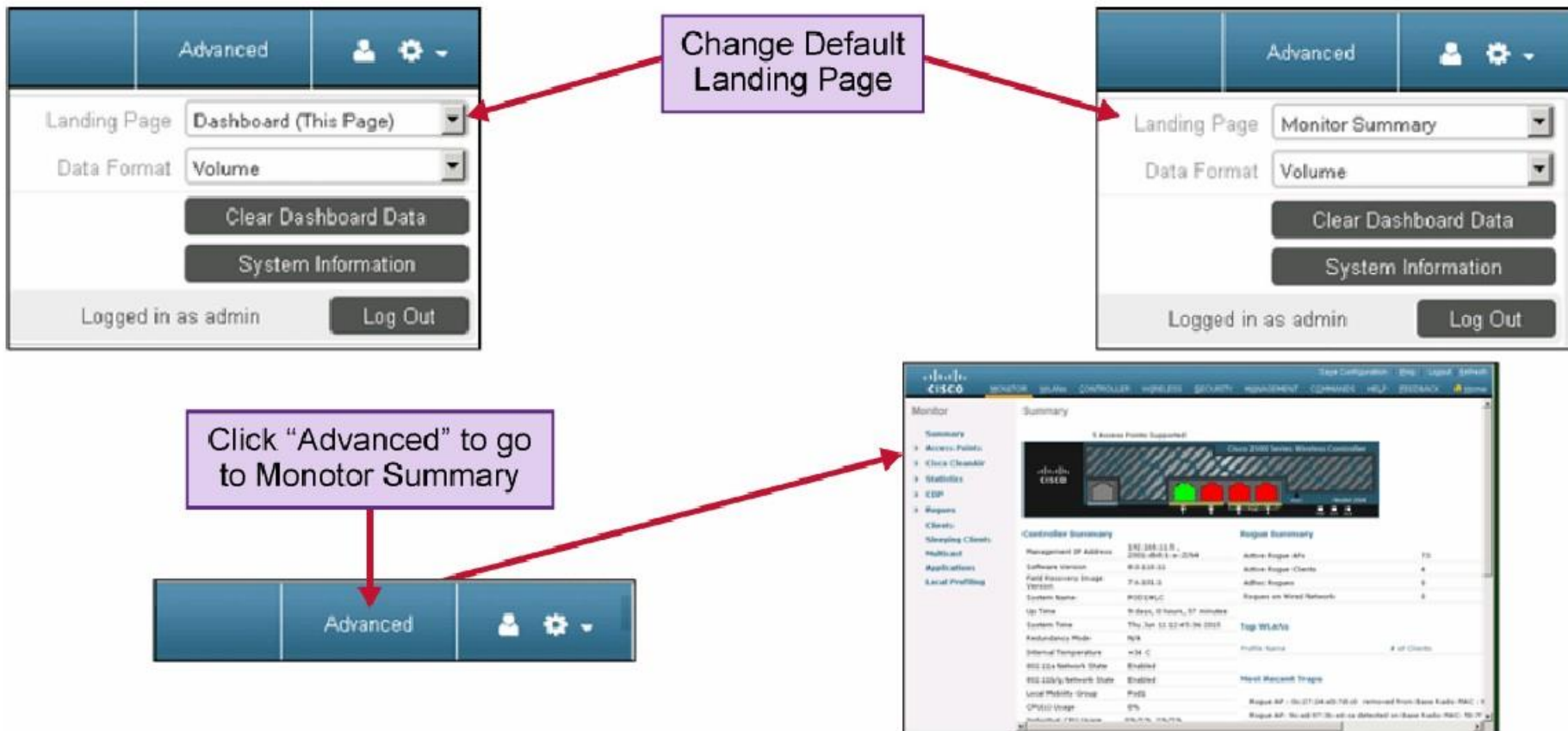
**Top Client Devices**

Description	Volume	% Usage
1 00:1e:e5:e2:38:0f - Microsoft-Workstation	45.58 KB	86.1%
2 d8:96:95:0e:5d:3c - Apple-Device	7.33 KB	13.9%

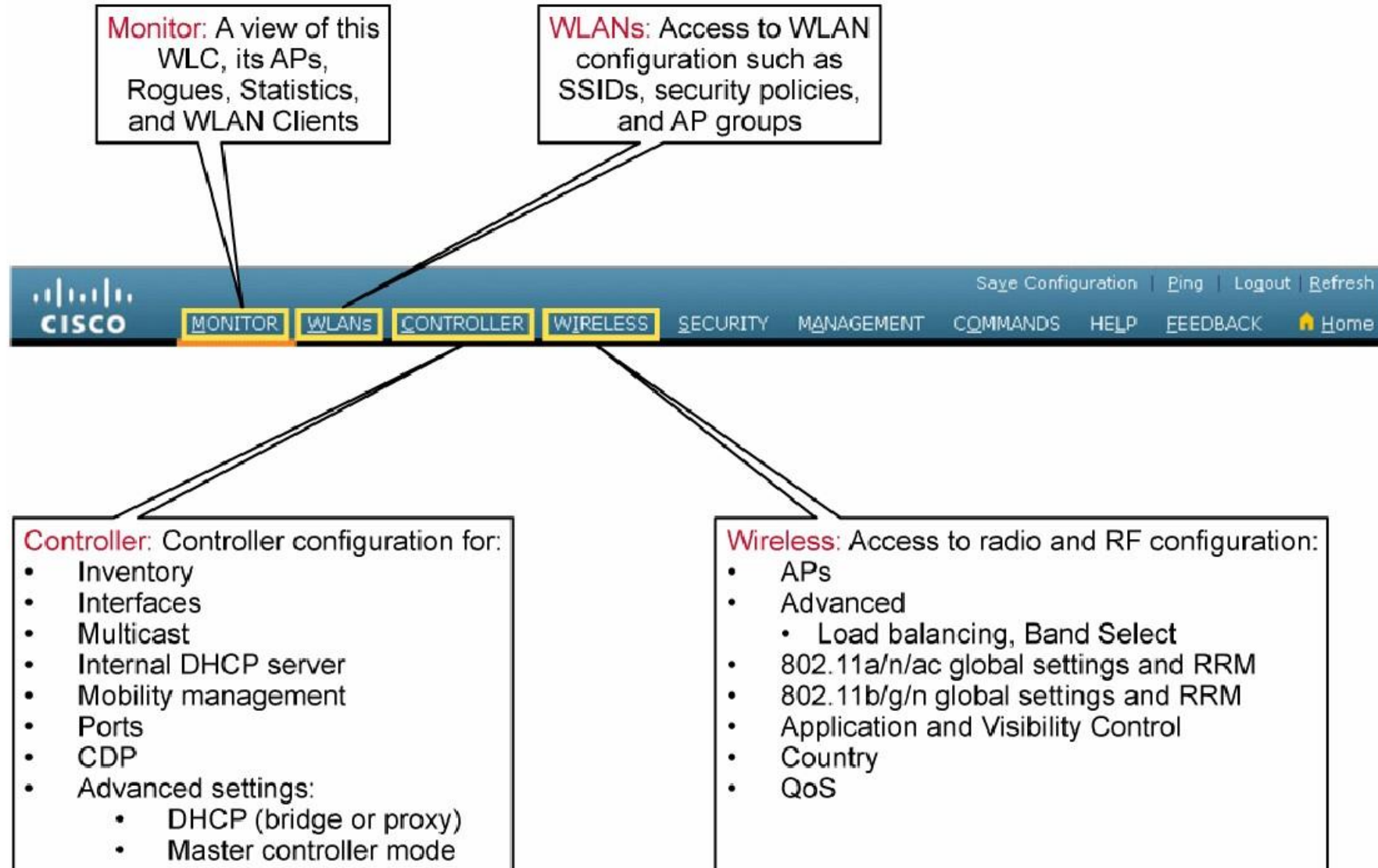


# WLC Landing Page Option (Cont.)

## Monitor Summary Screen option



## WLC Advanced Menu Tabs



# WLC Advanced Menu Tabs (Cont.)

**Security:** Security configuration for RADIUS or TACACS+ connectivity, local net users, local EAP configuration, ACL configuration, and other policies designed to protect the RF environment (certificates, ACLs, etc.)

**Commands:** Provides access to administrative options such as file uploads and downloads, configuration reset, controller reboots, manual time configuration, and login banner download.



**Management:** Provides access to controller settings such as SNMP configuration, serial port control, Telnet and SSH support, creation of local management user accounts, access to message logs and their configuration, and system technical information such as system resource information and crash files.

**Feedback:** Provides direct access to Cisco to provide detailed feedback and suggestions for improving the product ease of use for the controllers.

# WLC Advanced Menu Tabs (Cont.)

The screenshot displays the Cisco WLC Advanced menu tabs interface. The top navigation bar includes the Cisco logo and tabs for MONITOR, WLANs (selected), CONTROLLER, WIRELESS, SECURITY, MANAGEMENT, COMMANDS, HELP, and FEEDBACK. The left sidebar shows the WLANs menu with sub-items for WLANs and Advanced. The main content area shows a table of WLANs with columns for WLAN ID, Type, Profile Name, WLAN SSID, Admin Status, and Security Policies. A 'Create New' dropdown and 'Go' button are visible above the table. The table contains four entries, with the 'Remove' button for the last entry circled in red. A context menu is open over the 'Remove' button, showing options: Remove, Mobility Anchors, 802.11u, Foreign Maps, Service Advertisements, and Hotspot 2.0. The text 'Entries 1 - 4 of 4' is displayed below the table.

