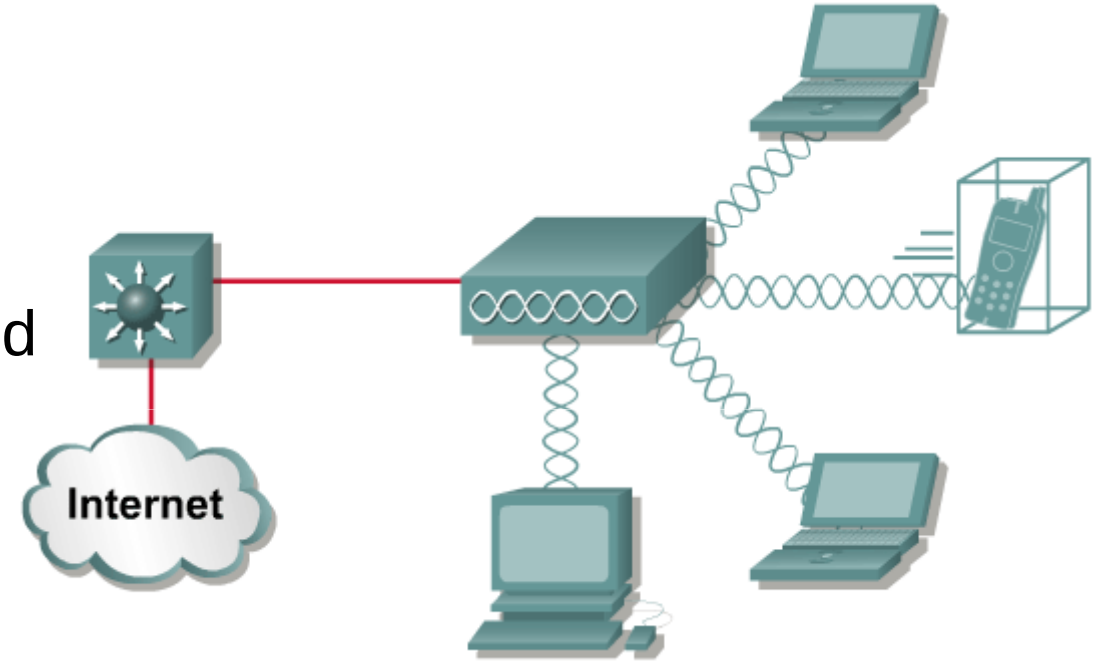
WLAN Topologies

Wireless LAN (WLAN)

- A WLAN is a shared network.
- An access point is a shared device and functions like a shared Ethernet hub.
- Data is transmitted over radio waves.
- Two-way radio communications (half-duplex) are used.
- The same radio frequency is used for sending and receiving (transceiver).



Similarities Between WLAN and LAN

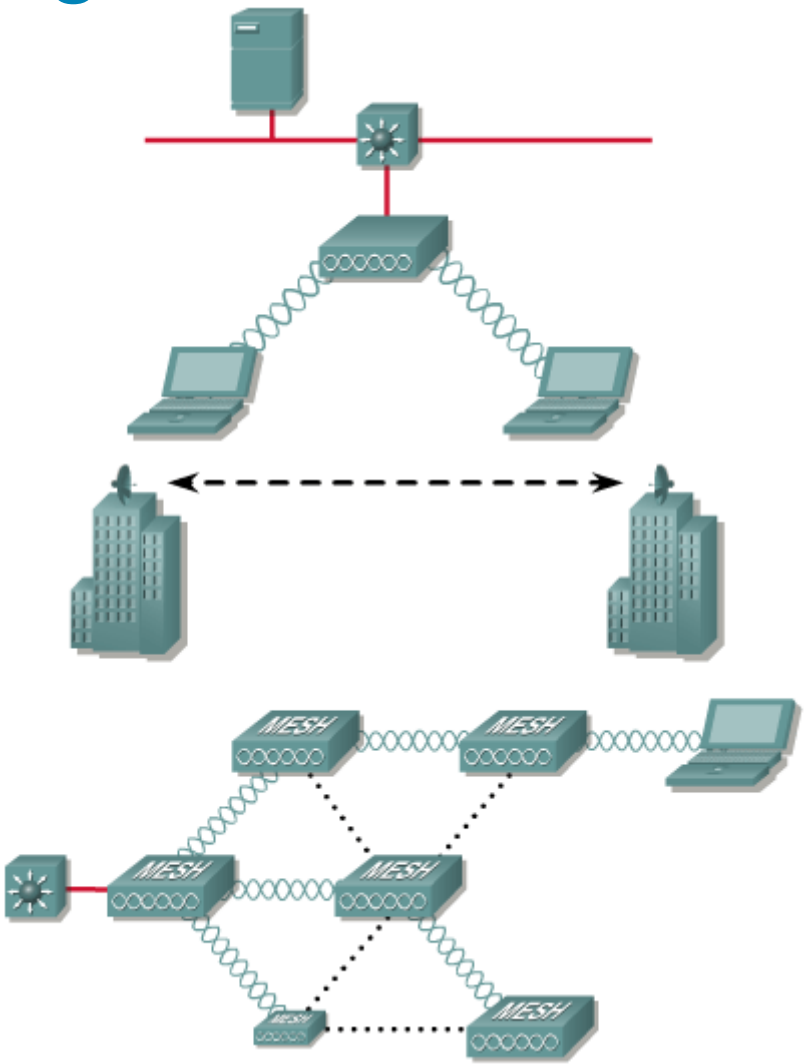
- A wireless LAN is an 802 LAN.
  - Transmits data over the air vs. data over the wire
  - Looks like a wired network to the user
  - Defines physical and data link layer
  - Uses MAC addresses
- The same protocols/applications run over both WLANs and LANs.
  - IP (network layer)
  - IPSec VPNs (IP-based)
  - Web, FTP, SNMP (applications)

