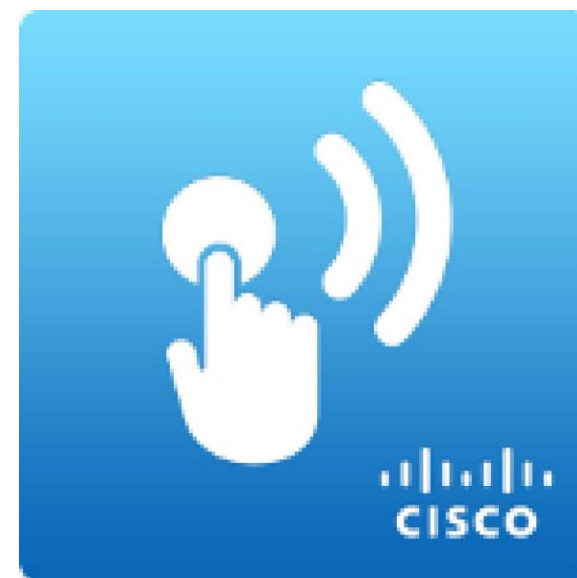


# 经典思科网络技术AireOS简介和基本操作内容

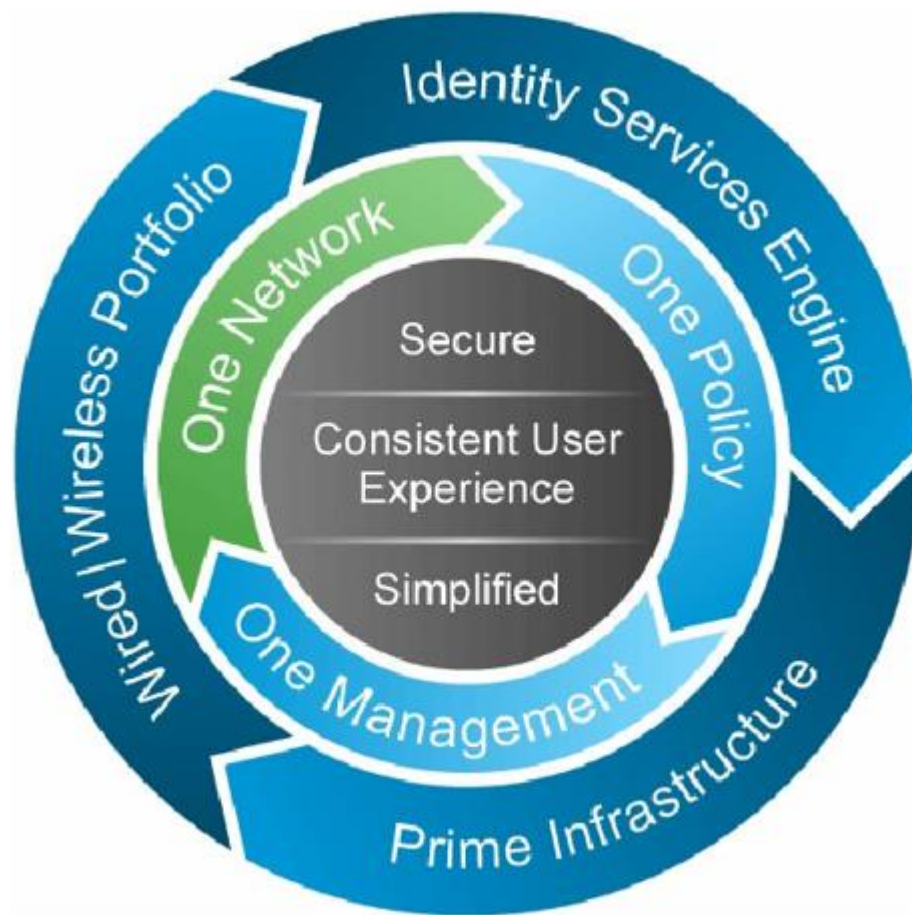
- 思科无线部署基本概念
  - 思科融合无线一体化解决方案
  - AireOS基本概念介绍
  - 控制器端口，接口和映射关系
- 思科无线部署操作实现
  - 基本配置流程图
  - 初始化WLC
  - AP初始化
  - WLC特性配置
  - 客户访问
  - 漫游特性



# 思科无线一体化解决方案

# 思科统一访问架构

- 一个网络
  - 有线无线一体化的基础架构
- 一个策略
  - 在一个地方定义策略
- 一套管理
  - 一个管理界面



# 一个网络

- 一个网络（5种部署方式）
  - 云管理-Meraki AP, 交换机, 安全应用
  - 企业部署
    - 胖AP-IOS
    - 融合 IOS-XE
    - 集中部署
      - AireOS (思科统一无线网络)
      - IOS-XE (使用5760等)
    - Flex链接 - AireOS (CUWN)

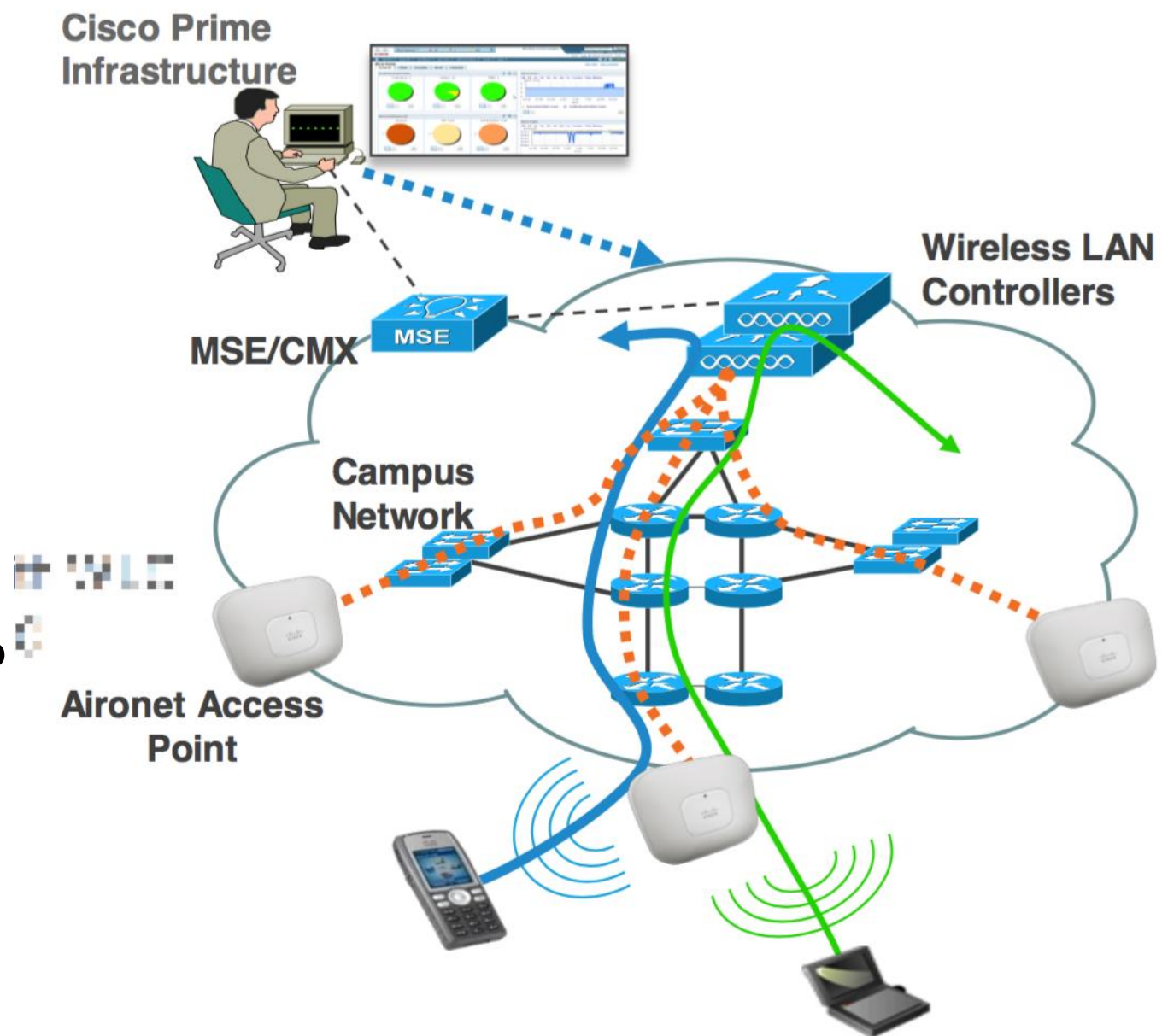
# 思科统一接入理论

## • 组成

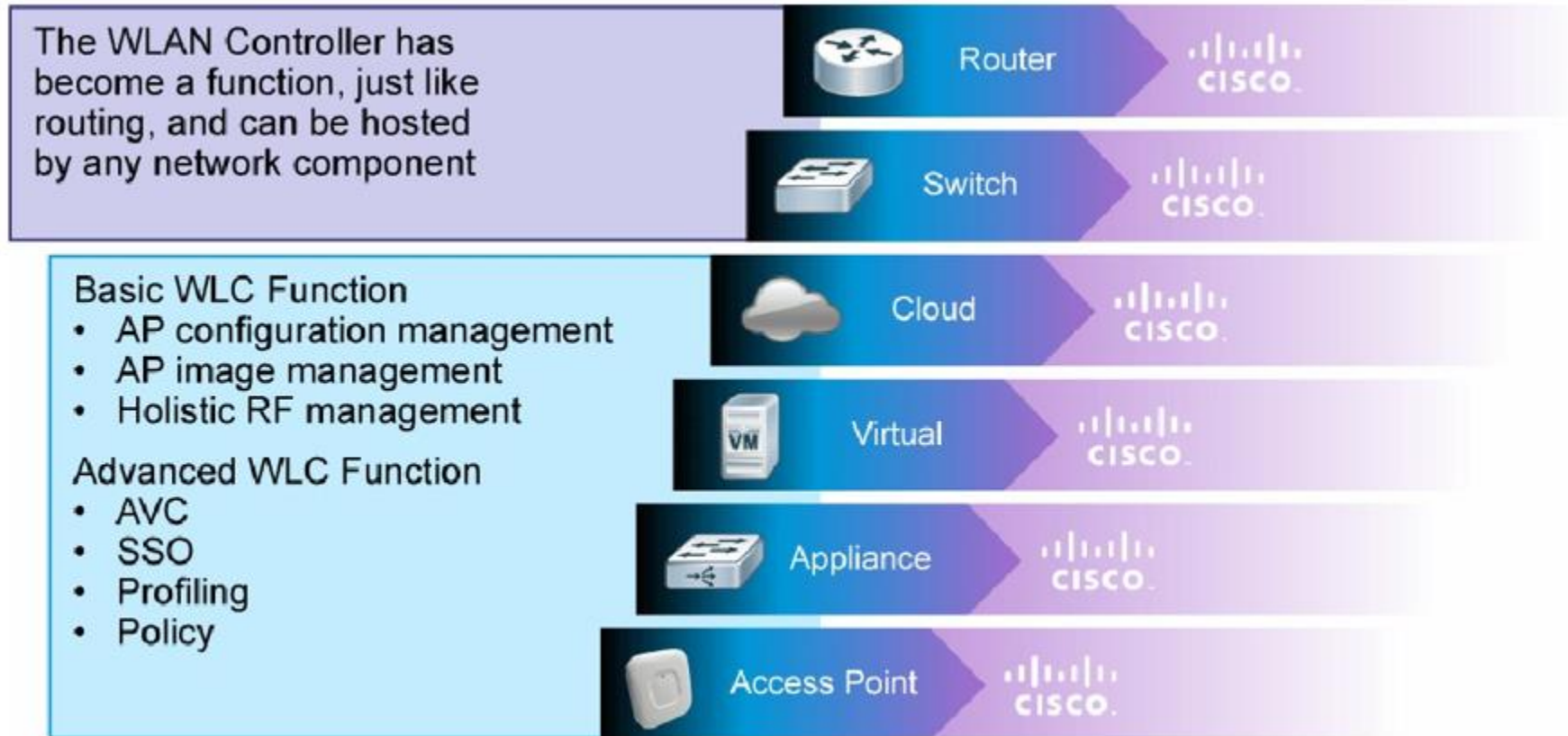
- 无线局域网控制器WLC
- Aironet访问点-AP
- 管理Prime Infrastructure-PI
- 移动服务引擎MSE/CMX

## • 理论

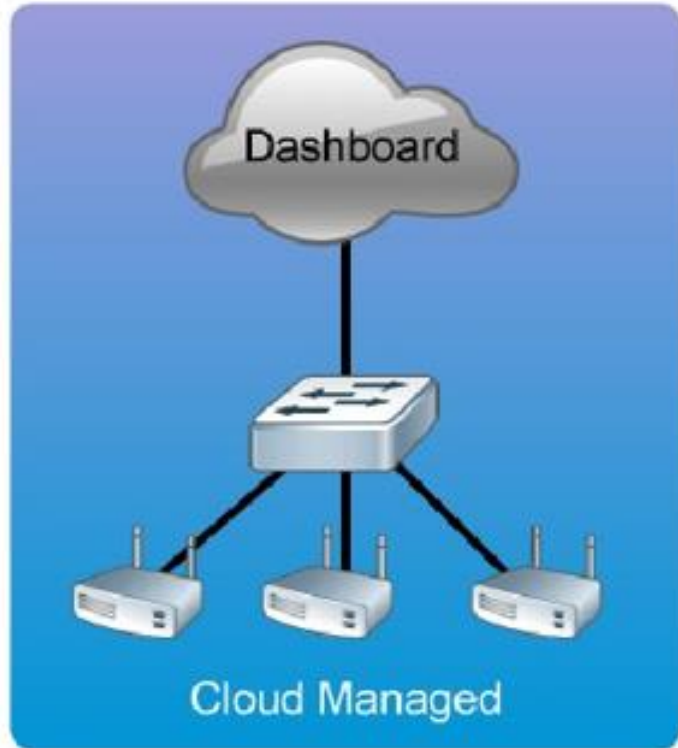
- AP必须和WLC链接: CAPWAP
- 配置从WLC下载到AP
- 所有的Wi-Fi流量转发到WLC



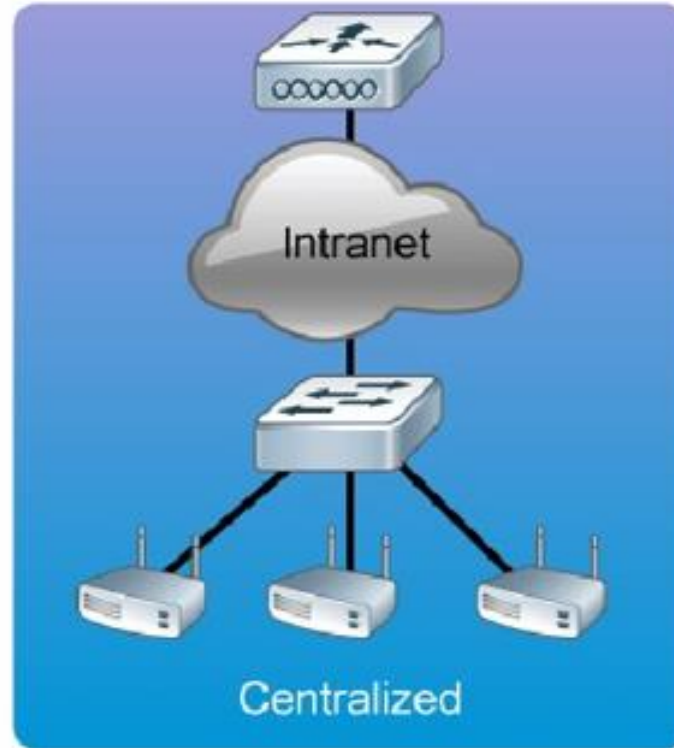
# 无线控制器作为功能服务



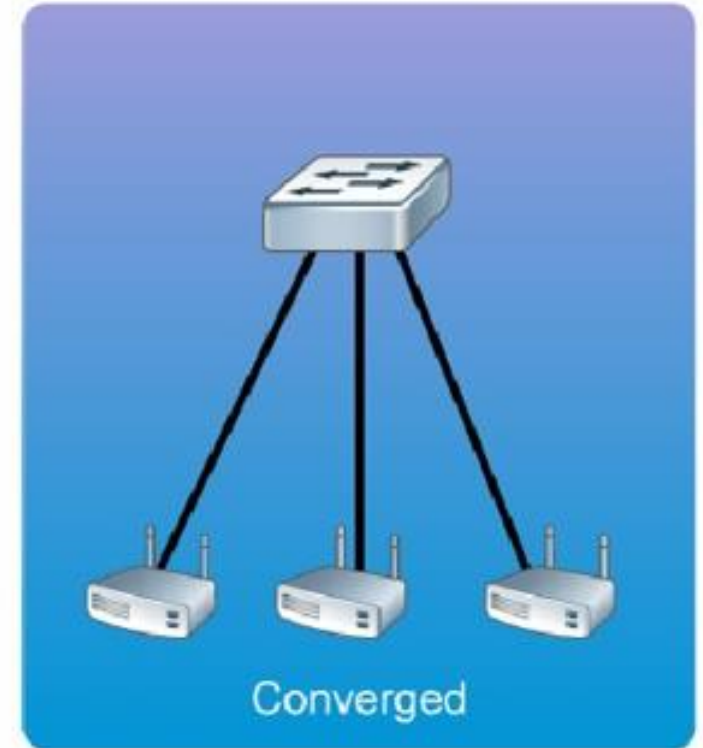
# 无线控制器作为功能服务-续



Controller:  
Dashboard



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



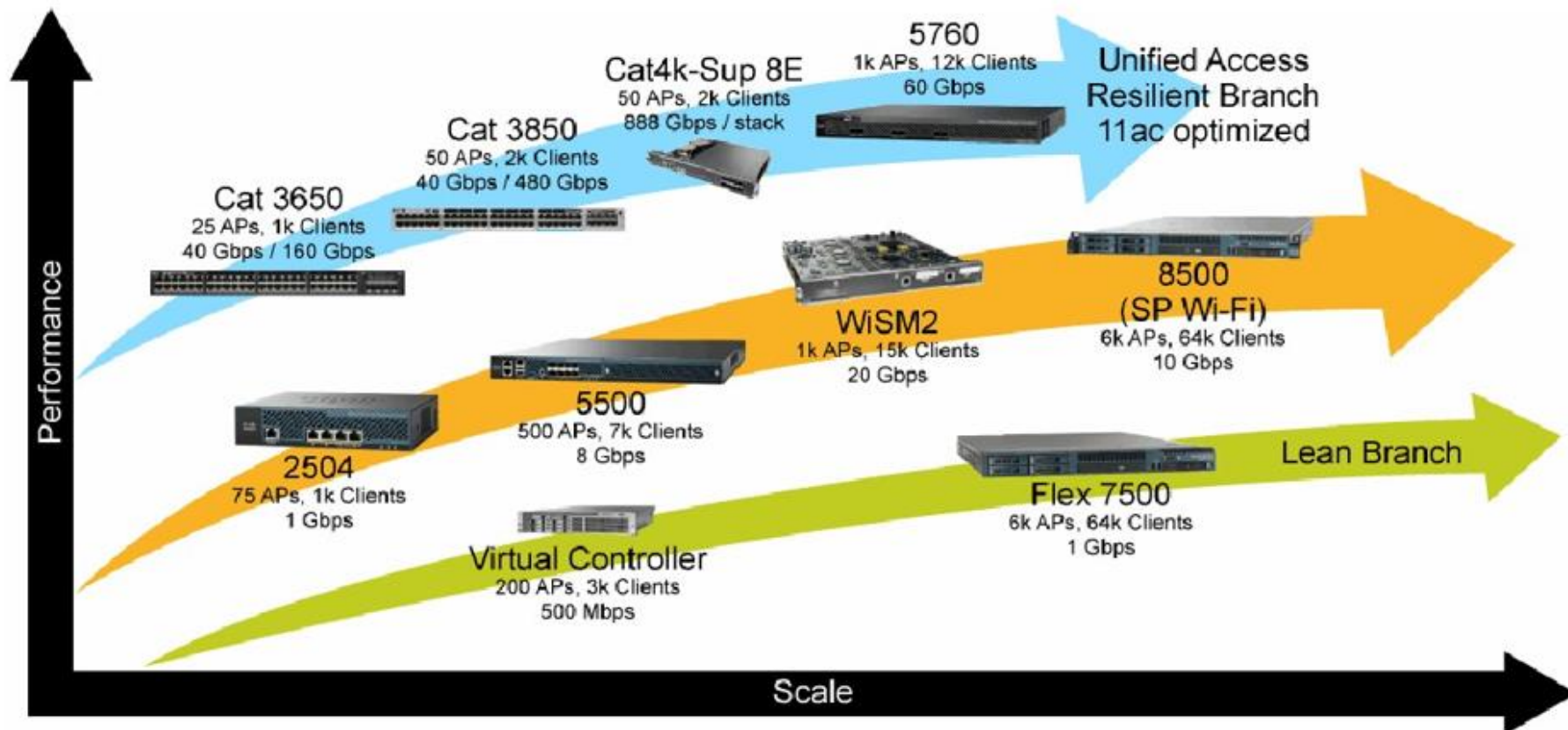
Controllers:  
Integrated 3850/3650  
WLC 5760