<input type="checkbox"/>	WLAN ID	Type	Profile Name	WLAN SSID	Admin Status	Security Policies	
<input type="checkbox"/>	1	WLAN	CCNA-WIRELESS-SPONSOR	ccnawireless-sponsor	Disabled	MAC Filtering	▼
<input type="checkbox"/>	2	WLAN	CCNA-WIRELESS-SELF	ccnawireless-self	Disabled	MAC Filtering	▼
<input type="checkbox"/>	3	WLAN	CCNA-WIRELESS-HOTSPOT	ccnawireless-hotspot	Disabled	MAC Filtering	▼
<input type="checkbox"/>	4	WLAN	Guest Access	guest	Disabled	Web-Auth	▼

Entries 1 - 4 of 4

Admin Status Security Policies

- Disabled MAC Filtering
- Disabled MAC Filtering
- Disabled MAC Filtering
- Disabled Web-Auth

Remove  
Mobility Anchors  
802.11u  
Foreign Maps  
Service Advertisements  
Hotspot 2.0



描述AP初始化

## Describe AP Initialization

Implement Centralized Wireless Access



AP发现过程

## Access Point Discovery Process

### AP CAPWAP Discovery—Overview

- AP issues a DHCP discover to obtain address
- AP attempts Layer 3 WLC discovery
  - CAPWAP discovery broadcast on local subnet
  - Local stored controller IP address from prior successful join process
  - DHCP option 43
  - DNS resolution of CISCO-CAPWAP-CONTROLLER

AP发现

## AP CAPWAP Discovery

AP obtains an IP address:

- Statically defined
- DHCP discover

Layer 3 WLC discovery order:

- Subnetwork broadcast mode
  - Connect Cisco AP directly to, or same subnet as, a Cisco WLC to learn Cisco controller IP address
  - Cisco AP will send a subnetwork broadcast
- Locally Stored
  - APs will also send a subnetwork broadcast to the IP addresses of previously associated controllers because it stores this information even after a reboot

## AP CAPWAP Discovery (Cont.)

DHCP vendor option mode:

- Place Cisco AP on remote network and have it use DHCP for a local and gateway address
- Use DHCP extension to learn a Cisco WLC management interface IP address from extension Option 43

DNS mode:

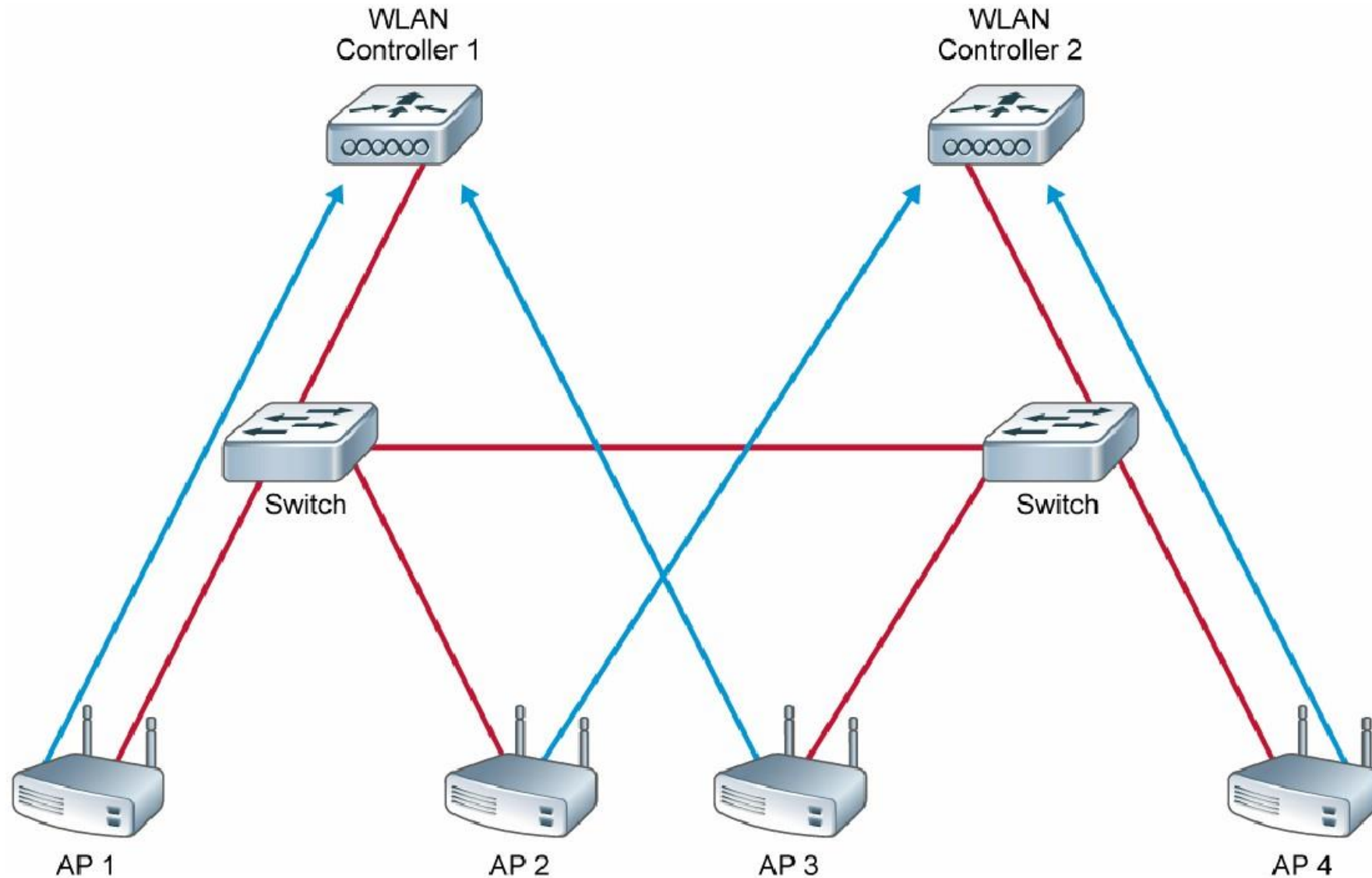
- Place Cisco AP on remote network and have it use DHCP for a local and gateway address
- Use DHCP extension to learn a DNS IP address
- Cisco AP will then make an address resolution call using the hostname CISCO-CAPWAP-CONTROLLER, which should be configured to return the management interface IP address of available controllers

## Access Point Join Order

- Response from primary, then secondary, and finally tertiary configured controller
- If no configured WLC, response from a master controller
- If no master controller response, response from the least loaded WLC
- Least loaded WLC

AP加入步驟

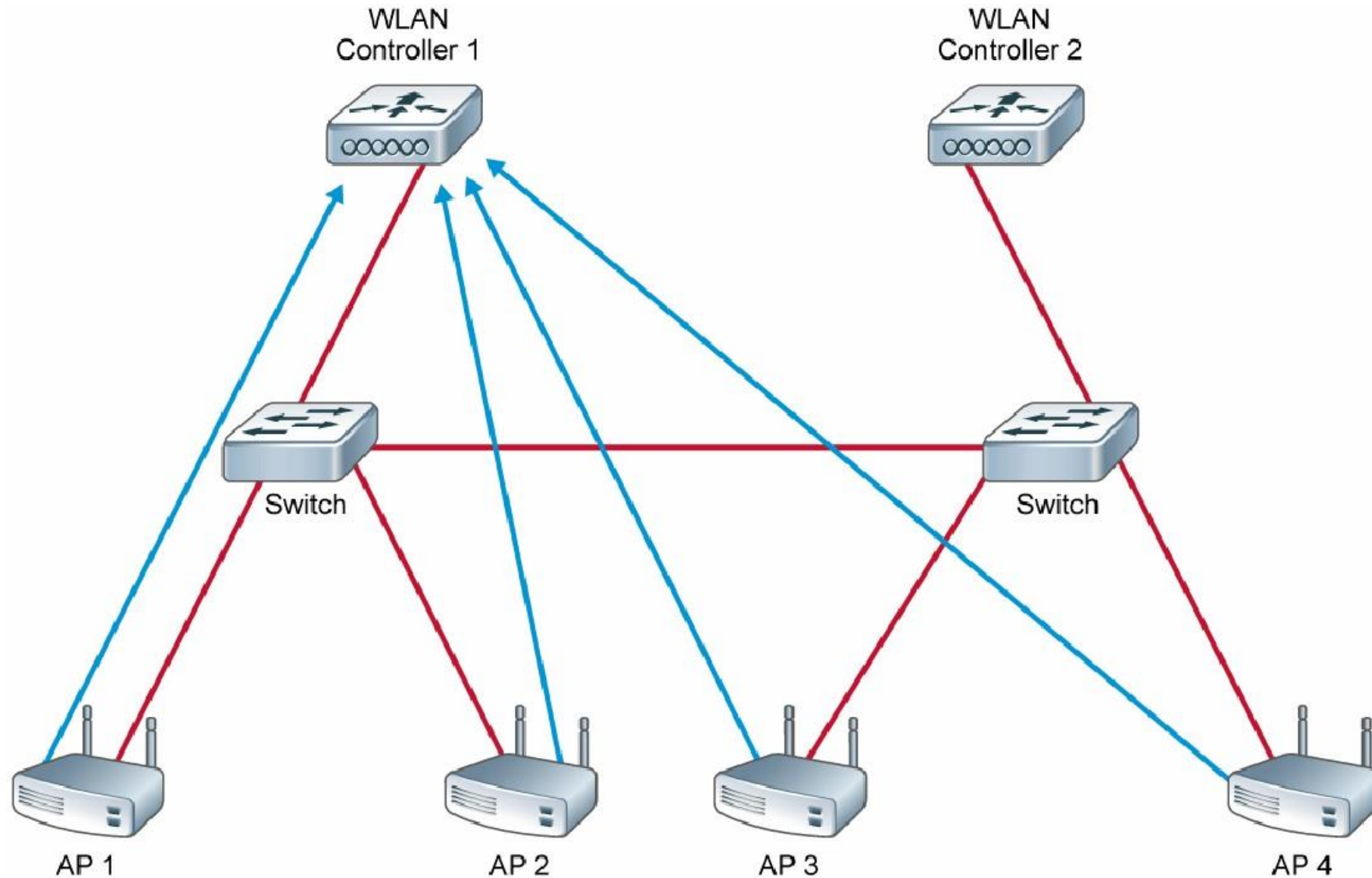
## AP Join Phase Without Master





Master!

