



An Overview Of Wi-Fi Components & Architectures

ine.com



Keith Bogart

CCIE #4923



kbogart@ine.com



[@keithbogart1](https://twitter.com/keithbogart1)



linkedin.com/in/keith-bogart-2a75042



CCIE Routing & Switching



- + High-level understanding of the roles of common Wi-Fi Components

Course Prerequisites

Course Objectives

- + To help you become familiar with the various WLAN architectures available
- + To allow you to differentiate between types and placements of WLAN controllers
- + To understand the different options of Cisco access point modes



What Is A Wireless Architecture?

ine.com

Topic Overview

- + What is a Wireless Architecture?
- + High-Level Architectural Differences

What Is A Wireless Architecture?

- + WLANs can be designed using a variety of devices and in a variety of configurations
- + These configurations and designs are called “Architectures”
- + Wireless Architectures we’ll be discussing:
 - + Autonomous architectures
 - + Cloud-based architectures
 - + Converged architectures
 - + Mesh architectures
 - + Centralized wireless architectures

High-Level Architectural Differences

- + All of these architectures fall into one of two categories:
 - + Distributed Architectures
 - + Centralized Architectures
- + Common questions that need to be answered:
 - + Where is management of the access points originated?
 - + Do the access points have a functional GUI or CLI for management?
 - + Who performs authentication of Wi-Fi clients?
 - + What is the path of user data as it leaves the Wi-Fi domain and enters the Distribution System?



Autonomous WLAN Architectures

ine.com

Topic Overview

- + Autonomous Architectures
- + Autonomous Decisions & Challenges

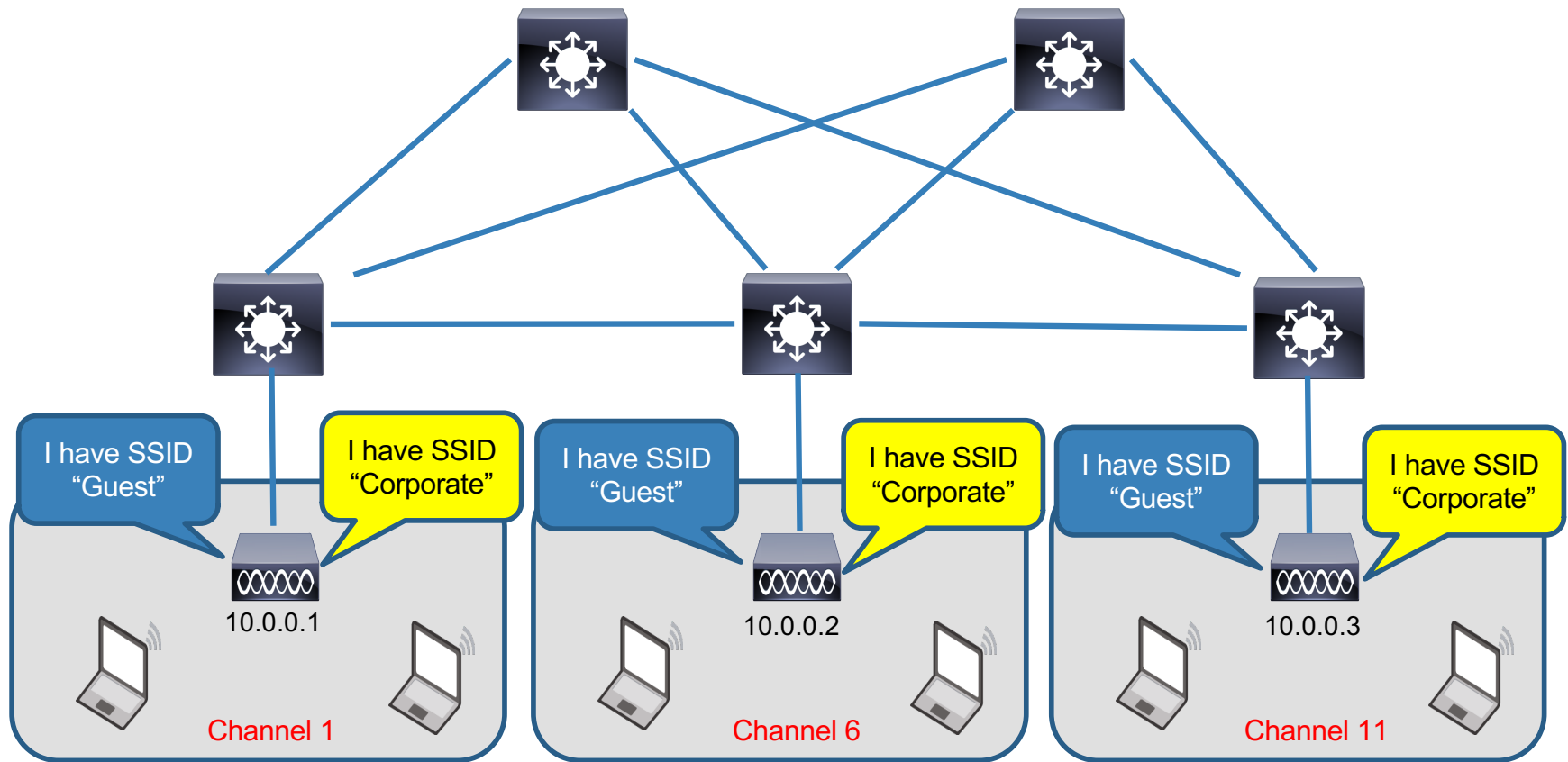
Autonomous Architectures

- + Autonomous access point = individually managed access point
- + Each has its own GUI and/or CLI for configuration and management
- + May advertise one or more WLANs (i.e. SSIDs)
 - + Multiple SSIDs utilize unique VLAN numbers
 - + Within a single access point, multiple SSIDs typically share a single RF channel
 - + RF contention exists whether the AP is advertising one, or several SSIDs
- + Typically a separate Management VLAN utilized for placement of the access point's IP address

Autonomous Decisions & Challenges

- + What decisions are made by the access point?
 - + Which RF channel to use (per 2.4GHz or 5GHz radio)
 - + How to authenticate connected clients
 - + How to implement QoS
 - + Segmenting traffic into different VLANs for bridging into the wired Distribution System
- + Challenges with this architecture:
 - + Additions of new SSIDs must be created one by one
 - + Changes to security or QoS policies must be implemented one by one
 - + Standardization across the entire corporate WLAN difficult to maintain
 - + Detection and mitigation of rogue APs is difficult

Autonomous Architectures





Cloud-Based WLAN Architectures

ine.com

Topic Overview

- + The “Why” & “Where” Of WLAN Controllers
- + Cloud-Based Architectures
- + Introduction To Cisco Meraki’s Wireless Cloud Service

The “Why” and “Where” Of WLAN Controllers

- + Architectures that utilize autonomous (or standalone) access points are not scalable
- + A central point of control can be implemented using a WLAN controller
- + Access points managed by a controller are called Lightweight APs (or LAPs)
- + The question then becomes...where do we place the controller?
 - + Cloud-based deployments
 - + On-site deployments