# AireOS控制器

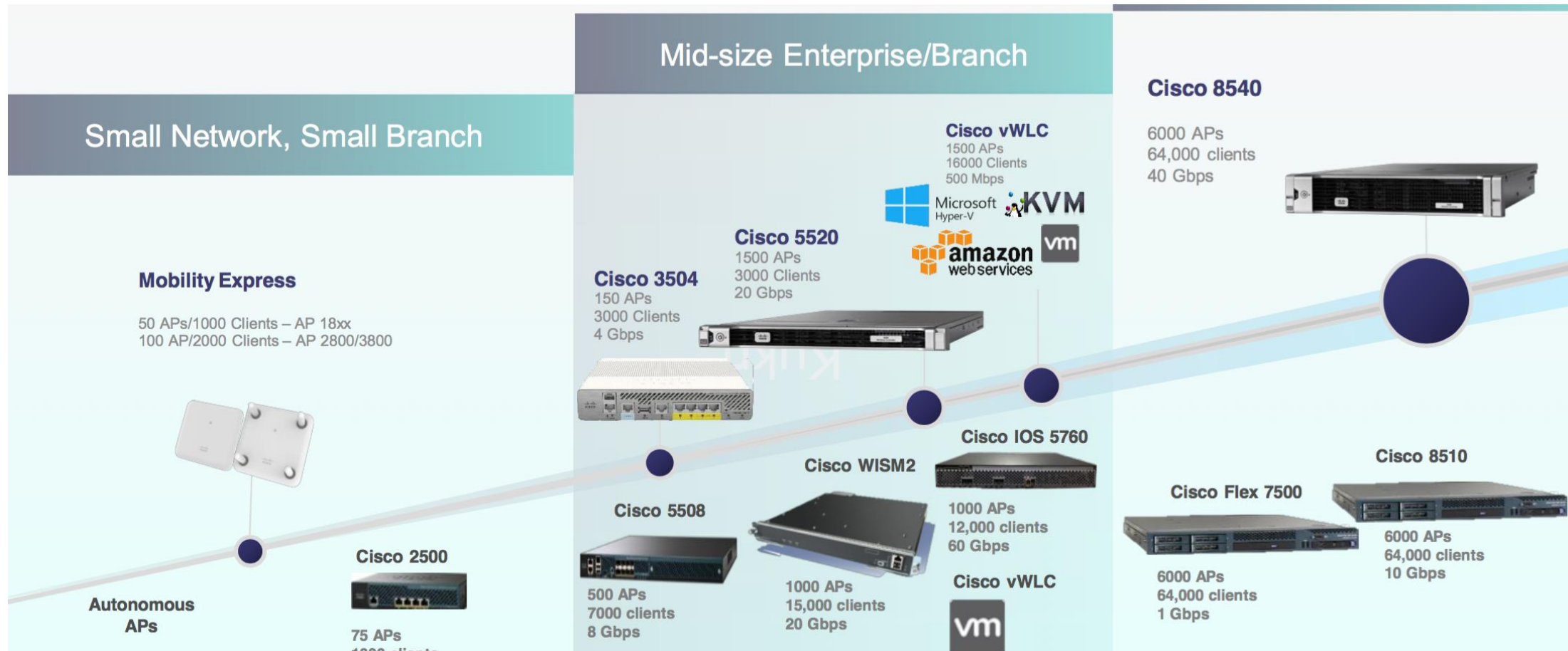
- 支持如下的部署模式
  - FlexConnect
  - 集中部署
  - Mesh
  - OfficeExtend
- 支持大部分无线特性和产品线功能
- GUI和CLI界面
- 一些控制器（Flex 7500和vWLC）不支持所有的部署模式和特性



# 基于无线控制的经典产品线



# 思科最新控制器



150APs

1500-6000APs

# 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



# 模块化和虚拟化的控制器

## WiSM2 (Catalyst6500模块)

- 中型和大的单一站点
- 支持1000个AP和15000个客户端
- 20Gbps吞吐量
- 集成的交换刀片
- 每个chassis支持到7个



## 虚拟化无线控制器 (vWLC)



# 思科Aironet访问点



# 思科最新AP-802.11AC Wave2

DNA Ready | RF Excellence | CMX | Centralized, FlexConnect or Mobility Express

Dual 5 GHz | Flexible Radio | HDX

Future Proof



## 1815

### Indoor / High-powered Indoor Wall Plate / Teleworker

- 2x2:2SS 80 MHz
- 867 Mbps Performance
- Tx Beam Forming
- Integrated BLE Gateway<sup>1</sup>
- Max Transmit Power (dBm) per local regulations<sup>2</sup>
- 3 GE Local Ports, including 1 PoE out<sup>3</sup>
- Local ports 802.1x ready<sup>3</sup>



## 1830

- 3x3:2SS 80MHz
- 867 Mbps Performance
- Tx Beam Forming
- 1 GE Port Uplink
- USB 2.0



## 1850

- 4x4:3SS 80MHz
- 1.7 Gbps Performance
- Internal or External Antenna
- Tx Beam Forming
- 2 GE Ports Uplink
- USB 2.0



## 2800

- 4x4:3SS 160 MHz
- 5 Gbps Performance
- 2.4 and 5GHz or Dual 5GHz
- 2 GE Ports Uplink
- CleanAir and ClientLink
- Internal or External Antenna
- Smart Antenna Connector
- USB 2.0



## 3800

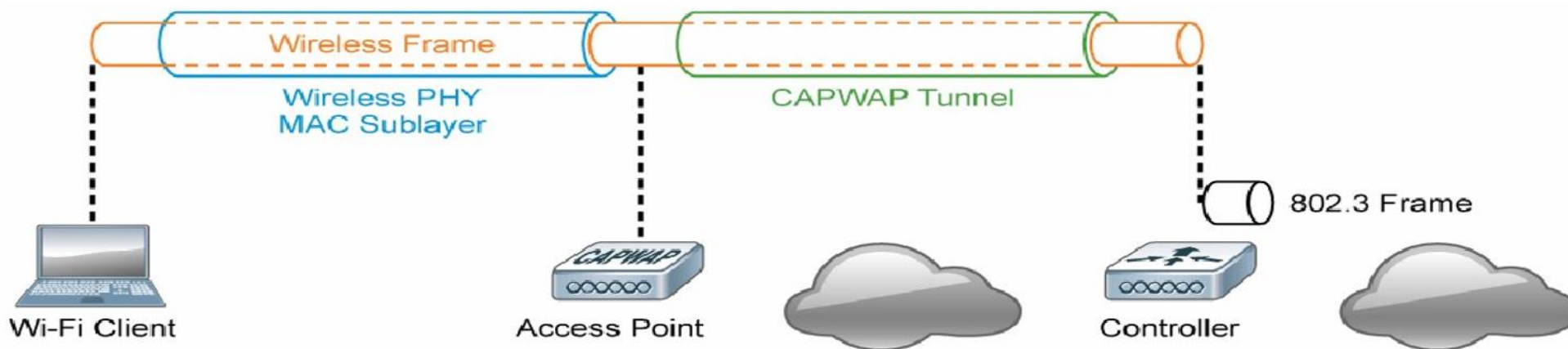
- 4x4:3SS 160 MHz
- 5 Gbps Performance
- 2.4 and 5GHz or Dual 5GHz
- 2 GE Ports Uplink or 1 GE + 1 mGig (5G)
- CleanAir and ClientLink
- StadiumVision
- Internal or External Antenna
- Smart Antenna Connector
- USB 2.0
- Investment Proof Modularity



# 无线基本重要理论

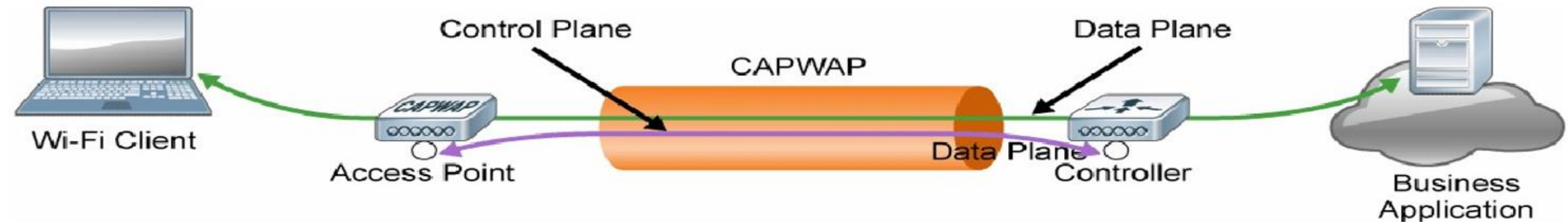
# 什么是CAPWAP

- Control and Provisioning of Wireless Access Points 用于AP和WLAN控制器之间，基于LWAPP运行于IPv4或者IPv6。标准开放协议 IETF RFC
- CAPWAP隧道功能
  - 控制平面 UDP 5246 DTLS加密
  - 数据平面 UDP 5247 加密可选

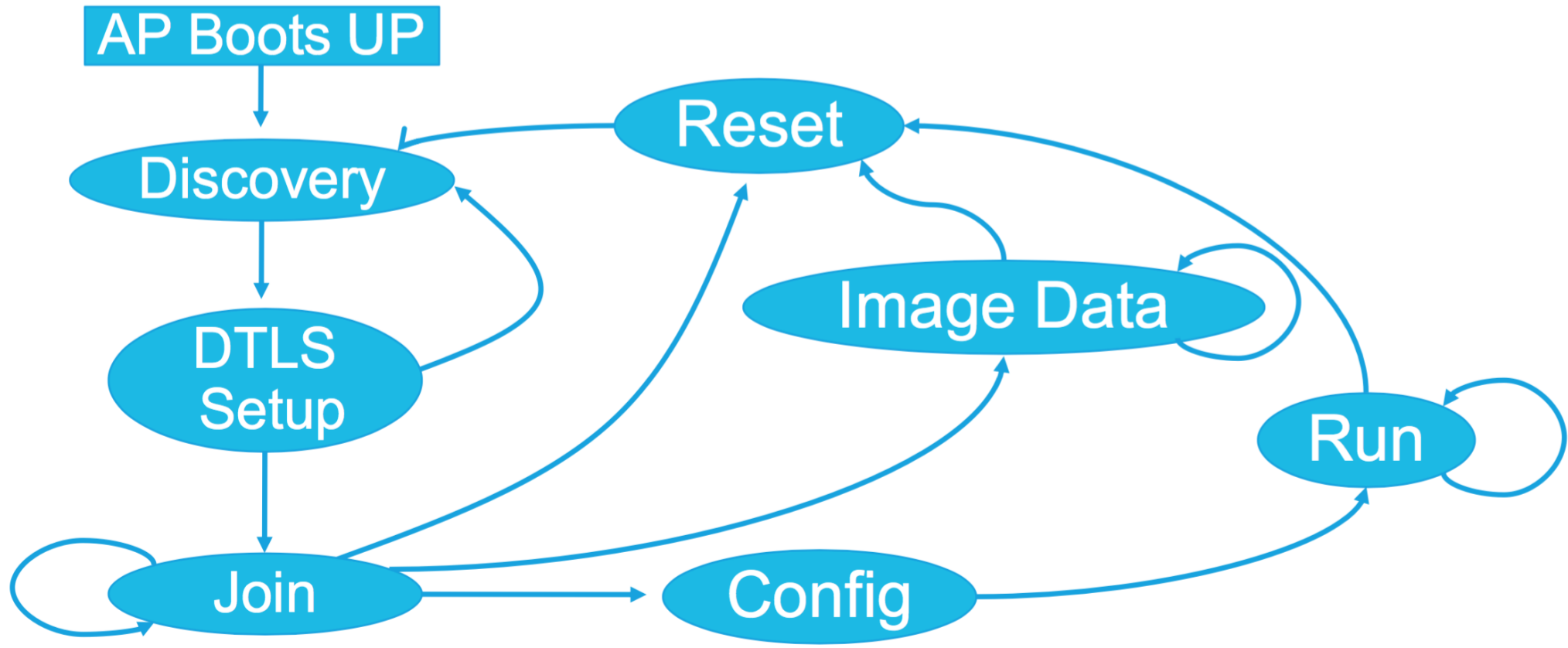


# CAPWAP 续

- 启用LWAPP的AP可以发现和加入CAPWAP控制器。CAPWAP不支持Layer2部署模式。
- 从控制器下推配置和Firmware
- 统计和无线安全。



# CAPWAP状态机/轻量级AP的工作原理

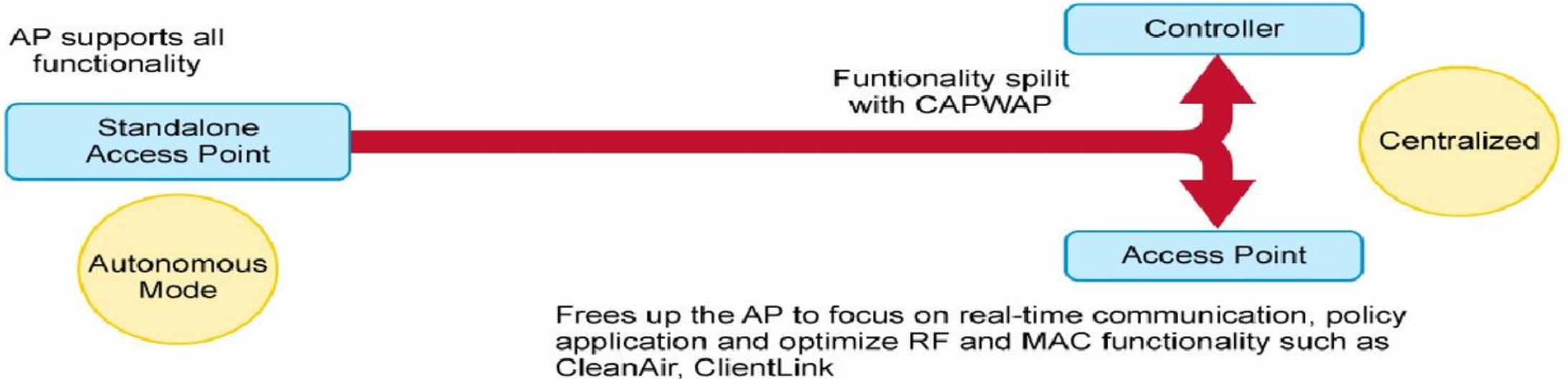


# WLC功能

- 动态分配信道
- 优化发射功率
- 自我修复无线覆盖范围
- 灵活的客户端漫游
- 动态的客户端负载均衡
- RF监控
- 安全性管理

# 思科WLAN体系架构: Split MAC

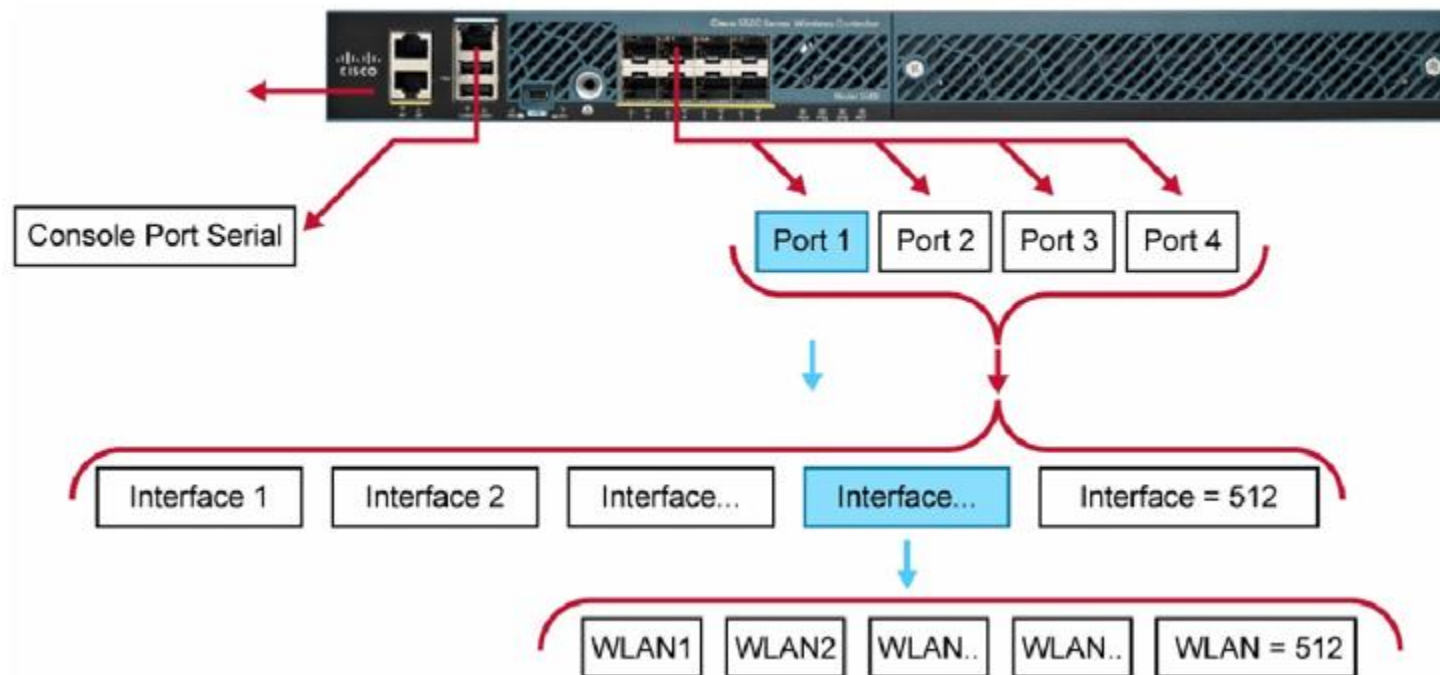
- Centralized tunneling of user traffic to controller (data plane and control plane)
- System-wide coordination for channel and power assignment, rogue detection, security attacks, interference, roaming



# 漫游

- 漫游
  - 无线客户端同谁协商关联 AP or WLC
  - 漫游的时候, 关联发生在哪儿? AP or WLC
- 控制器内漫游
- 控制器间漫游
  - Anchor
  - Ether-IP
- 漫游组

# 控制器端口，接口和映射关系

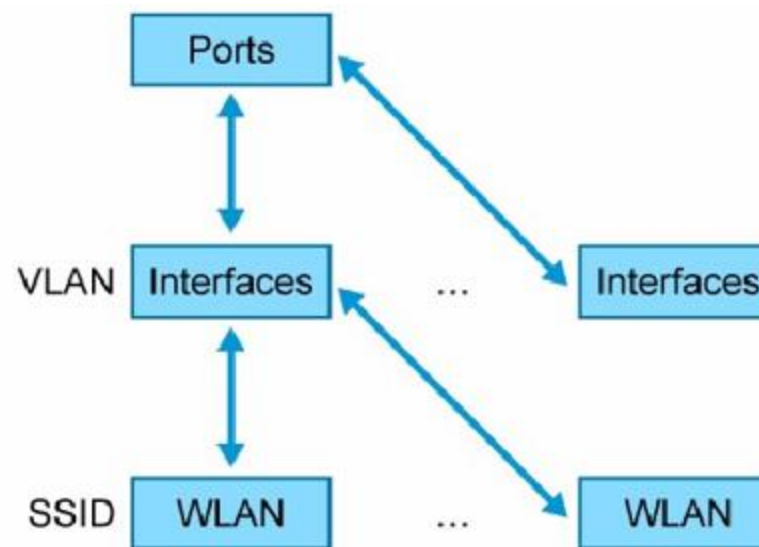




# 物理端口

- 思科无线控制器使用端口：
  - 控制相关的思科无线AP
  - 分布式系统DS接到企业网络
    - 可以分配多个接口道一个物理端口
    - 数据被打标记，在一个trunk口上支持多个VLAN。

- 封装的数据帧头的BSSID识别WLAN和AP
- 传送进入DS端口的VLAN标记



# 逻辑接口

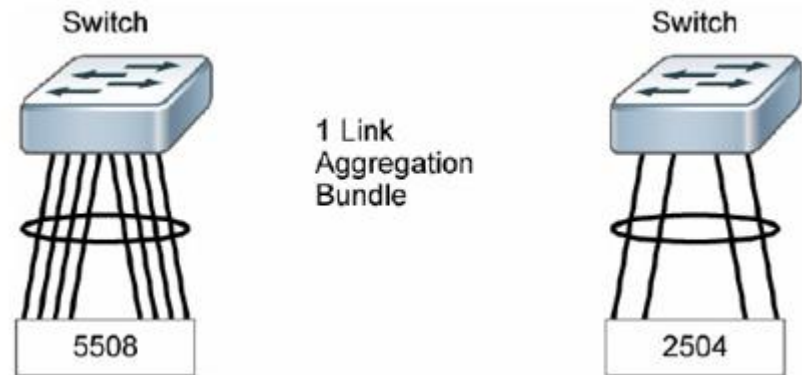
- 思科无线接口配置允许关联一个VLAN的名字到VLAN的ID，然后映射物理端口和WLAN。
  - 必须分发每一个接口道一个端口，为了能够分发到企业网络。
  - 不能分发多个物理端口到一个接口。
  - 可以分发多个WLAN到一个接口。
- VLAN ID可以表示未打标流量（0）或者IEEE802.1Q标记流量（1-4095）。
  - 可以分配多个接口到一个端口。
- 多种接口：
  - 静态-管理（缺省AP管理），服务端口，虚拟接口
  - 动态接口-用户定义。

# 管理接口

- 带内管理
- 连接到企业服务例如AAA
- 控制器和AP之间的通信

# 链路聚合

- 链路聚合- 不需要配置基本和第二个端口，简化了在控制器上的冗余设置。
- 如果控制器的一个口挂掉，流量自动切换到其他的端口。
- 只要有一个控制器的端口存活，系统将继续运行，AP保持连接到网络，无线客户端可以继续发包。



# 服务接口

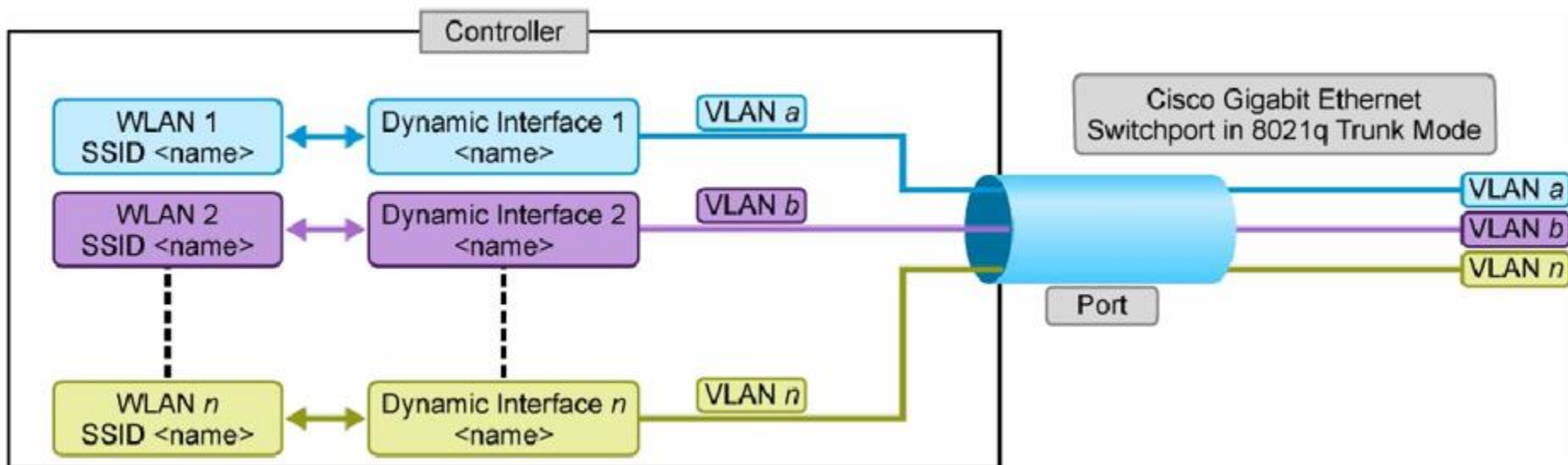
- 无线控制器的物理端口
- 前面板10/100/1000 Base-T专用带外管理
- 服务端口不会autosensing。