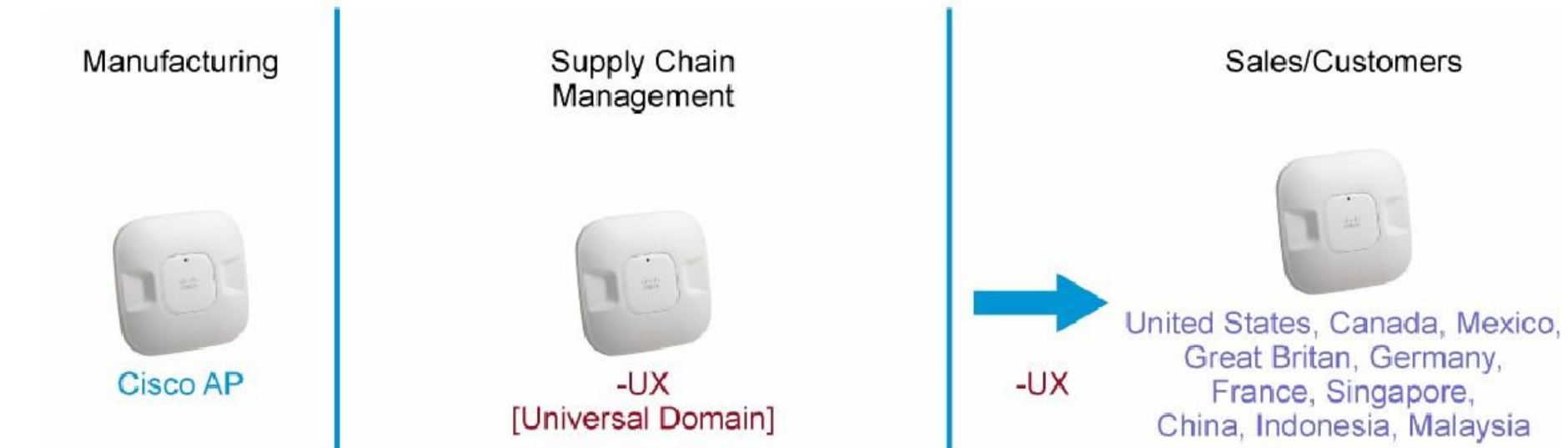
## AP Join Phase with Master



## Explain Universal AP Priming

### Universal AP Priming—New Feature—Overview

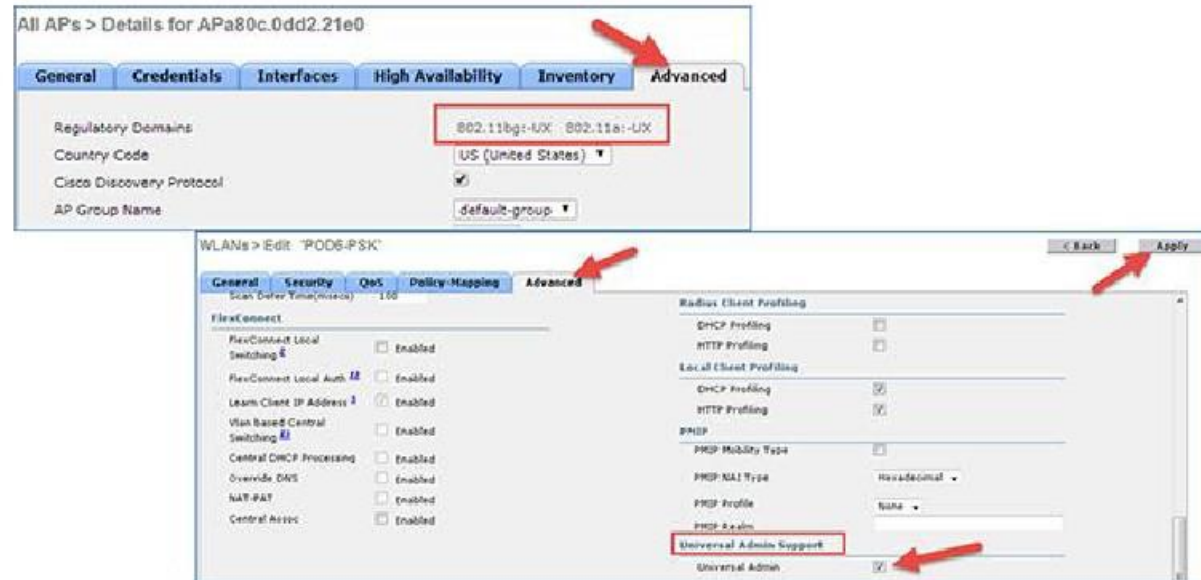
- APs universal (not country specific)
- Geographic specific (set country and regulatory domain)
- Manual or Automatic Priming



# Universal AP Priming—Manual

## Manual Priming configuration steps

- Step 1: AP Joins as a Universal domain – UX AP
- Step 2: Enable Universal domain support on the WLC



# Universal AP Priming—Manual (Cont.)

## Manual Priming configuration steps

- Step 3: Priming through Cisco AirProvision App

Download AirProvision app and login with CEC credentials

Cisco AirProvision

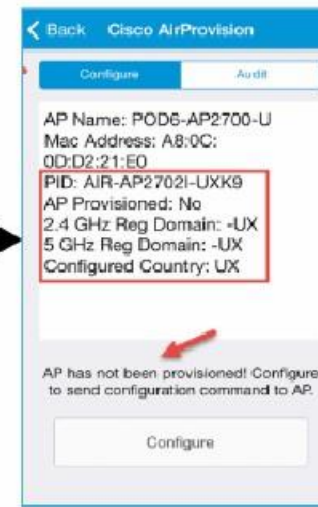


Connect to Universal Admin SSID



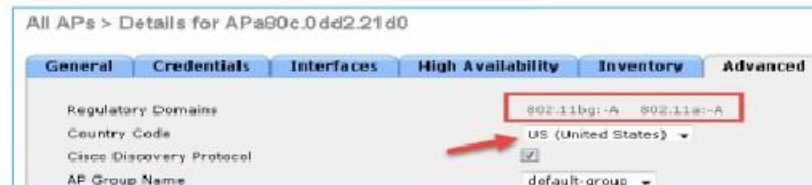
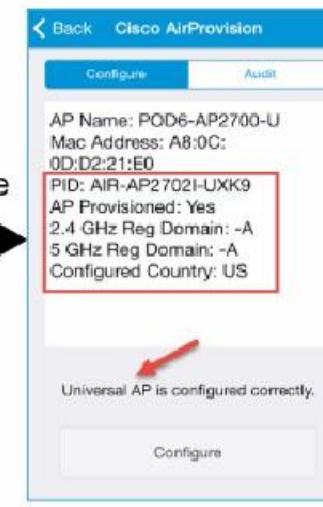
Log In

Shows Unprimed with UX Domain



Configure

Comes Back up with Correct Domain



## Universal AP Priming—Automatic

### Automatic Priming configuration steps

- Step 1: Universal AP boots and joins a WLC
- Step 2: The universal AP will be scanning the 2.4 GHz and 5 GHz band for NDP messages from neighboring universal APs
- Step 3: If automatic priming is available, then the universal AP receives country information, reboots, and rejoins the controller as a primed AP
- Step 4: If automatic priming is unavailable or does not work, the lightweight AP waits for you to manually prime it



## AP Failover Process

- Primary WLC fails, the AP will failover to the backup WLC.
- When the primary WLC is back online, the AP by default will fall back to the primary.
- Heartbeat verifies reachability from the AP to the WLC.
- Heartbeat ACK verifies that the WLC is reachable.
- Heartbeat is sent every 30 seconds.
- Heartbeat no ACK, resends five times at 1-second intervals before being declared unreachable.



## AP Failover Priority

- Individual AP Setting
- WLC Wireless Global Setting to Recognize Failover Priority

All APs > Details for Centralized\_AP

General Credentials Interfaces High Availability Inventory Advanced

	Name	Management IP Address(Ipv4/Ipv6)
Primary Controller	192.168.11.5	wlc1
Secondary Controller	192.168.11.6	wlc2
Tertiary Controller	192.168.11.7	wlc3

AP Failover Priority

Low  
Medium  
High  
Critical

**AP Failover Priority**

Global AP Failover Priority Enable ▾

# AP Fallback

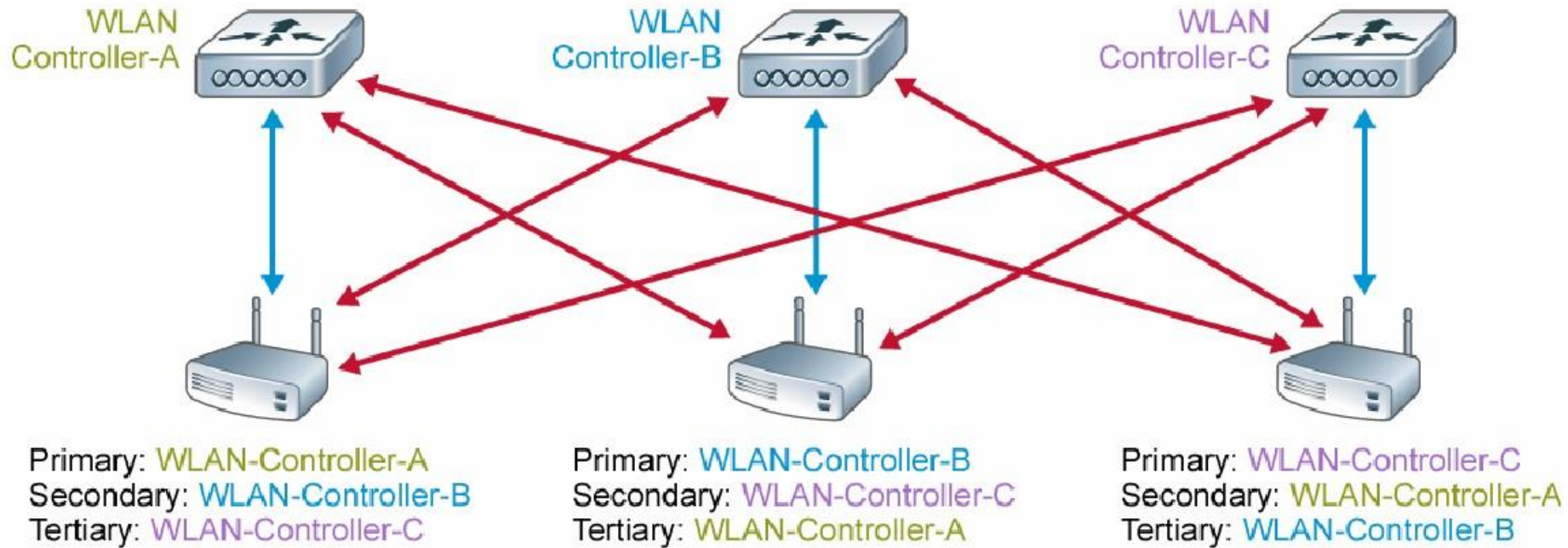
## General WLC Controller Setting

Controller	General	
<b>General</b>	Name	<input type="text" value="POD1WLC"/>
<b>Inventory</b>	802.3x Flow Control Mode	<input type="button" value="Disabled"/>
<b>Interfaces</b>	LAG Mode on next reboot	<input type="button" value="Disabled"/> (LAG Mode is currently disabled).
<b>Interface Groups</b>	Broadcast Forwarding	<input type="button" value="Disabled"/>
<b>Multicast</b>	AP Multicast Mode <a href="#">?</a>	<input type="button" value="Multicast"/> <input type="text" value="239.0.1.1"/> Multicast Group Address
▶ <b>Internal DHCP Server</b>	AP IPv6 Multicast Mode <a href="#">?</a>	<input type="button" value="Multicast"/> <input type="text" value="ff1e::239:100:100:94"/> IPv6 Multicast Group Address
▶ <b>Mobility Management</b>	<b>AP Fallback</b>	<input type="button" value="Enabled"/>
<b>Ports</b>	CAPWAP Preferred Mode	<input type="button" value="ipv4"/>
▶ <b>NTP</b>		