Differences Between WLAN and LAN

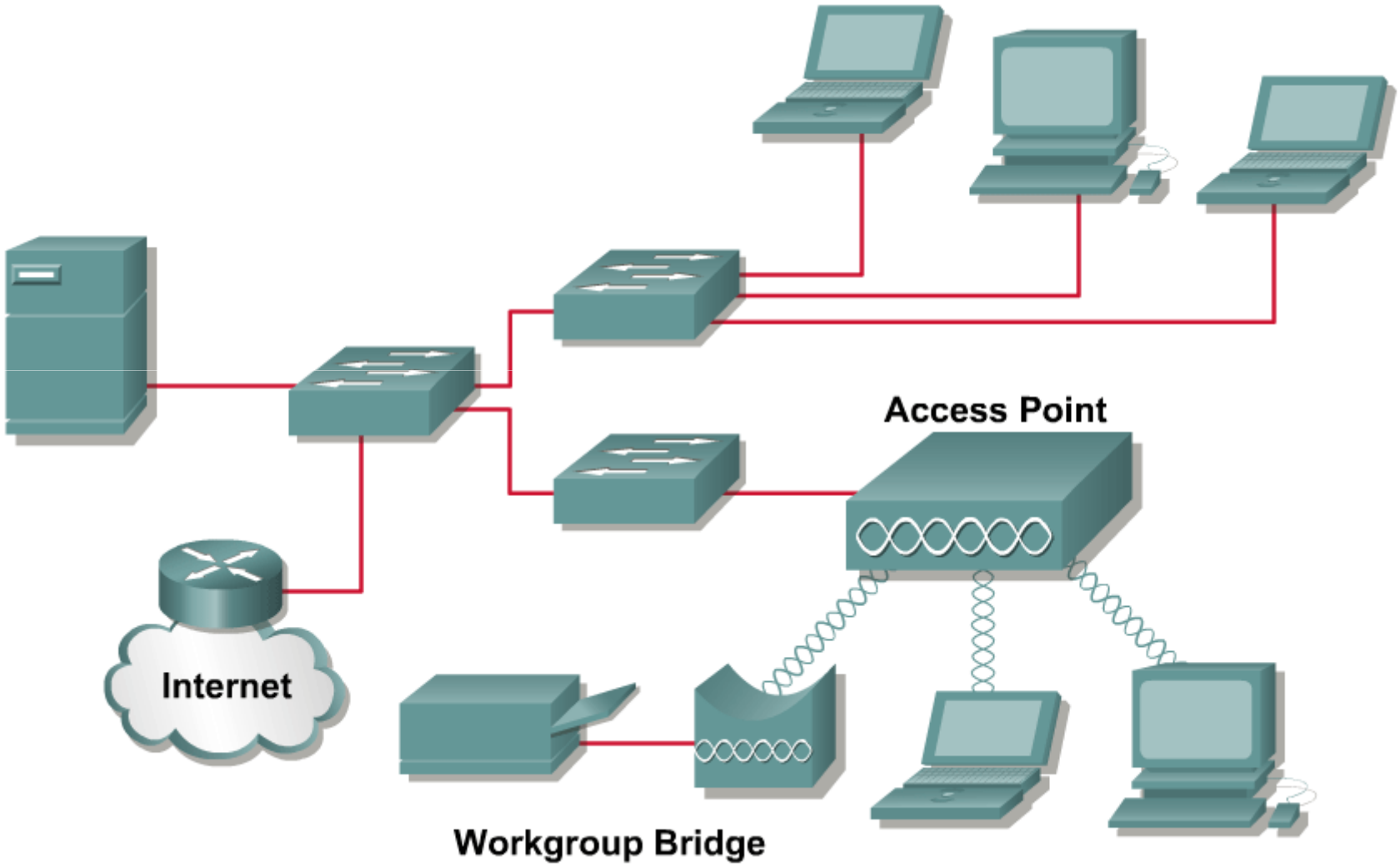
- WLANs use radio waves as the physical layer.
  - WLANs use CSMA/CA instead of CSMA/CD to access the network
- Radio waves have problems that are not found on wires.
  - Connectivity issues
  - Coverage problems
  - Multipath issues
  - Interference, noise
  - Privacy issues
- WLANs use mobile clients.
  - No physical connection
  - Battery-powered
- WLANs must meet country-specific RF regulations.