# 虚拟接口

- 漫游管理
  - 移动客户端使用同一个虚拟IP地址跨越多个控制器。
- DHCP Relay
  - 客户端使用虚拟IP地址作为DHCP服务器地址。
- 三层安全
  - Web认证使用虚拟接口作为网关IP地址。

# 动态接口

- 也被称为VLAN接口
- 管理员需要手工配置如下接口
- 为无线客户端配置DHCP relay
- 多个WLAN SSID映射到一个动态接口

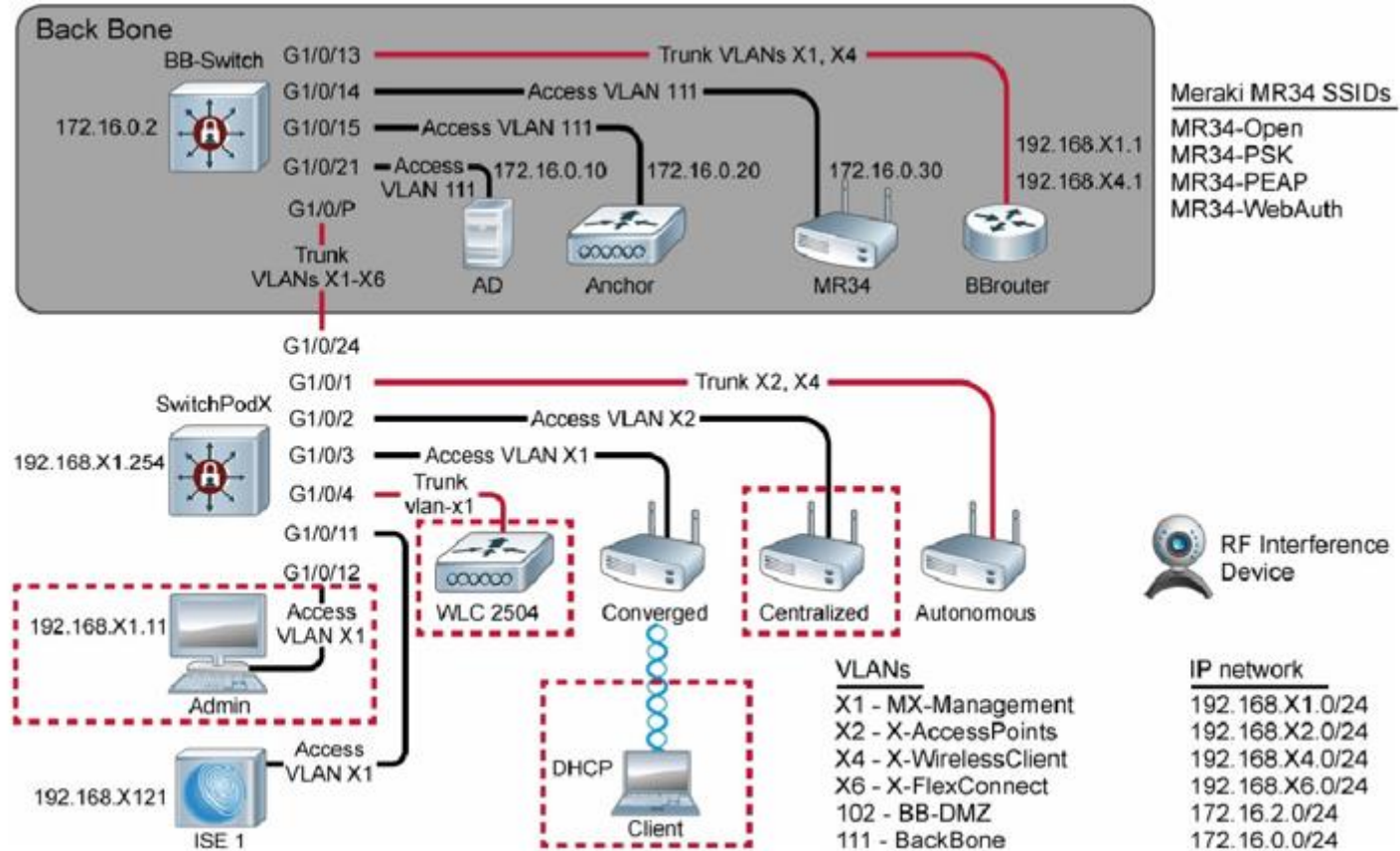


# 网管软件PI2.X和WLC

- 从Prime Infrastructure配置和监控WLC
- AireOS 8.X WLC只能被PI2.2或者更高版本管理
- PI使用WLC模板添加或者更改WLC
- PI管理和监控如下设备:
  - WLC
  - AP
  - 客户端设备



# 初始化集中的WLAN部署



# 无线配置流程及相关配置内容

### 图例

无线控制器物理接口

无线控制器逻辑接口

配置步骤

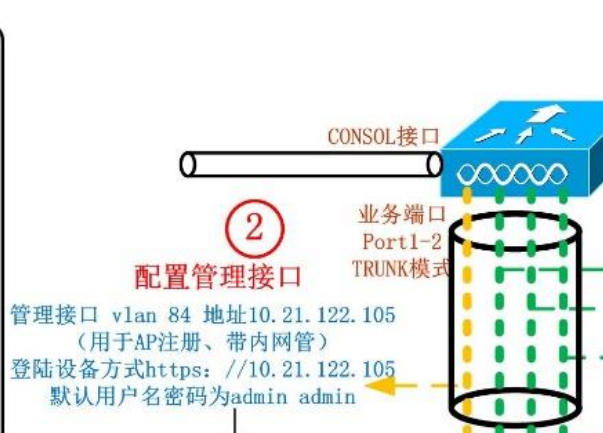
配置顺序

关联内容

物理接口说明 **褐色字体**

逻辑接口说明 **蓝色字体**

接入交换机及AP对于无线部分无需特殊配置，仅需将AP接口划分到AP VLAN中即可，本次项目规划AP VLAN为83



Service-port  
用于带外网管，配置为同一网段即可通过网页登陆设备

Interfaces > Edit

General Information

Interface Name: service-port  
MAC Address: 4c4d397a884c

Interface Address

DHCP Protocol:  Enable

IP Address: 192.168.1.1  
Netmask: 255.255.255.0

**1 DHCP配置**

两台核心6509 DHCP配置

```

ip dhcp pool AP #AP地址池#
network 10.21.122.192 255.255.255.192 #AP地址段#
default-router 10.21.122.254 #AP默认网关#
option 43 hex f108.0a15.7a69
#option 43用于通告AP控制器地址用于注册，f108为固定字段，0a15.7a69为无线控制器管理接口地址
option 60 ascii "Cisco AP c1240" #通告AP型号#
ip dhcp pool WUXIANYONGHUJIERU
network 10.21.119.0 255.255.255.0 #无线用户地址段#
default-router 10.21.119.254 #AP默认网关#
dns-server 219.149.194.55 219.146.0.130 #用户DNS服务器#
    
```

! WUXIANFANGKE1及WUXIANFANGKE2配置同WUXIANYONGHUJIERU类似，此处不做一一列举

Interfaces

Interface Name	VLAN Identifier	IP Address	Interface Type	Dynamic AP Management
management	84	10.21.122.105	Static	Enabled
service-port	N/A	192.168.1.1	Static	Not Supported
virtual	N/A	1.1.1.1	Static	Not Supported
yqjr-guest-wireless-1	81	10.21.120.123	Dynamic	Disabled
yqjr-guest-wireless-2	82	10.21.120.251	Dynamic	Disabled
yqjr-wireless	80	10.21.119.251	Dynamic	Disabled

Interface Name	VLAN Identifier	IP Address	Interface Type	Dynamic AP Management
84	84	10.21.122.105	Static	Enabled
81	81	10.21.120.123	Dynamic	Disabled
82	82	10.21.120.251	Dynamic	Disabled
80	80	10.21.119.251	Dynamic	Disabled

Port Number	Backup Port	Active Port	Enable Dynamic AP Management
1	2	1	<input type="checkbox"/>

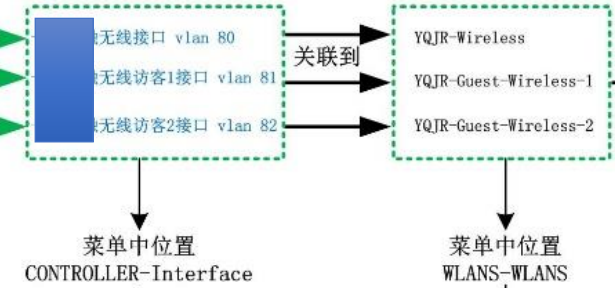
  

Port Number	Backup Port	Active Port	Enable Dynamic AP Management
1	2	1	<input type="checkbox"/>

**3 配置用户接口**

**4 无线配置**

**5 配置AP组，将AP加入到AP组中**



WLANS > New

Type: WLAN

Profile Name: YQJR-Wireless

SSID: YQJR-Wireless

ID: 79

WLANS > Edit

General Security QoS Advanced

Security Policy: [None]

Radio Policy: [None]

Interface: [Selected Interface]

WLANS > Edit

General Security QoS Advanced

Layer 2 Security: WPA/WPA2

WPA/WPA2 Parameters: WPA2 Encryption: AES, WPA2 Key Mgmt: GTKP

将注册上的AP加入自定义AP组，并将SSID和WLAN进行管理，即可搜索到无线信号并连接使用  
此处定义AP组为yqjr，关联内容如下

WLAN ID	WLAN SSID	Interface Name	Status
80	YQJR-Wireless	yqjr-wireless	Disabled
81	YQJR-Guest-Wireless-1	yqjr-guest-wireless-1	Disabled
82	YQJR-Guest-Wireless-2	yqjr-guest-wireless-2	Disabled

AP Groups

Add New AP Group

AP Group Name: yqjr

AP Group Description: yqjr

Ap Groups > Edit 'yqjr'

General WLANS APs

Add New

WLAN ID: 80, WLAN SSID: YQJR-Wireless, Interface Name: yqjr-wireless, Status: Disabled

Ap Groups > Edit 'yqjr'

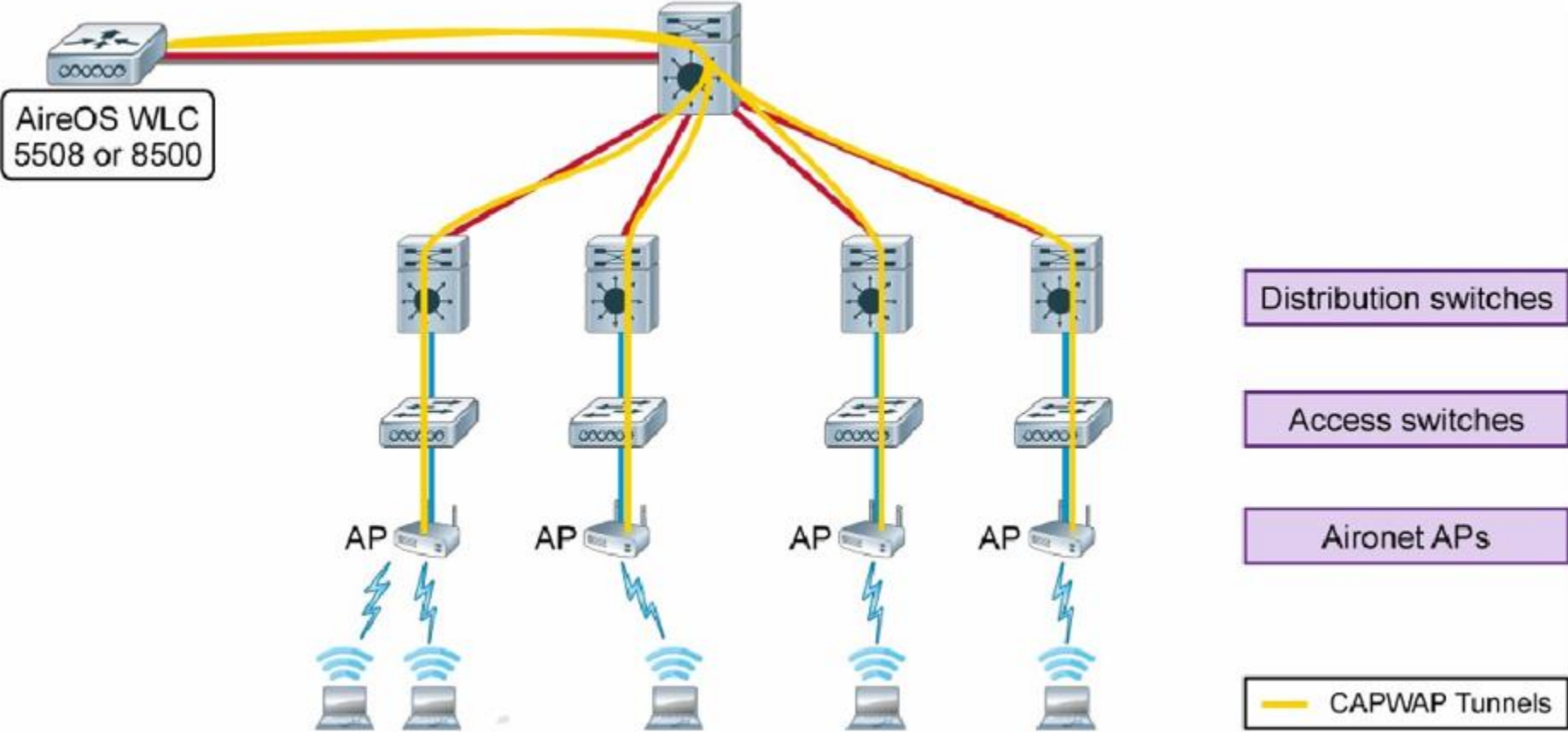
General WLANS APs

APs members in the Group

AP Name: yqjr-wireless, WLAN ID: 80, Status: Disabled

初始化WLC

# AireOS WLC部署配置



# WLC命令行界面

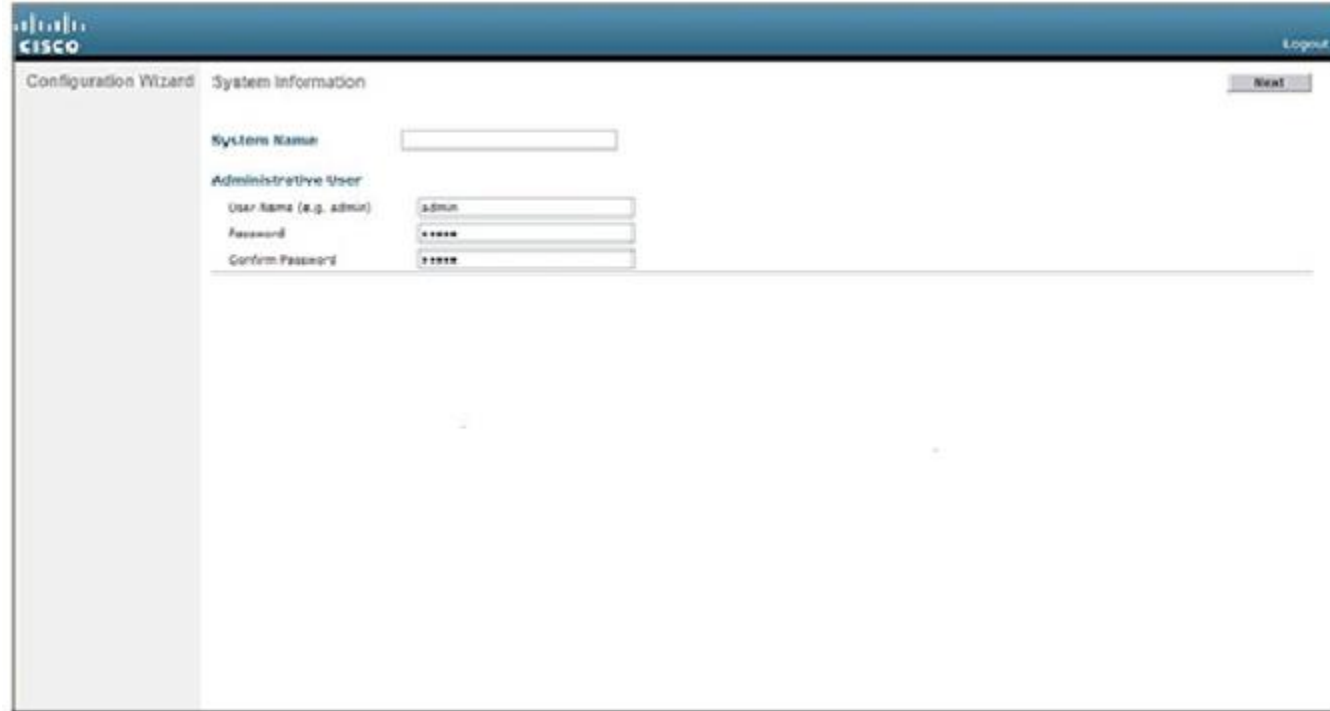
- Telnet
- SSH
- Console Port
  - RJ-45 port on all current models
  - WLC 5500 系列有mini USB口
  - 缺省端口配置
    - 9800波特率, 8数据位, 1个停止位, 没有奇偶校验, 不能做硬件流控

# WLC AireOS命令行设置向导

- 串行控制端口连接
  - 使用VT-100模拟器，设置参数
- 加电，观察输出

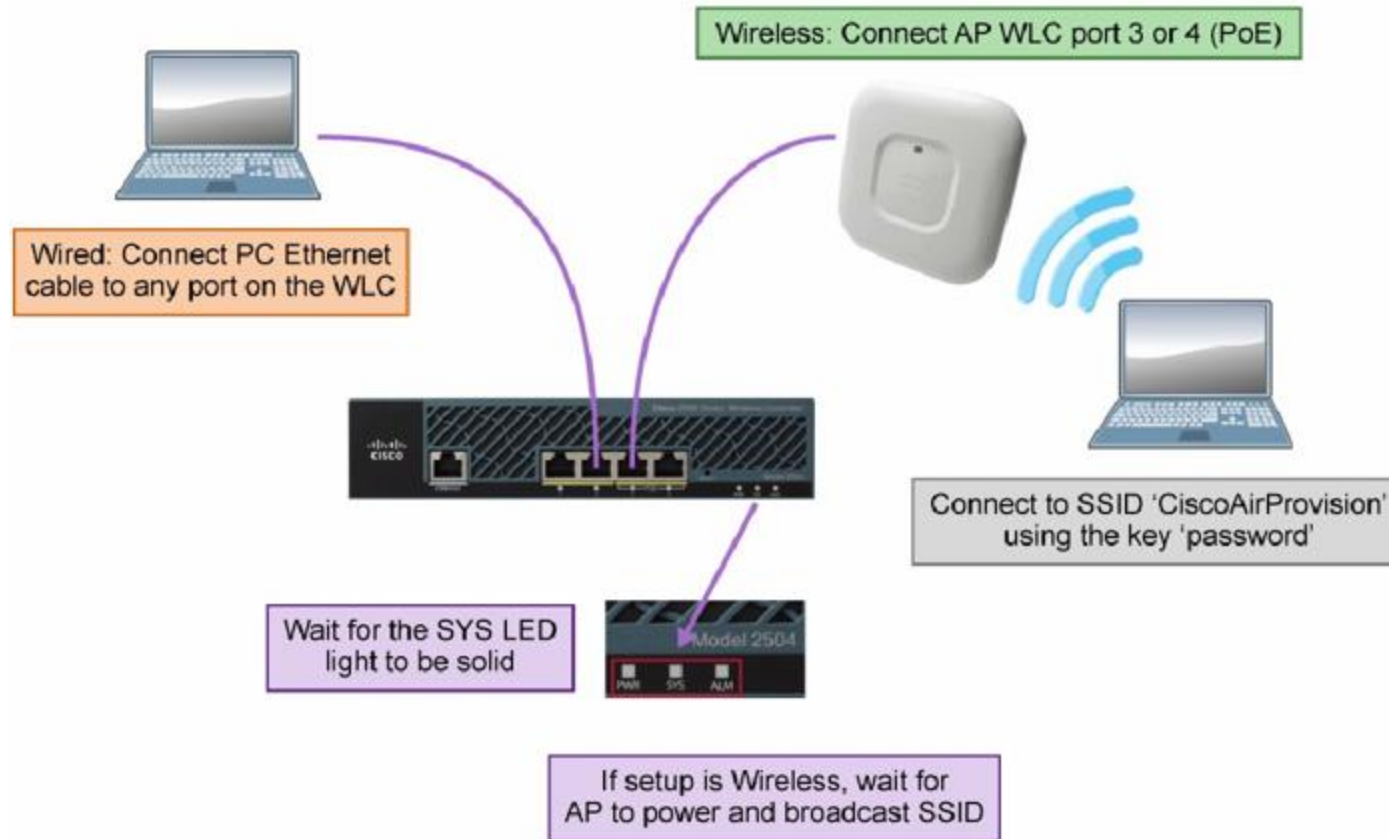
# WLC AireOS图形界面设置向导

- WLC 5500
- 连接PC到服务端口
- 浏览器输入<http://192.168.1.1>
- 配置向导开始



The screenshot shows the Cisco Configuration Wizard interface for System Information. The page includes a 'System Name' field, an 'Administrative User' section with 'User Name (e.g. admin)', 'Password', and 'Confirm Password' fields, and a 'Next' button in the top right corner. The Cisco logo is visible in the top left, and a 'Logout' link is in the top right.