解释高可靠性

# Explain High Availability

## Controller Redundancy: N + 1 Failover



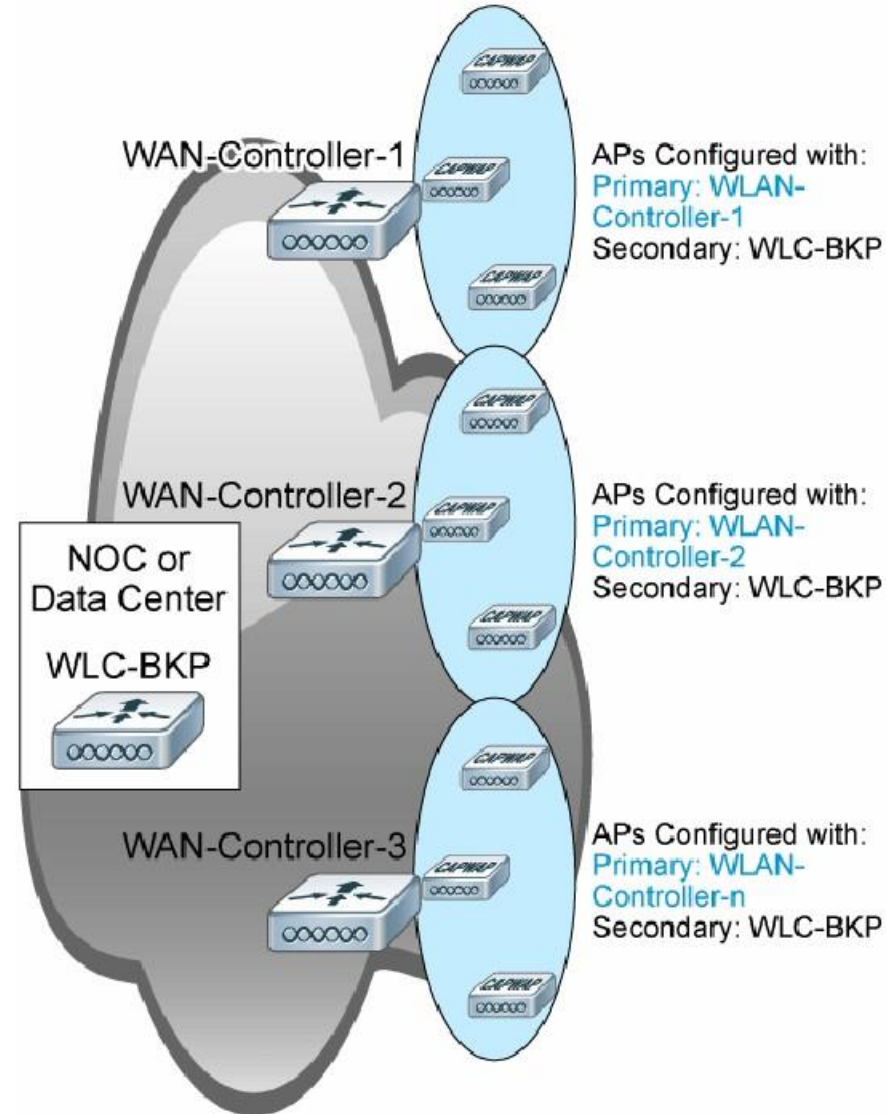
All APs > Details for Centralized\_AP

	Name	Management IP Address(Ipv4/Ipv6)
Primary Controller	192.168.11.5	wlc1
Secondary Controller	192.168.11.6	wlc2
Tertiary Controller	192.168.11.9	wlc3

## 控制器冗余

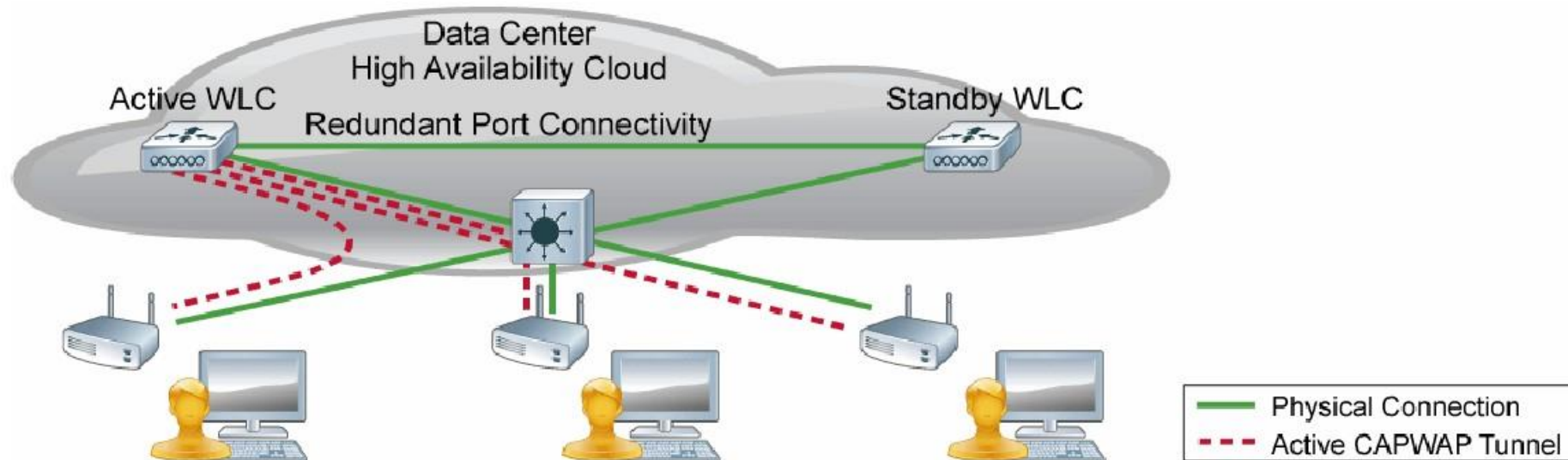
# Controller Redundancy: N + 1 Failover

- Redundant WLC geographically separate
- Configure high availability parameters
- AP Priority



# High Availability

- 1:1 Redundancy
- One Active WLC – One Hot Standby WLC
- Connected via Redundant Port





# High Availability (Cont.)

## Rel. 7.3 AP SSO

- Active – Standby 1:1 Redundancy
- Both WLC share IP Address of management interface
- Bulk and Incremental Config Sync
- AP does not go in Discovery state when Active WLC fails
- Supported on 5500 / 7500 / 8500 and WiSM-2 WLC
- Downtime 5 - 1000 msec in case of Box failover, ~3 seconds in case of Network Issues

## Rel. 7.5 Client SSO

- Active – Standby can be geographically separated over L2 VLAN/Fiber
- Client database is synced to the Standby
  - Client information is synced when client moves to RUN state
  - Client re-association is avoided on switch over
- Fully authenticated clients (RUN state) are synced to the peer
- Effective service downtime = Detectoin time + Switch Over Time (Network recovery/ convergence)

## Rel. 8.0 Enhancements

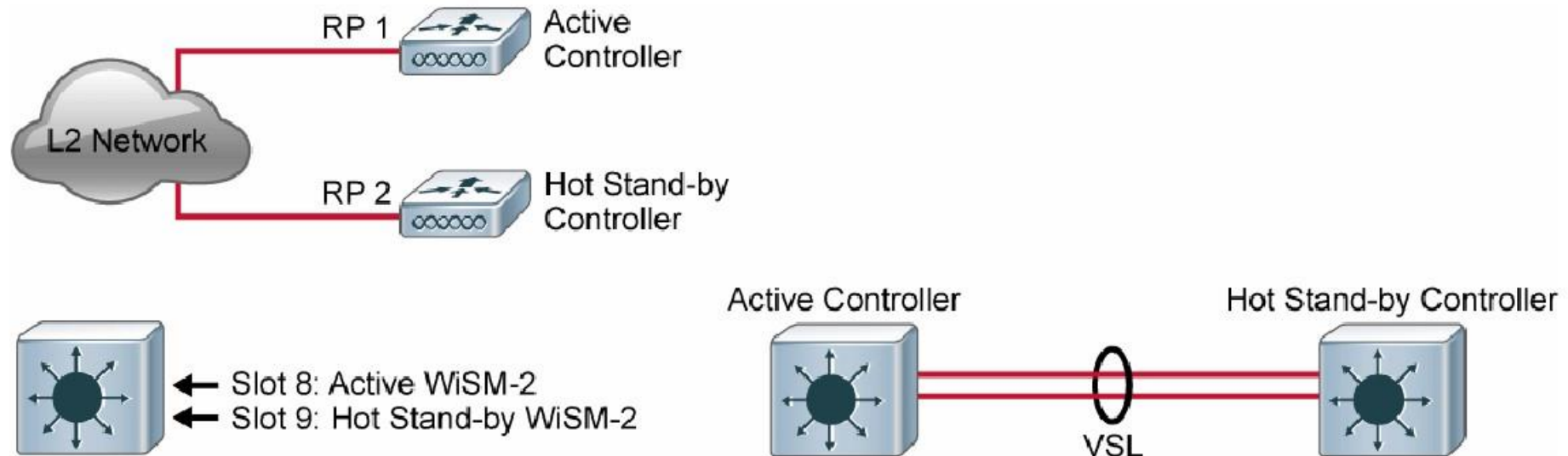
- Standby WLC on-the-fly maintenance mode
- SSO Support for Internal DHCP Server
- SSO support for sleeping clients
- SSO support for 802.11ac configuration
- Enhanced GW reachability check mechanism enhanced to avoid false positives
- Peer RMI ICMP ping replaced with UDP messages
- Faster HA Pair-up