Wireless LAN Topologies

- Wireless client access
  - Mobile user connectivity
- Wireless bridging
  - LAN-to-LAN connectivity
- Wireless mesh networking
  - Combination of bridging and user connectivity

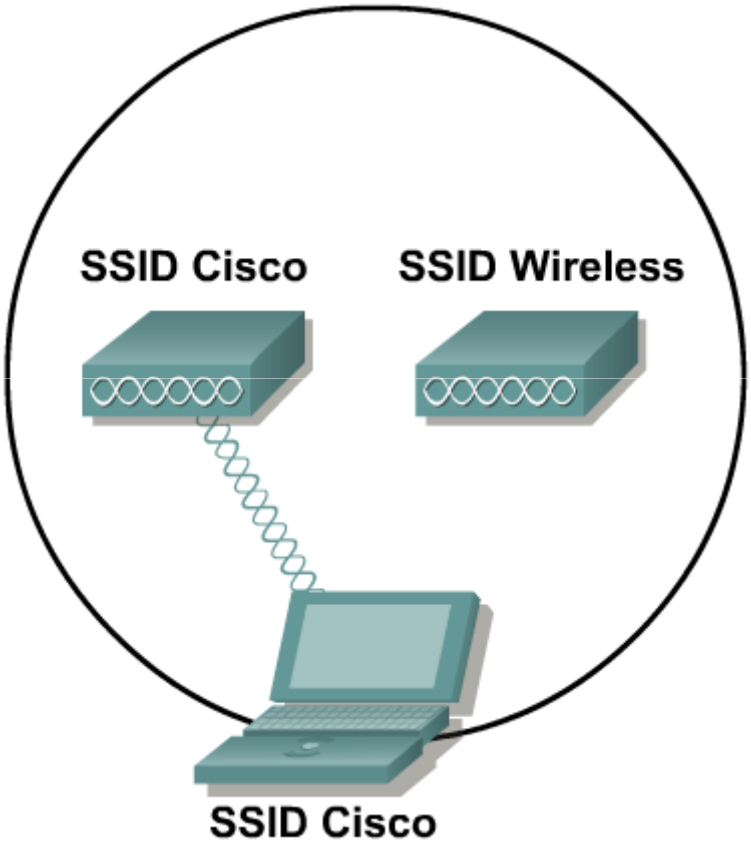


WLAN and LAN

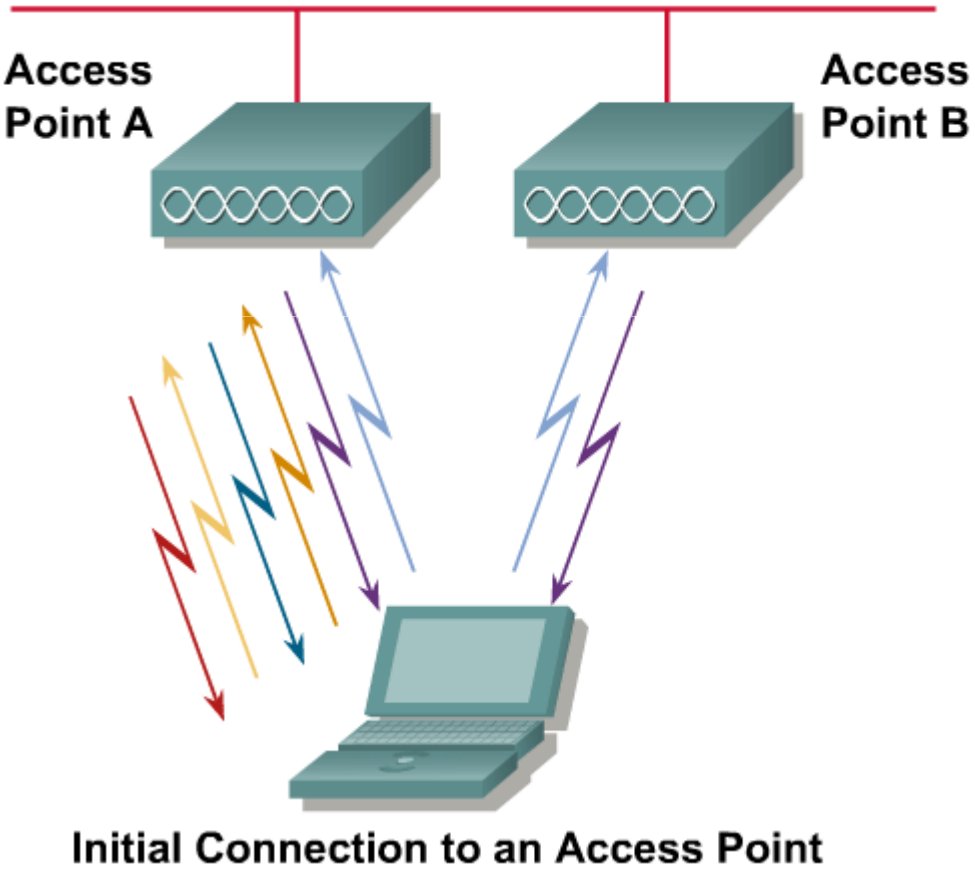