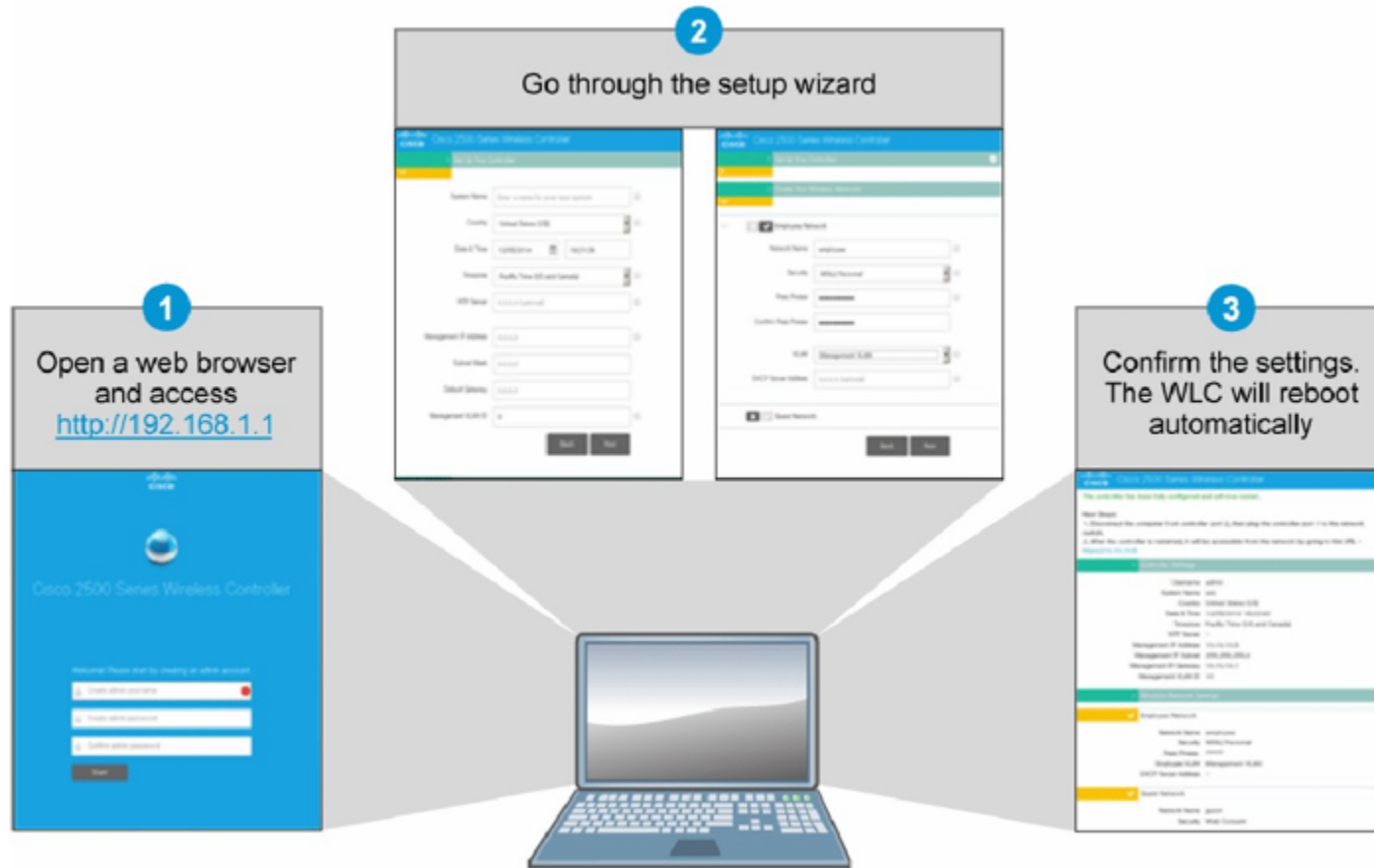
# WLAN精简设置 (WES)



Example: WLC 2504



# WES续



# WES续

- WES缺省参数变为：
  - 会话超时关闭
  - Aironet IE没有勾上
  - Profiling启用
  - Guest ACL应用到Guest SSID
  - CleanAir和EDRRM启用
  - 5GHZ信道绑定启用 (40MHZ)
  - AVC启用
  - 无线管理和Web访问 (HTTP/HTTPS)
  - 虚拟IP地址是192.0.2.1
  - RF组的名字是“default”

# WLC登陆界面选项

- 登陆界面-HTTP或者HTTPS



# WLC登陆界面选项-续

- 缺省登陆界面-仪表盘

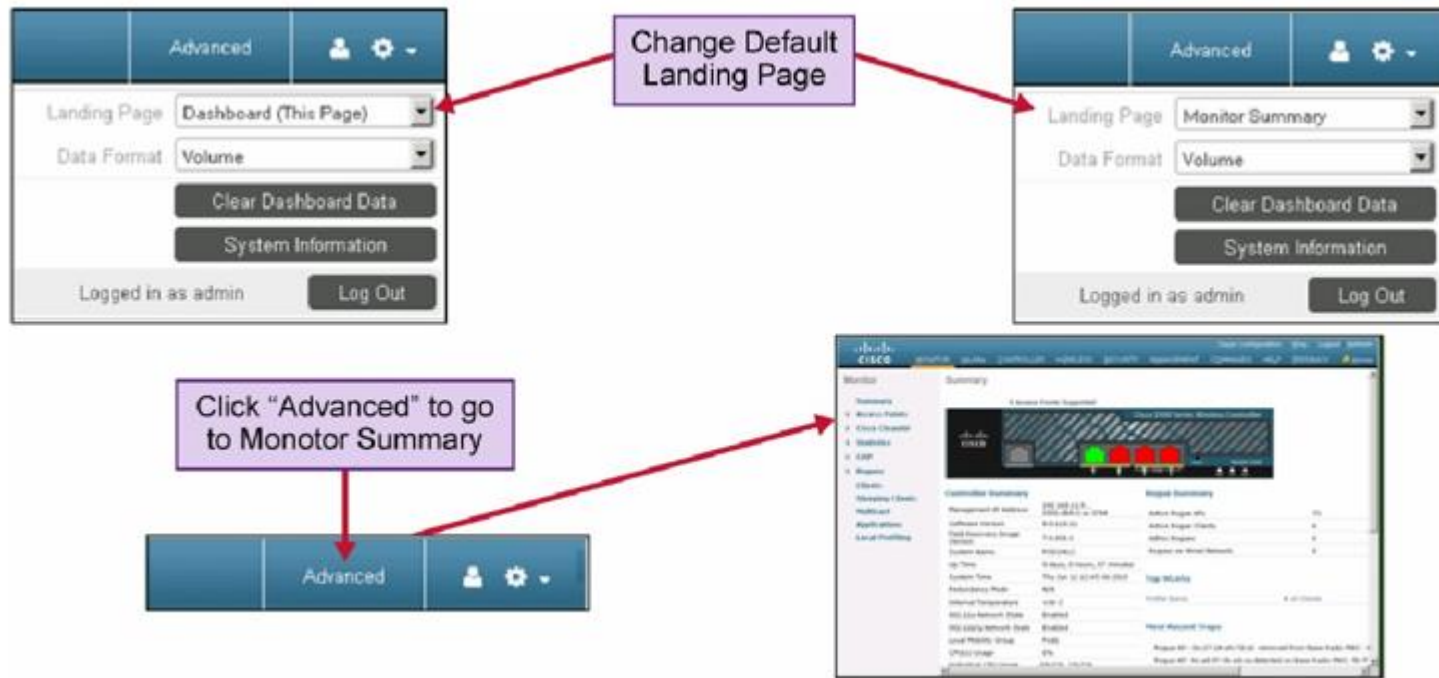
Switch from Table to Pie Chart

Elements are clickable links to interface or item



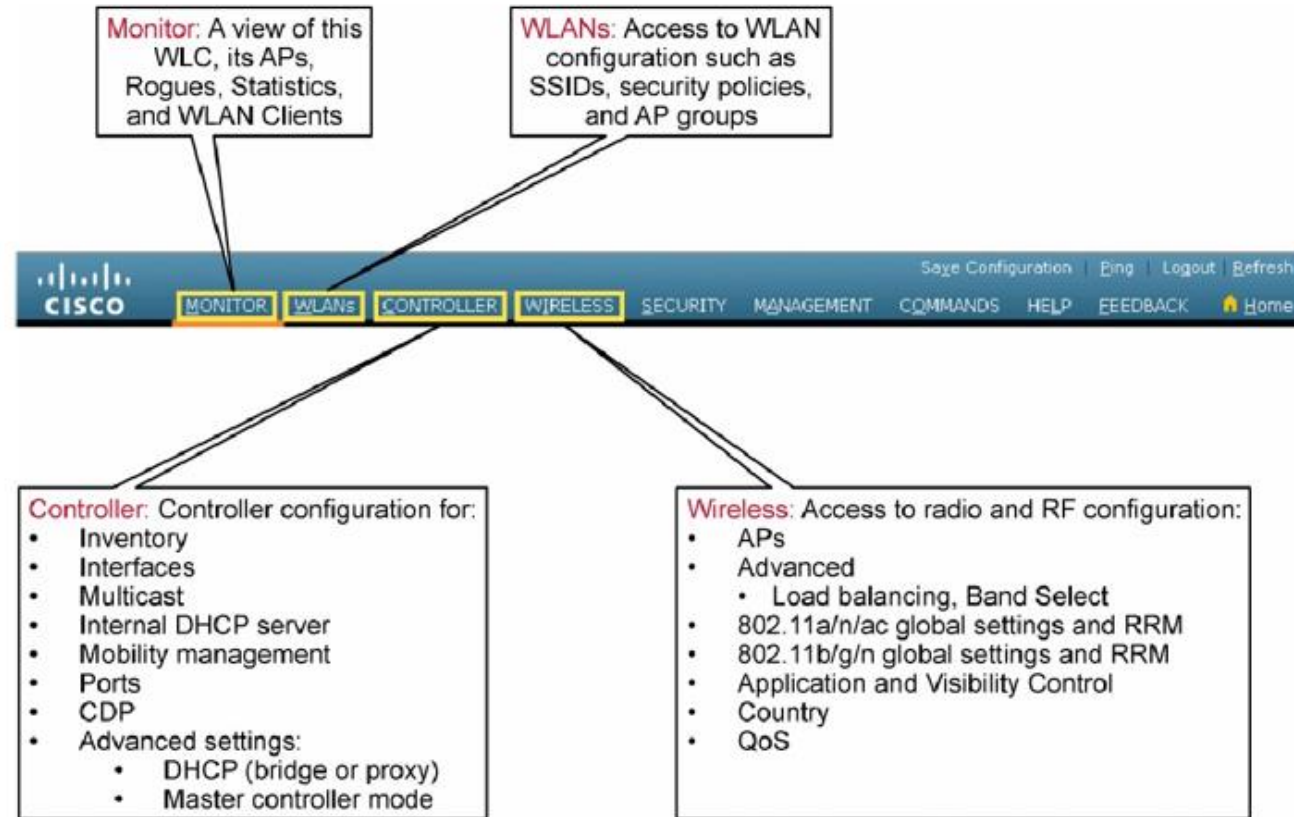
# WLC登陆界面选项-续

- 监控汇总屏幕



# WLC高级菜单选项

## WLC Advanced Menu Tabs



# WLC高级菜单选项-续

**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.)

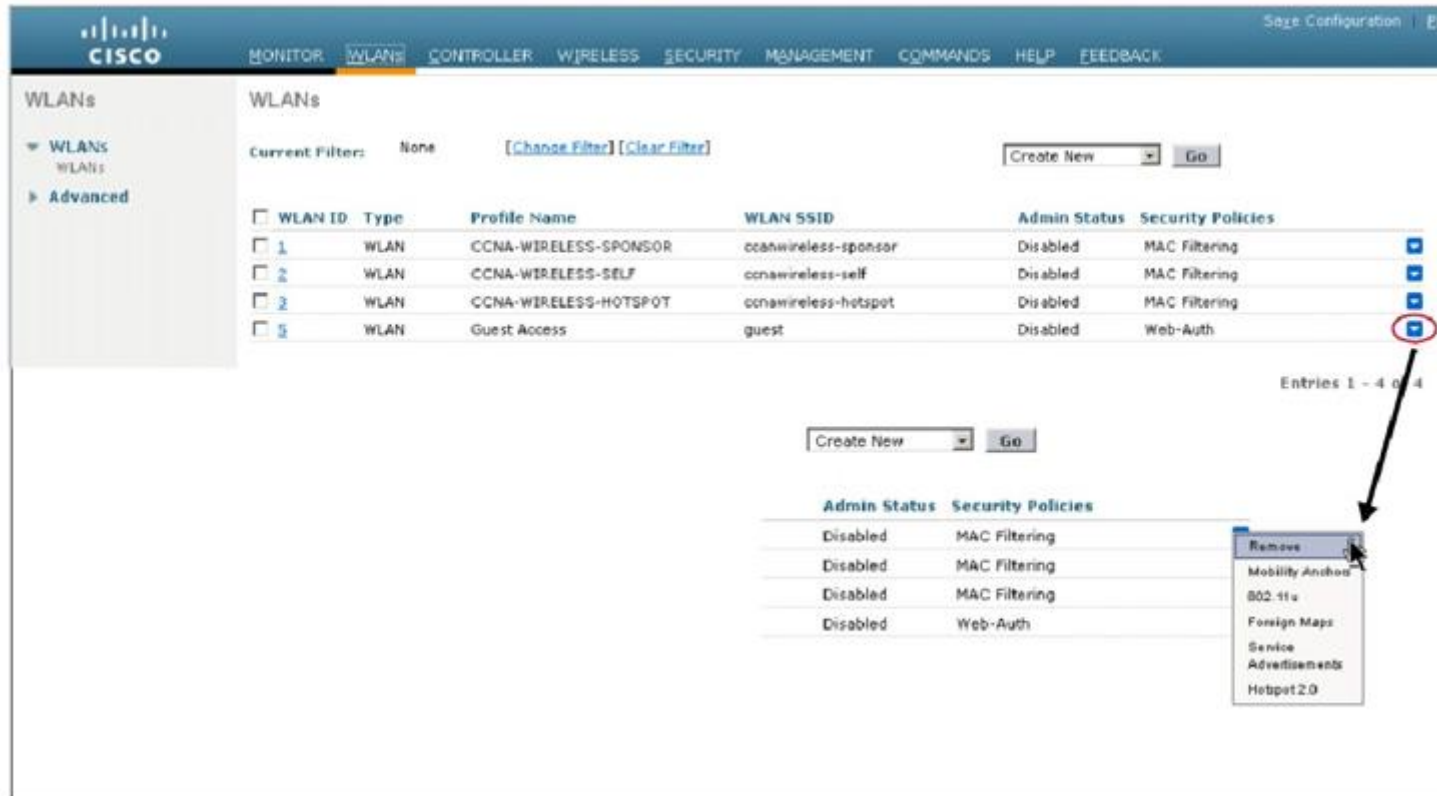
**Commands:** Provides access to administrative options such as file uploads and downloads, configuration reset, controller reboots, manual time configuration, and login banner download.



**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高级菜单选项-续



The screenshot shows the Cisco WLC Advanced menu for WLANs. The interface includes a navigation bar with tabs for MONITOR, WLANs, CONTROLLER, WIRELESS, SECURITY, MANAGEMENT, COMMANDS, HELP, and FEEDBACK. The main content area displays a table of WLANs with columns for WLAN ID, Type, Profile Name, WLAN SSID, Admin Status, and Security Policies. A red circle highlights the dropdown arrow for the third WLAN entry (WLAN ID 3). An arrow points from this dropdown to a secondary menu that lists various advanced options: Remove, Mobility Anchor, 802.11u, Foreign Maps, Service Advertisements, and Hotpot2.0.

WLAN ID	Type	Profile Name	WLAN SSID	Admin Status	Security Policies
1	WLAN	CCNA-WIRELESS-SPONSOR	ccnawireless-sponsor	Disabled	MAC Filtering
2	WLAN	CCNA-WIRELESS-SELF	ccnawireless-self	Disabled	MAC Filtering
3	WLAN	CCNA-WIRELESS-HOTSPOT	ccnawireless-hotspot	Disabled	MAC Filtering
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 Anchor
- 802.11u
- Foreign Maps
- Service Advertisements
- Hotpot2.0



AP初始化

# AP发现过程

- AP CAPWAP发现综述
- AP使用DHCP发现获取地址
- AP使用三层WLC发现
  - CAPWAP子网内发送广播
  - 控制器存储了上次成功加入过程使用的IP地址
  - DHCP选项43
  - DNS解析CISCO-CAPWAP-CONTROLLER

# AP CAPWAP发现

- AP获取IP地址
  - 静态定义
  - DHCP发现
- 三层WLC发现顺序
  - 子网广播模式
    - 直接连接思科AP，同一个子网，思科WLC学习控制器IP地址
    - 思科AP将会发送子网广播
  - 本地存储
    - AP将发送子网广播给之前关联的控制器，即使重启他也会存储信息

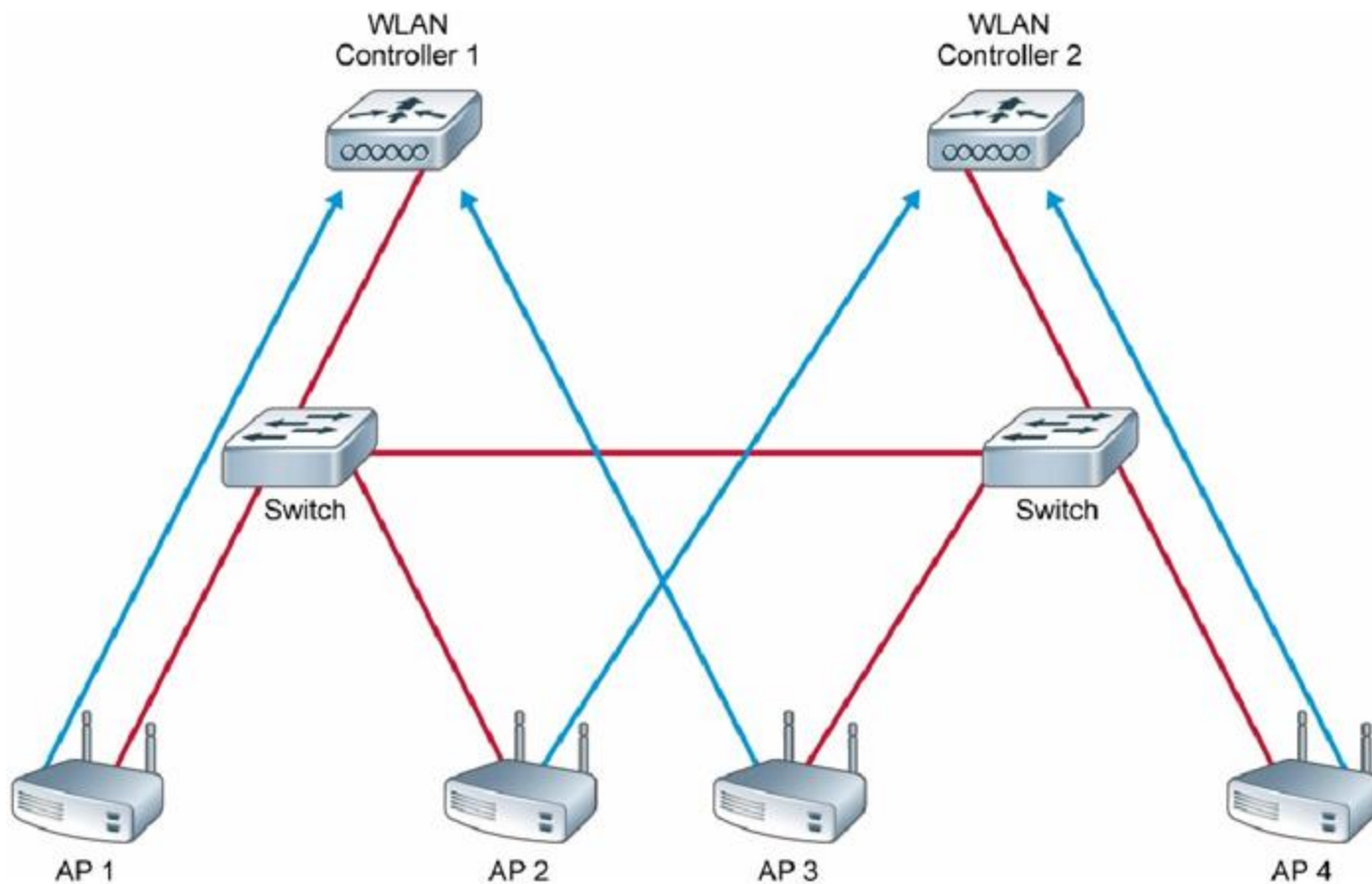
# AP CAPWAP发现-续

- DHCP厂家选项模式:
  - AP放置在远端网络，使用DHCP获取本地和网关地址
  - 使用DHCP扩展区学习思科WLC管理接口IP地址，以扩展的Option 43模式。
- DNS模式
  - AP放置在远端网络，使用DHCP获取本地和网关地址
  - 使用DHCP扩展学习DNS IP地址
  - 思科AP使用主机解析，配置返回有效的控制器IP地址。

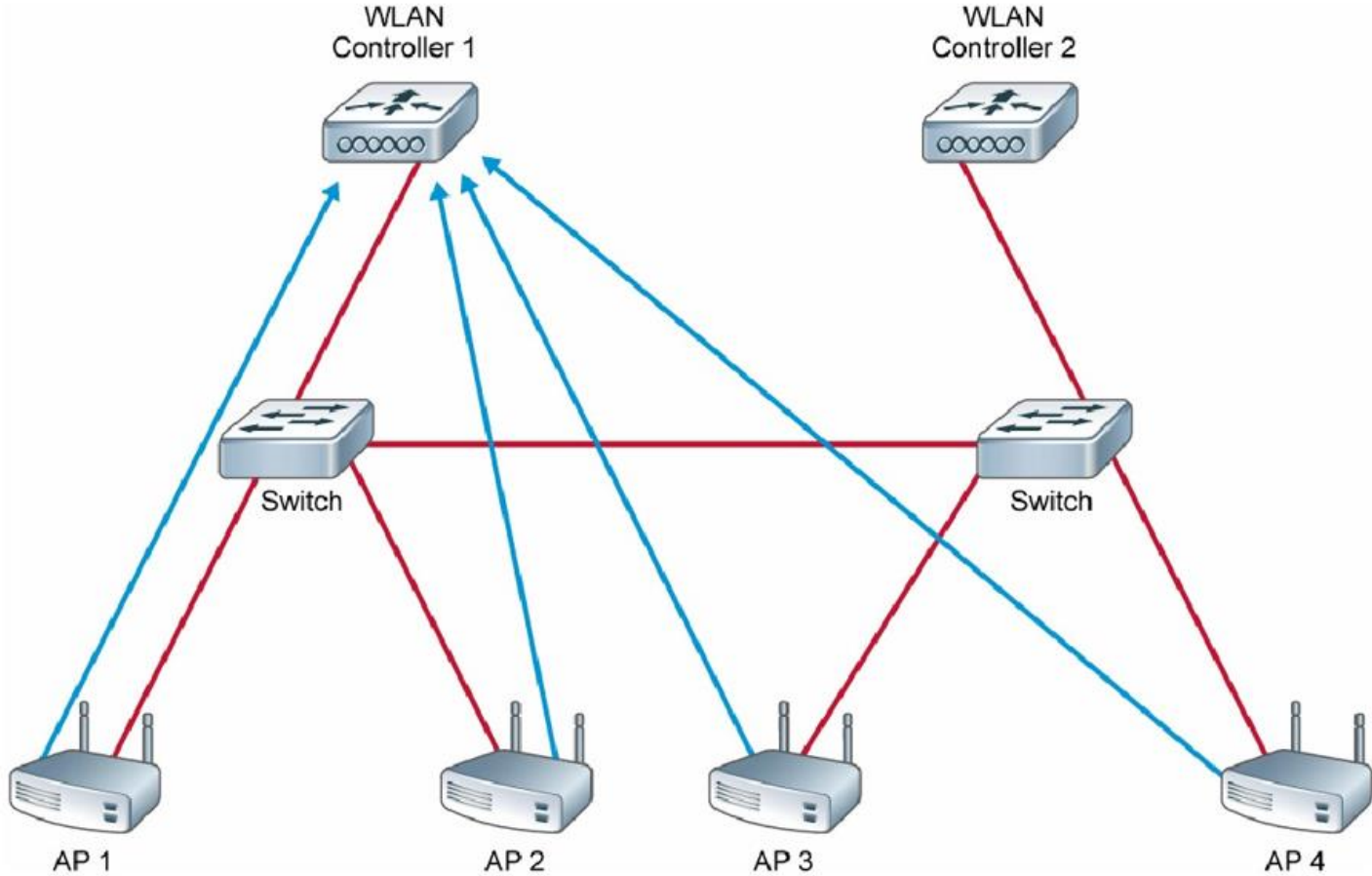
# AP加入顺序

- 响应顺序: Primary, secondary, tertiary
- 没有配置WLC, 从master控制器响应
- 如果内有master控制器响应, 从最近加载过得WLC响应
- 加载WLC

