

Identifying Wireless Networking Considerations



Designing for Cisco Internetwork Solutions (DESGN) v2.0

Introducing the Cisco Unified Wireless Network

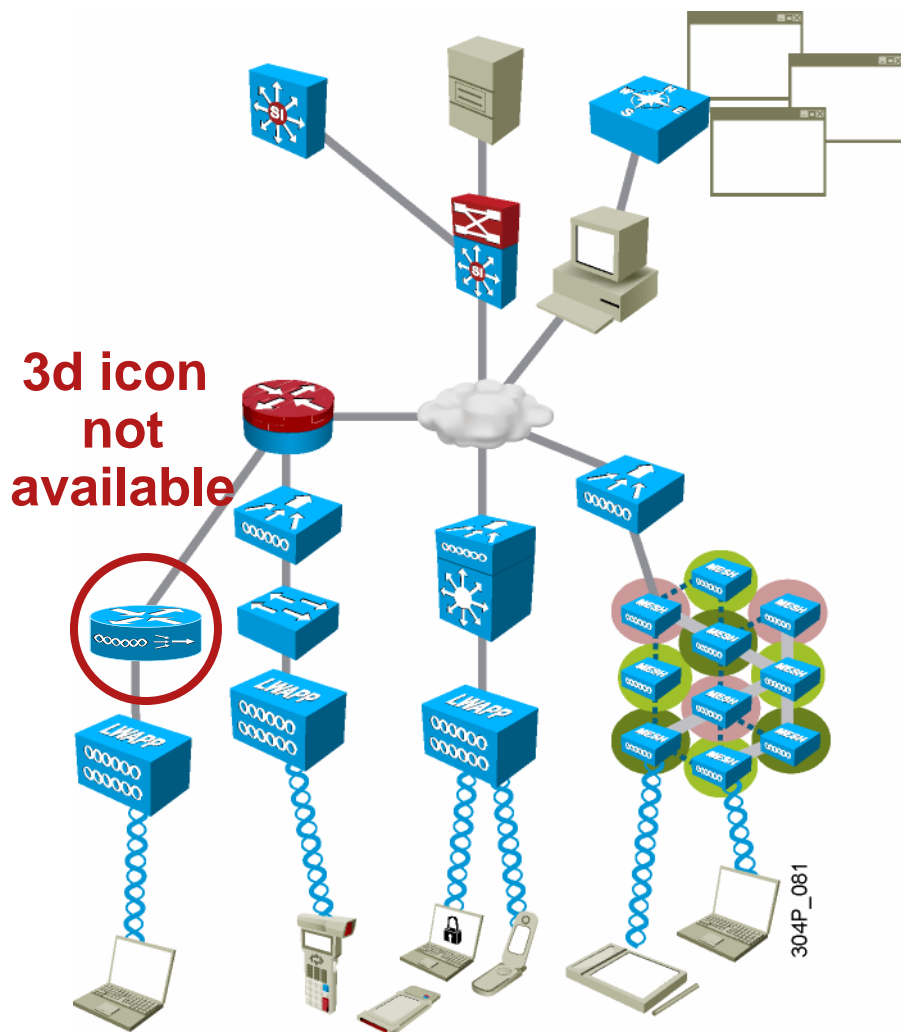


Identifying Wireless Networking Considerations

Wireless LAN Background

- WLANs provide network connectivity over radio waves.
- Wireless stations connect to wireless access points.
- Access points connect to the wired network.
 - Access points were traditionally autonomous.
 - Scaling the design and adding applications was challenging.