集中模式：状态切换

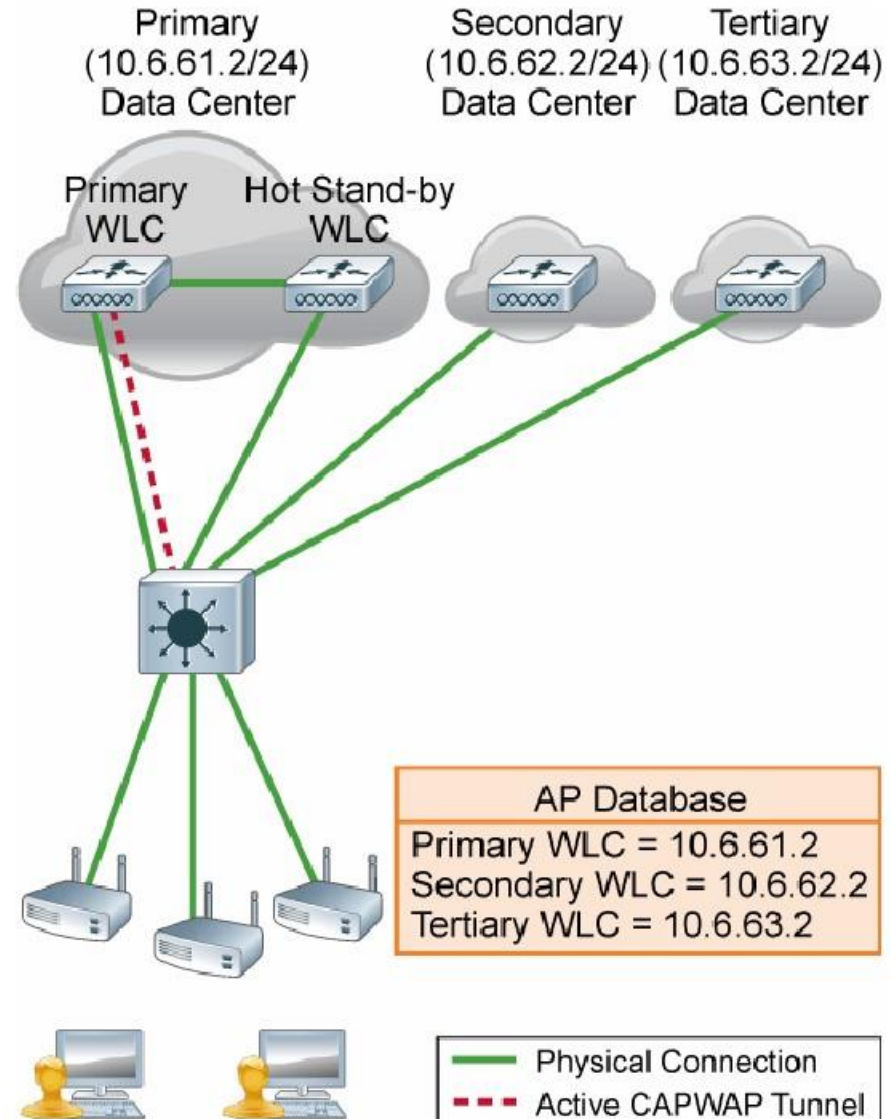
## Centralized Mode: Stateful Switch Over

- Controller Physical connectivity
  - 5500/7500/8500 have dedicated Redundancy Port
  - WiSM-2 have dedicated Redundancy VLAN which is used to synch configuration from Active to Standby WLC



## Centralized Mode: Stateful Switch Over (Cont.)

- Integrating with N+1 Design
  - SSO can be deployed with Secondary and Tertiary Controllers
  - Both Active and Standby combined in SSO setup are configured as primary.
  - On failure of both Active and Standby WLC in SSO setup, APs will fall back to secondary and further to configured tertiary controller.



## AP Modes of Operation

### Access Point Local Mode

- Default mode for an AP
- Data services
- Monitoring services
  - AP will scan all channels over 180 seconds by default
  - Only management packets are inspected for IDS signature matches

The screenshot shows the configuration page for an Access Point, with the 'General' tab selected. The page has four tabs: 'General', 'Credentials', 'Interfaces', and 'High Availability'. The 'General' tab contains the following fields and values:

Field	Value
AP Name	APf07f.06da.6c34
Location	default location
AP MAC Address	f0:7f:06:da:6c:34
Base Radio MAC	f0:7f:06:e0:22:a0
Admin Status	Enable
AP Mode	local
AP Sub Mode	local
Operational Status	
Port Number	
Venue Group	
Venue Type	
Venue Name	
Language	

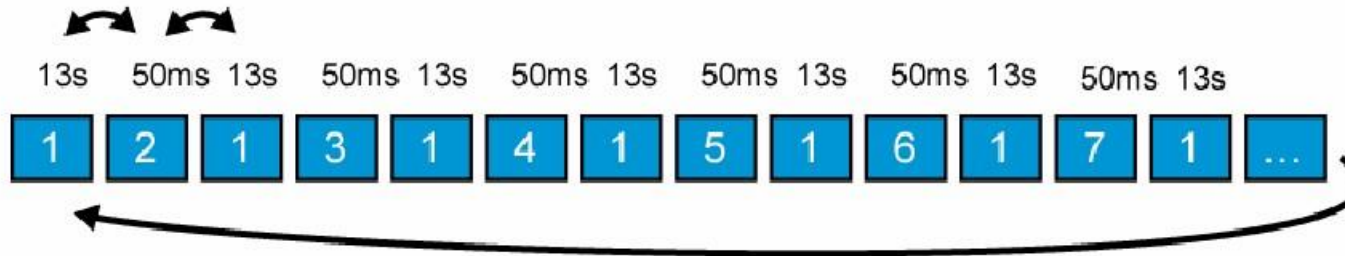
The 'AP Sub Mode' dropdown menu is open, showing the following options: local, FlexConnect, monitor, Rogue Detector, Sniffer, Bridge, Flex+Bridge, SE-Connect, and Unspecified.

本地模式：监控

## Local Mode Monitor Timing

AP on Channel 1

802.11b/g



AP on Channel 36

802.11a



Round trip = 180 seconds (If noise measurement parameter set to 180)



## wIPS Enhanced Local Mode

- ELM provides wIPS detection “on-channel”
- Complete scanning of all packets on the servicing channel, not just management packets
  - No signature detection during off-channel scanning
- Allows use of deployed APs to provide IDS protection without needing a separate overlay network
- Sub Mode of Local Mode and FlexConnect Mode

General	
AP Name	AP1cdf.0f66.64a5
Location	default location
AP MAC Address	1c:df:0f:66:64:a5
Base Radio MAC	68:bd:ab:67:fd:40
Admin Status	Enable
AP Mode	local
AP Sub Mode	WIPS
Operational Status	WIPS
Port Number	13
Network Spectrum Interface Key	766C6E6214647260D3DD41C23CD547E6

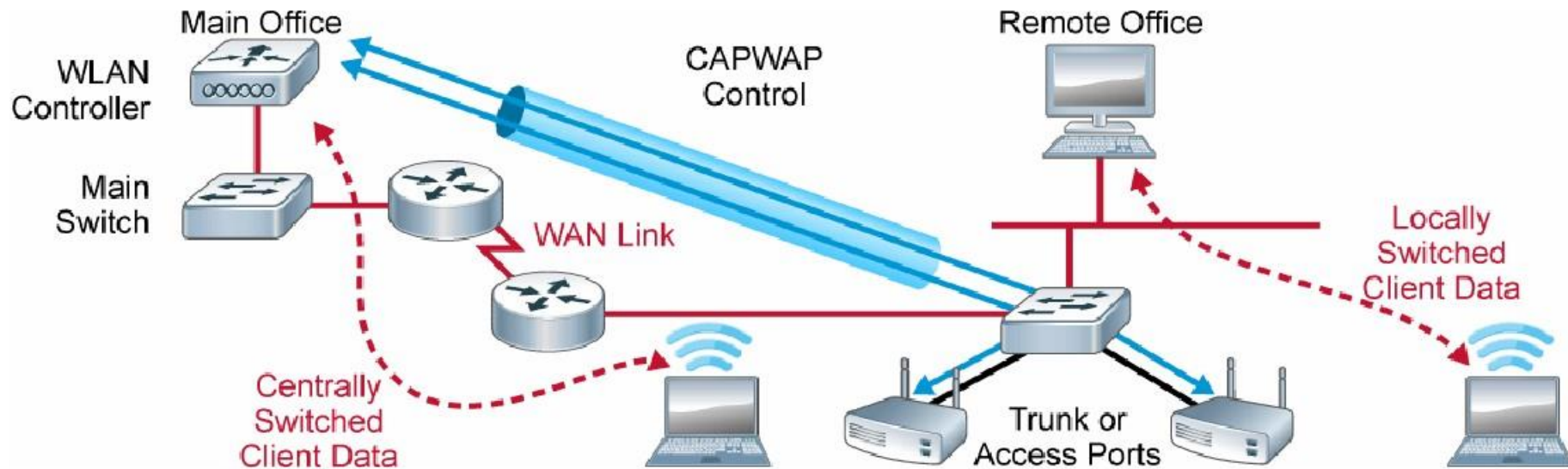
MSE and Prime Infrastructure with wIPS licensing are required for ELM functionality.

Simply selecting the submode will not enable ELM functionality.