# AP加入步骤：没有Master

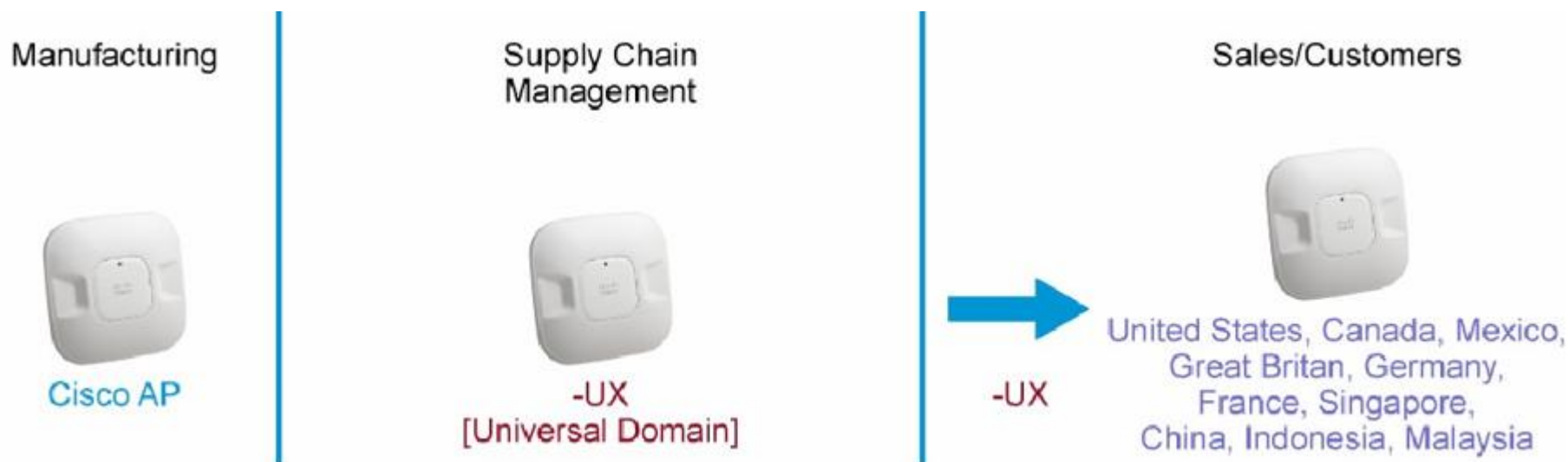


# AP加入步驟：有Master



# Universal AP Priming

- Universal AP Priming – 新特性 – 综述
- AP通用（没有国家指定）
- 地理范围
- 手动设置或者自动化的Priming

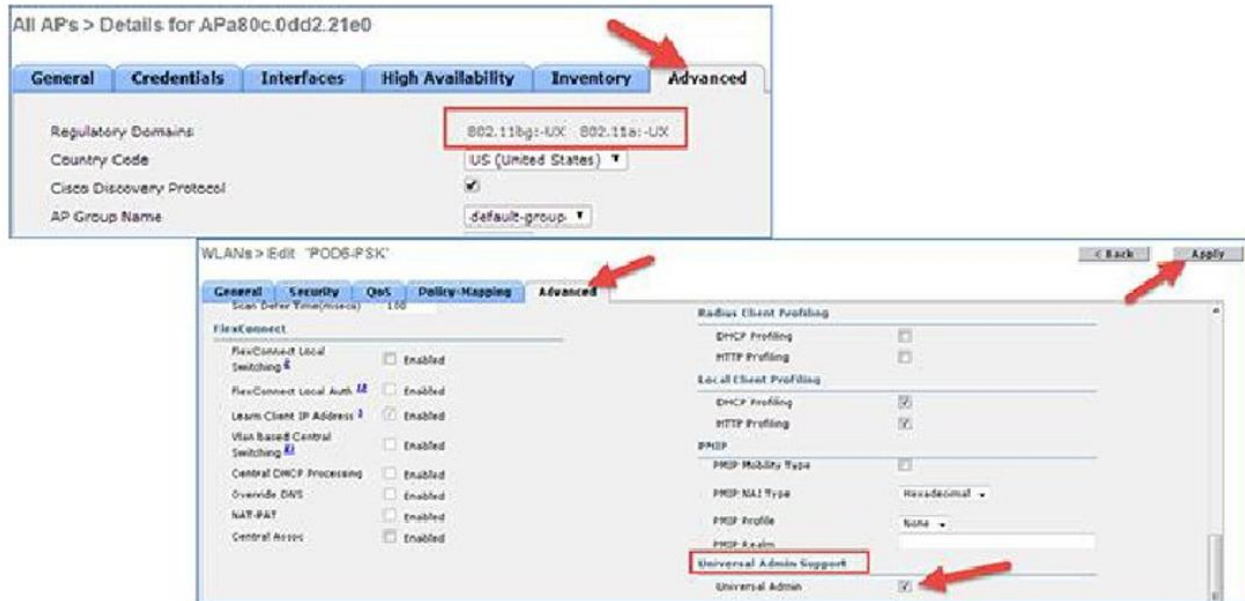




# Universal AP Priming-手动配置

- 手动Priming配置步骤

- 步骤1: AP加入, 作为universal域-UX AP
- 步骤2: 在WLC上启用Universal区域支持



# Universal AP Priming-手动配置 续

- 手动Priming配置步骤
  - 步骤3: 通过思科AirProvision APP进行Priming

Download AirProvision app and login with CEC credentials

Cisco AirProvision

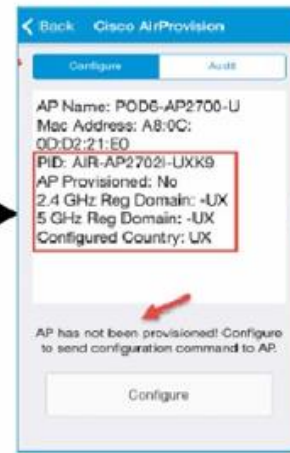


Connect to Universal Admin SSID



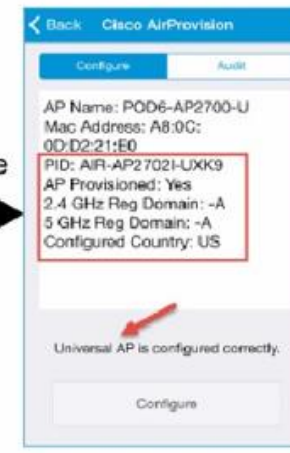
Log In

Shows Unprimed with UX Domain



Configure

Comes Back up with Correct Domain



# Universal AP Priming-自动配置

- 自动Priming配置步骤
  - 步骤1: 通用AP启动并加入WLC。
  - 步骤2: 通用AP从邻居的universal AP的NDP信息扫描2.4GHz和5GHz频宽。
  - 步骤3: 如果自动的priming有效, 然后universal AP接受国家信息, 重启和重新加入控制器作为一个primed AP。
  - 步骤4: 如果自动priming无效或者不能工作, 轻量级AP等你手动prime它。

# AP失效切换步骤

- 基本WLC失效，AP会切换到备份的WLC。
- 当基本的WLC重新在线，AP缺省会切回基本的WLC。
- 心跳验证AP到WLC的可达性。
- 心跳ACK验证WLC是否可达。
- 心跳30秒发送一次。
- 心跳收不到ACK，将会在被宣判不可达前每隔秒重发五次。

# AP失效切换优先级

- 独立的AP设置
- WLC无线全局设置识别失效切换优先级。

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

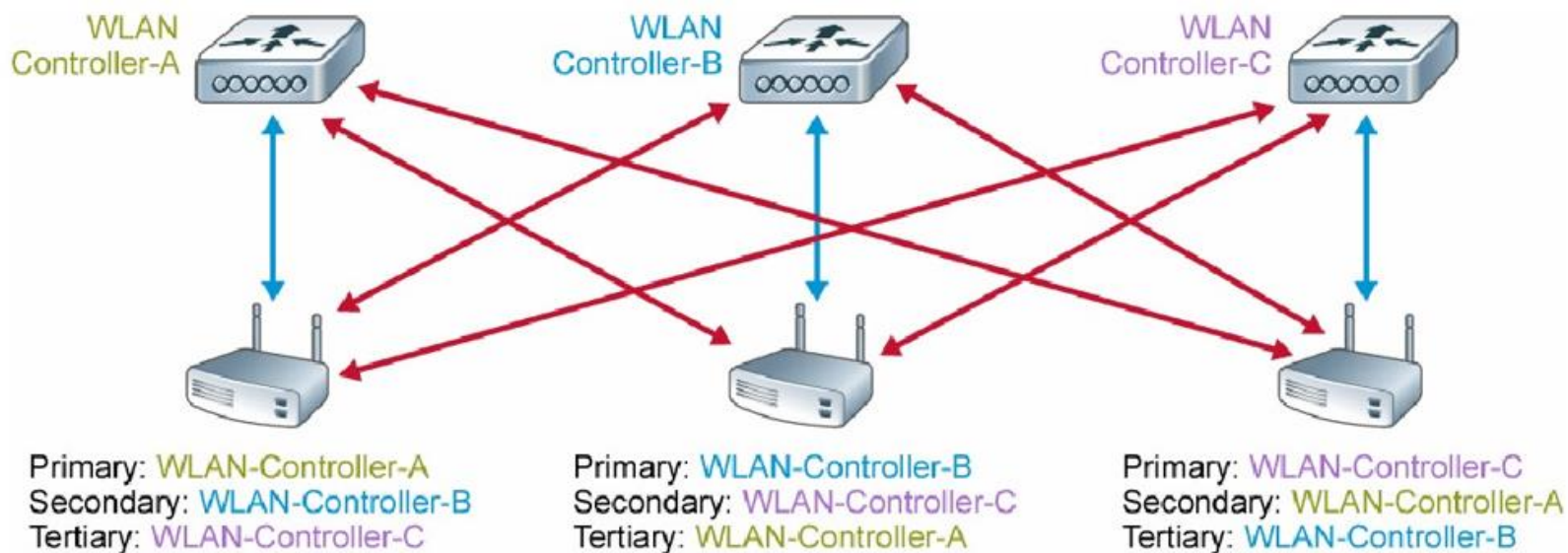
# AP回切

- 全局WLC控制器设置

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

# 解释高可用性

Controller Redundancy: N + 1 Failover

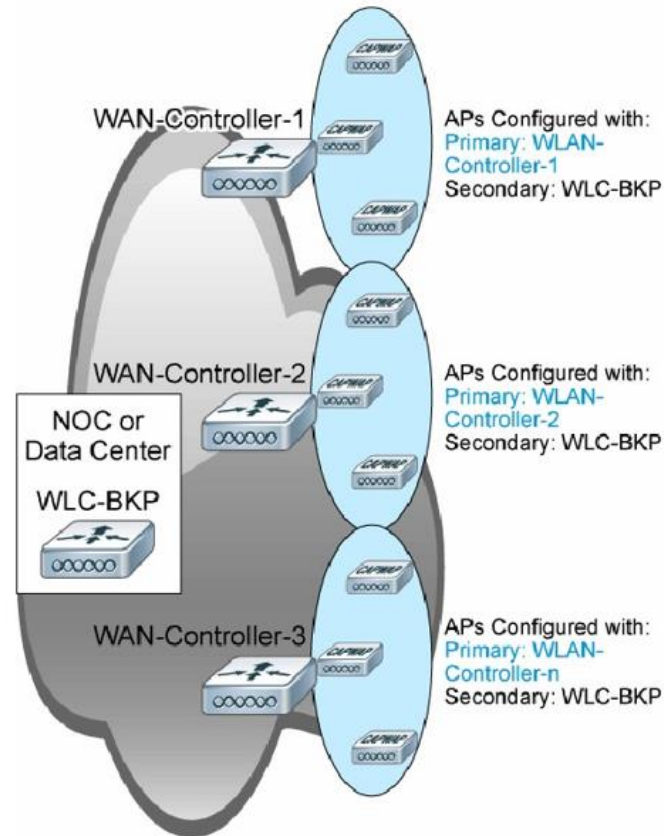


All APs > Details for Centralized\_AP

	Name	Management IP Address (IPv4/IPv6)
Primary Controller	192.168.11.5	[wlc1]
Secondary Controller	192.168.11.8	[wlc2]
Tertiary Controller	192.168.11.9	[wlc3]

# 控制器冗余：N+1 失效切换

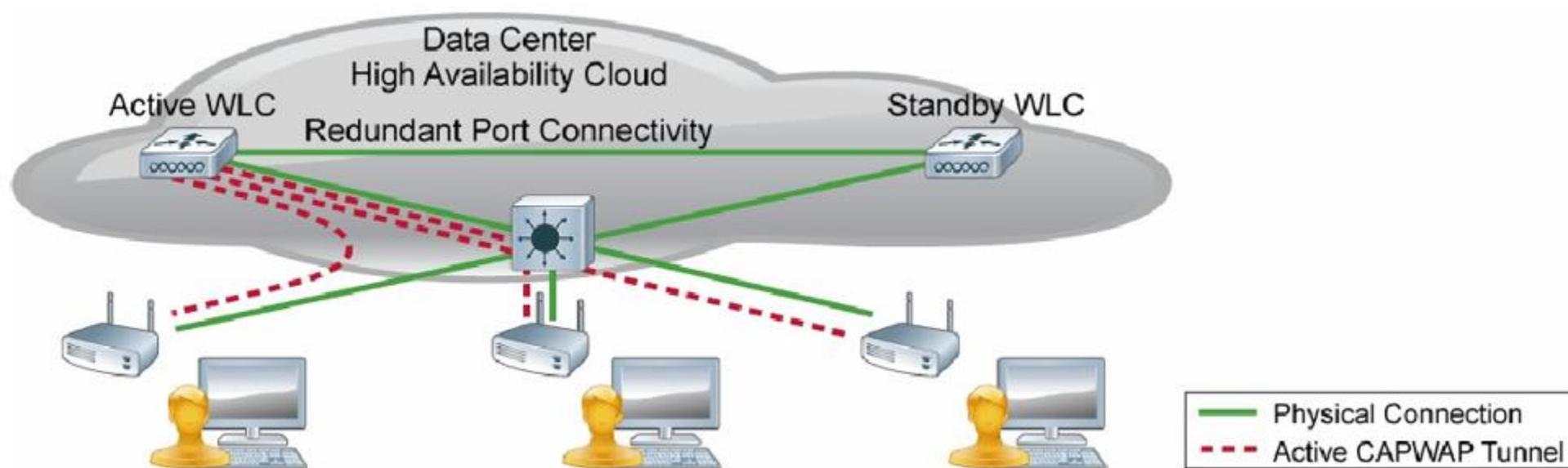
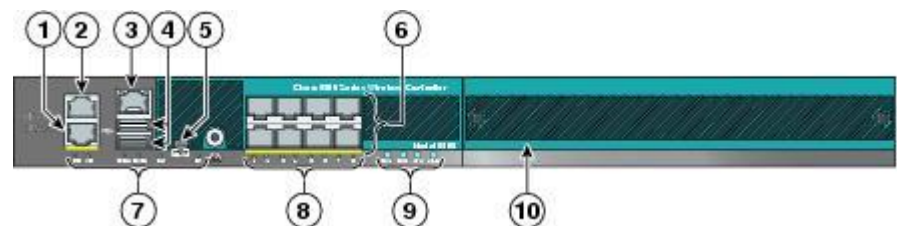
- 冗余的WLC物理隔离
- 配置高可用性参数
- AP优先级





# 高可用性

- 1:1冗余
- 一个使用中的WLC-一个热备的WLC
- 通过冗余端口①链接



# 高可用性 - 续

## 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

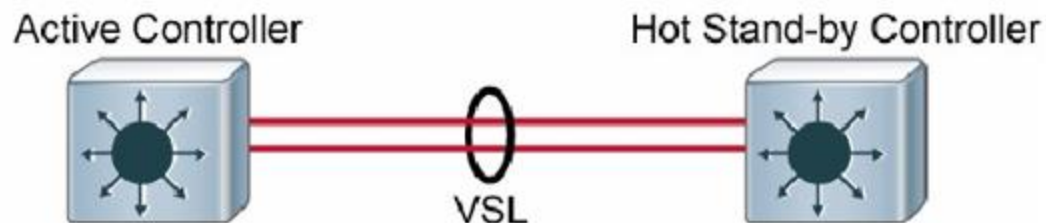
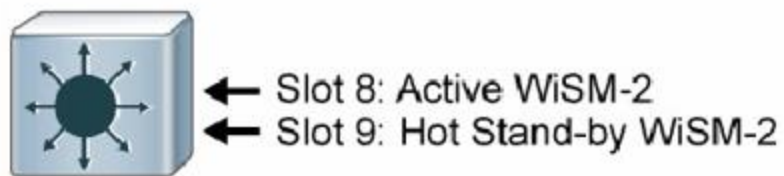
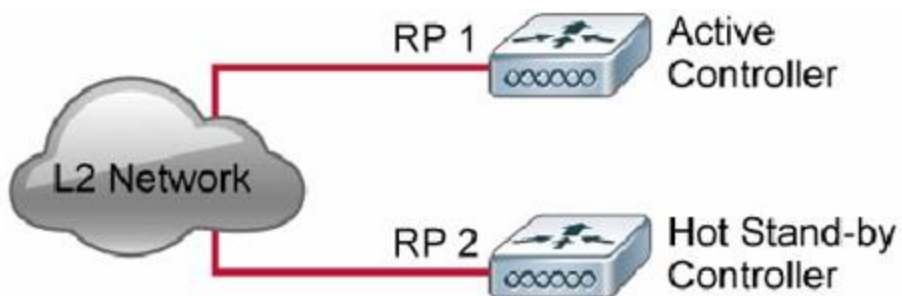
- Active – Standby can be geographically separated over L2 VLAN/Fiber
- Client database is synced to the Standby
  - Client information is synced when client moves to RUN state
  - Client re-association is avoided on switch over
- Fully authenticated clients (RUN state) are synced to the peer
- Effective 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SSO

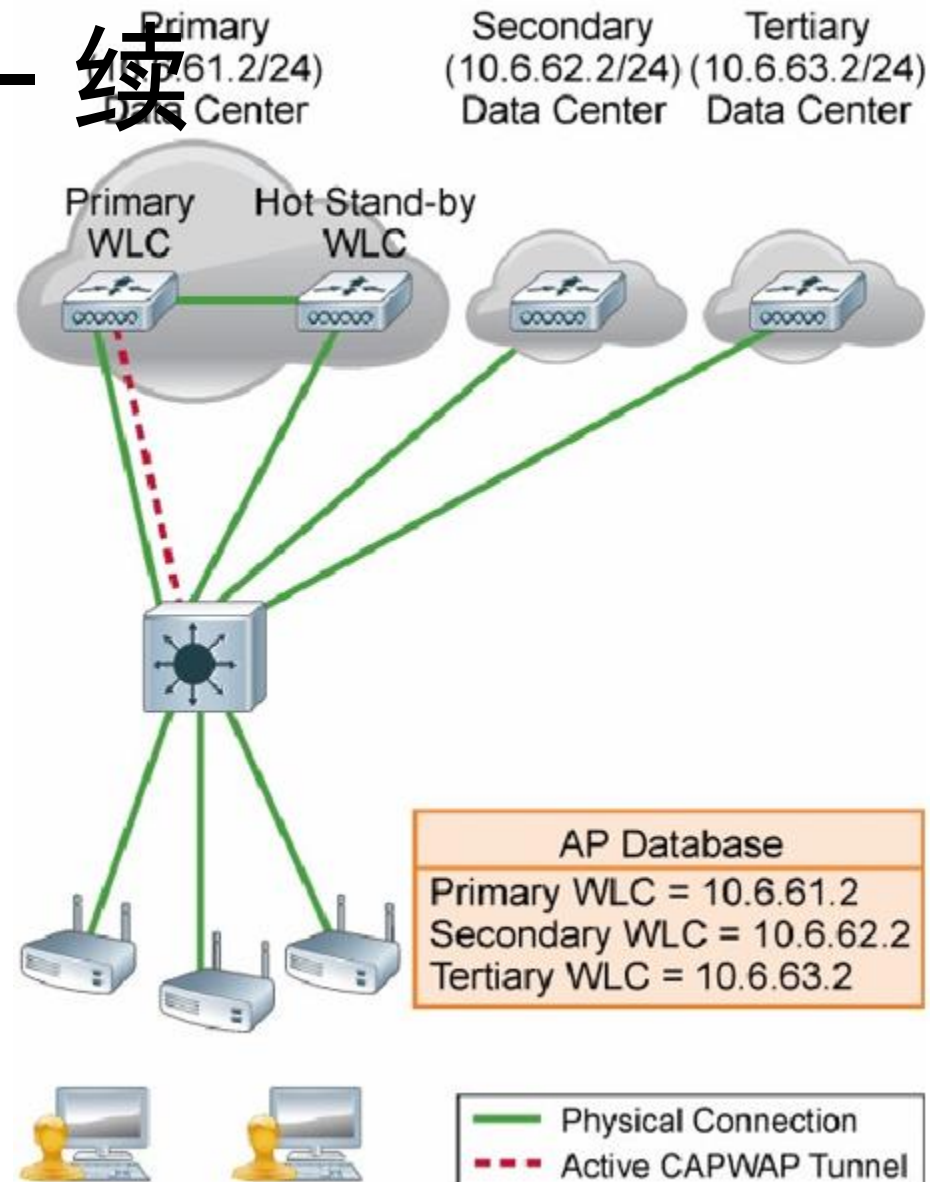
- 控制器物理连接
  - 5500/7500/8500有专用的冗余端口
  - WISM-2有专用的冗余VLAN，用于同步活动和备份WLC之间的配置。