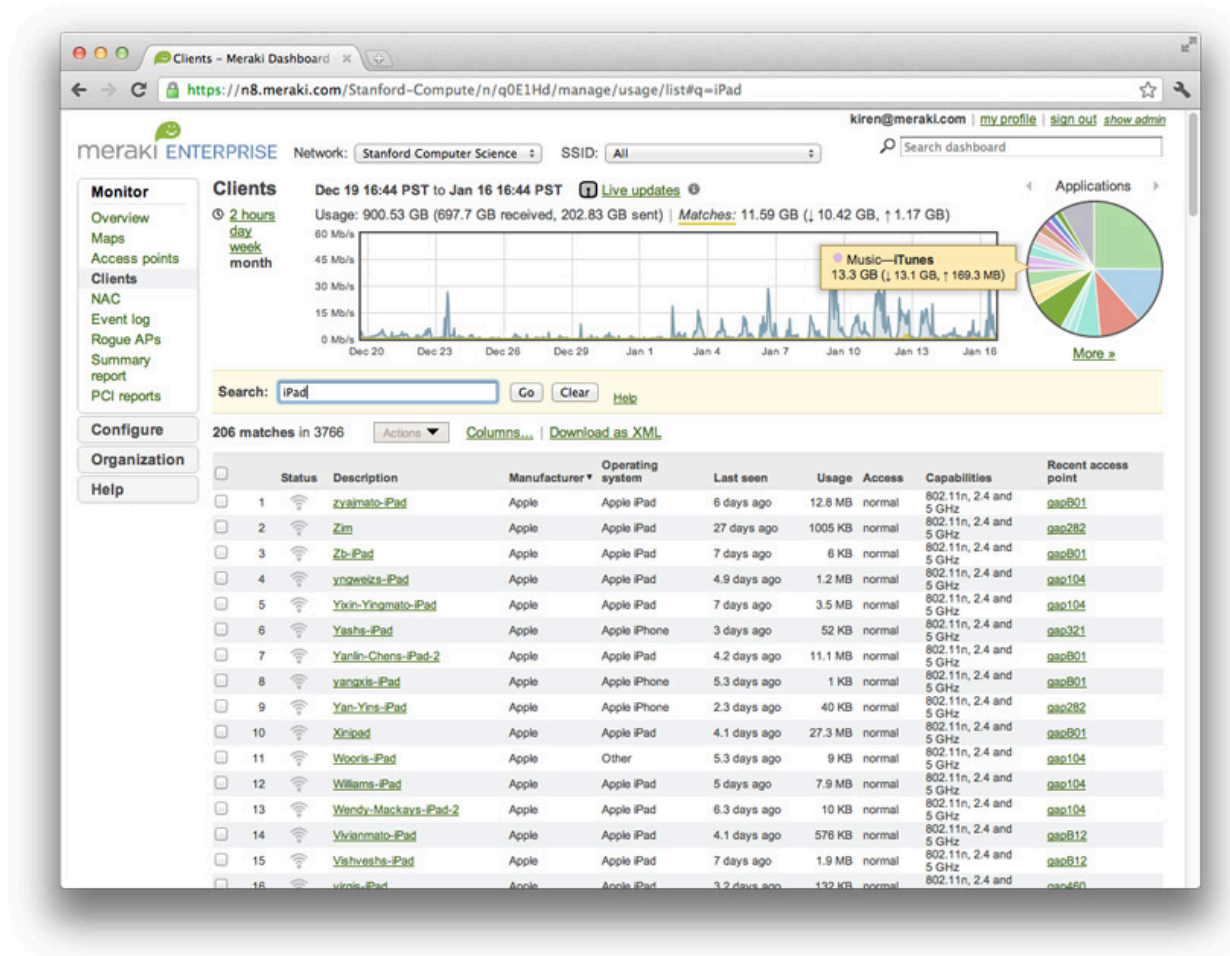
Cloud-Based Architectures

- + WLAN controller is located in a public or private cloud
- + Two Cisco options available:
 - + Meraki wireless cloud service
 - + Cisco Catalyst 9800-CL cloud-based controller
- + This terminology commonly refers to the Meraki solution
- + Cloud connection is only used for control plane and management plane traffic.

Cisco Meraki

- + Allows centralized management of Cisco Meraki products
 - + APs
 - + Switches
 - + Security Products
- + Provides for automatic deployment of managed nodes after customer register with the Meraki cloud.
 - + APs contact the cloud and self-configure
 - + Code upgrades and configuration changes
 - + RF channel selection and transmit power
 - + Collection of information from AP such as rogue devices, wireless usages statistics

Cisco Meraki Dashboard





Split-MAC WLAN Architectures

ine.com

Topic Overview

- + Challenges With Managing Autonomous Access Points
- + Introducing The Split-MAC Architecture

Challenges With Managing Autonomous APs

- + Requires manual selection of RF Channels and Transmit power
- + You must manually deal with Rogue APs that are detected
- + Manual selection of Wi-Fi cell coverage to provide overlap in the event of an AP failure
- + Manual configuration of security policies

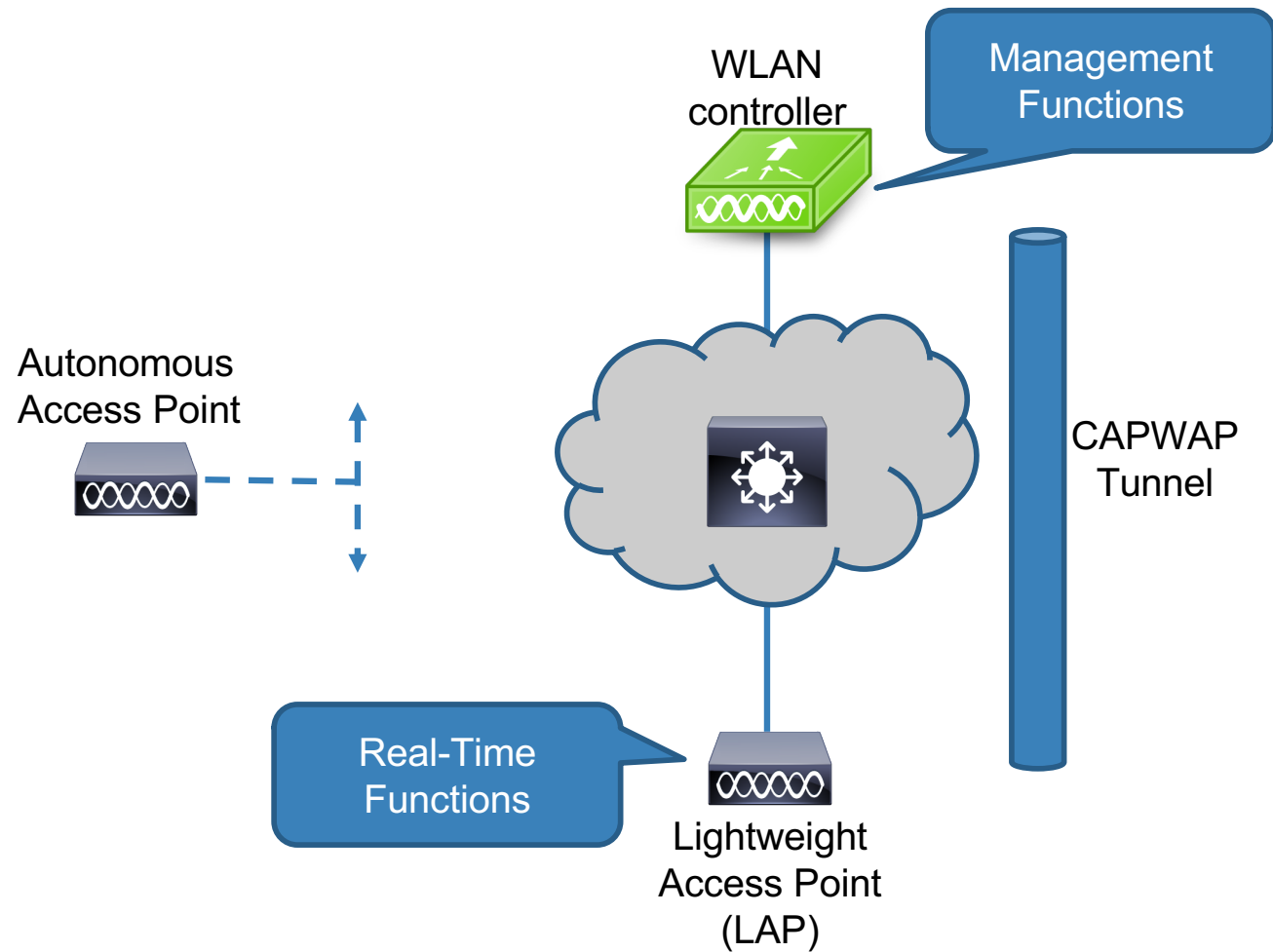
Divide & Conquer

- + Split-MAC architectures involve the following:
 - + Implementing an on-premise controller
 - + Utilizing lightweight access points (LAP) that essentially split the functionality of autonomous APs into two sections
- + Real-time functions handled locally by Lightweight AP (LAP)
- + Management Functions offloaded to a WLAN controller

What Is Split?