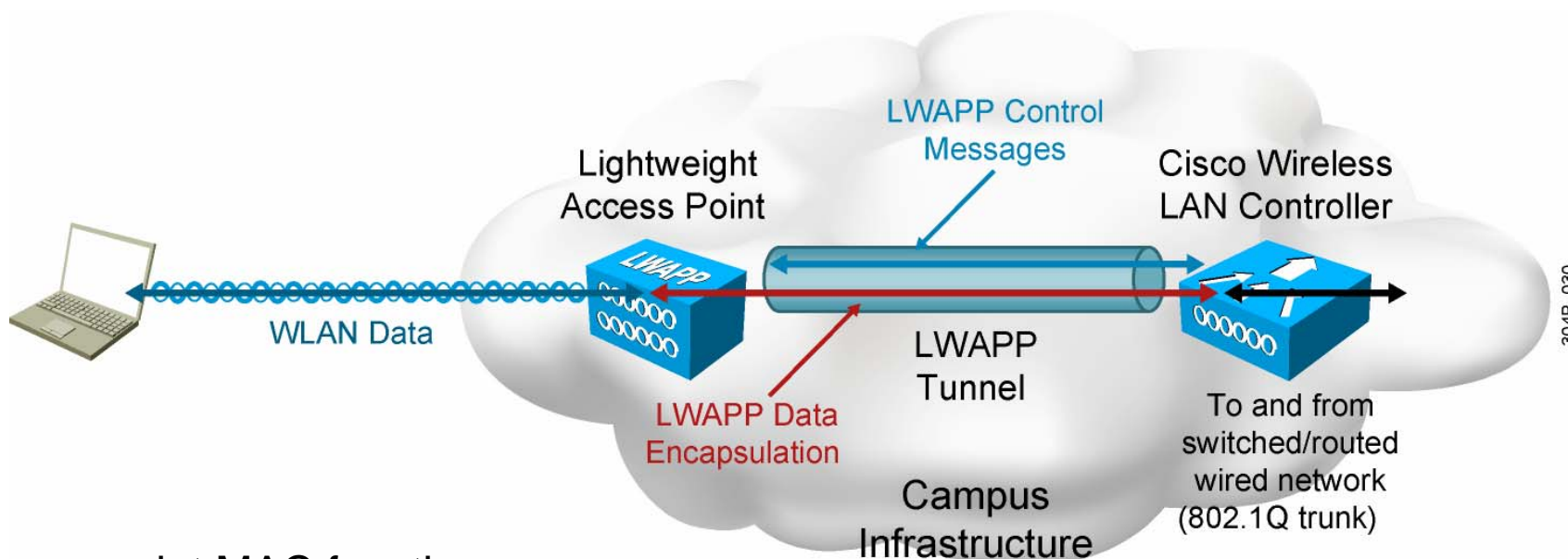
Cisco Unified Wireless Network Elements



Intelligent information network elements:

- Mobility services
- Network management
- Network unification
- Access points
- Client devices

Cisco Unified Wireless Network— Split-MAC Operation



Access point MAC functions:

- 802.11: Beacons, probe response
- 802.11 control: Packet acknowledgment and transmission
- 802.11e: Frame queuing and packet prioritization
- 802.11i: MAC layer data encryption and decryption

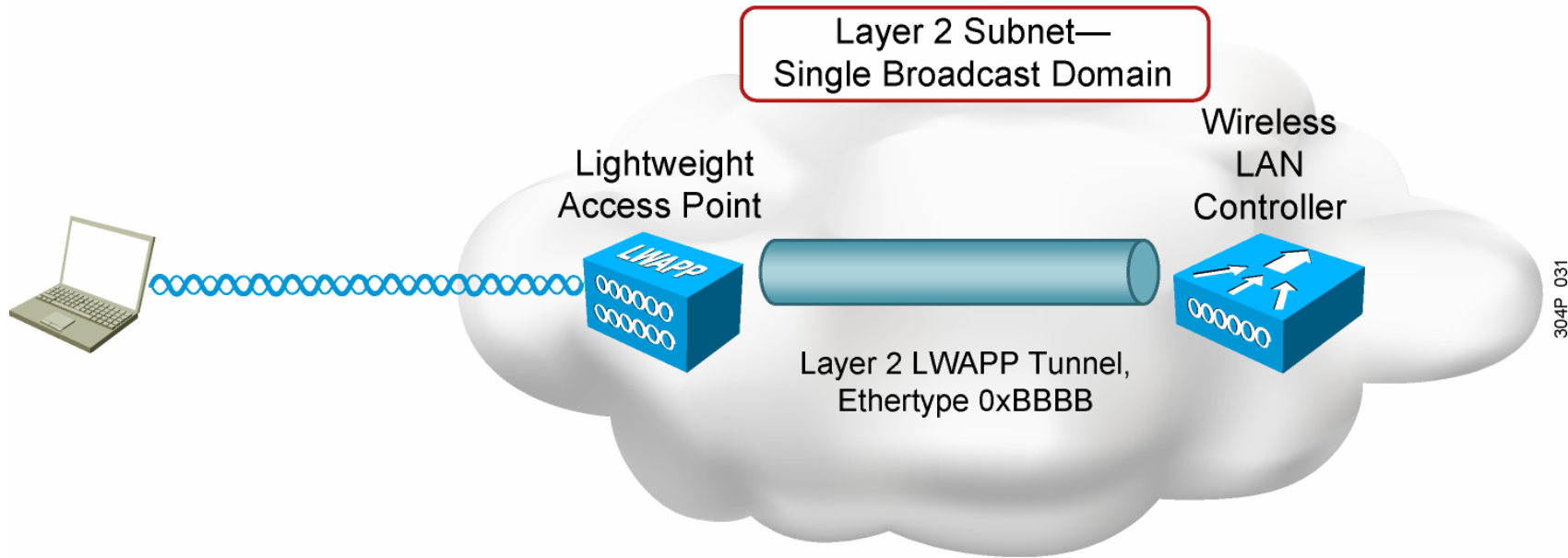
Controller MAC functions:

- 802.11 MAC management: Association requests and actions
- 802.11e Resource reservation
- 802.11i Authentication and key management

LWAPP Fundamentals

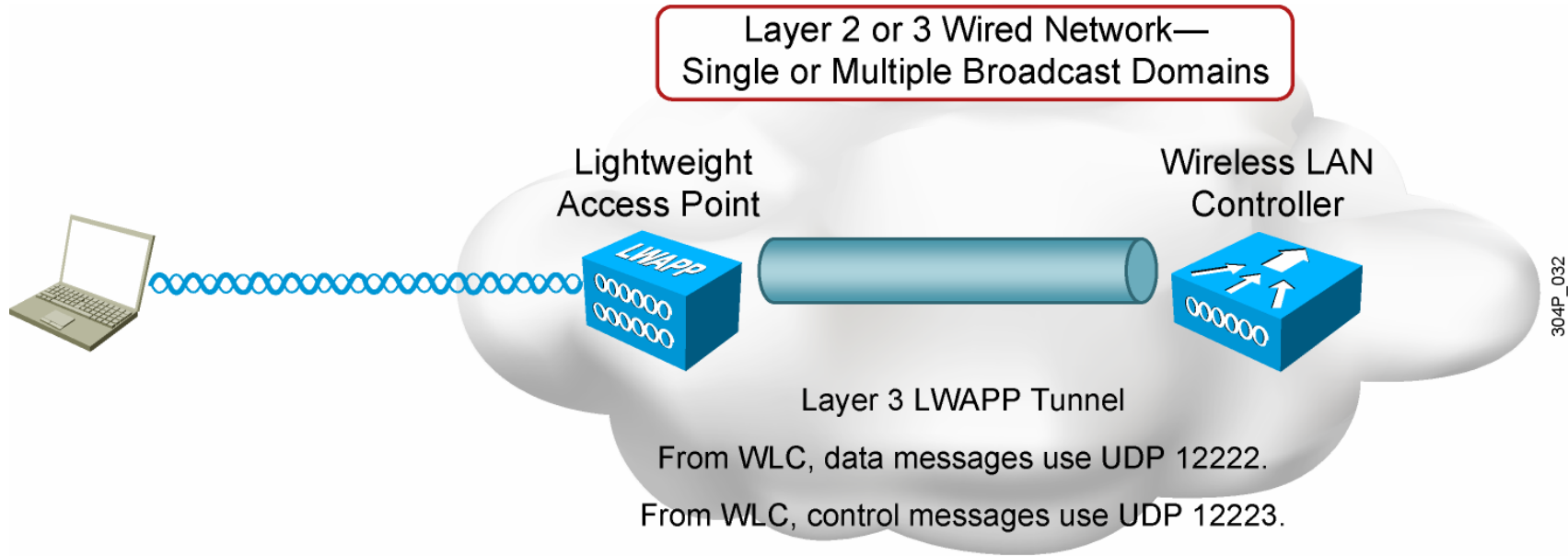
- LWAPP is an IETF draft specification.
- Access points communicate with a WLC using LWAPP:
 - LWAPP control messages are exchanged between a WLC and access points.
 - LWAPP data messages encapsulate data frames.
- LWAPP tunnel can be Layer 2 or Layer 3.
- One WLC can manage multiple access points.
 - The WLC supplies configuration and firmware updates to access points.

Example: Layer 2 LWAPP Architecture



- Access points do not require IP addressing.
- Controllers need to be on **every** subnet on which access points reside.
- Layer 2 LWAPP was an early part of the architecture; many current products do not support this functionality.