Service Set Identifier (SSID)

- SSID is used to logically separate WLANs.
- The SSID must match on client and access point.
- Access point can broadcast SSID in beacon.
- Client can be configured without SSID.



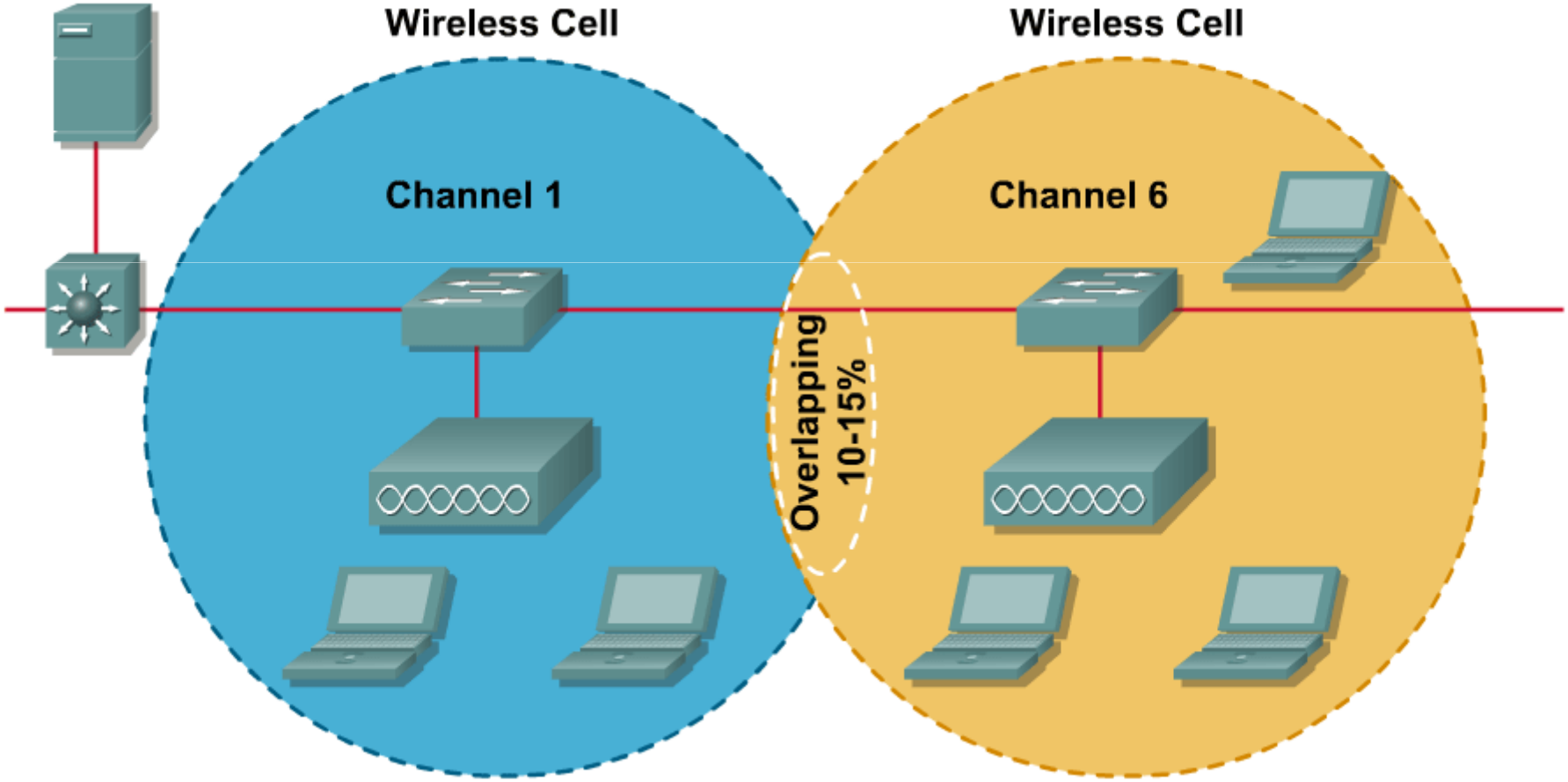
Association Process (Active Scanning)