- + Real-time functions handled locally by Lightweight AP (LAP)
 - + RF transmit/receive of frames (management, control and data)
 - + MAC management (DCF)
 - + Encryption
- + Management Functions offloaded to a WLAN controller
 - + RF Management (channel selection, transmit power, etc)
 - + Association and Roaming Management
 - + Client authentication
 - + Security Policy Management
 - + QoS

Split-MAC Architectures





Introduction To CAPWAP

ine.com

Topic Overview

- + CAPWAP Overview
- + CAPWAP Tunnel Types

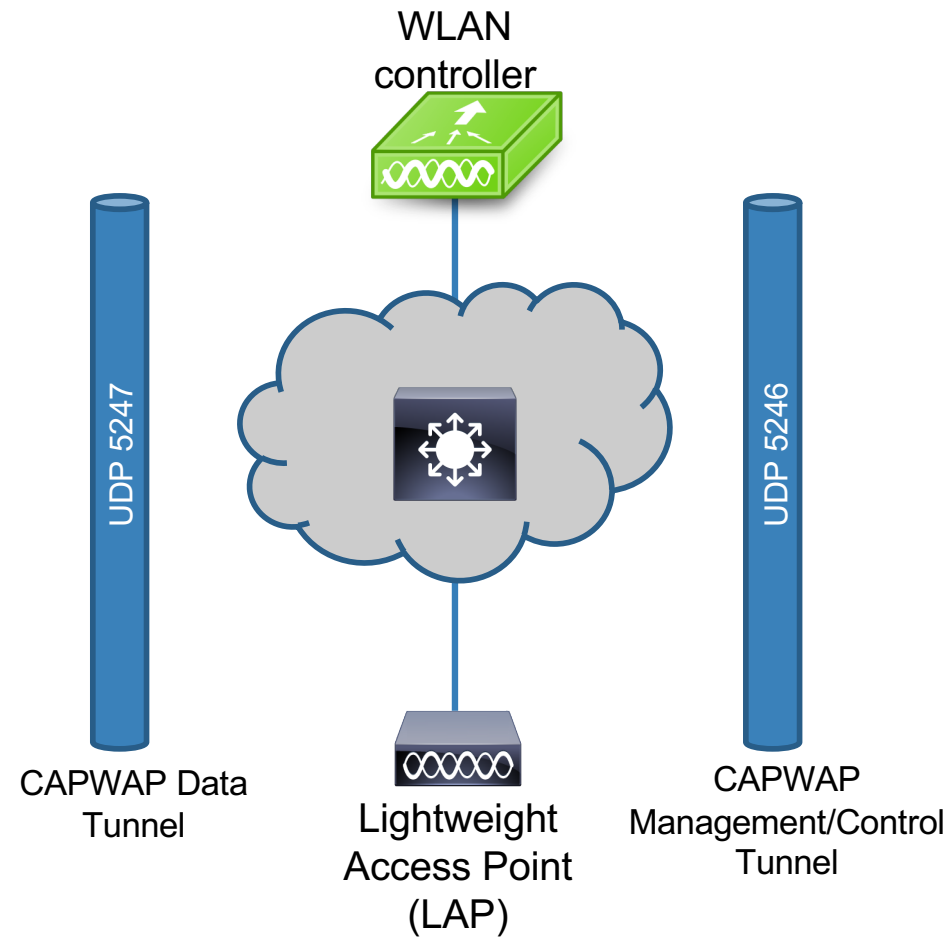
CAPWAP

- + Control and Provisioning of Wireless Access Points
- + Defined in RFCs 5415, 5416, 5417, and 5418.
- + Tunneling protocol between LAP and WLAN controller
- + Encapsulates data between LAP and controller in new IP Headers

CAPWAP Tunnels

- + Access points and controllers build two CAPWAP tunnels between themselves.
- + One tunnel is used to transmit CAPWAP Control Messages
- + The other is for tunneling CAPWAP Data

CAPWAP Tunnels



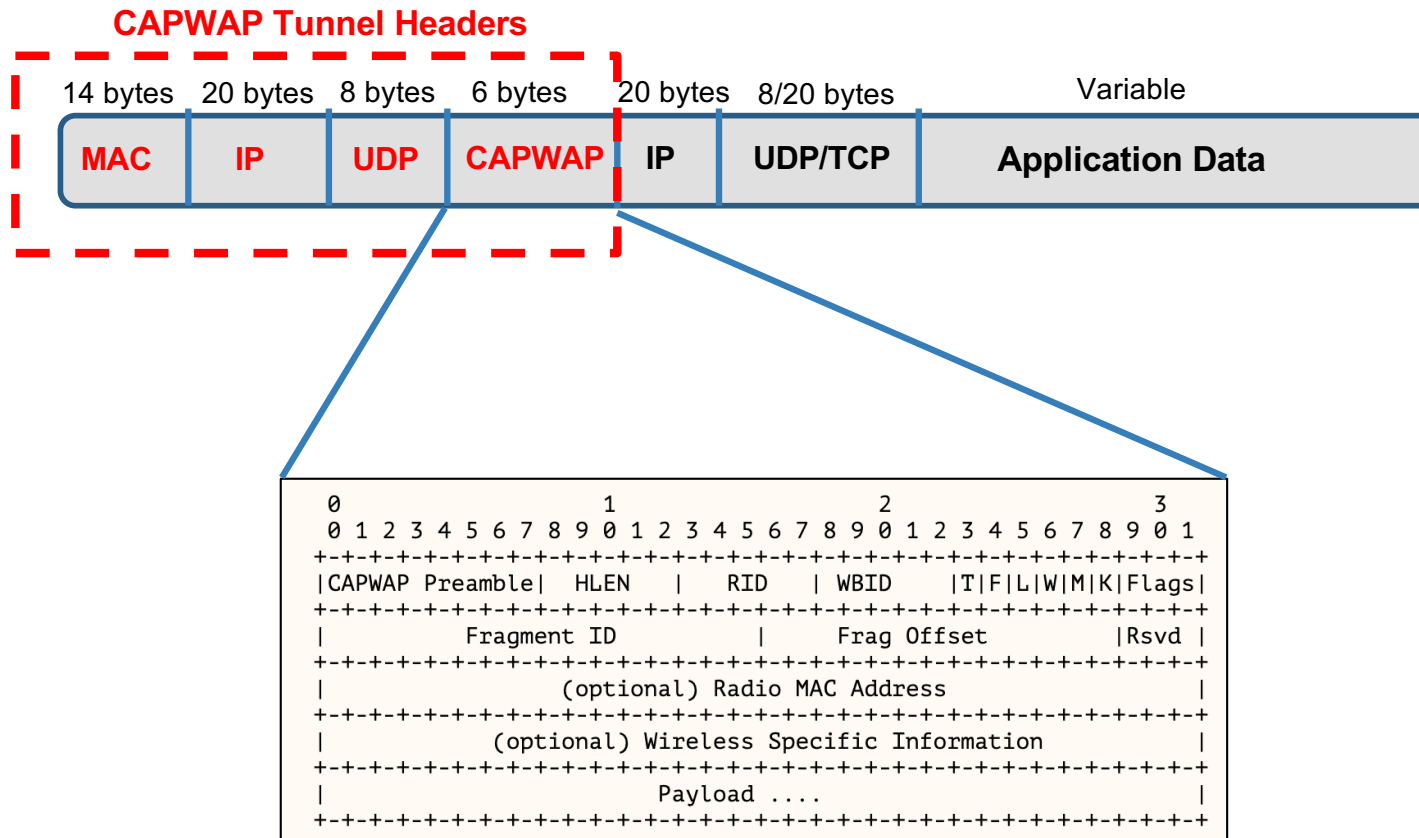
CAPWAP Tunnels For Control

- + CAPWAP Control Messages
 - + Used to control and manage LAP
 - + Messages are authenticated and encrypted
 - + Utilizes DTLS with X.509 Digital Certificates
 - + Pre-installed on devices at time of purchase
 - + Utilizes UDP port 5246 at the controller

CAPWAP Tunnels For Data

- + CAPWAP Data
 - + All Wi-Fi data frames use this tunnel, even frames going between two Wi-Fi clients on the same AP.
 - + Uses UDP port 5247
 - + Not encrypted by default
 - + DTLS (Datagram Transport Layer Security) can be added for encryption