Example: Layer 3 LWAPP Architecture



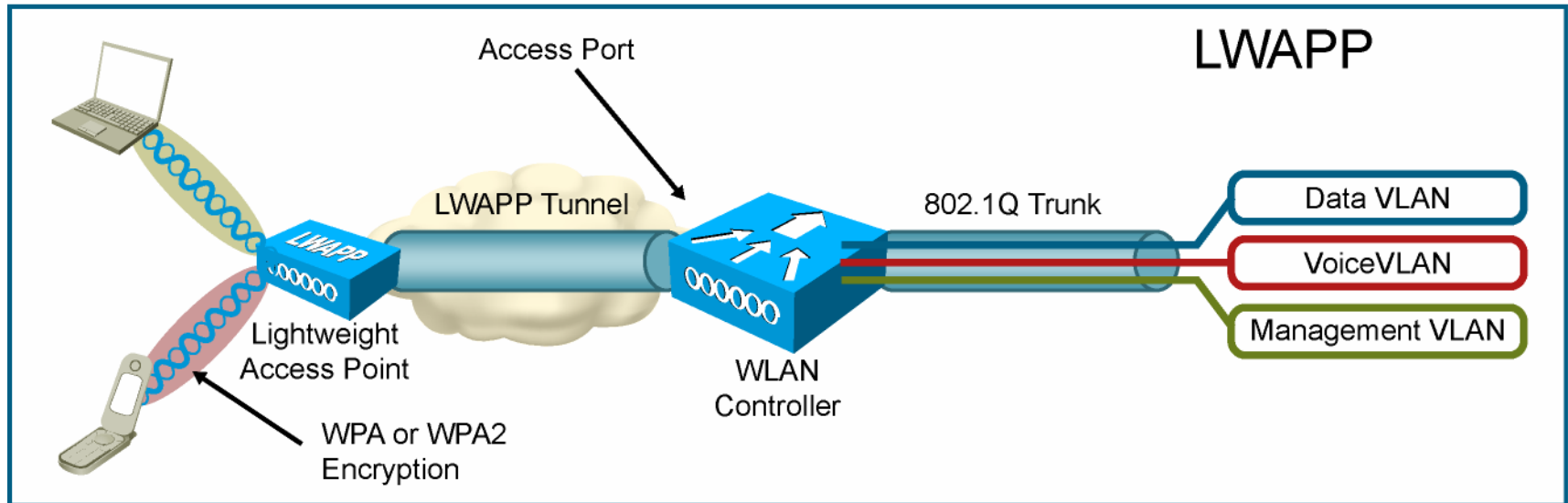
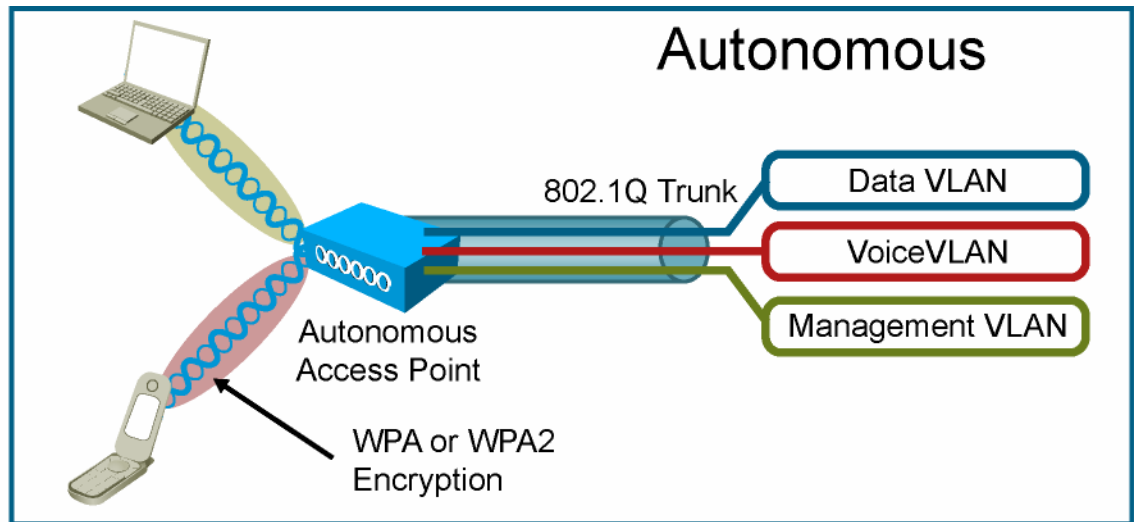
- Access points require IP addressing.
- Access points can communicate with a WLC across routed boundaries.
- Layer 3 LWAPP is more flexible than Layer 2 LWAPP; most current products support this LWAPP mode.

Access Point Modes

- **Local mode** is the default mode of operation.
- **REAP mode** enables a remote access point across a WAN link to communicate with the WLC.
- **Rogue detector mode** allows the access point to monitor rogue access points but cannot contain rogue access points.
- **Monitor mode** allows the access points to act as dedicated sensors for IDS and supports deauthentication capability.
- **Sniffer mode** functions as a network sniffer and captures and forwards all the packets on a particular channel to a remote machine that runs AiroPeek.
- **Bridge mode** allows the Cisco Aironet 1030 (indoor) and 1500 (outdoor mesh) access points to support point-to-point and point-to-multipoint bridging.