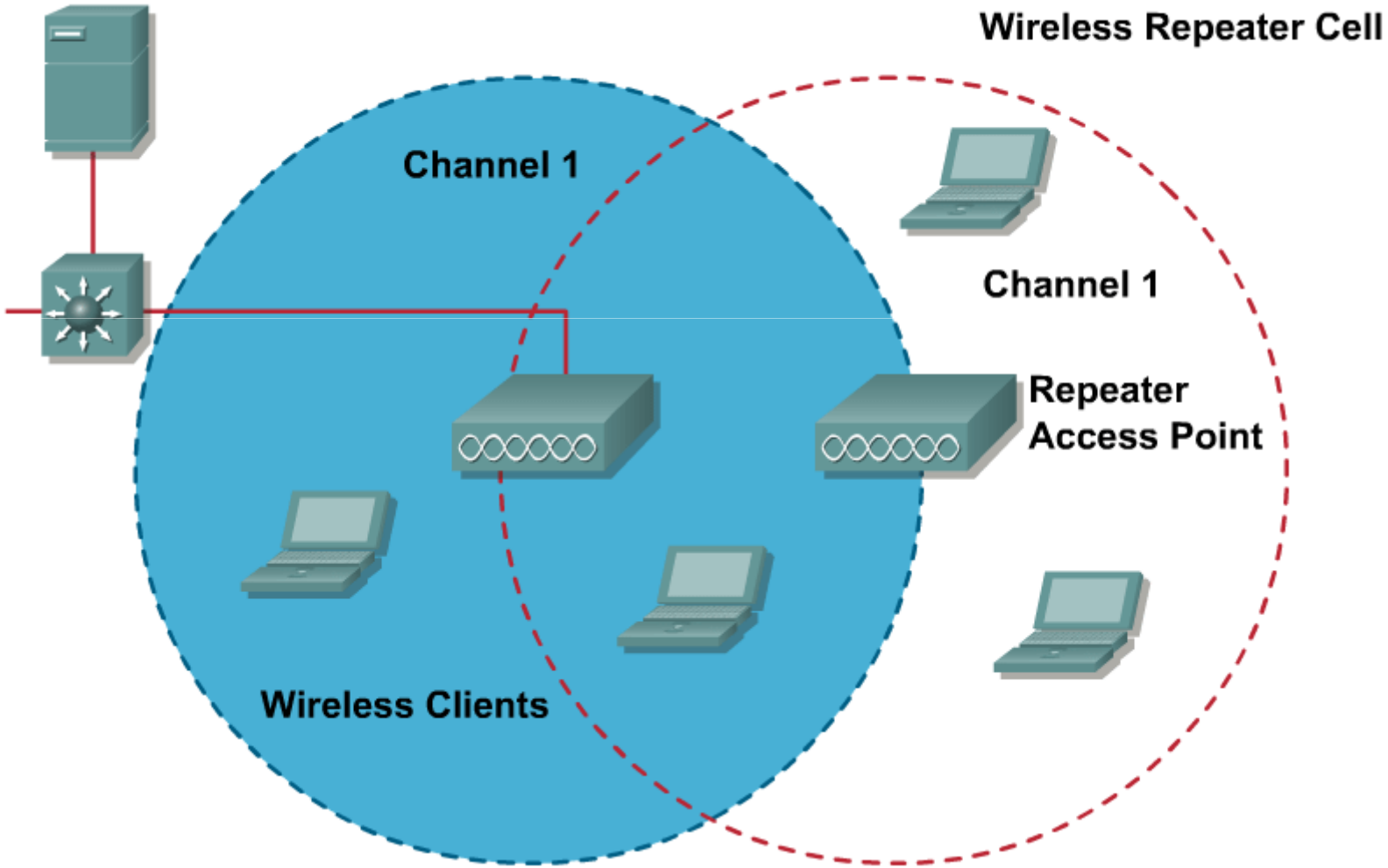
Steps to Association:

- Client Sends Probe
- AP Sends Probe Response
- Client Evaluates AP Response, Selects Best AP
- Client Sends Authentication Request to Selected AP (A)
- AP A Confirms Authentication and Registers Client
- Client Sends Association Request to Selected AP (A)
- AP A Confirms Association and Registers Client

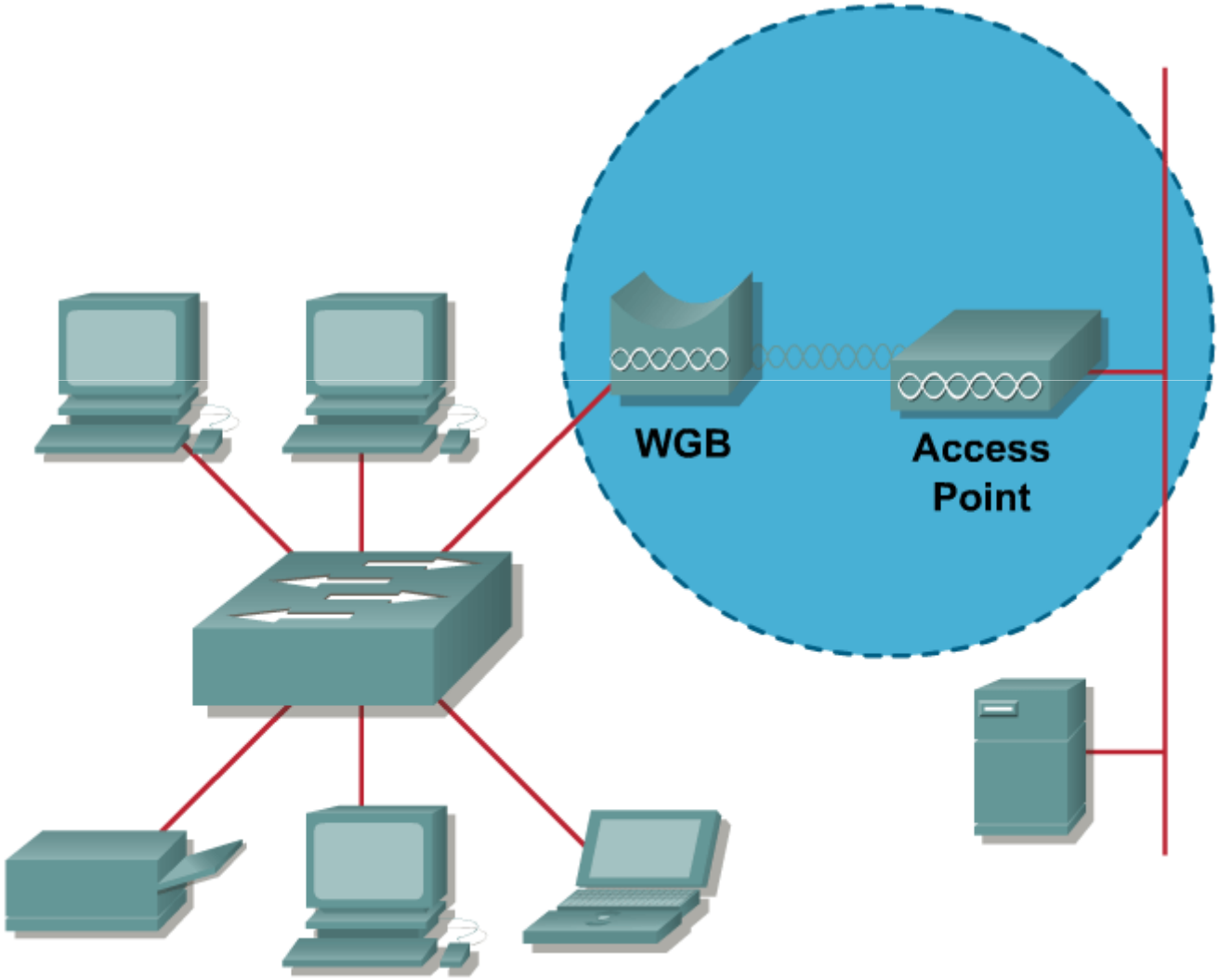
WLAN Access Topology



Wireless Repeater Topology

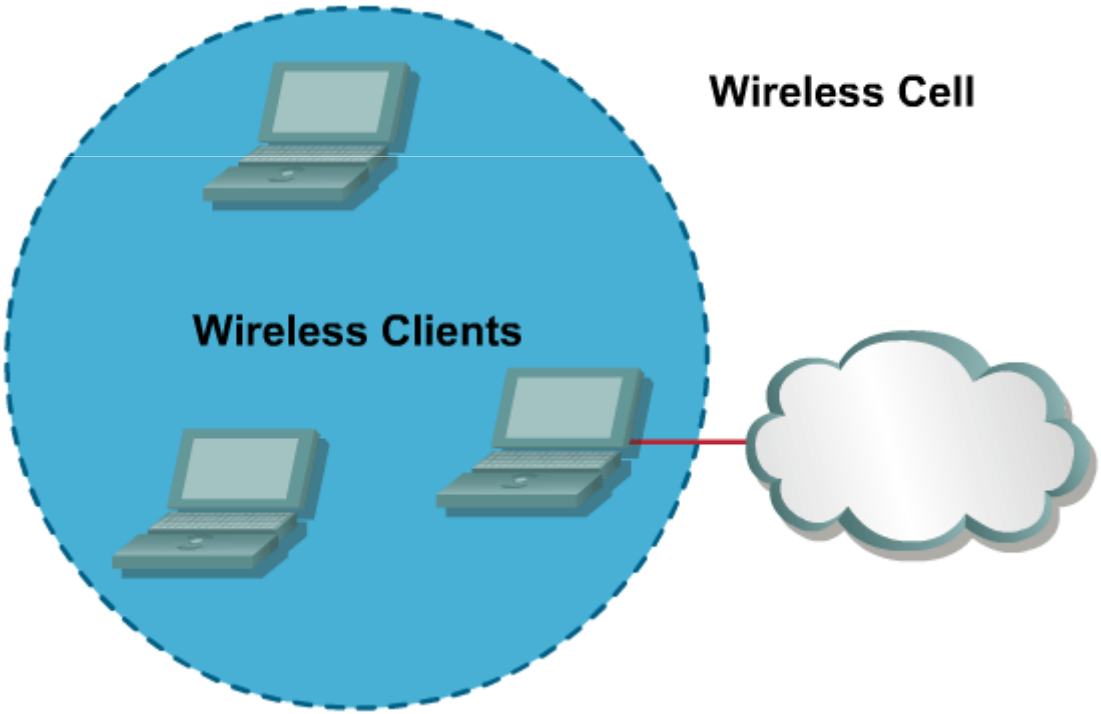


Workgroup Bridge Topology



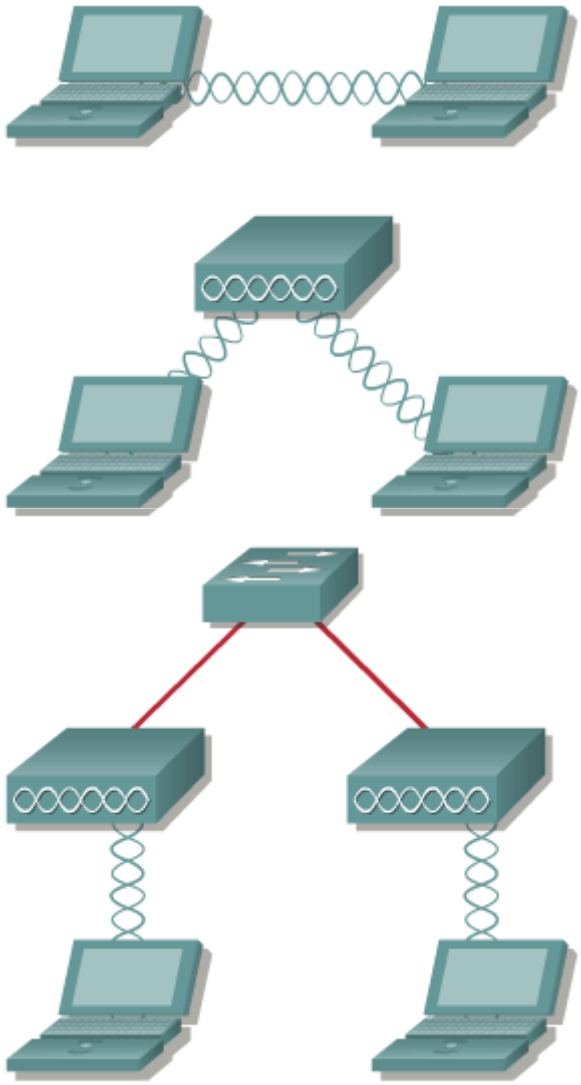
Alternative Peer-to-Peer Topology

Peer-to-Peer Configuration
(Ad Hoc Mode)