CAPWAP Tunnel Packet Format





WLAN Controller Deployment Options

ine.com

Topic Overview

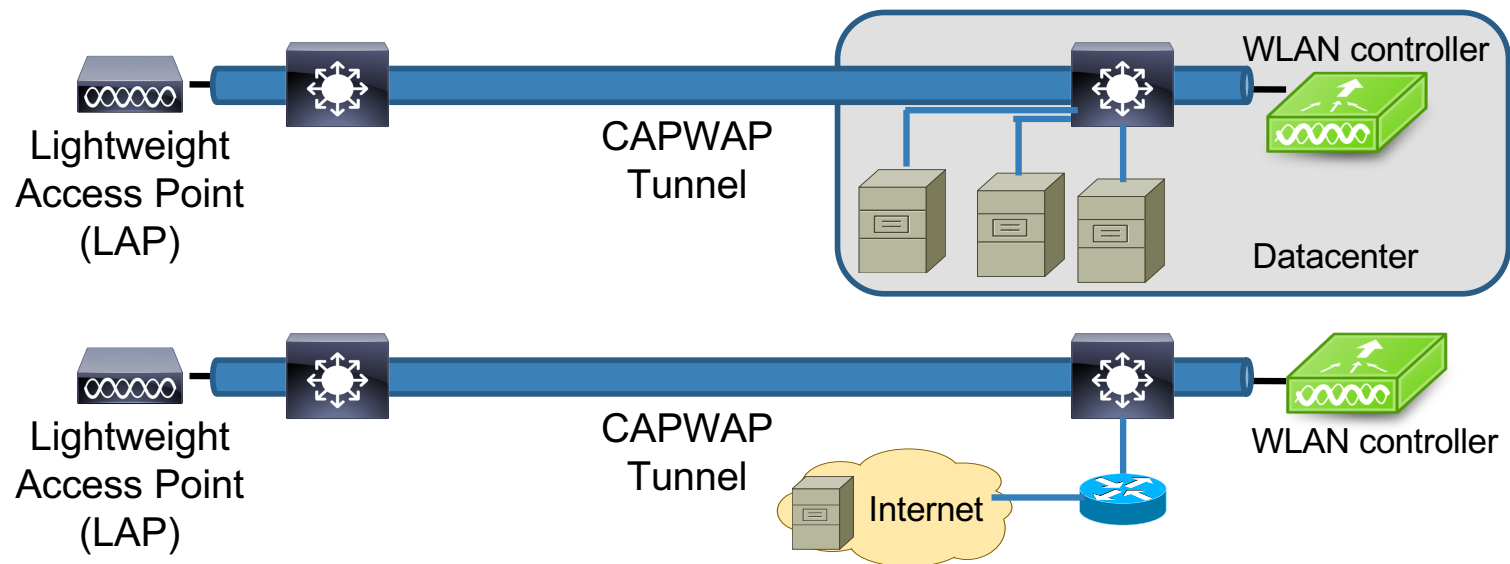
- + WLAN Controller Deployments
- + Centralized Wireless Network Architecture
- + FlexConnect Overview
- + Converged Wireless Network Architecture

WLAN Controller Deployments

- + There are two options for deploying WLAN controllers on-site
 - + Centralized Wireless Network Architecture
 - + Converged Wireless Network Architecture
- + Each option affects data path of frames

Centralized Wireless Network Architecture

- + Single controller placed in a centralized location
- + Maximizes quantity of APs each controller can control
- + RTT (Round-trip time) should be 100ms (or less) between LAP and controller



Centralized Architecture – Pros & Cons

+ Benefits

- + Controller placed in datacenter or close to Internet access point
- + Assumption is that most client data would need to reach that point anyway

+ Drawbacks:

- + All WLAN client data must pass through CAPWAP tunnel before it can be placed natively onto the wired network
- + Not a great option when destination resources needed by the WLAN client are located closer to the AP
- + Not a great option for client-to-client communications (long traffic paths)
- + When branch office LAPs are associated to a controller at the central office:
 - + Long hair-pins induced for branch office users to access local resources
 - + If CAPWAP tunnel goes down, no Wi-Fi connectivity to anything

FlexConnect Wireless Network Architecture

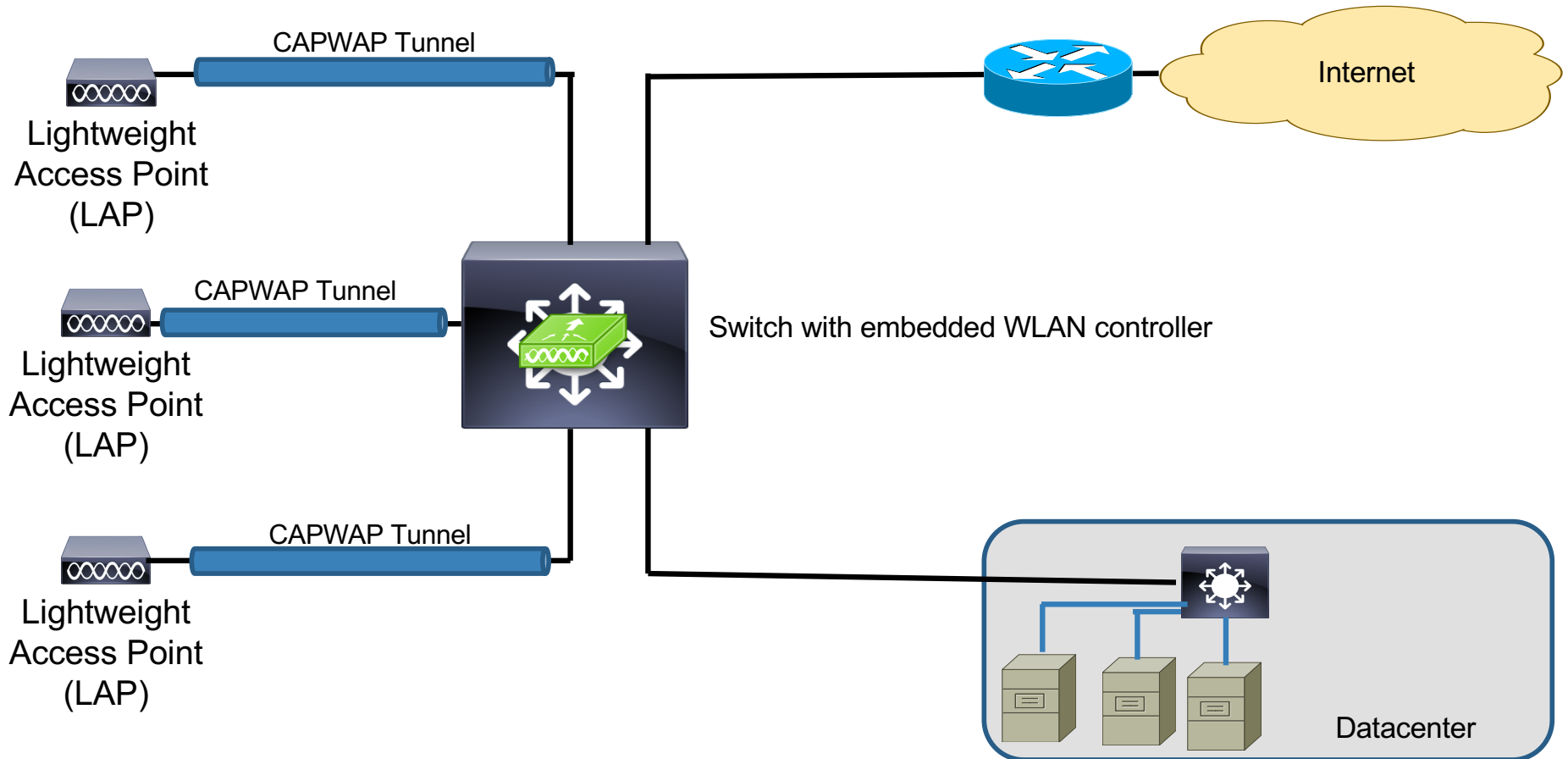
- + A mode available on LAPs
- + Primarily designed for Remote-Site/Branch LAPs utilizing a controller located at the HQ
- + Designed to alleviate long hairpins
- + Wireless traffic destined for local resources switched locally by LAP onto wired LAN
- + LAP also allowed to locally authenticate WLAN clients
- + Works even when CAPWAP tunnel goes down due to WAN failure
- + FlexConnect LAPs operate in two modes:
 - + Connected mode - When LAP has connectivity to remote controller
 - + Standalone mode - When LAP has lost connectivity to remote controller

Converged Wireless Network Architecture

- + Moving the WLAN controller away from the core towards the access or distribution layers
- + Implementing multiple controllers to divide the load from APs
- + Typically implemented using embedded WLAN controllers based on IOS-XE software



Converged Wireless Network Architecture



Converged Wireless Network Architecture

- + Benefits:
 - + Short CAPWAP data tunnels reduces the impact of hairpins
 - + Better support for faster Wi-Fi technologies (802.11ad, 802.11ax, etc)
 - + When these technologies used, Wi-Fi clients are operating at multi-gigabit speeds which would be hard to support using long CAPWAP tunnels
 - + Less APs per embedded controller reduces load on the controller
 - + Controller functionality can be placed at the Branch site
- + Drawbacks - More initial \$\$\$ outlay because several controllers needed or higher-cost switches are required