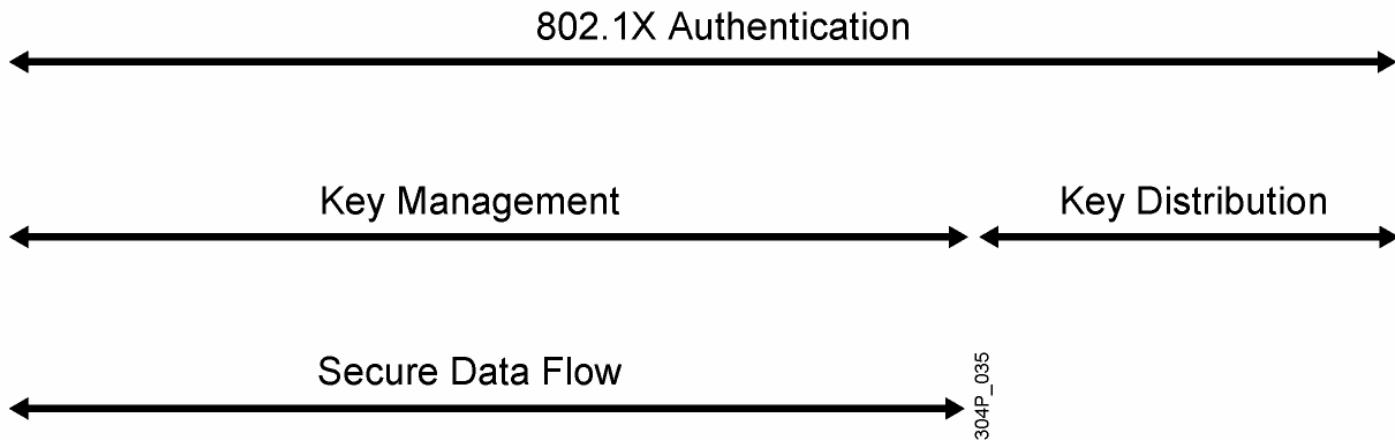
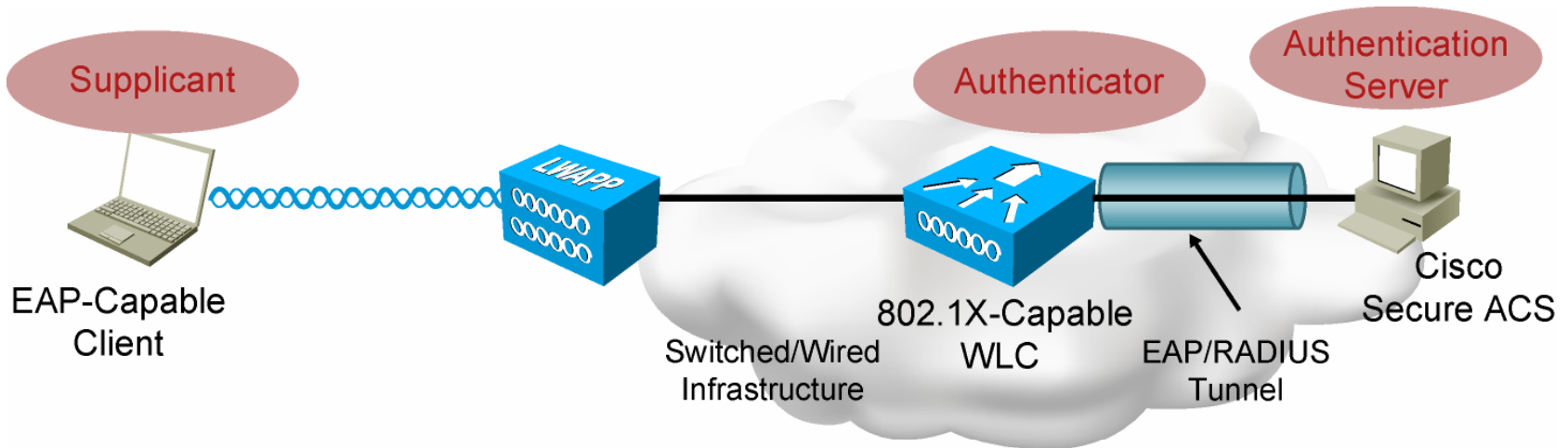
Wireless Infrastructure

- Autonomous access point is an 802.1Q translational bridge.
- WLAN controller bridges client traffic centrally.



304P_085

Wireless Authentication



Example: Supported EAP Types

- EAP-Transport Layer Security (EAP-TLS)
 - Mutual client and server authentication using digital certificates
- EAP-Protected EAP (EAP-PEAP)
 - Authentication of RADIUS server in TLS using digital certificate
 - Authentication of client using EAP-GTC or EAP-MSCHAPv2
- EAP Tunneled Transport Layer Security (EAP-TTLS)
 - Authentication of RADIUS server in TLS using server certificate
 - Authentication of client using username and password
- Cisco LEAP
 - Early EAP method supported in Cisco Compatible Extensions
- Cisco EAP-FAST
 - Three-phase EAP method supported in Cisco Compatible Extensions