# 集中模式：状态切换SSO - 续

- N+1设计

- SSO和第二，第三个WLC部署
- 活动和备份使用SSO设置可配置为基本。
- 一旦活动和备份的失效，AP切换到第二和或者第三个控制器。



# AP的运行模式

- AP的本地模式

- 缺省

- 数据服务

- 监控服务

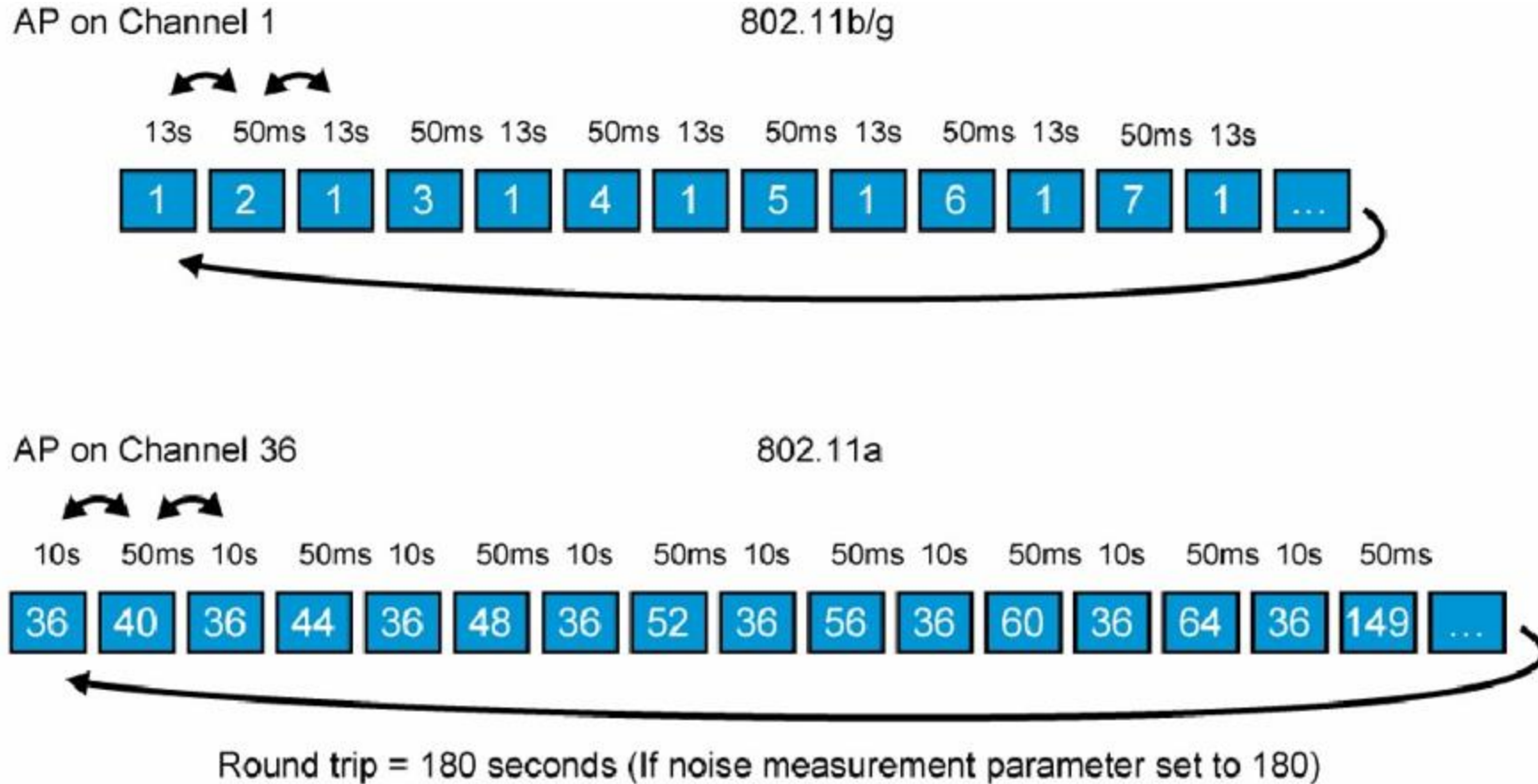
- AP缺省180秒扫描一次所有信道

- 只有管理数据包被插入用于IDSsignature匹配。

The screenshot shows a configuration page with tabs for General, Credentials, Interfaces, and High Availability. The General tab is active, displaying various configuration fields for an AP. The 'AP Mode' dropdown menu is open, showing the following options: local, FlexConnect, monitor, Rogue Detector, Sniffer, Bridge, Flex+Bridge, SE-Connect, and unspecified. The 'local' option is currently selected.

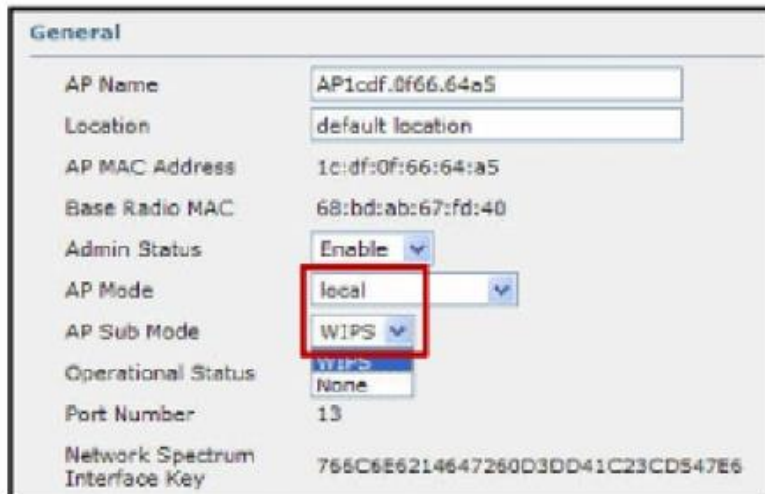
Field	Value
AP Name	APf07f.06da.6c34
Location	default location
AP MAC Address	f0:7f:06:da:6c:34
Base Radio MAC	f0:7f:06:e0:22:a0
Admin Status	Enable
AP Mode	local
AP Sub Mode	local
Operational Status	
Port Number	
Venue Group	
Venue Type	unspecified
Venue Name	
Language	

# 本地模式监控Timing



# wIPS增强本地模式ELM

- ELM提供了wIPS检测“on-channel”
- 在服务信道完成所有的数据包的扫描，不只是在管理数据包。
- Off-channel扫描期间没有signature检测。
- 使用AP部署提供IDS检测，不需要提供一个overlay的网络。
- Local模式和FlexConnect模式的子模式。



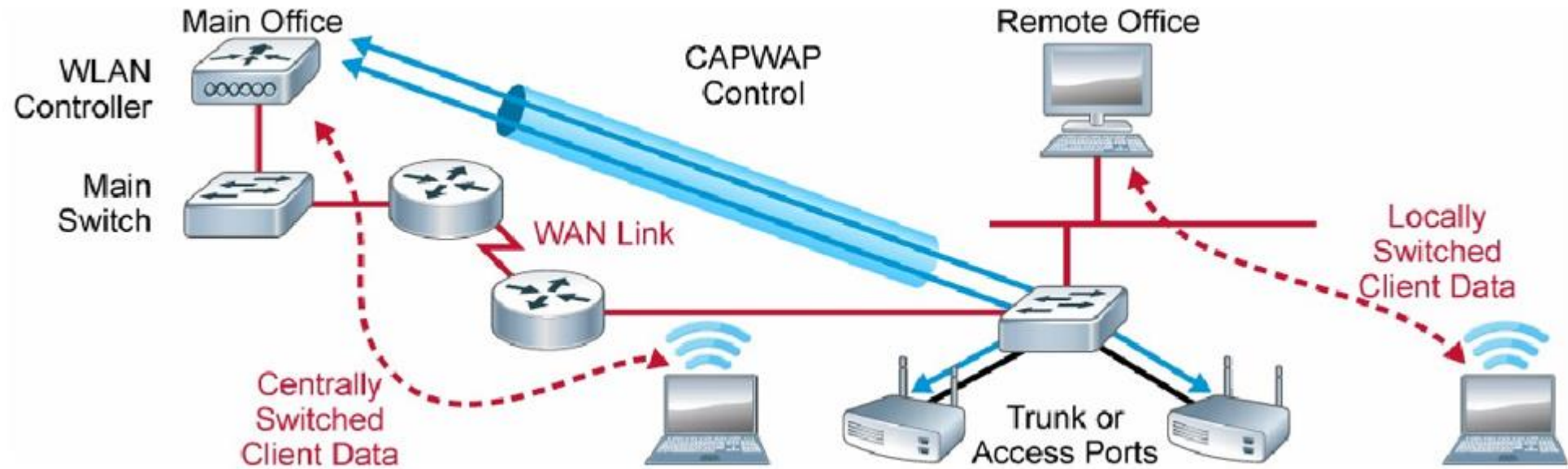
General	
AP Name	AP1cdf.0f66.64a5
Location	default location
AP MAC Address	1c:df:0f:66:64:a5
Base Radio MAC	68:bd:ab:67:fd:40
Admin Status	Enable
AP Mode	local
AP Sub Mode	WIPS
Operational Status	WIPS
Port Number	13
Network Spectrum Interface Key	755C6E6214647260D3DD41C23CD547E6

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

Simply selecting the submode will not enable ELM functionality.

# AP的FlexConnect模式

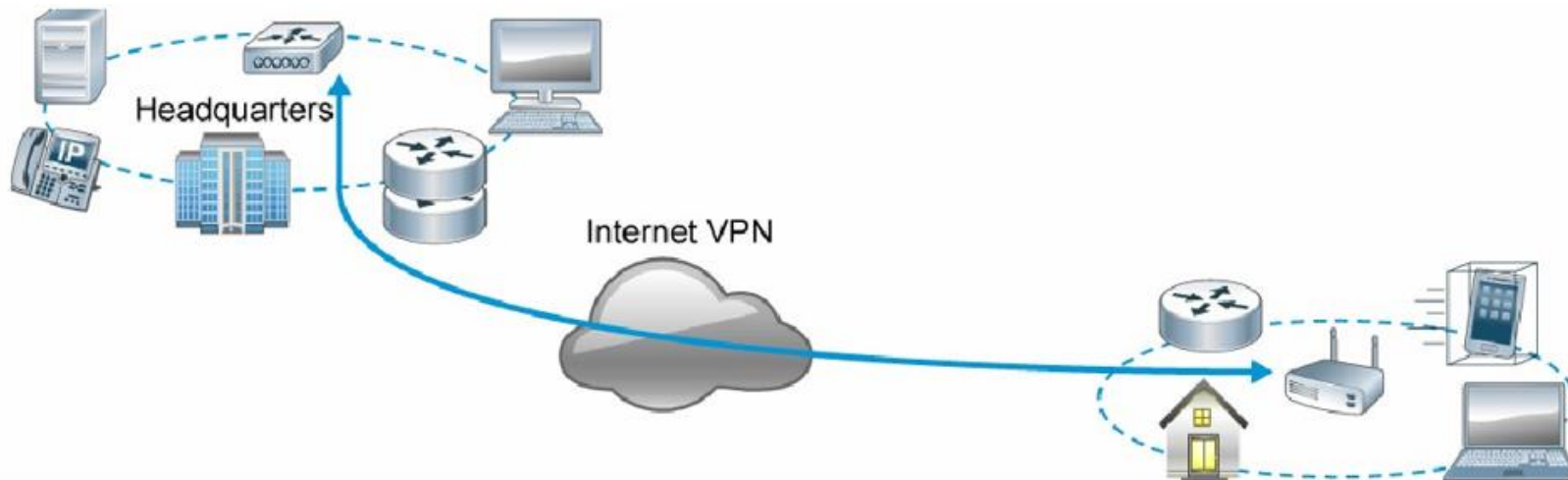
- 分支和远程办公室部署使用
  - 集中地配置和控制。





# AP的OfficeExtend模式

- 思科控制器安装在公司网络的DMZ区域。
- OEAP安装在家里。
- 集中配置
- 通过SSID访问互联网
- 使用集成天线。



# AP监控模式

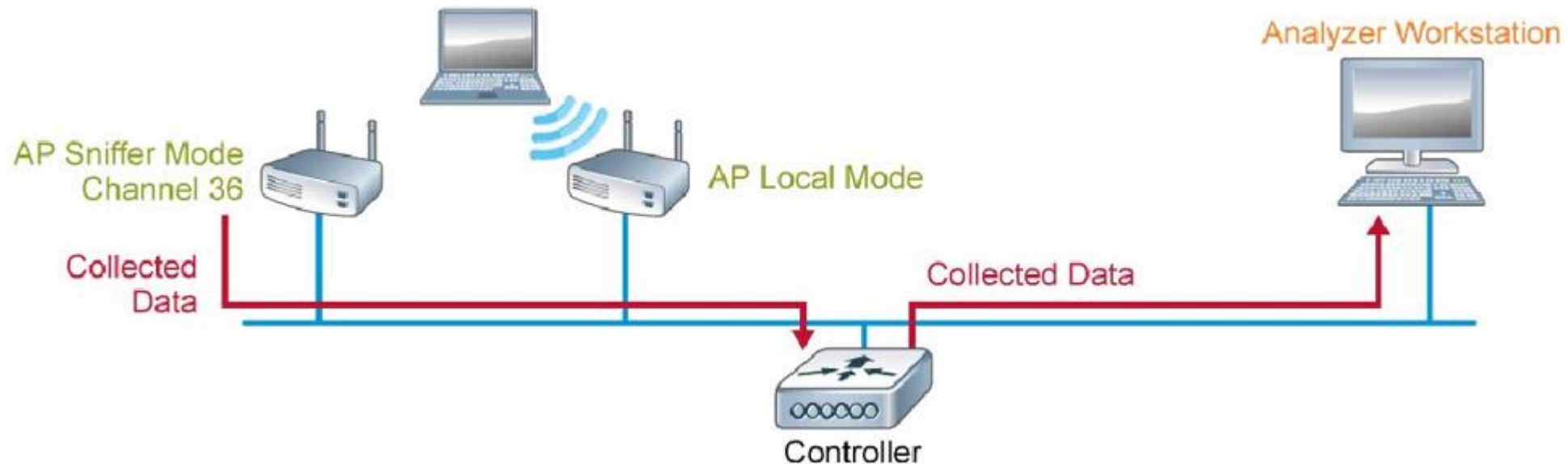
- 在每一个AP上执行WLAN的监控的软件配置会降低AP性能：
  - 可信的AP策略
  - 非法策略
  - 特征码
    - 数据包和管理包被插入IDS的特征码匹配。
    - AP将在1.1秒扫描所有的信道。
  - 有两个子模式：
    - 跟踪优化：优化为RFID跟踪
    - wIPS：每个信道250毫秒扫描的时间。

# AP非法检测模式

- 每一个AP上执行非法检测降级AP性能:
- 监听非法设备
- 比较ARP请求，网络上的和控制器上非法MAC地址。
- 当无线非法检测的MAC出现在有线测，产生告警。
- 不允许客户端连接：radio关闭，CPU专用在非法检测。
- 不执行非法containment。

# AP Sniffer模式

- 和抓包软件协同工作，例如OmniPeek，Wireshark，或者AirMagnet监控一个无线信道。
- 要求外部服务器抓数据包。
- 搜集数据：时间戳，信号强度和数据包大小。



# AP桥接模式

(Cisco Controller) >config country CN,AU

Changing country code could reset channel & RRM grouping configuration.  
If running in RRM One-Time mode, reassign channels after this command.  
Check customized APs for valid channel values after this command.  
Are you sure you want to continue? (y/n) Y

Error - Command failed - Mesh APs not currently supported by Multiple-Country. Use Single-Country or remove Mesh APs from network

- 需要特定的AP型号。
- 在所有AireOS WLC上均支持。
- 用于建立室内和室外mesh网络。
- 允许AP作为无线CAPWAP桥。
- AP可以配置为桥模式作为缺省模式。
- 802.11ac支持80MHz作为backhaul。

(Cisco Controller) >

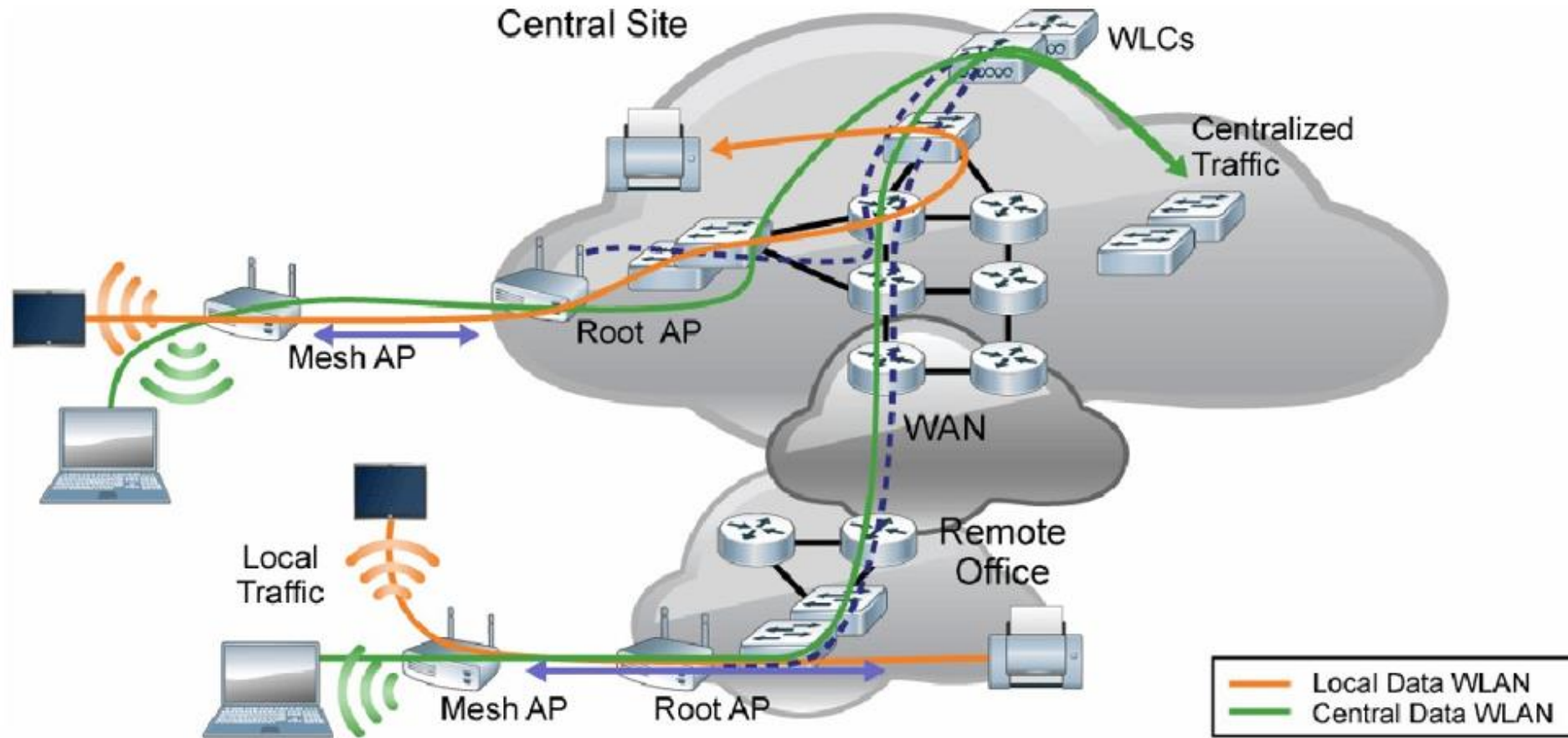
```
*spamApTask5: Nov 30 02:01:51.874: 00:1e:bd:e5:06:40 DTLS Session established server (157.0.9.11:5246), client (192.168.2.117:16069)
*spamApTask5: Nov 30 02:01:51.874: 00:1e:bd:e5:06:40 Starting wait join timer for AP: 192.168.2.117:16069

*spamApTask2: Nov 30 02:01:51.876: 08:17:35:31:a4:80 Join Request from 192.168.2.117:16069

*spamApTask2: Nov 30 02:01:51.876: 00:1e:bd:e5:06:40 Deleting AP entry 192.168.2.117:16069 from temporary database.
*spamApTask2: Nov 30 02:01:51.877: 08:17:35:31:a4:80 Bridge AP can not join MultiCountry Controller: Bridge mode AP
192.168.2.117:16069 cannot be supported on Multi Country Control
*spamApTask2: Nov 30 02:01:51.877: 08:17:35:31:a4:80 Finding DTLS connection to delete for AP (192:168:2:117/16069)
*spamApTask2: Nov 30 02:01:51.877: 08:17:35:31:a4:80 Disconnecting DTLS Capwap-Ctrl session 0x17aa76b8 for AP (192:168:2:117/16069)

*spamApTask2: Nov 30 02:01:51.877: 08:17:35:31:a4:80 CAPWAP State: Dtls tear down
*spamApTask2: Nov 30 02:01:51.877: acDtlsPlumbControlPlaneKeys: Irad:192.168.2.117(16069) mwar:157.0.9.11(5246)
*spamApTask2: Nov 30 02:01:51.878: 08:17:35:31:a4:80 DTLS keys for Control Plane deleted successfully for AP 192.168.2.117
*spamApTask2: Nov 30 02:01:51.884: 08:17:35:31:a4:80 Join Request failed!
```

# AP Flex+Bridge模式



# AP SE-Connect模式

- 在特定思科AP有效
- 允许AP作为链接的网络的传感器。
- 同时可以监控2.4GHz和5GHZ频谱。
- 不支持无线客户端。
- 分析冲突干扰interference。
- 只会在启用CleanAir的AP上使用。

# WLC的其它特性



# Radio Resource Management

What are the objectives of RRM?