FlexConnect模式

## Access Point FlexConnect Mode

- Solution for branch and remote office deployments:
  - Centralized configuration and control

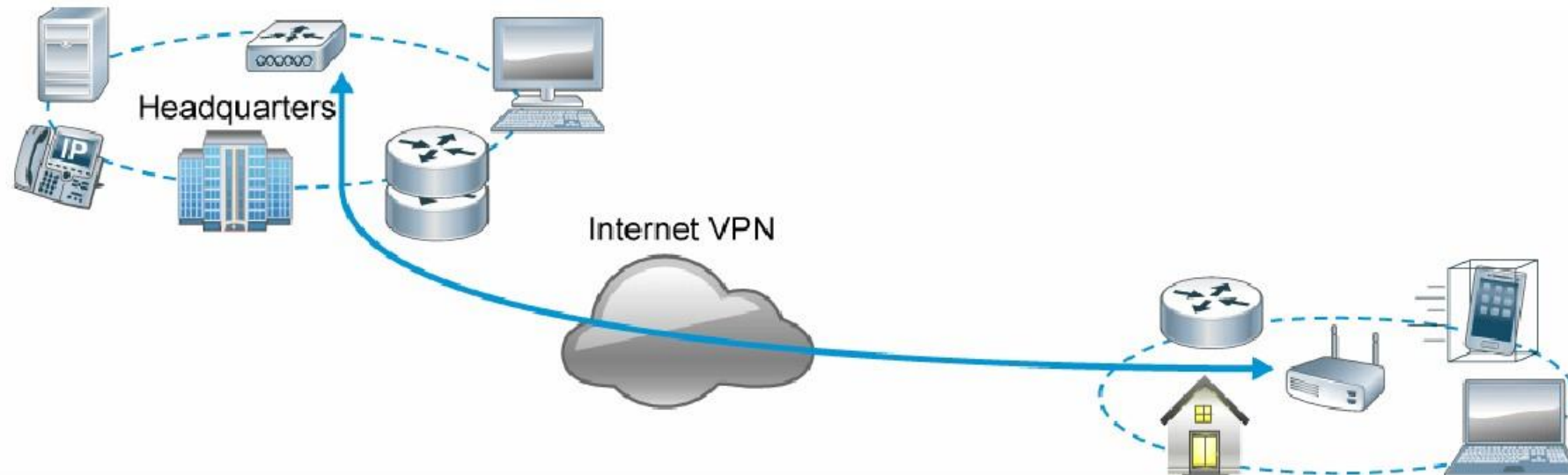




OfficeExtend模式

## AP OfficeExtend Mode

- Cisco controllers installed in the DMZ of the corporate network
- OEAP installed at a teleworker home
- Corporate access to employee over centrally configured
- Family Internet access over a locally configured SSID
- Only AP models with integrated antennas



## AP Monitor Mode

Software configuration to reduce AP capabilities to perform only WLAN monitoring on a per-AP basis:

- Trusted AP policies
- Rogue policies
- Signatures
  - Both data and management packets are inspected for IDS signature matches
  - AP will scan all channels for 1.1 seconds
- Two submodes available
  - Tracking Optimization: Optimized for RFID tracking
  - wIPS: Fixed scan time of 250 ms per channel

## AP Rogue Detector Mode

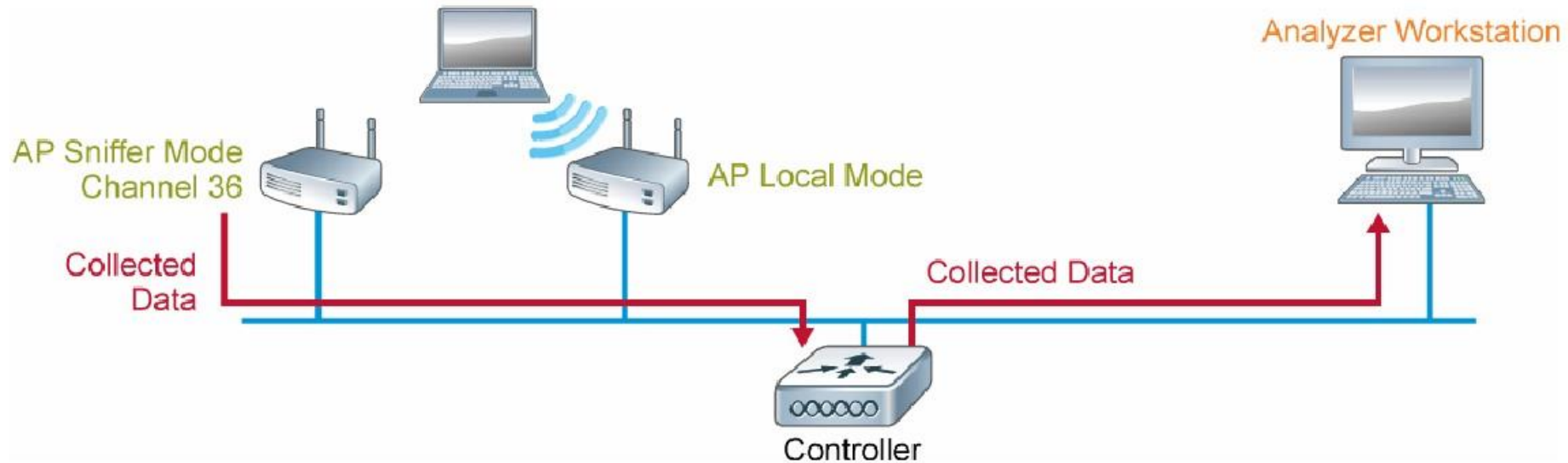
Software configuration to reduce AP capabilities to perform only rogue detection on a per-AP basis:

- Listens for rogue devices on the wired network
- Compares ARP request heard on the network to rogue MAC address reported by the controller
- Generates an alarm when a wireless rogue is seen on the wired side
- Does not allow client connectivity—radios are shut down, 100% of CPU dedicated to rogue detection
- Does not perform rogue containment

嗅探模式

## AP Sniffer Mode

- Works with products like OmniPeek, Wireshark, or AirMagnet to monitor a single wireless channel
- Requires an external server to capture the packets
- Gathers data; time stamp, signal strength, and packet size



桥接模式

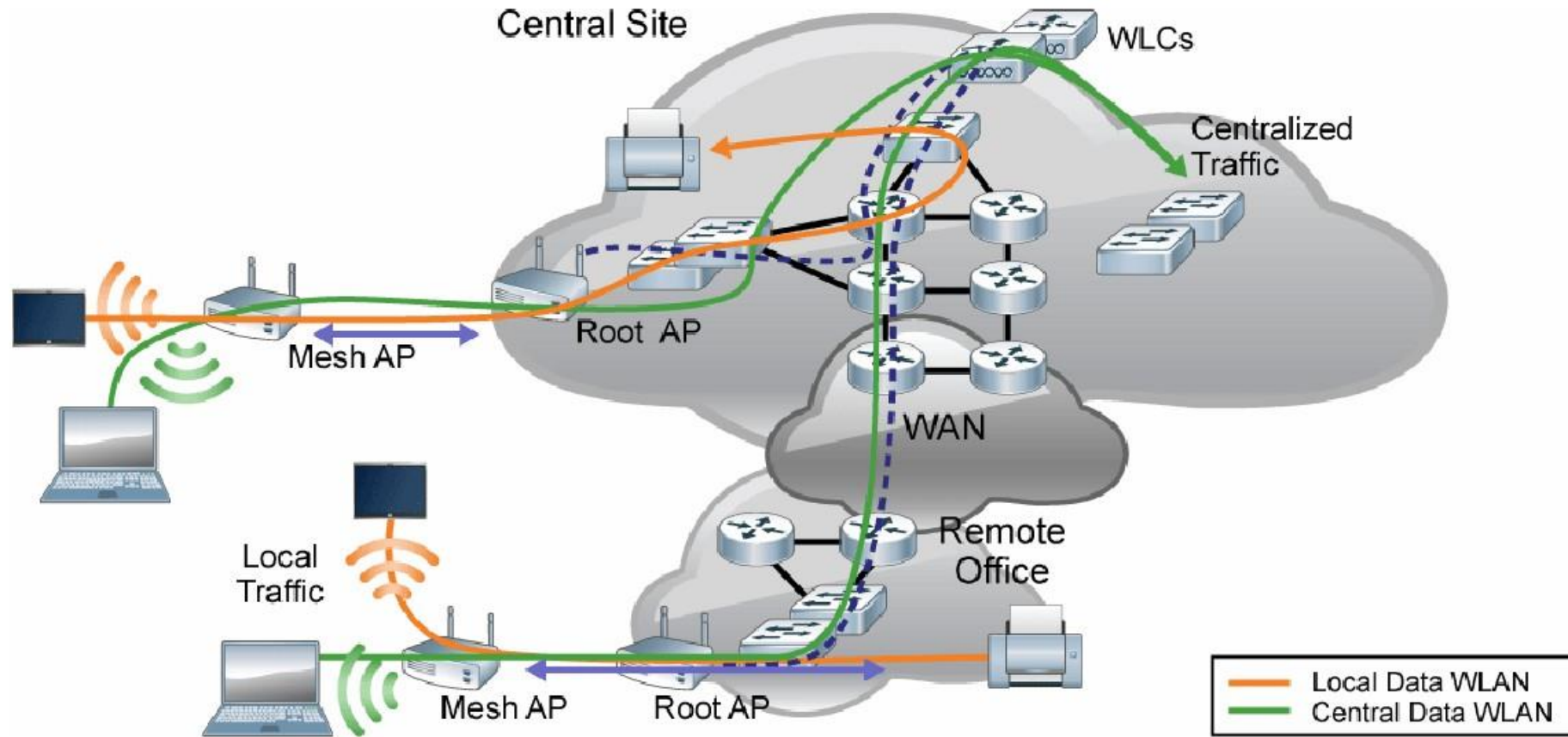
## AP Bridge Mode

- Available on supported AP models
- Supported on all AireOS WLCs
- Used to set up indoor/outdoor mesh network
- Allows APs to act as a wireless CAPWAP bridge
- APs may be configured for bridge mode as the default mode
- 802.11ac supported with up to 80 MHz channels for backhaul



混合模式

# AP Flex+Bridge Mode



## AP SE-Connect Mode

- Also referred to as SOMM
- Available on select Cisco Access Points
- Allows AP to act as a network-connected sensor
- Monitors 2.4 GHz and 5GHz spectrum simultaneously
- Does not support wireless clients
- Eliminates need for travel to analyze interference
- Only shows up on CleanAir enabled APs