Important WLAN Controller Components

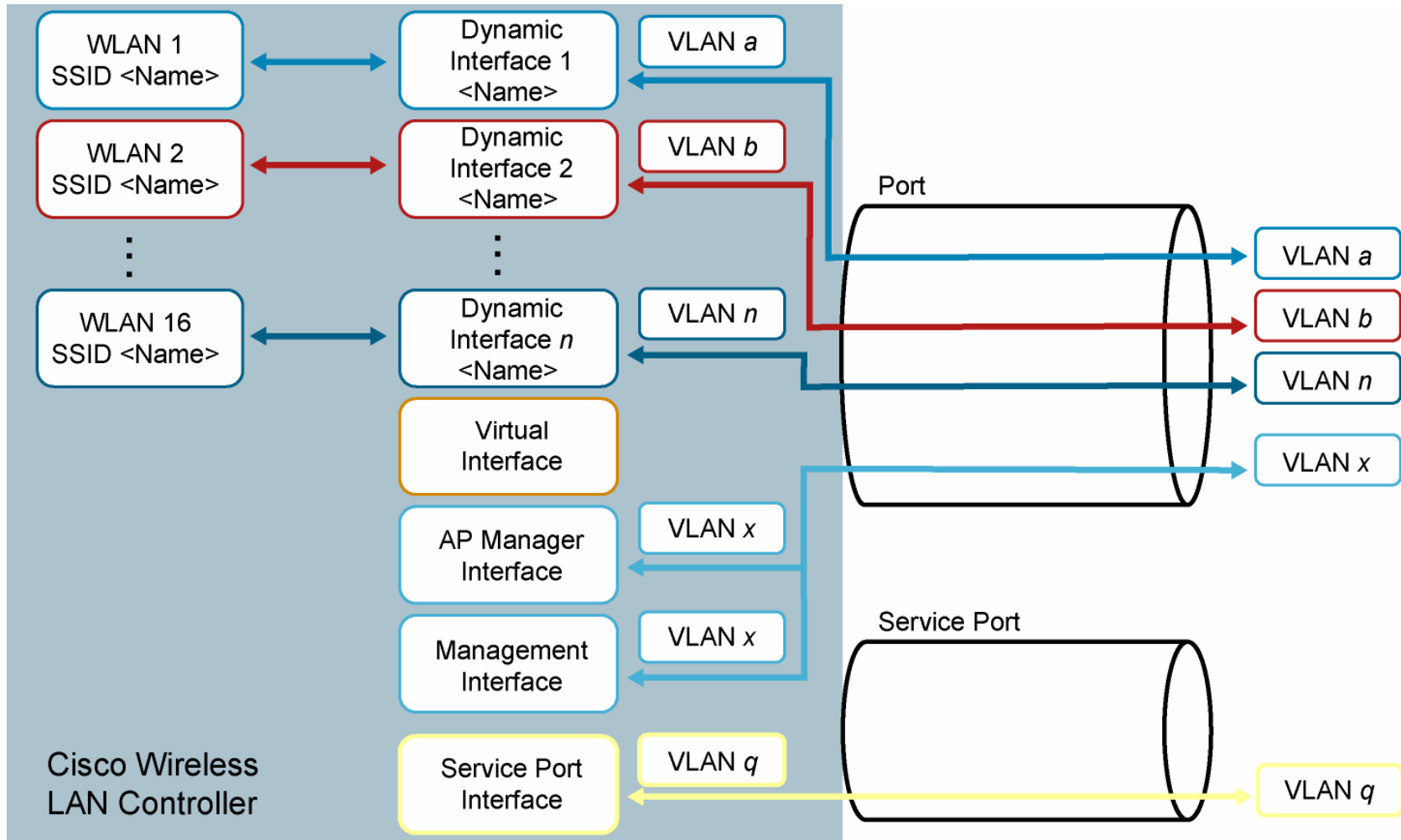
Three important components to understand:

- **Port**—Physical connection to a neighbor switch or router
- **Interface**—Logical connection mapping to a VLAN on the wired network
- **WLAN**—Logical entity that maps an SSID to an interface at the controller, along with security, QoS, radio policies, and other wireless networking parameters

Summary of WLC Interfaces






- **Management interface**—Is used for in-band management, connectivity to AAA and other enterprise services, and for Layer 2 access point auto discovery and association
- **AP-manager interface**—Is the source IP address used for access point-to-controller communication and Layer 3 access point autodiscovery and association
- **Dynamic interface**—Is designated for WLAN client data and analogous to a VLAN
- **Virtual interface**—Supports DHCP relay, Layer 3 security authentication, and mobility management
- **Service-port interface**—Provides out-of-band management of the controller

Example: WLANs, Interfaces, and Ports



004P_008

Cisco Wireless LAN Controller Platforms

	Platform	Number of Access Points Supported
	Cisco 2000 Series Wireless LAN Controller	6
	Cisco Wireless LAN Controller Module for ISRs	6
	Cisco Catalyst 3750G Integrated Wireless LAN Controller	Up to 50
	Cisco 4400 Series Wireless LAN Controller	Up to 100
	Cisco Catalyst 6500 Series Wireless Services Module	Up to 300