Cisco WLAN Controllers

ine.com

Topic Overview

- + Categories Of WLAN Controllers
- + Physical Controllers
- + Cloud-Based Controllers
- + Embedded Wireless
- + Cisco Mobility Express

Categories Of WLAN Controllers

- + Cisco WLAN controllers fall into four categories
 - + Physical controllers
 - + Cloud controllers
 - + Embedded wireless
 - + Mobility Express

Physical Controllers

- + Provide a dedicated appliance for WLAN access point control
- + Provide the greatest quantity of features of all the different types of WLAN controllers
- + Some examples:
 - + Catalyst 9800 series
 - + Cisco 8540
 - + Cisco 5520
 - + Cisco 3504



Catalyst 9800 WLAN controller
(image courtesy of cisco.com)

Cloud-Based Controllers

- + Meraki wireless cloud service
 - + Scales to support an unlimited number of APs and clients
 - + Requires a subscription to the Meraki cloud service
- + Catalyst 9800-CL
 - + Cloud-based controller for installation on public or private clouds
 - + AWS, KVM and VMware
 - + Packaged as a virtual machine
 - + Supports up to 6000 APs and 64,000 clients

Embedded Wireless

- + WLAN controller functionality is embedded within another network device (typically a switch)
- + Cisco 9800 can be embedded within Catalyst 9300 switch
 - + Supports up to 200 APs and 4000 clients



Cisco 9300 Switch with embedded Catalyst 9800 WLAN controller
(image courtesy of cisco.com)

Cisco Mobility Express

- + WLAN controller functionality built into certain models of Cisco access points
- + Allows one access point to serve as a WLAN controller for (up to 100) other LAPs
- + Supports redundancy in which multiple Mobility Express controllers elect one to service all APs and clients
 - + AP serving as a controller can also service local WLAN clients
 - + This is a special software image that replaces the normal CAPWAP AP image
 - + No special license is required





Infrastructure Connections Of WLAN Components

ine.com

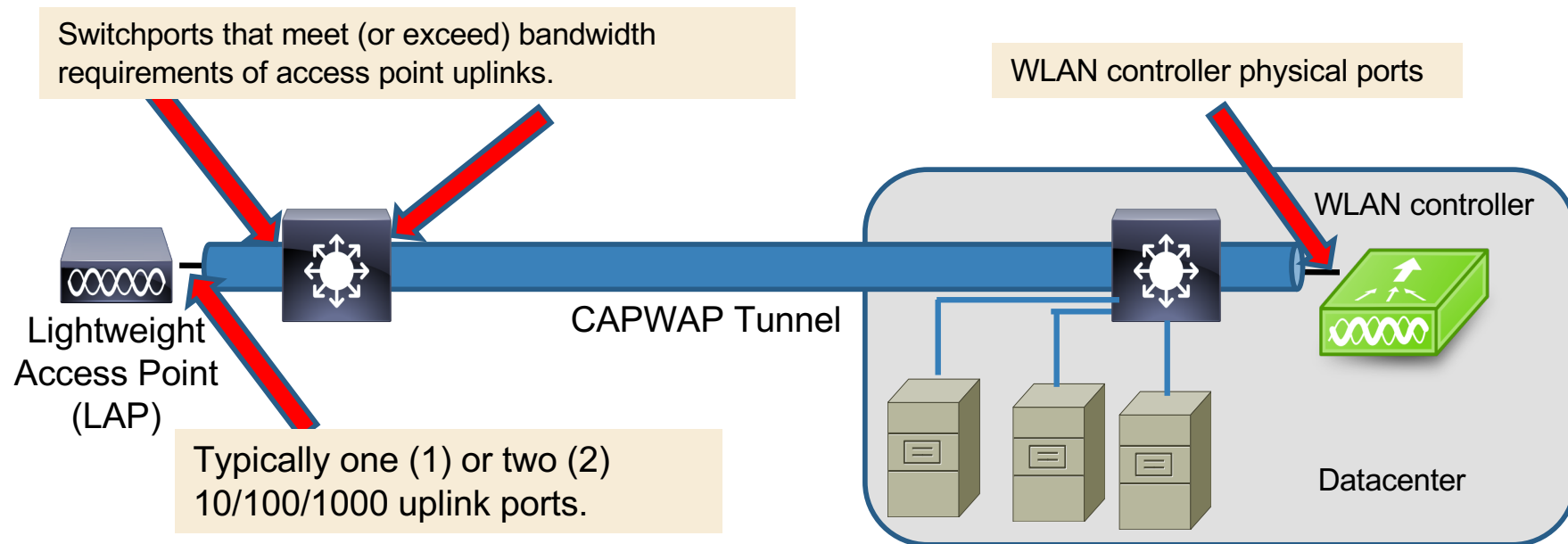
Topic Overview

- + WLAN Infrastructure Connections
- + Access Point Connections
- + Controller Connections
- + Introduction To LAG

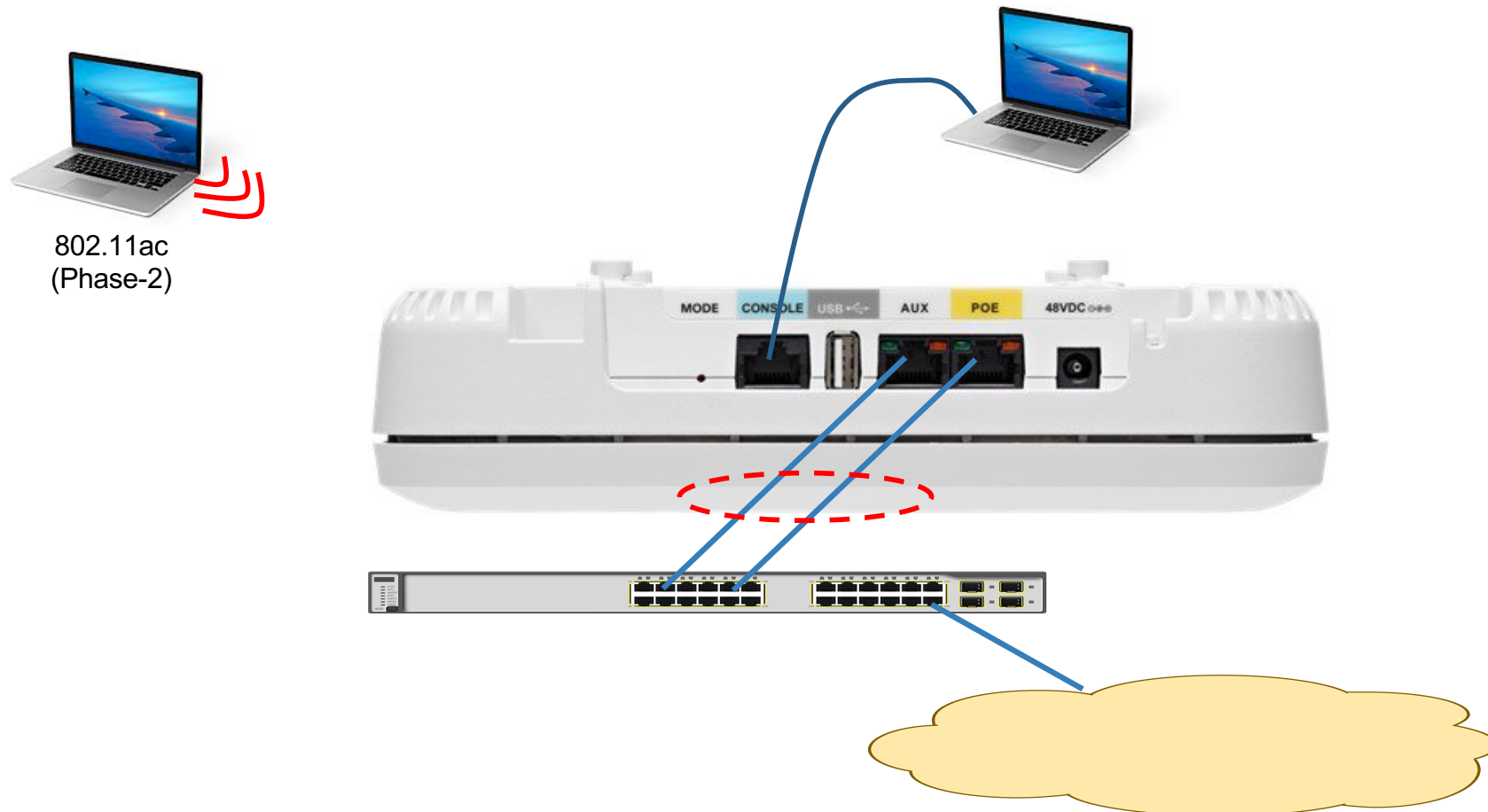
Connection Of WLAN Components

- + The components of a WLAN consist of:
 - + Access points (Autonomous and/or Lightweight)
 - + Wireless NICs on host devices
 - + Wireless transceivers built into Wi-Fi hosts and access points
 - + WLAN controllers (optional)
- + WLAN access points and controllers rely on physical connections in order to exchange data and control messages
- + So what do these connections look like?