- To dynamically balance the infrastructure and mitigate changes
- To monitor and maintain coverage for all clients
- To manage spectrum efficiency to provide the optimal throughput under changing conditions

What RRM does not do

- Substitute for a site survey
- Correct an incorrectly designed network
- Manufacture spectrum

# Radio Resource Management 续

## Radio Resource Monitoring

- Detects and configures new Cisco WLCs and access points as they are added to the network

## Dynamic Channel Assignment (DCA)

- Each AP radio gets a transmit channel assigned to it
- Changes in “air quality” are monitored, AP channel assignment is changed when deemed appropriate

## Transmit Power Control (TPC)

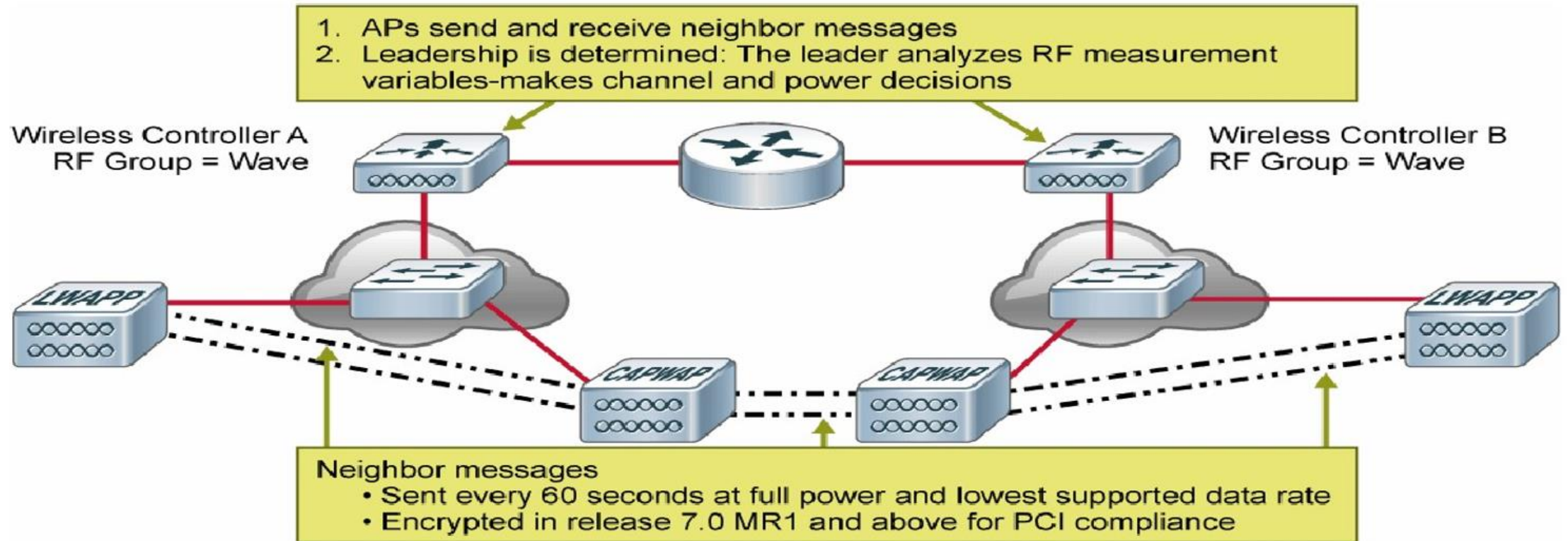
- Transmit power assignment is based on radio to radio pathloss.
- TPC is in charge of reducing Tx on some APs—but may also increase Tx by defaulting back to a power level higher than the current Tx level
- There are two versions of TPC, v1 and v2. v1 should be preferred

## Coverage Hole Detection and Mitigation (CHDM)

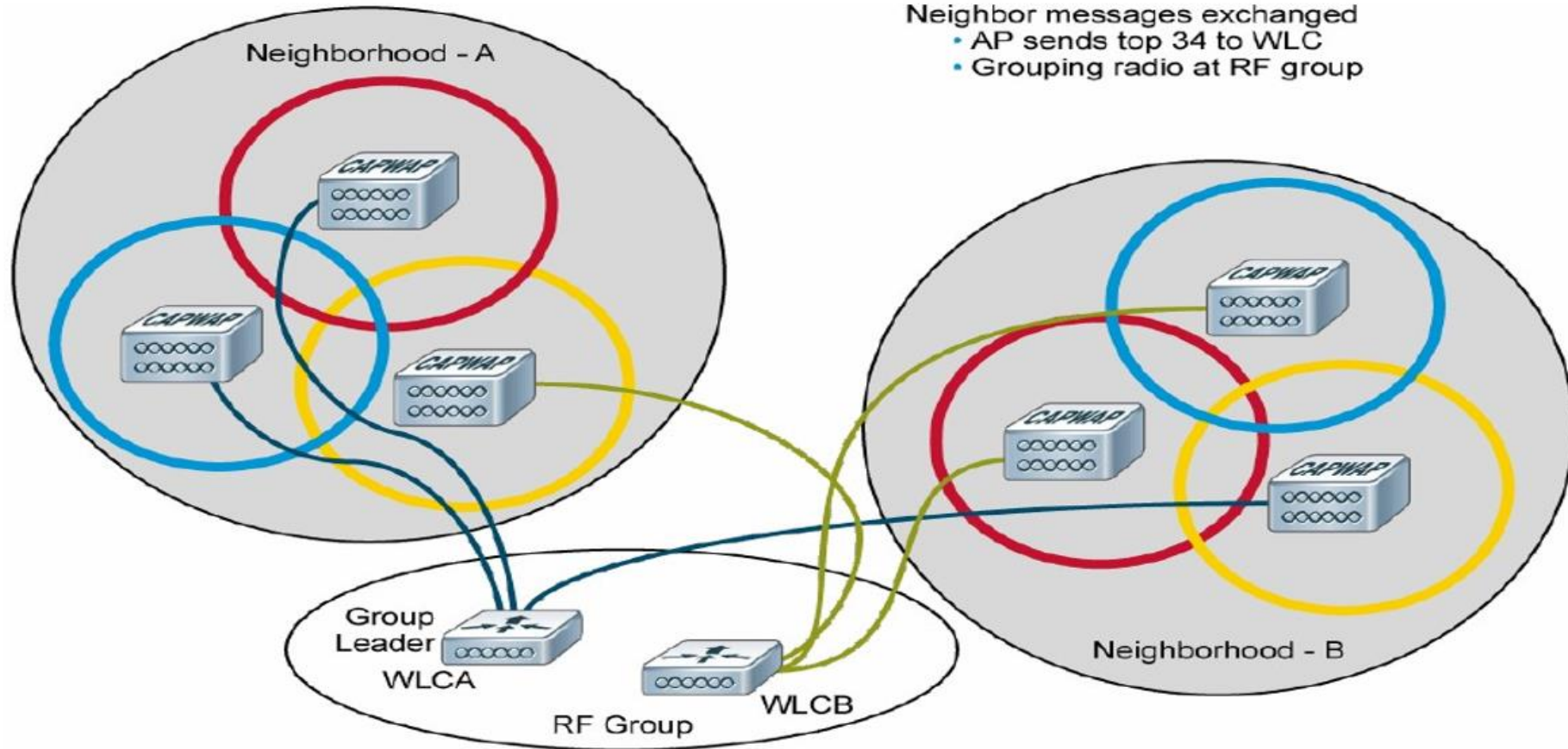
- Detects clients in coverage holes
- Decides on Tx adjustment (typically Tx increase) on certain APs based on adequacy or inadequacy of estimated downlink client coverage.

# RG组

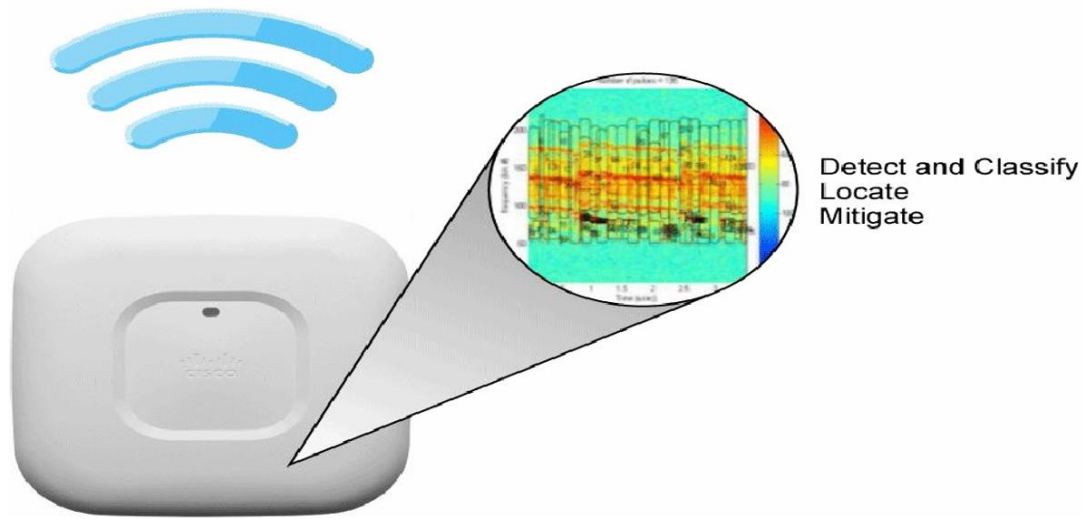
- How RRM is accomplished



# RG组 - 续

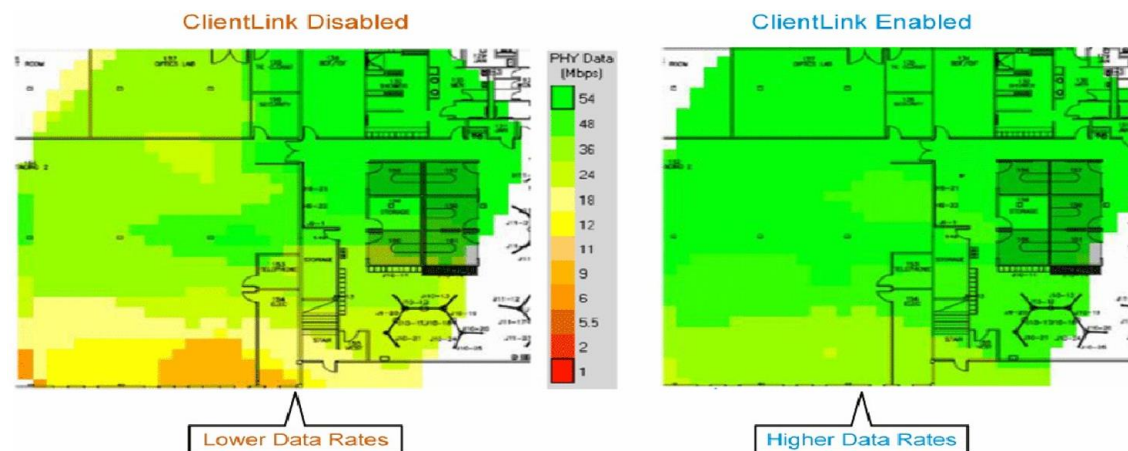


# CleanAir



# ClientLink

- 使用AP的MIMO天线提升SNR
- “beamforming”
- 只能命令行修改
- 按照radio类型全局配置或者按照radio类型的AP去配置。
- AP需要支持
- 不支持所有的数据速率。



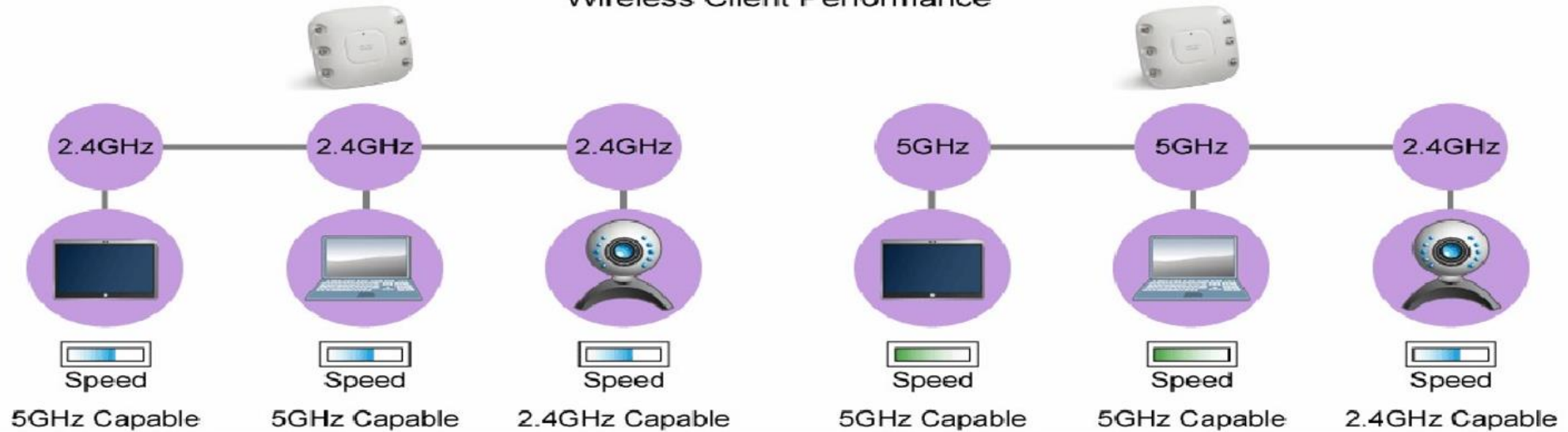
# Band选择

- Automatic band steering and selection for 5 GHz-capable devices
- Balances client load across the available spectrum

Before  
All clients crowd the 2.4GHz  
spectrum lowering performance

After  
5GHz clients are automatically  
moved to cleaner 5GHz spectrum

Wireless Client Performance



# Band选择配置

- 用于将双频宽调整为5GHZ频宽。
- 缺省全局启用。
- 可以每个WLAN激活。

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"/>



# 本地Profiling和策略

- 当一个客户端企图关联，可能从收到的信息中检测到客户端的类型。
- ISE提供了丰富的设备标示，onboarding, posture, 和策略。
- 客户不需要部署ISE。但是仍然能够识别设备，部署策略。
- WLC可以提供如下性能策略：
  - WLC 分类设备基于MAC-OUI, HTTP和DHCP信息，识别网络上的终端设备。
  - 可以配置基于设备的策略，按照用户或者设备部署网络的策略。
  - WLC基于用户或者终端设备显示统计信息。

# Client Profiling

- Profiling和策略是2个独立的部分。
- Profiling可以基于：
  - 角色，定义用户类型或者用户所属的用户组
  - 设备类型，例如windows, 手机, pad, iphone, android等。
  - 用户名密码
  - 定位，基于终端连接的AP
  - 时间，基于时间访问网络。
  - EAP类型，检查客户端连接EAP方法。
- 基于Profile，策略用于：
  - VLAN, QoS级别, ACL, 会话超时值。

# 配置客户端Profiles

- 在WLAN级别，启用本地客户端Profiling（DHCP和HTTP）
- DHCP请求自动检查，选择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"/>

# 配置策略

- 基于客户端识别部署策略

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

- General:** Policy Name: Android, Policy Id: 1.
- Match Criteria:** Match Rule String (empty), Match RADIUS Type (none).
- Device List:** Device Type (Android), with an 'Add' button. A list below shows 'Android' with a blue square icon.
- Action:** IPv4 ACL (none), VLAN 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 (ms)) (720), Flexconnect ACL (none), AVC Profile (none), mDNS Profile (none).
- Active Hours:** Day (Mon), Start Time (Hours, Mins), End Time (Hours, Mins), with an 'Add' button.

Two callout boxes are present:

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

# 应用策略

- 按照顺序配置策略到WLAN（每个WLAN可配置16个策略）

WLANs > Edit 'Pod1\_Open'

General Security QoS Policy-Mapping Advanced

Priority Index (1-16)  ← Choose an index

Local Policy  ← Choose a policy

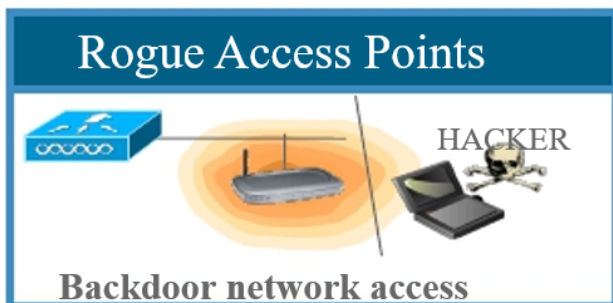
← Add

Priority Index	Local Policy Name
1	Android <input type="button" value="v"/>

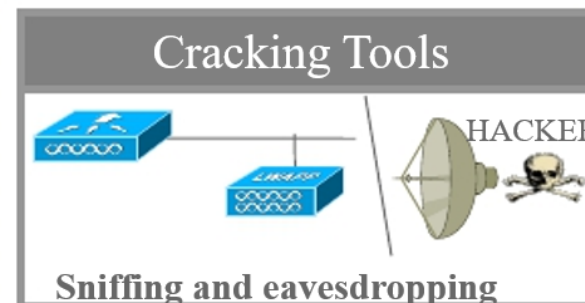
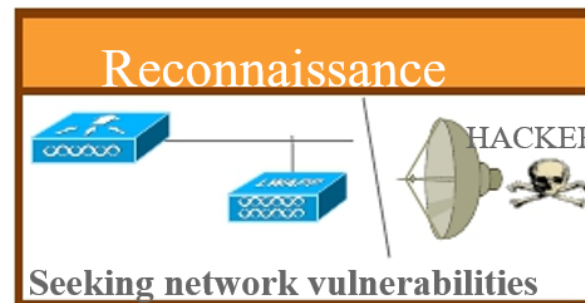
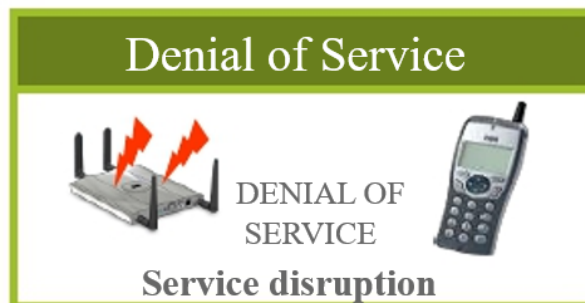
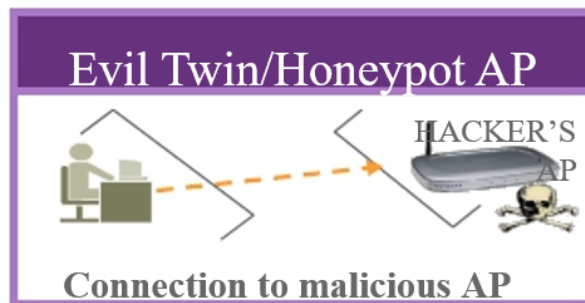
# 配置客户端访问

# 安全环境

## On-Wire Attacks



## Over-the-Air Attacks



# 经济的共计手段



OR



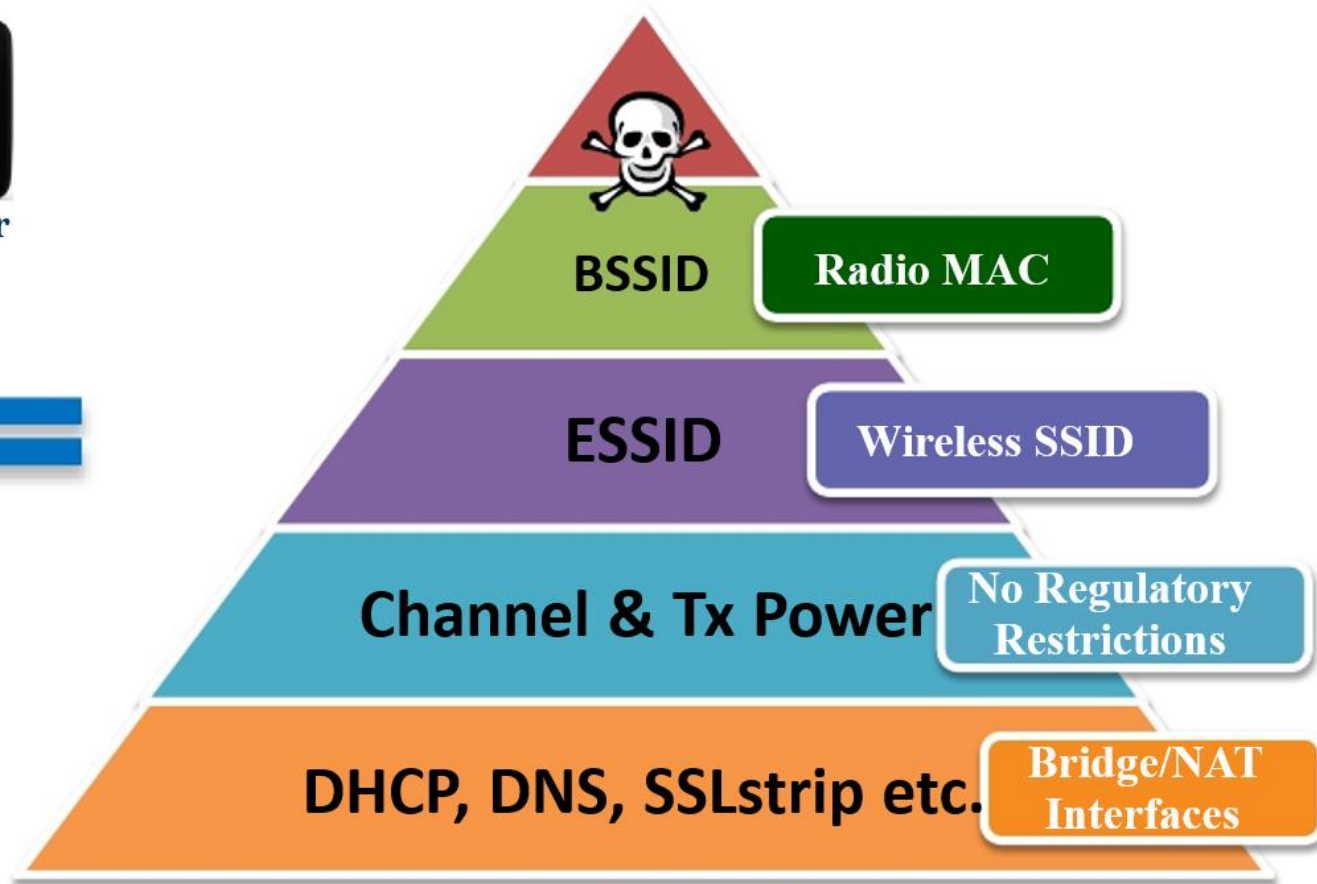
**Kali NetHunter**  
(Post-2014)