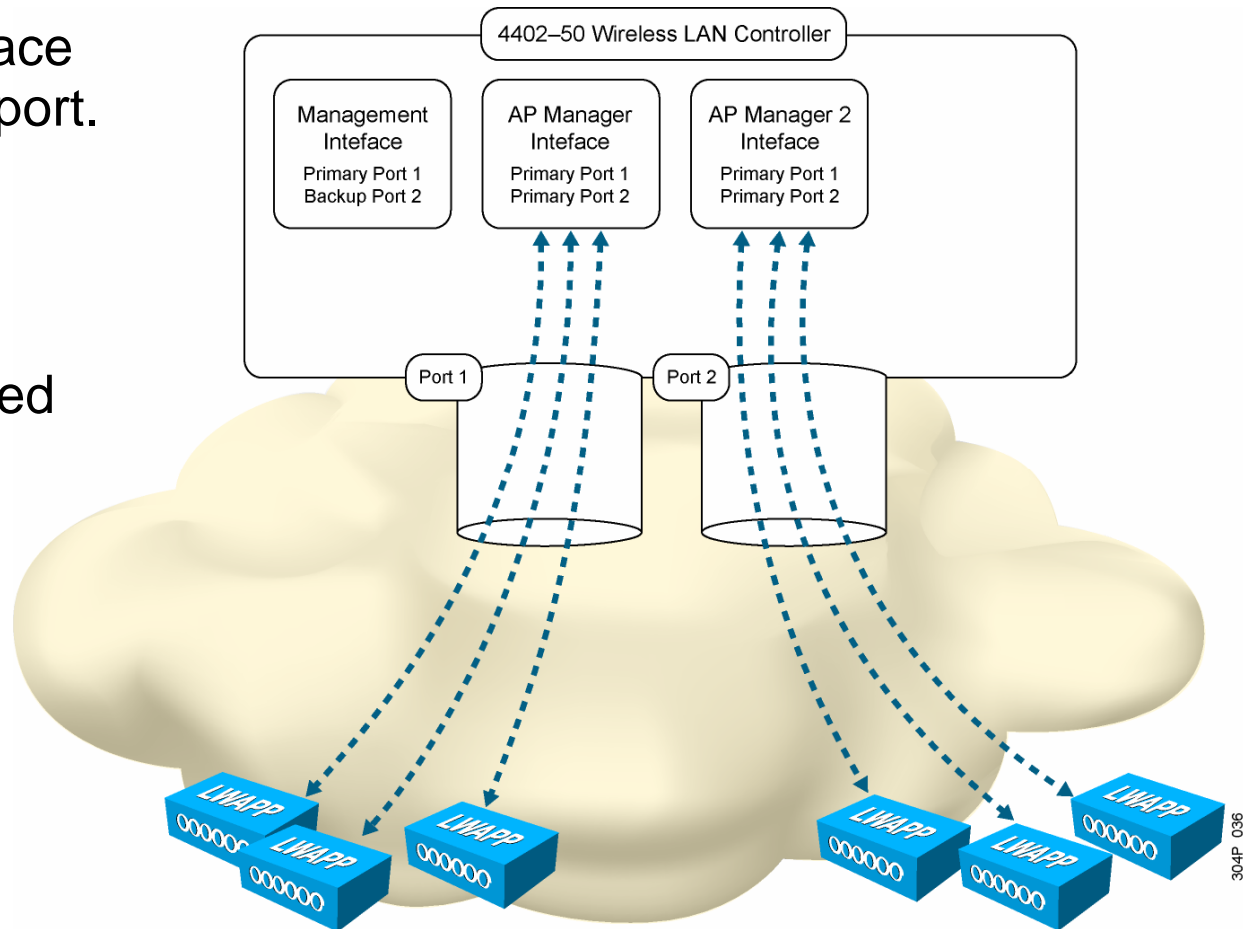
Note: The number of access points supported may change as products are updated. Check www.cisco.com for the latest information.

Access Point Scalability Considerations

- 4400x series controllers allow 48 access points per port in the absence of link aggregation.
- Two options for scaling are:
 - Multiple AP manager interfaces (supported only on 4400x appliance controllers).
 - Link aggregation (supported on 4400x appliances, Cisco WiSM, Cisco 3750G Integrated Wireless LAN Controller).
- With multiple AP manager interfaces, the LWAPP algorithm load-balance access points across the AP manager interfaces.
- With LAG, one AP manager interface load-balances traffic across an EtherChannel interface.