Wireless Infrastructure Connections

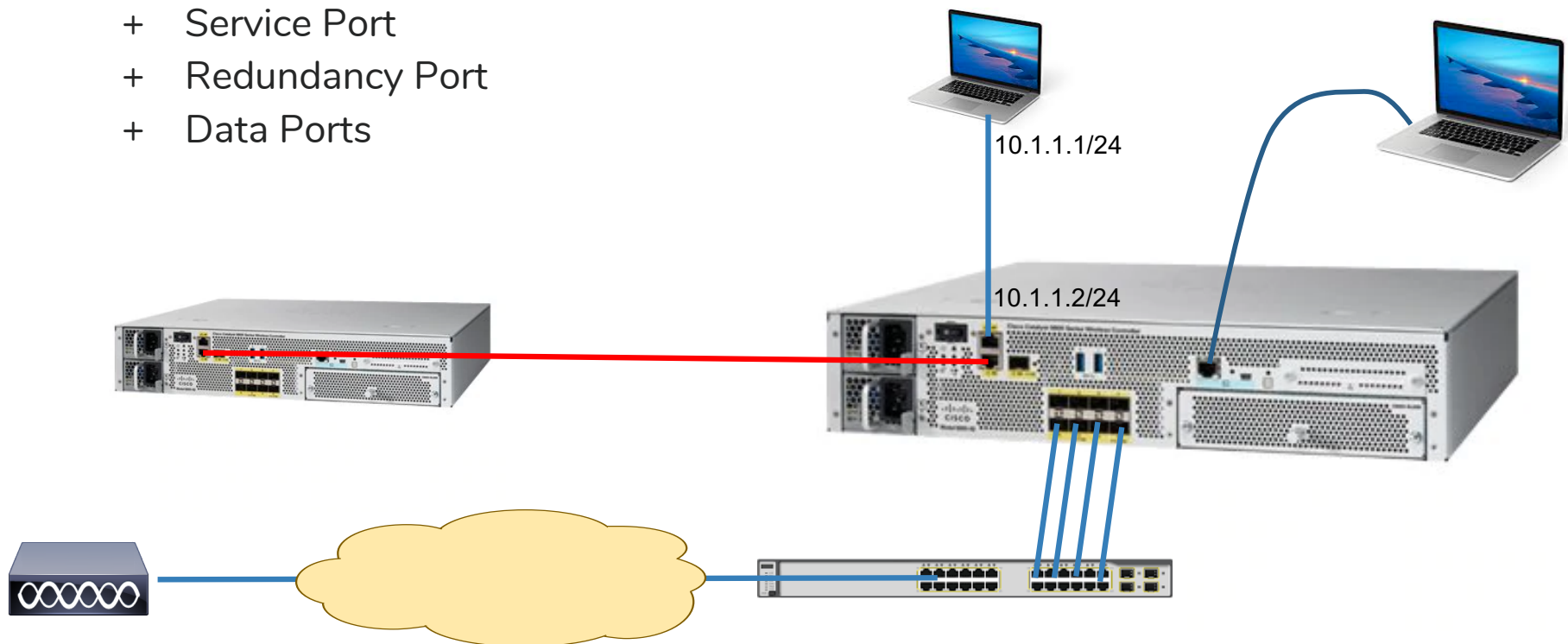


Access Point Physical Interfaces



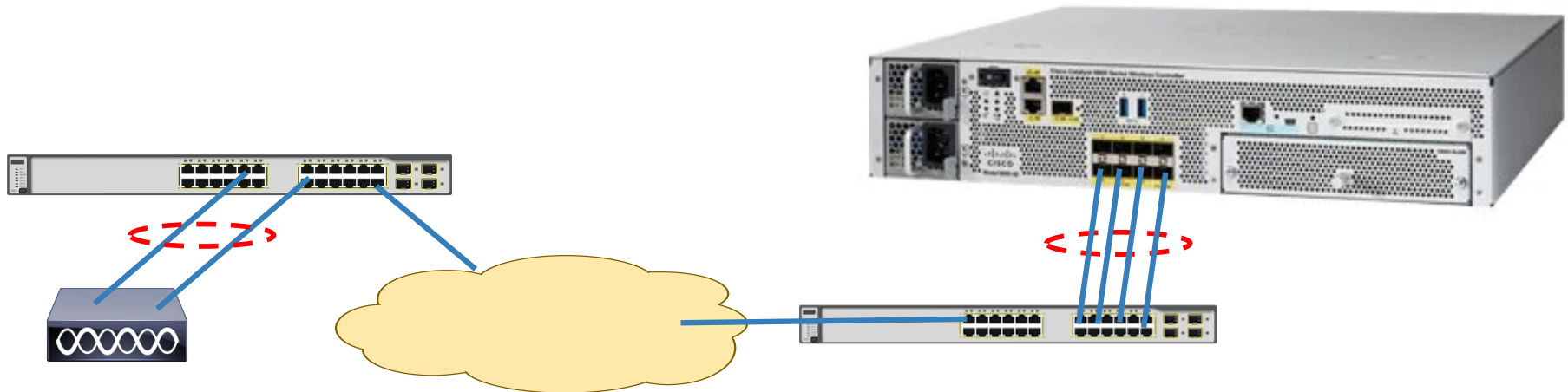
Controller Physical Interfaces

- + Physical interfaces on most controllers are divided into four categories:
 - + Console port
 - + Service Port
 - + Redundancy Port
 - + Data Ports



LAG

- + LAG = Link Aggregation Group
- + Bundles multiple physical interfaces into a single logical port group
- + Can be implemented on access points, controllers, or both
- + Provides redundancy and load-balancing
- + Requires that the connected switch support load balancing on the layer 4 (L4) source and destination ports



Access Point LAG considerations

- + Only works when access point is in Local Mode
- + Not tested between Cisco access points and non-Cisco switches
- + WLAN controller must be configured to support LAG on the access points
- + Access points only support LACP or “On” modes. PAgP not supported
- + Required on the AP in order to get maximum 802.11ac Phase-2 (and above) supported bandwidth

Controller LAG considerations

- + Controllers configured for LAG don't support LACP or PAgP
- + Load-balancing of frames leaving the controller across the LAG is done in a proprietary manner by the controller
- + Only one (1) AP-Manager interface is allowed when ports are bundled into a LAG
- + Without LAG, if a physical port fails, any access points that registered across the port must reboot



Cisco Access Point Modes

ine.com

Topic Overview

- + Introduction To Access Point Modes
- + Local & Bridged Modes
- + FlexConnect Mode
- + Monitor Mode
- + Sniffer Mode
- + Sensor Mode
- + Mesh Mode