OR



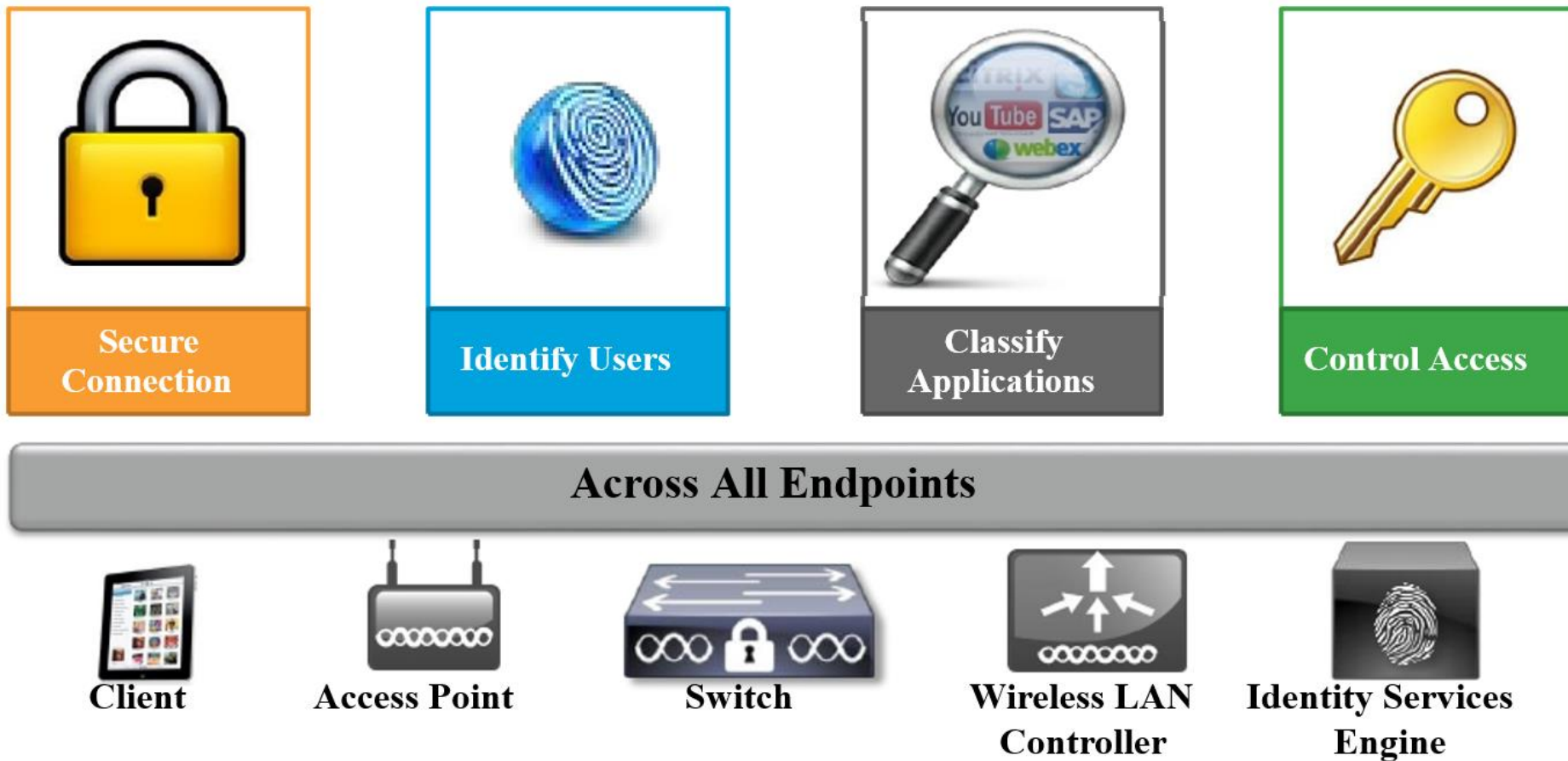
**USB Wireless Cards**



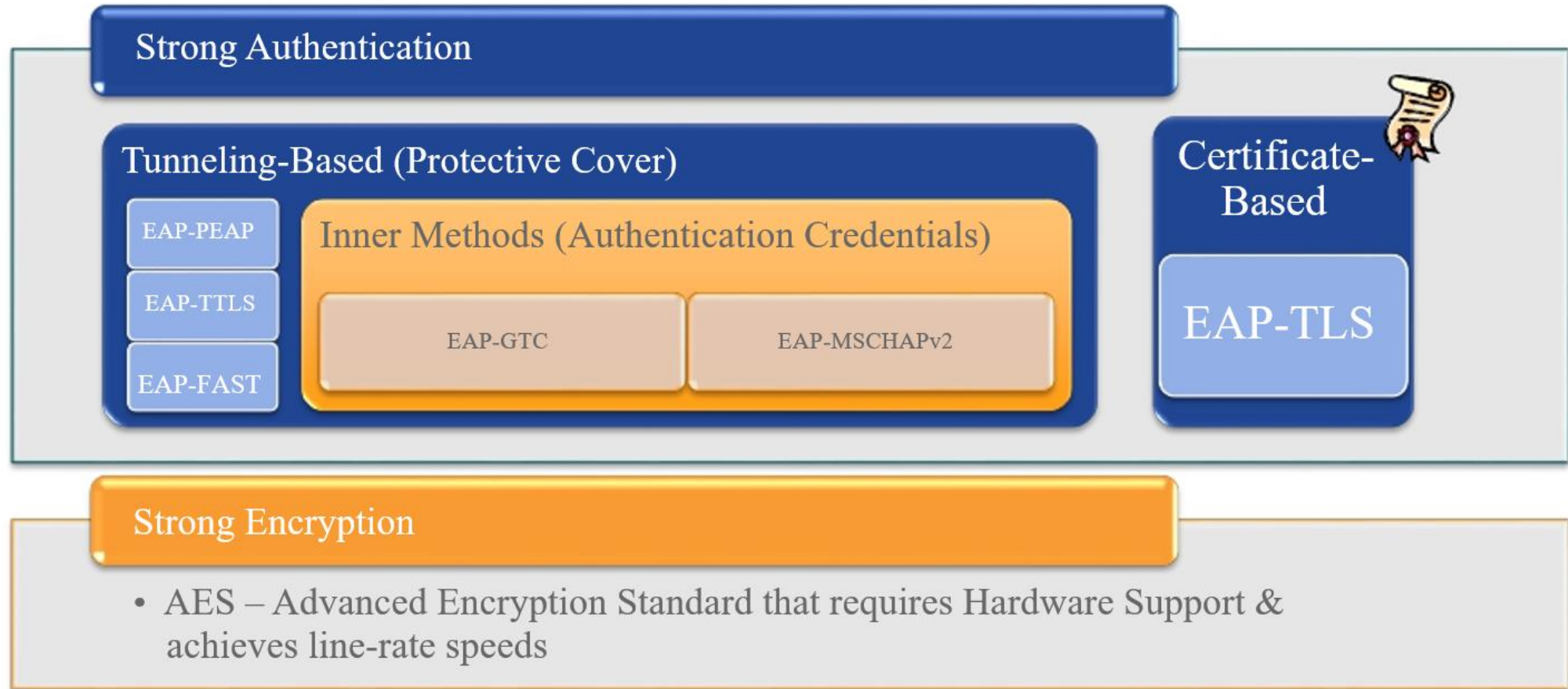
Sniffing Demand



# 思科无线安全解决方案



# 安全认证最佳实践



# WLAN开放认证

WLANs > Edit 'Pod1\_Open'

**General** Security QoS Policy-Mapping Advanced

Profile Name

Type WLAN

SSID

Status  Enabled

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

Radio Policy

Interface/Interface Group(G)

Multicast Vlan Feature  Enabled

Broadcast SSID  Enabled

NAS-ID

**General** Security QoS Policy-Mapping Advanced

**Layer 2** Layer 3 AAA Servers

Layer 2 Security <sup>6</sup>

MAC Filtering<sup>2</sup>

**Fast Transition**

Fast Transition

# WLAN预共享密钥认证

The image displays two overlapping screenshots of a network configuration interface for WLAN settings.

**Left Screenshot (General Tab):**

- 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

**Right Screenshot (Security Tab):**

- 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
  - PSK: .....
  - WPA gtk-randomize State: Disable

# WLAN EAP和RADIUS认证: 本地-EAP

The left side of the image shows three overlapping screenshots from the Cisco WLC configuration interface:

- Local Net Users > Edit:** Shows configuration for a user named 'wlcuser'. Fields include Password (masked with '\*\*\*'), Confirm Password (masked with '\*\*\*'), Creation Time (Thu Apr 9 20:49:38 2015), Remaining Time (N/A), and WLAN Profile (Any WLAN).
- Local EAP Profiles > New:** Shows the 'Profile Name' field set to 'WLC\_Local\_EAP'.
- Local EAP Profiles:** A table listing the configured profile:

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"/>

The right side of the image shows two overlapping screenshots from the Cisco WLC configuration interface:

- Layer 2 Security:** Shows 'Layer 2 Security' set to 'WPA+WPA2' and 'MAC Filtering' disabled. Under 'Protected Management Frame', 'PMF' is set to 'Disabled'. Under 'WPA+WPA2 Parameters', 'WPA Policy' is disabled and 'WPA2 Policy-AES' is enabled. Under 'Authentication Key Management', '802.1X' is enabled, while 'CCKM', 'PSK', and 'FT 802.1X' are disabled.
- AAA Servers:** Shows 'Interim Update' checked with an 'Interim Interval' of 0. Under 'LDAP Servers', all three servers are set to 'None'. Under 'Local EAP Authentication', 'Local EAP Authentication' is checked and 'EAP Profile Name' is set to 'WLC\_Local\_EAP'.

# WLAN 使用RADIUS认证

The image shows two screenshots from the Cisco Identity Services Engine (ISE) configuration interface. The left screenshot displays the configuration for a Network Device (POD1WLC). The right screenshot displays the configuration for a Network Access User (pod1user).

**Network Device Configuration (POD1WLC):**

- Name: POD1WLC
- IP Address: 192.168.11.5 / 32
- Model Name: [Dropdown]
- Software Version: [Dropdown]
- Network Device Group: [Dropdown]
- Location: All Locations
- Device Type: All Device Types
- Authentication Settings:
  - Enable Authentication Settings:
  - Protocol: RADIUS
  - Shared Secret: [Masked]
  - Enable KeyWrap:
  - Key Encryption Key: [Masked]
  - Message Authenticator Code Key: [Masked]
  - Key Input Format: ASCII

**Network Access User Configuration (pod1user):**

- Name: pod1user
- Status: Enabled
- Password: [Masked]
- Re-Enter Password: [Masked]
- User Information: [Fields for First Name and Last Name]

The image shows the configuration for RADIUS Authentication Servers in the Cisco Identity Services Engine (ISE) interface. The configuration is for a single server (Server Index 1).

**RADIUS Authentication Servers > Edit**

- Server Index: 1
- Server Address(Ipv4/Ipv6): 192.168.11.21
- Shared Secret Format: ASCII
- Shared Secret: [Masked]
- Confirm Shared Secret: [Masked]
- 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
- IPSec:  Enable

**Advanced Configuration:**

- Layer 2:  Enabled
- Layer 3:  Enabled
- AAA Servers:  Enabled
- Radius Server Accounting:  Interim Update, Interim Interval: 0
- LDAP Servers: Server 1, 2, 3: None
- Local EAP Authentication:  Enabled

# WLAN WebAuth认证

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

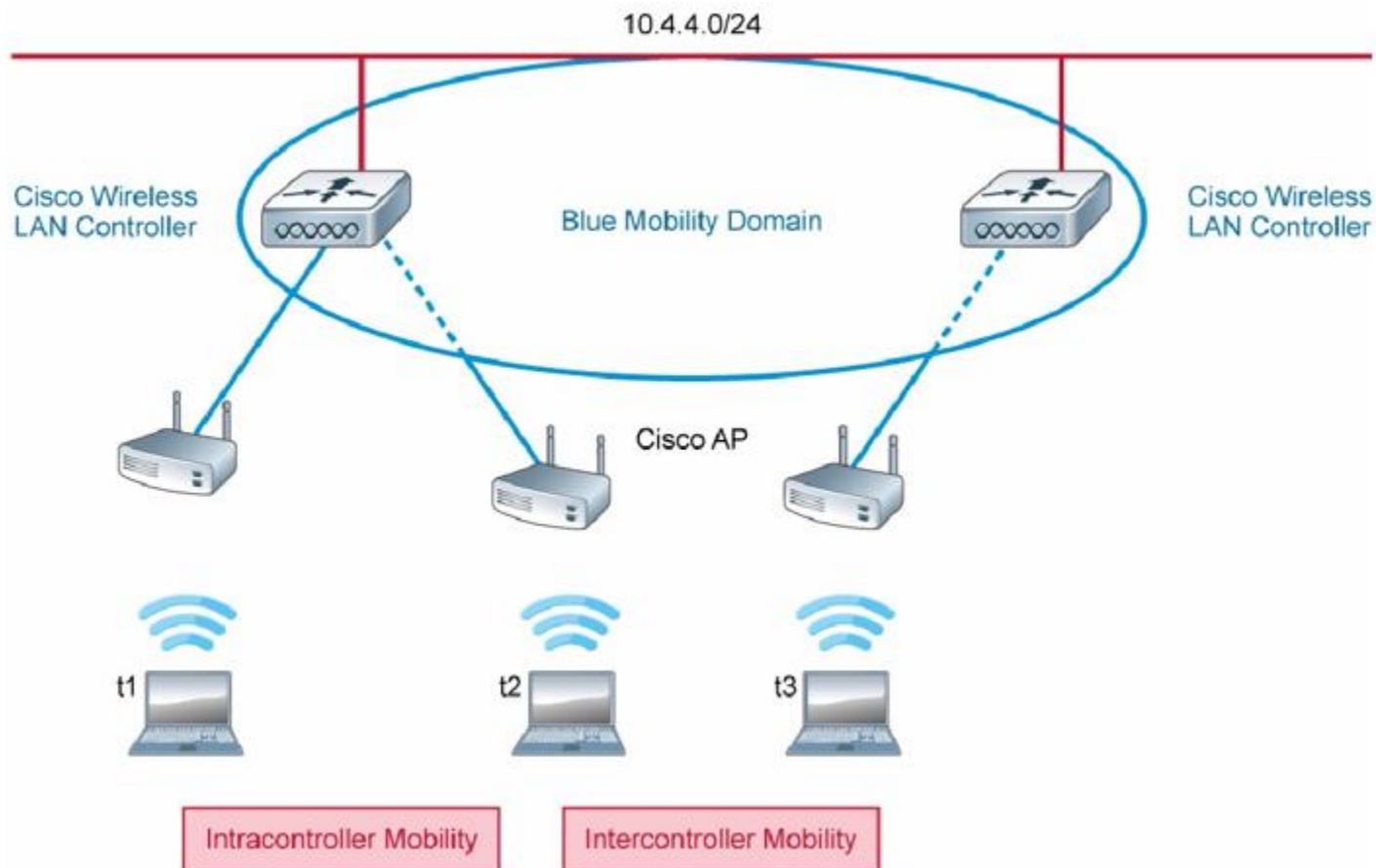
Sleeping Client  Enable

Over-ride Global Config  Enable

# 漫游的配置

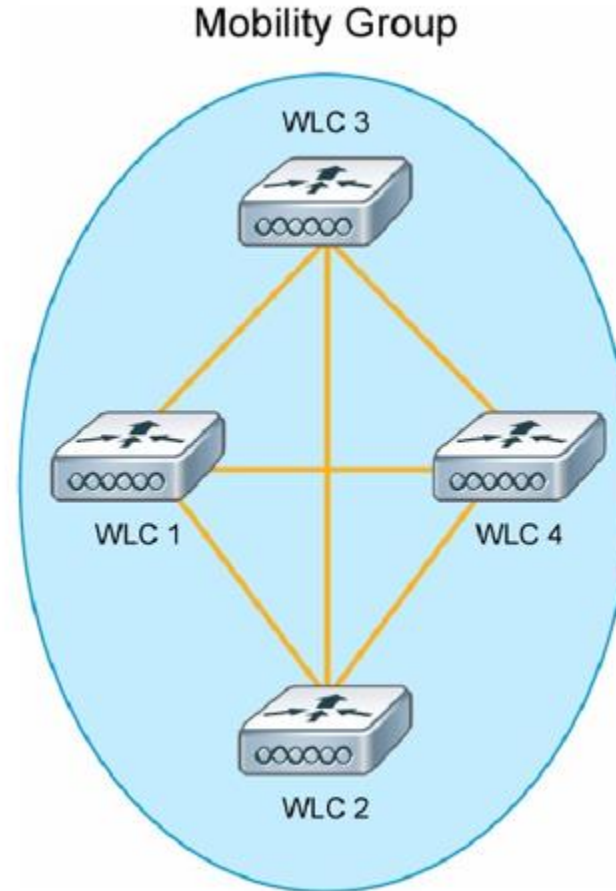


# 控制器内和控制期间的漫游



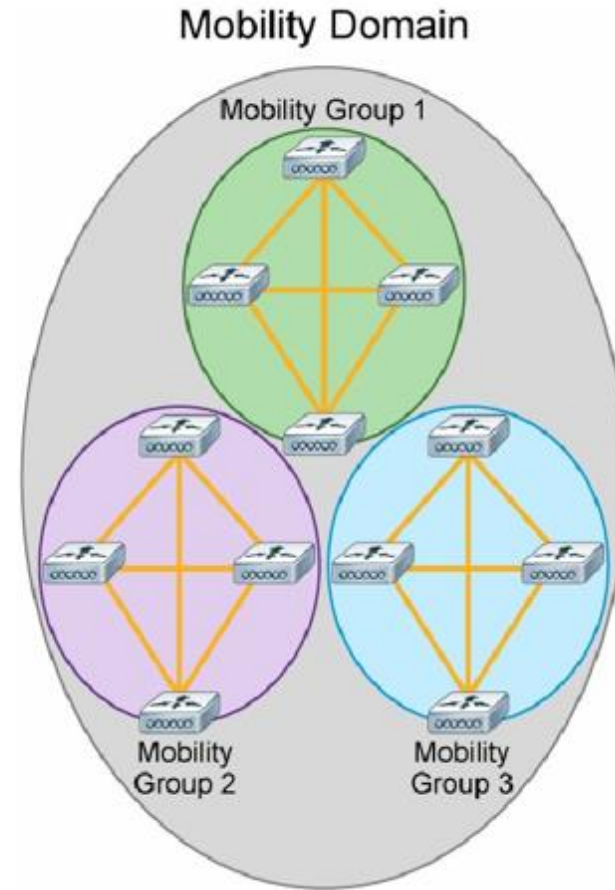
# 漫游组

- 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



# 漫游区域

- 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



# AireOS常用命令

## Wireless LAN Controller

### General Commands

Display common system information:	<b>show sysinfo</b>
Display more system information:	<b>show tech-support</b>
Allow to display output without breaks:	<b>config paging disable</b>
Display current running configuration:	<b>show run-config</b>
Display list of configured commands:	<b>show run-config commands</b>
Display log messages:	<b>show msglog</b>
Display general info about all interfaces:	<b>show interface summary</b>
Display redundancy summary info:	<b>show redundancy summary</b>
Save current configurations:	<b>save config</b>
Exit the current session:	<b>logout</b>
Display details about a specific interface:	<b>show interface detailed</b> <i>interface_name</i>

### Radio Commands

Display the 5GHz radios config:	<b>show 802.11a</b>
Display the 2.4GHz radios config:	<b>show 802.11b</b>
Display a summary of the RF profiles:	<b>show rf-profile summary</b>
Display details of a RF profile:	<b>show rf-profile details</b> <i>rf-profile_name</i>
Display stats of current APs radios:	<b>show advanced 802.11a b summary</b>
Display config and stats of 2.4GHz or 5GHz channels:	<b>show advanced 802.11a b channels</b>
Display config and stats of 2.4GHz or 5GHz transmit powers:	<b>show advanced 802.11a b txpower</b>
Display specific AP radio statistics:	<b>show ap stats 802.11a b</b> <i>ap_name</i>
Restart the Dynamic Channel Assignment (DCA) process (part of RRM):	<b>config 802.11a b channel global restart</b>

### Access Points Commands

Display the list of current APs:	<b>show ap summary</b>
Display images associated with APs:	<b>show ap image all</b>
Display uptimes of joined APs:	<b>show ap uptime</b>
Display APs joined to the WLC:	<b>show ap join stats summary all</b>
Display config of a specific AP:	<b>show ap config general</b> <i>ap_name</i>

### Clients Commands

Display details about associated clients:	<b>show client summary</b>
Test the Wi-Fi connection of a client:	<b>linktest</b> <i>client_MAC_address</i>
Display clients associated to a SSID:	<b>show client wlan</b> <i>wlan_id</i>
Display details info for a client connected with a username:	<b>show client username</b> <i>username</i>
Deauthenticate a client:	<b>config client deauthenticate</b> <i>client_MAC_address</i>
Display full details about specific client:	<b>show client detail</b> <i>client_MAC_address</i>

### Debug Commands

Display current debug config:	<b>show debug</b>
Disable all debug sessions:	<b>debug disable-all</b>
Debug a specific client:	<b>debug client</b> <i>MAC_address</i>
Enable debug for remote AP:	<b>debug ap enable</b> <i>ap_name</i>
Enable AAA debug:	<b>debug aaa all enable</b>
Enable CAPWAP debug:	<b>debug capwap detail enable</b>
Display log of remote AP:	<b>debug ap command "show logging"</b> <i>ap_name</i>

## Access Point Operations

### Default Settings

Default username:	<b>Cisco</b>	Default password:	<b>Cisco</b>
Default enable password:	<b>Cisco</b>		

### Reset AP to Factory Defaults

- 1 - Connect a console cable to the AP
- 2 - Power up the AP while pressing the RESET button
- 3 - Release the RESET button after about 15-20 seconds
- 4 - You should see the "ap:" prompt
- 5 - Enter the following commands:  
**ap: dir flash:**  
**ap: delete flash:private-multiple-fs** **reload**  
**ap: reset**
- 6 - AP will reboot with factory defaults
- 7 - Use the default credentials to login (Cisco/Cisco)

### Convert Lightweight AP to Autonomous

- 1 - Download the right autonomous image (k9w7)
- 2 - Connect a TFTP server to the Ethernet port of the AP
- 3 - Connect a console cable to the AP
- 4 - Enter the following commands to configure the network interface:  
**AP# show ip interface brief**  
**AP# debug capwap console cli**  
**AP# conf t**  
**AP(config)# ip default-gateway** *ip\_tftp\_server*  
**AP(config)# int g0**  
**AP(config-if)# ip address** *ip\_in\_same\_VLAN* *mask*  
**AP(config-if)# no shutdown**
- 5 - Test network connectivity:  
**AP# ping** *ip\_tftp\_server*
- 6 - Download autonomous to the AP:  
**AP# archive download-sw /force-reload /overwrite**  
**tftp://ip\_tftp\_server/image\_name.tar**
- 7 - The AP will reload with the new image. Once restarted, verify that the new image is installed using this command:  
**AP# show version**

# 下一步学习:

- CSC论坛以及之前的视频讲座系列
- 《设计和部署企业无线局域网》 CiscoLive
- 融合无线网络技术: IOS-XE
- 实践: 思科无线的虚拟化技术