浏览附加的WLC特性

## Explore Additional WLC Features

Implement Centralized Wireless Access

## Explain and Configure Client Link

- Used by APs with MIMO antennas to improve SNR
- Now called “beamforming” when configuring
- Can be changed at CLI only
  - Configured globally by radio type or by AP by radio type
- AP must be capable of supporting Client Link
- Not supported for all data rates

## 频宽选择

# Explain and Configure Band Select

- Used to move dual-band clients to 5GHz band
- Enabled globally by default
- Can be activated per WLAN

### WLC - Wireless>Advanced>Band Select

Band Select	
Probe Cycle Count	<input type="text" value="2"/>
Scan Cycle Period Threshold (1-1000 milliseconds)	<input type="text" value="200"/>
Age Out Suppression (10-200 seconds)	<input type="text" value="20"/>
Age Out Dual Band (10-300 seconds)	<input type="text" value="60"/>
Acceptable Client RSSI (dBm)	<input type="text" value="-80"/>
Acceptable Client Mid RSSI (dBm)	<input type="text" value="-60"/>

*\* Band Select is configurable per WLAN.*

### WLC - WLAN>WLAN ID>Advanced

Load Balancing and Band Select	
Client Load Balancing	<input type="checkbox"/>
Client Band Select	<input type="checkbox"/>



## Local Profiling and Policy

- When a client tries to associate, it is possible to determine the client type from the information received in the process.
- Using this information ISE offers a rich set of features which provides device identification, onboarding, posture, and policy.
- Customers that do not deploy ISE—but still require the ability to identify a device and apply appropriate policy.
- The WLC provides these capabilities:
  - WLC profiles devices based on the MAC-OUI, HTTP, and DHCP information to identify the end devices on the network.
  - You can configure the device-based policies and enforce per user or per device policy on the network.
  - WLC also displays statistics based on per user or per device end points and policies applicable per device.

## Client Profiling

- Profiling and policy enforcement are 2 separate elements
- Profiling can be based on:
  - Role, defining user type or the user group the user belongs to
  - Device type, such as Windows machine, Smart phone, iPad, iPhone, Android, etc.
  - Username / password pair
  - Location, based on the AP group the end point connected to
  - Time of day, based on what time of the day end-points are allowed on the network
  - EAP Type, to check what EAP method the client is getting connected to
- Based on Profile, a policy is decided, that can be:
  - VLAN, QoS level, ACL, and Session timeout value

# Configuring Client Profiles

At the WLAN level, enable Local Client Profiling (DHCP and HTTP)

- DHCP required is checked automatically when selecting DHCP profiling

WLC - WLAN>WLAN ID>Advanced

General	Security	QoS	Policy-Mapping	Advanced
Allow AAA Override	<input type="checkbox"/>	Enabled		
Coverage Hole Detection	<input checked="" type="checkbox"/>	Enabled		
Enable Session Timeout	<input checked="" type="checkbox"/>	<input type="text" value="1800"/>		
		Session Timeout (secs)		
Aironet IE	<input checked="" type="checkbox"/>	Enabled		
				<b>DHCP</b>
				DHCP Server <input type="checkbox"/> Override
				DHCP Addr. Assignment <input checked="" type="checkbox"/> Required
<b>Local Client Profiling</b>				
				DHCP Profiling <input checked="" type="checkbox"/>
				HTTP Profiling <input checked="" type="checkbox"/>

Profiles 和 Profiling

配置策略

# Configuring Policies

You can assign a policy based on the client identification.

The screenshot shows the 'Policy > Edit' configuration page for a policy named 'Android'. The left sidebar contains a navigation menu with categories like AAA, Local EAP, and Advanced EAP. The main content area is divided into several sections:

- Match Criteria:** Includes 'Match Role String' (empty text field) and 'Match EAP Type' (dropdown menu set to 'none').
- Device List:** Includes 'Device Type' (dropdown menu set to 'Android') with an 'Add' button, and a checked checkbox for 'Android'.
- Action:** Includes various settings such as 'IPv4 ACL' (none), 'WLAN ID' (20), 'QoS Policy' (none), 'Average Data Rate' (0), 'Average Real time Data Rate' (0), 'Burst Data Rate' (0), 'Burst Real time Data Rate' (0), 'Session Timeout (seconds)' (1800), 'Sleeping Client Timeout (min.)' (720), 'Flexconnect ACL' (none), 'AVC Profile' (none), and 'mDNS Profile' (none).
- Active Hours:** Includes 'Day' (Men), 'Start Time' (Hours and Mins), and 'End Time' (Hours and Mins) with an 'Add' button.

Two callout boxes are present on the right side of the screenshot:

- A box labeled 'How to identify device' is positioned to the right of the Match Criteria and Device List sections.
- A box labeled 'What policy to apply' is positioned to the right of the Action section.

## Applying Policies

Apply the policies to the WLANs in the order you want them to be applied (up to 16 policies per WLAN)

WLANs > Edit 'Pod1\_Open'

**General** **Security** **QoS** **Policy-Mapping** **Advanced**

Priority Index (1-16)

Local Policy

Choose an index

Choose a policy

Add

Priority Index	Local Policy Name
1	Android





配置客户访问

# Configure Client Access

Implement Centralized Wireless Access

# WLAN Open Authentication

WLANs > Edit 'Pod1\_Open'

**General** | **Security** | QoS | Policy-Mapping | Advanced

Profile Name: Pod1\_Open  
Type: WLAN  
SSID: Pod1\_Open  
Status:  Enabled

Security Policies: None  
(Modifications done under security tab will appear after applying the changes.)

Radio Policy: All  
Interface/Interface Group(G): client  
Multicast Vlan Feature:  Enabled  
Broadcast SSID:  Enabled  
NAS-ID: POD1WLC

**General** | **Security** | QoS | Policy-Mapping | Advanced

**Layer 2** | Layer 3 | AAA Servers

Layer 2 Security: None  
MAC Filtering:

**Fast Transition**  
Fast Transition:

# PSK认证

## WLAN PSK Authentication

The image shows two overlapping screenshots of a network configuration interface. The left screenshot displays the 'General' tab for a WLAN profile named 'Pod1\_PSK'. The right screenshot displays the 'Security' tab, specifically the 'AAA Servers' sub-tab, for the same profile.

**General Tab (Left Screenshot):**

- Profile Name: Pod1\_PSK
- Type: WLAN
- SSID: Pod1\_PSK
- Status:  Enabled
- Security Policies: [WPA2][Auth(802.1X)] (Modifications done under securit)
- Radio Policy: All
- Interface/Interface Group(G): client
- Multicast Vlan Feature:  Enabled
- Broadcast SSID:  Enabled
- NAS-ID: POD1WLC

**Security Tab - AAA Servers (Right Screenshot):**

- Layer 2 Security: WPA+WPA2
- MAC Filtering:
- Fast Transition:
- Protected Management Frame (PMF): Disabled
- WPA+WPA2 Parameters:
  - WPA Policy:
  - WPA2 Policy-AES:
- Authentication Key Management:
  - 802.1X:  Enable
  - CCKM:  Enable
  - PSK:  Enable
  - FT 802.1X:  Enable
  - FT PSK:  Enable
  - PSK Format: ASCII
  - WPA gtk-randomize State: Disable

EAP和RADIUS认证

# WLAN EAP and RADIUS Authentication

## WLAN Local-EAP Authentication

The image displays three screenshots from the Cisco Wireless LAN Controller (WLC) configuration interface, illustrating the setup of Local EAP authentication.

**Top Screenshot: Local Net Users > Edit**

This screenshot shows the configuration for a local net user named 'wlcuser'. The fields are as follows:

User Name	wlcuser
Password	•••
Confirm Password	•••
Creation Time	Thu Apr 9 20:49:38 2015
Remaining Time	N/A
WLAN Profile	Any WLAN

**Middle Screenshot: Local EAP Profiles > New**

This screenshot shows the configuration for a new Local EAP profile. The Profile Name is 'WLC\_Local\_EAP'.

**Bottom Screenshot: Local EAP Profiles**

This screenshot shows the Local EAP Profiles table. The profile 'WLC\_Local\_EAP' is selected, and the PEAP checkbox is checked.

Profile Name	LEAP	EAP-FAST	EAP-TLS	PEAP
<a href="#">WLC_Local_EAP</a>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>

# WLAN EAP and RADIUS Authentication (Cont.)

## WLAN Local-EAP Authentication

The image displays two screenshots of a network configuration interface, likely from a Cisco Wireless LAN Controller (WLC), showing WLAN security settings.

**Left Screenshot: Layer 2 Security Settings**

- General tabs: General, Security, QoS, Policy-Mapping, Advanced
- Sub-tabs: Layer 2, Layer 3, AAA Servers
- Layer 2 Security: WPA+WPA2 (dropdown)
- MAC Filtering:
- Fast Transition:
- Protected Management Frame (PMF): Disabled (dropdown)
- WPA+WPA2 Parameters:
  - WPA Policy:
  - WPA2 Policy-AES:
- Authentication Key Management:
  - 802.1X:  Enable
  - CCKM:  Enable
  - PSK:  Enable
  - FT 802.1X:  Enable

**Right Screenshot: Local EAP Authentication Settings**

- General tabs: General, Security, QoS, Policy-Mapping, Advanced
- Sub-tabs: Layer 2, Layer 3, AAA Servers
- Interim Update:  Interim Interval: 0
- LDAP Servers:
  - Server 1: None (dropdown)
  - Server 2: None (dropdown)
  - Server 3: None (dropdown)
- Local EAP Authentication:
  - Local EAP Authentication:  Enabled
  - EAP Profile Name: WLC\_Local\_EAP (dropdown)



# WLAN with RADIUS Authentication

The screenshot displays the Cisco Identity Services Engine (ISE) configuration interface. The top navigation bar includes 'Home', 'Operations', 'Policy', 'Guest Access', and 'Administration'. Below this, there are tabs for 'System', 'Identity Management', 'Network Resources', 'Device Portal Management', 'pxGrid Services', and 'Feed Service'. The 'Identity Management' section is active, with sub-tabs for 'Identities', 'Groups', 'External Identity Sources', 'Identity Source Sequences', and 'Settings'.