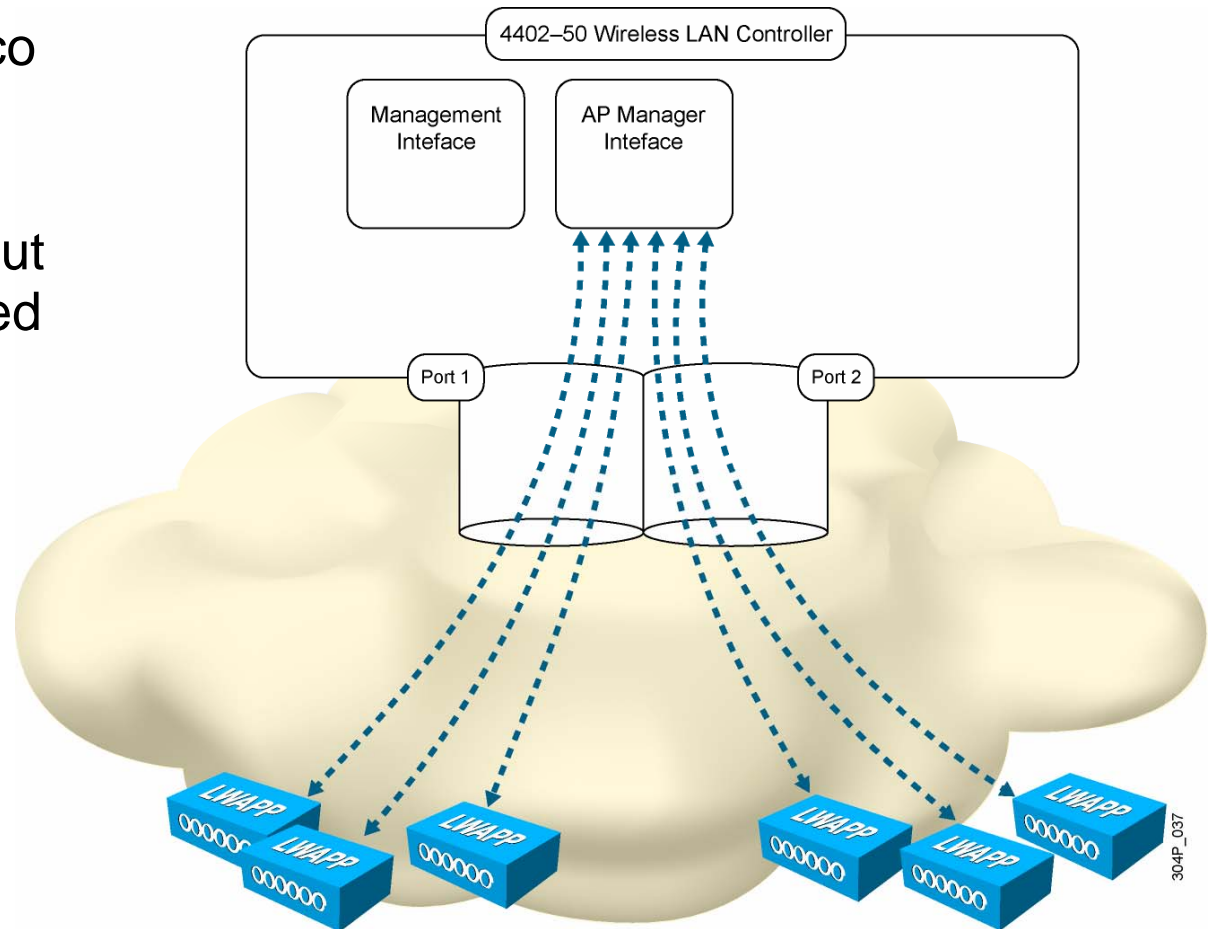
Example: Multiple AP Manager Interfaces

- Each AP manager interface is mapped to a physical port.
- Access point load is dynamically distributed.
- Redundancy advantage: Platform can be connected to multiple devices.
- Redundancy concern: Only 48 access-points are supported per port.



Example: LAG with a Single AP Manager Interface

- One LAG group per Cisco Wireless LAN Controller is supported.
- Packets are forwarded out the same port they arrived on.
- It is recommended that you use LAG if possible.



Summary

- The Cisco Unified Wireless Network architecture centralizes WLAN configuration and control on Cisco Wireless LAN Controllers.
- Cisco Wireless LAN Controllers manage access points using LWAPP.
- The Cisco Unified Wireless Network is based on devices connecting to access points using RF signals, access points sending client traffic to controllers across an LWAPP tunnel, and Cisco Wireless LAN Controllers placing the traffic in the appropriate VLAN in the wired network.
- Cisco Wireless LAN Controllers components include ports (physical connections), interfaces (logical mappings to a VLAN), and WLANs (logical mappings of an SSID to an interface).
- Cisco Wireless LAN Controller platforms can support 6 to 300 access points.