Access Point Modes

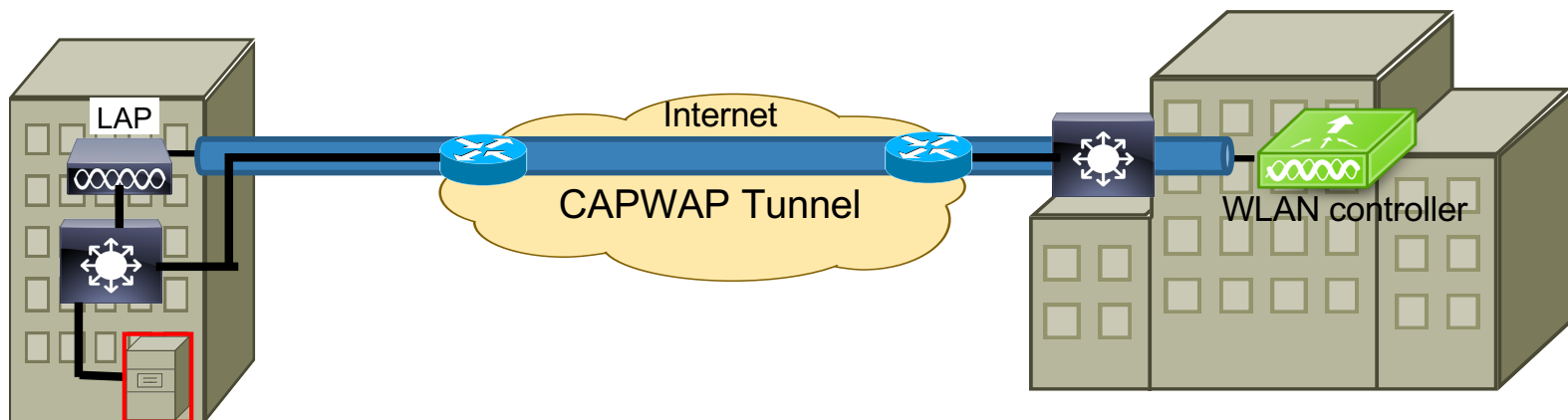
- + Cisco access points can operate in any of several modes
- + The mode-of-operation determines things such as:
 - + Is the AP associated with a controller, or not?
 - + Can the AP accept Wi-Fi clients?
 - + How will the AP switch frames from Wi-Fi clients?
 - + Can the AP report on RF conditions, capture Wi-Fi traffic or detect rogue devices?
- + Let's look these various modes...

Local & Bridged Modes

- + Local mode
 - + Default mode for lightweight access points (LAPs)
 - + AP creates CAPWAP tunnels to WLAN controller
 - + All control and data flows across CAPWAP tunnel
 - + Should CAPWAP tunnel fail (WAN failure, etc) AP disconnects all WLAN clients and must find another, available controller
- + Bridged mode
 - + Allows an autonomous access point to act as a WLAN client and associate to a LAP
 - + Wired clients (without a Wi-Fi NIC) can connect to the Ethernet port(s) on the back of the autonomous AP and have their traffic bridged across the WLAN to gain access to the Distribution System

FlexConnect Mode

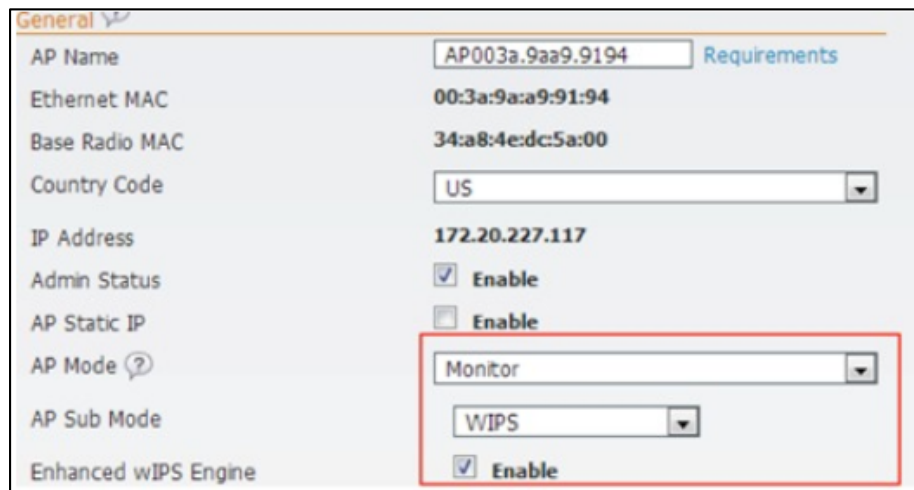
- + FlexConnect mode (a.k.a H-REAP)
 - + Access point utilizes services of controller, just like Local Mode
 - + This mode must be supported/configured on WLAN controller and AP
 - + Primarily designed for access points placed at remote sites
 - + Allows AP to locally bridge Wi-Fi traffic onto the wired LAN for clients associated to specific SSIDs/VLANs
 - + Allows AP to continue to operate even if link to controller fails



Monitor Mode

- + Cisco access points spend about 0.2% of their time performing off-channel scanning
 - + This allows the AP to generate access point rogue alerts, signature attacks, (IDS, IPS) and report about other environmental events
 - + This function is a part of RRM (Radio Resource Monitoring/Management)
- + By default, AP spends roughly 0.2% of its total time performing off-channel scanning which translates to about 60ms per scan
- + Monitor mode is a receive-only mode (no WLAN clients allowed) which scans pre-configured channels every 12-seconds
 - + Listens for (and reports to controller) any Wi-Fi traffic “heard” on the selected channel
 - + AP will reboot when set to this mode

Attacks That Can Be Detected By Monitor Mode



The screenshot shows the 'General' configuration page for a Cisco Access Point. The 'AP Mode' dropdown menu is highlighted with a red box and set to 'Monitor'. Other visible settings include AP Name (AP003a.9aa9.9194), Ethernet MAC (00:3a:9a:a9:91:94), Base Radio MAC (34:a8:4e:dc:5a:00), Country Code (US), IP Address (172.20.227.117), Admin Status (Enabled), AP Static IP (Disabled), AP Sub Mode (WIPS), and Enhanced WIPS Engine (Enabled).

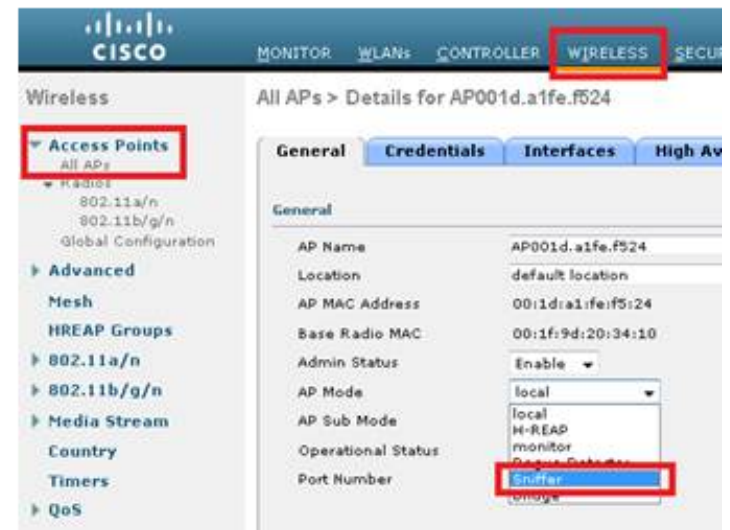
AP Name	AP003a.9aa9.9194	Requirements
Ethernet MAC	00:3a:9a:a9:91:94	
Base Radio MAC	34:a8:4e:dc:5a:00	
Country Code	US	
IP Address	172.20.227.117	
Admin Status	<input checked="" type="checkbox"/> Enable	
AP Static IP	<input type="checkbox"/> Enable	
AP Mode (?)	Monitor	
AP Sub Mode	WIPS	
Enhanced WIPS Engine	<input checked="" type="checkbox"/> Enable	

Images courtesy of cisco.com

Smartphone tethering detection and containment
Location tracking and containment for DoS attacker and non-authorized device that is trying to associate internal access point
Wired Equivalent Privacy (WEP) cracking detection
MAC spoofing rogue's detection and containment
Auto MAC learning
Internet connection sharing (ICS) detection
Enterprise-level alarm/event correlation
Attack signature threshold customization
Off-channel rogue detection and location, integrated into infrastructure
DoS signature updates
Wireless intrusion signature updates
Attack forensics (all signatures)

Sniffer Mode

- + Very similar to Monitor mode
- + Unlike Monitor mode (in which all 2.4GHz and 5GHz channels are scanned), Sniffer mode requires you select an individual channel
- + All Wi-Fi traffic caught on this channel sent to WLAN controller
- + Controller configured with LAN IP address of a host running:
 - + Wireshark
 - + Omnipcap
 - + Airopeek
 - + AirMagnet
- + Packets sent to LAN host encapsulated in UDP:
 - + Source port 5555
 - + Destination port 5000



Sensor Mode

- + An AP functioning in Sensor mode is part of a solution involving:
 - + A WLAN controller
 - + An access point
 - + Cisco DNA Center
- + WLAN controller receives a series of preconfigured tests to be run from DNA Center, which is then pushed down to access point
- + SSIDs are selected on controller for which tests are to be performed
- + AP in Sensor Mode will associate to all other LAPs it can hear (advertising the selected SSID) and perform tests including:
 - + Onboarding tests
 - + Network tests
 - + Application tests
- + All test results sent directly from AP back to DNA Center appliance