The main content area is divided into two panels. The left panel, titled 'Network Resources', shows the configuration for a network device named 'POD1WLC'. The configuration includes:

- Name: POD1WLC
- Description: (empty)
- IP Address: 192.168.11.5 / 32
- Model Name: (dropdown)
- Software Version: (dropdown)
- Network Device Group: (empty)
- Location: All Locations (dropdown) with 'Set To Default' button
- Device Type: All Device Types (dropdown) with 'Set To Default' button
- Authentication Settings (checked):
  - Enable Authentication Settings: (checked)
  - Protocol: RADIUS
  - \* Shared Secret: (password field) with 'Show' button
  - Enable KeyWrap: (unchecked)
  - \* Key Encryption Key: (password field) with 'Show' button
  - \* Message Authenticator Code Key: (password field) with 'Show' button
  - Key Input Format: ASCII (selected) / HEXADECIMAL

The right panel, titled 'Network Access Users List > pod1user', shows the configuration for a network access user:

- Network Access User: pod1user
- \* Name: pod1user
- Status: Enabled (dropdown)
- Email: (empty)
- Password: (password field) with 'Need help with password policy?' link
- \* Re-Enter Password: (password field)
- User Information:
  - First Name: (empty)
  - Last Name: (empty)

# WLAN with RADIUS Authentication (Cont.)

**RADIUS Authentication Servers > Edit**

Server Index: 1  
Server Address(Ipv4/Ipv6): 192.168.11.21  
Shared Secret Format: ASCII  
Shared Secret: ...  
Confirm Shared Secret: ...  
Key Wrap:  (Designed for FIP)  
Port Number: 1812  
Server Status: Enabled  
Support for RFC 3576: Disabled  
Server Timeout: 2 seconds  
Network User:  Enable  
Management:  Enable  
[Realm List](#)  
IPSec:  Enable

**General** | **Security** | **QoS** | **Policy-Mapping** | **Advanced**

**Layer 2** | **Layer 3** | **AAA Servers**

Enabled  Enabled  Enable

Server	Layer 2	Layer 3
Server 1	None	None
Server 2	None	None
Server 3	None	None
Server 4	None	None
Server 5	None	None
Server 6	None	None

**Radius Server Accounting**

Interim Update:  Interim Interval: 0

**LDAP Servers**

Server	Value
Server 1	None
Server 2	None
Server 3	None

**Local EAP Authentication**

Local EAP Authentication:  Enabled

# 认证

## WLAN WebAuth Authentication

General Security QoS Policy-Mapping Advanced

Profile Name

Type WLAN

SSID

Status  Enabled

General Security QoS Policy-Mapping

Layer 2 Layer 3 AAA Servers

Layer 2 Security

MAC Filtering

Fast Transition

Fast Transition

General Security QoS Policy-Mapping Advanced

Layer 2 Layer 3 AAA Servers

IUWNE\_30\_WLAN\_WebAuth\_Authentication\_001

Layer 3 Security

Authentication

Passthrough

Conditional Web Redirect

Splash Page Web Redirect

On MAC Filter failure<sup>10</sup>

Preauthentication ACL IPv4  IPv6  WebAuth FlexAcl

Email Input

Sleeping Client  Enable

Over-ride Global Config  Enable



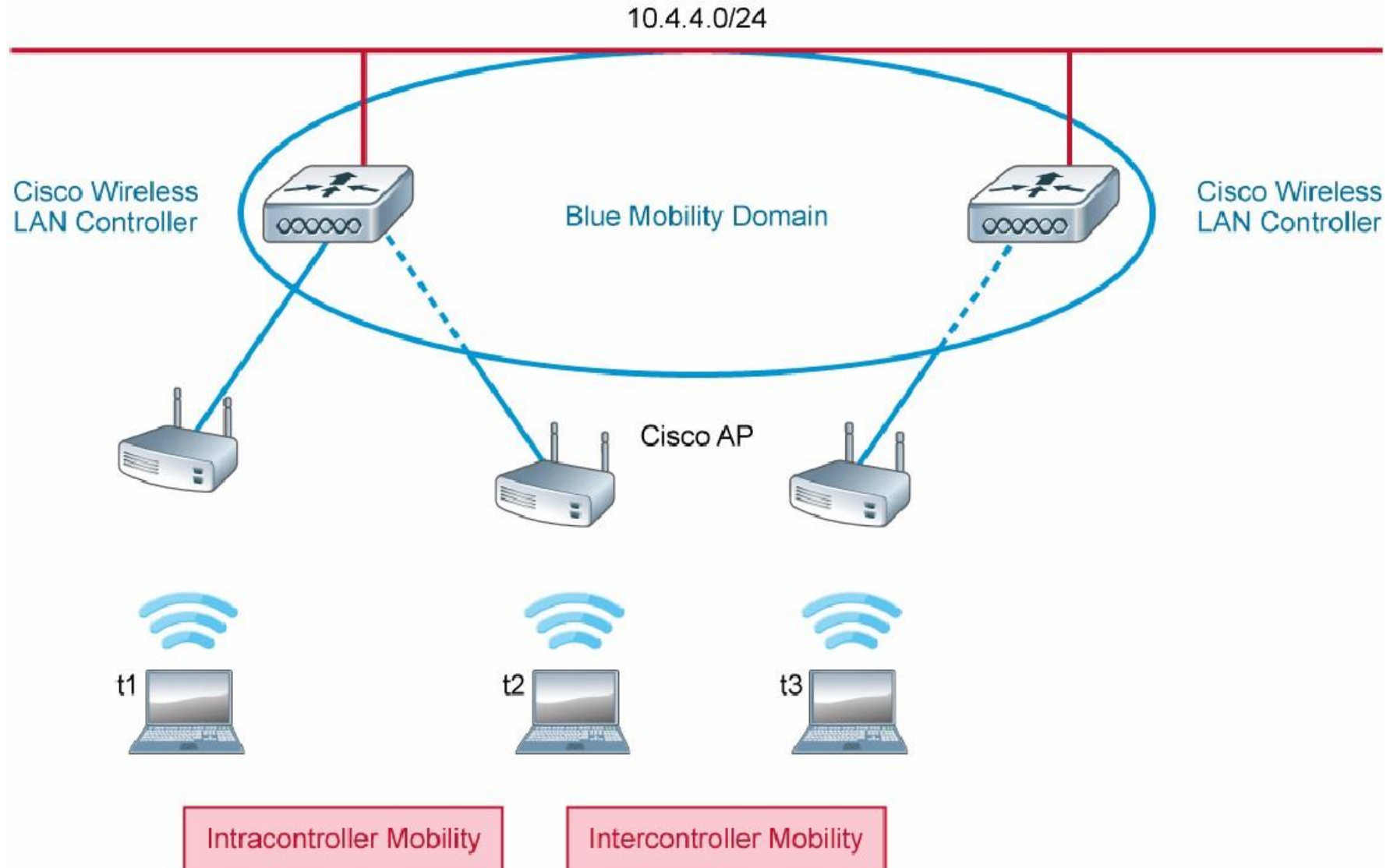
集中架构下的漫游配置

# Implement Roaming in the Centralized Architecture

Implement Centralized Wireless Access

控制器下的漫游

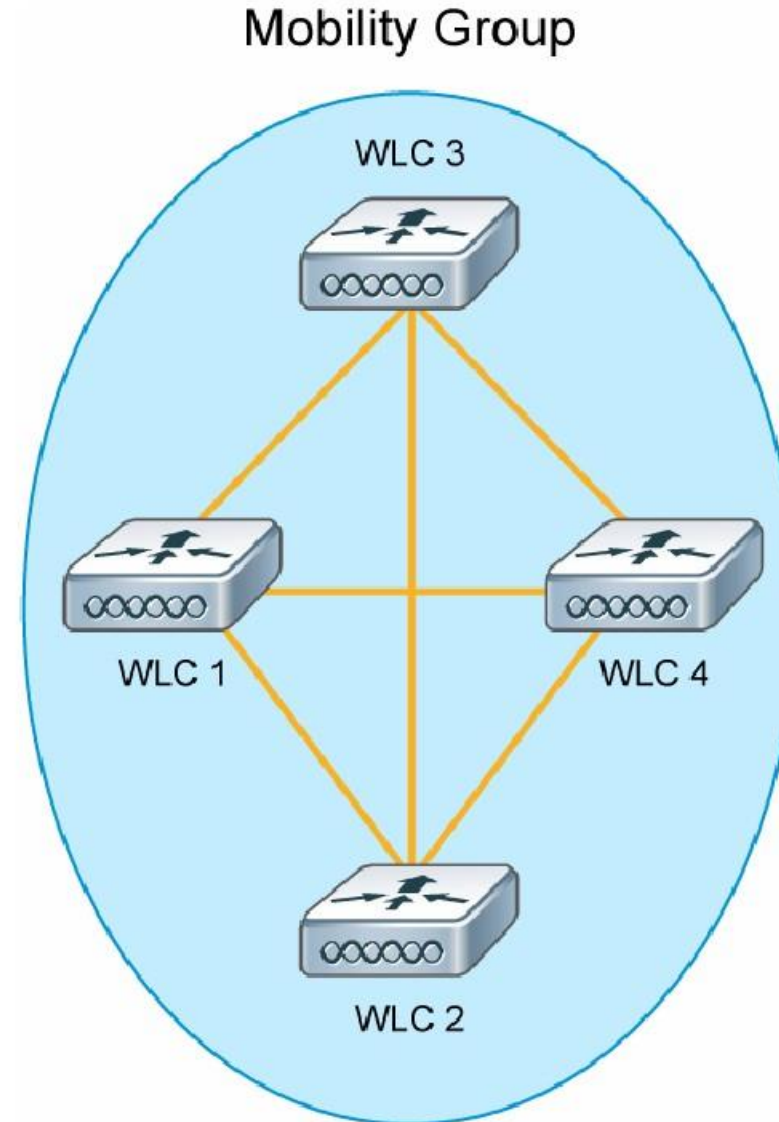
# Intra-Controller/Inter-Controller Roaming





## Mobility Groups

- Group of Wireless LAN Controllers (WLCs) in a network with the same Mobility Group name
- Provides Seamless Mobility and roaming for clients
- Up to 24 WLCs members in one Mobility Group, statically configured
- Full mesh of tunnels between members
- Mobility Control Messages



## Mobility Domains

- Group of controllers configured on a single WLC that specifies members in different mobility groups
- Provides seamless Mobility for clients (client keep original IP address)
- Up to 72 WLCs in one WLC's Mobility List
- Full mesh of tunnels between members
- Mobility Control Messages