Sensor Mode Tests

Network Tests		Application Tests	
IP Addressing Tests		Email Tests	
<input checked="" type="checkbox"/> DHCPv4		<input type="checkbox"/> POP3 (IPv4)	
DNS Tests		Enter POP3 Server	
<input type="checkbox"/> DNS (IPv4)		+	
Hostname to resolve			
Host Reachability Tests		<input type="checkbox"/> IMAP (IPv4)	
<input type="checkbox"/> User Defined Host (IPv4)		Enter IMAP Server	
		+	
Internal IP Address		URL	
External IP Address		User Name	
<input type="checkbox"/> Default Gateway Reachability (IPv4)		Password	
		+	
RADIUS Tests		Web Tests	
<input type="checkbox"/> RADIUS Server (IPv4)		<input type="checkbox"/> HTTP (IPv4)	
IP Address / Hostname		Enter URL	
		+	
User Name			
Shared Secret			
Password			
Port		File Transfer Tests	
Protocol		<input type="checkbox"/> FTP (IPv4)	
		Server Name	
		User Name	
		Password	
		Protocol	
		ftp	
		Transfer Type	
		Download File Path/Upload Path	
		+	

Mesh Mode

- + In some environments, providing Wi-Fi to clients is desired but there may be no physical connection for access points to connect to a wired LAN
 - + Parks
 - + City streets
 - + Amphitheaters
 - + Warehouses
- + Access points may be configured in Mesh mode in which they will associate with each other to carry data from a Wi-Fi client, through multiple Mesh nodes, and ultimately place that data onto the wired Distribution System.

Sample Mesh Topology

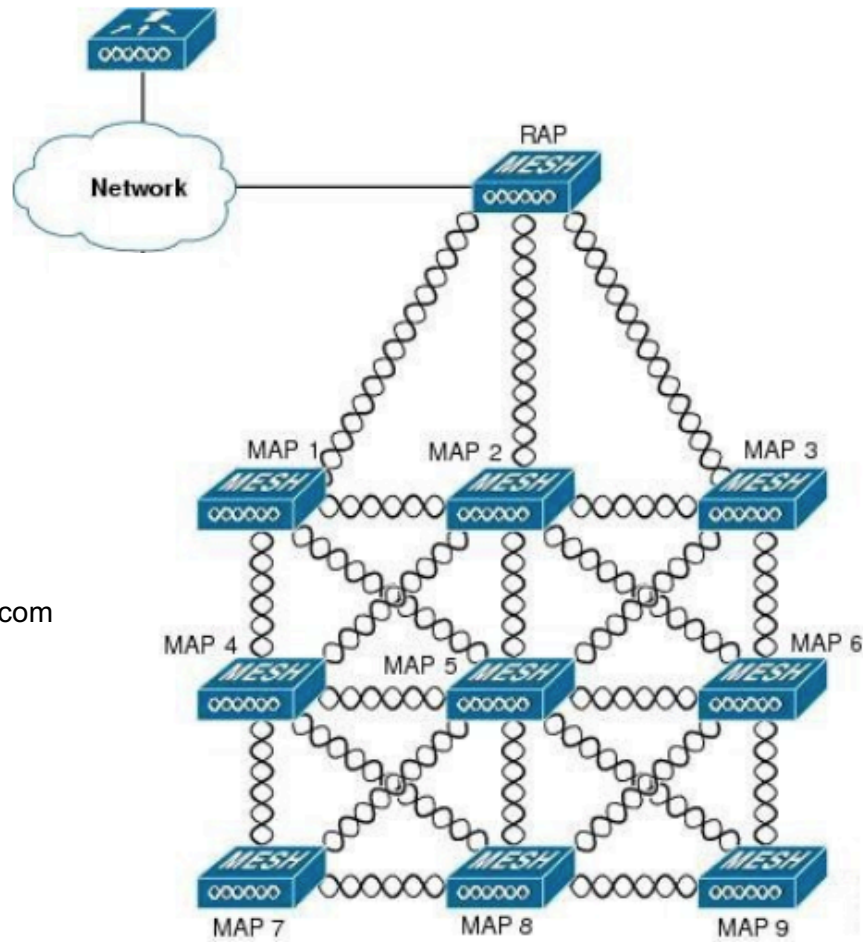
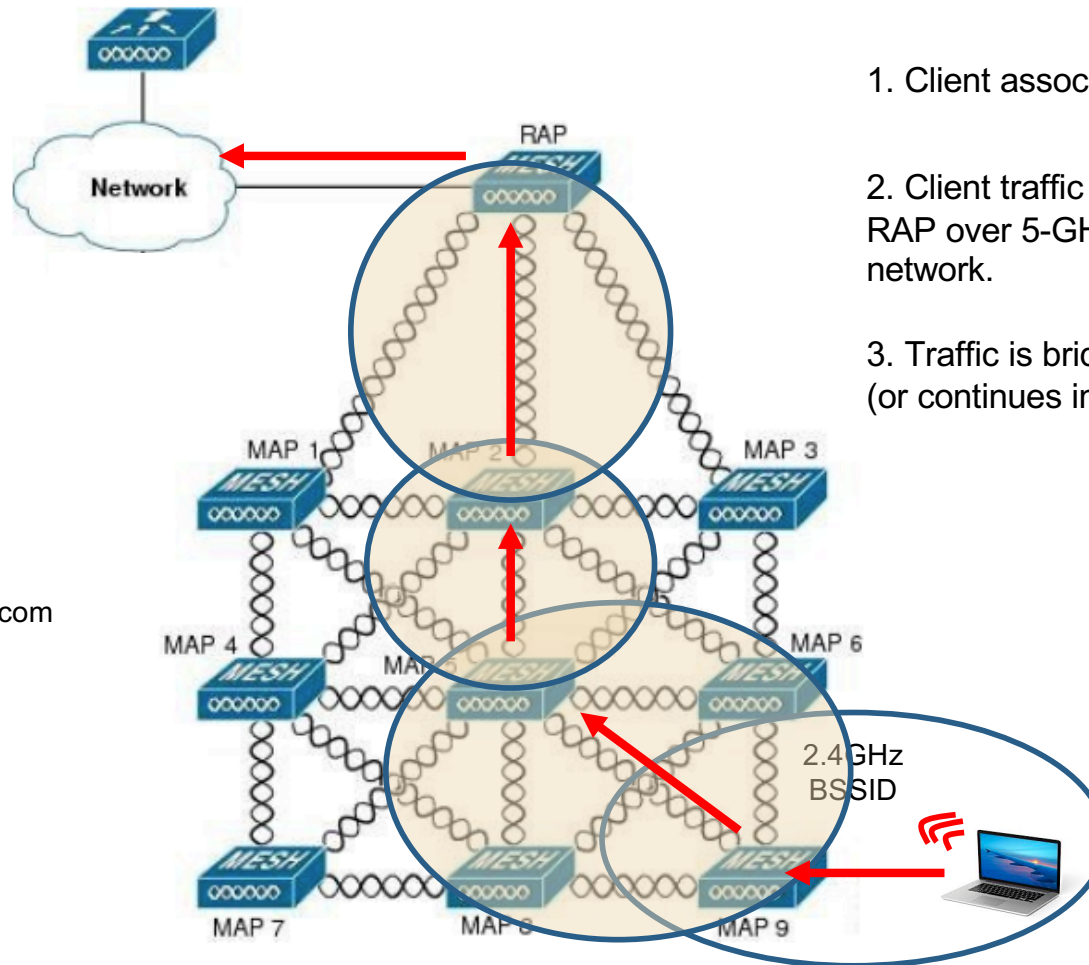


Image courtesy of cisco.com

Mesh Mode

- + Access points in mesh mode operate in one-of-two ways:
 - + Root access point (RAP): Has wired access to controller
 - + Mesh access point (MAP): Has wireless access to controller
- + A mesh Wi-Fi network requires at least one RAP
- + MAPs use the Cisco Adaptive Wireless Path Protocol (AWPP) to determine the best path through the other mesh access points to the controller
- + Mesh access points can also simultaneously operate in any of the previously-mentioned modes (Sniffer, Monitor, Sensor, etc)

Mesh Client Traffic Flow



1. Client associates on 2.4GHz BSSID of MAP

2. Client traffic is then bridged from MAP to RAP over 5-GHz channels as a backhaul network.

3. Traffic is bridged by RAP onto wired LAN (or continues in CAPWAP tunnel to controller)

Image courtesy of cisco.com



Thanks for Watching!