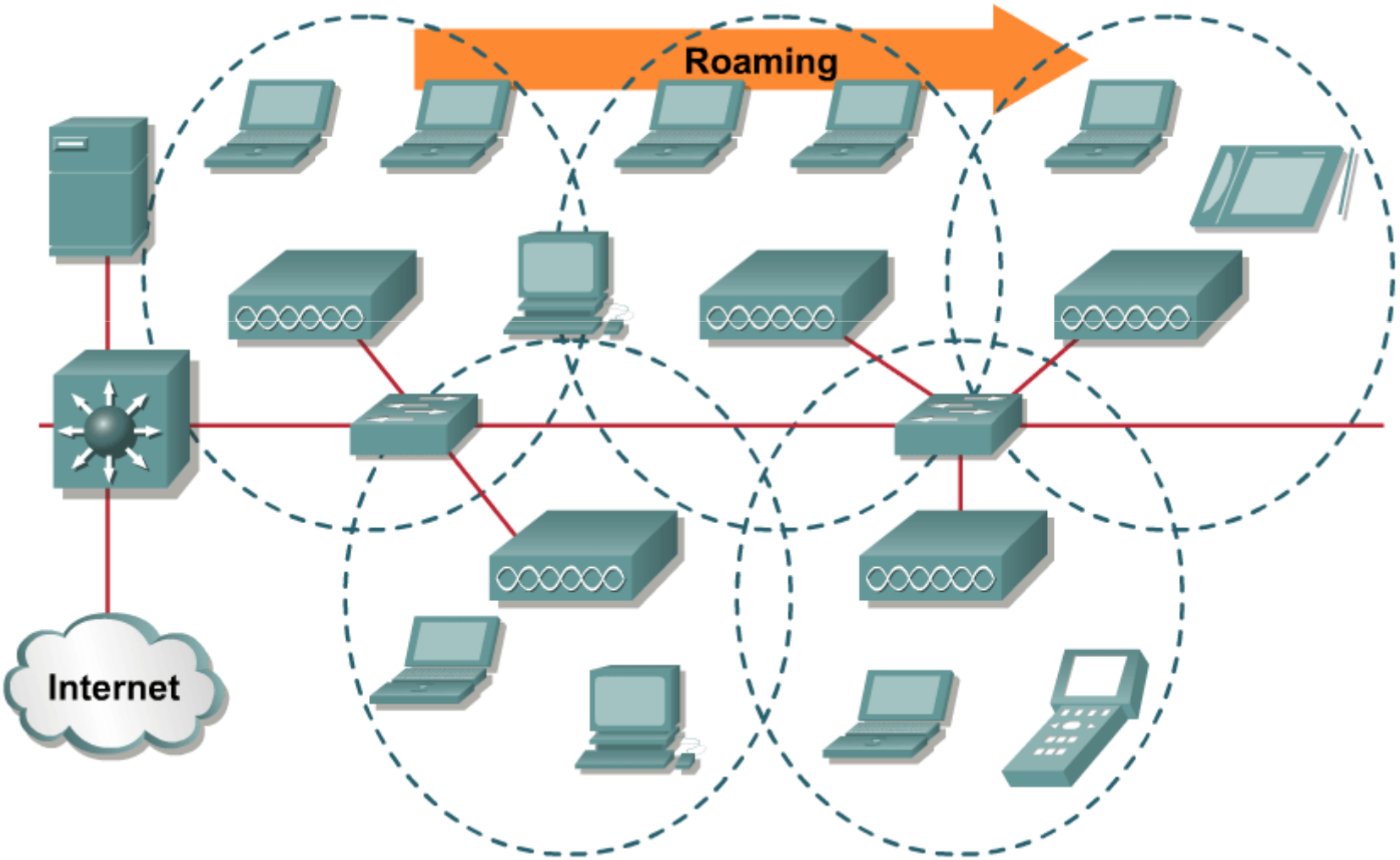


Service Sets & Modes

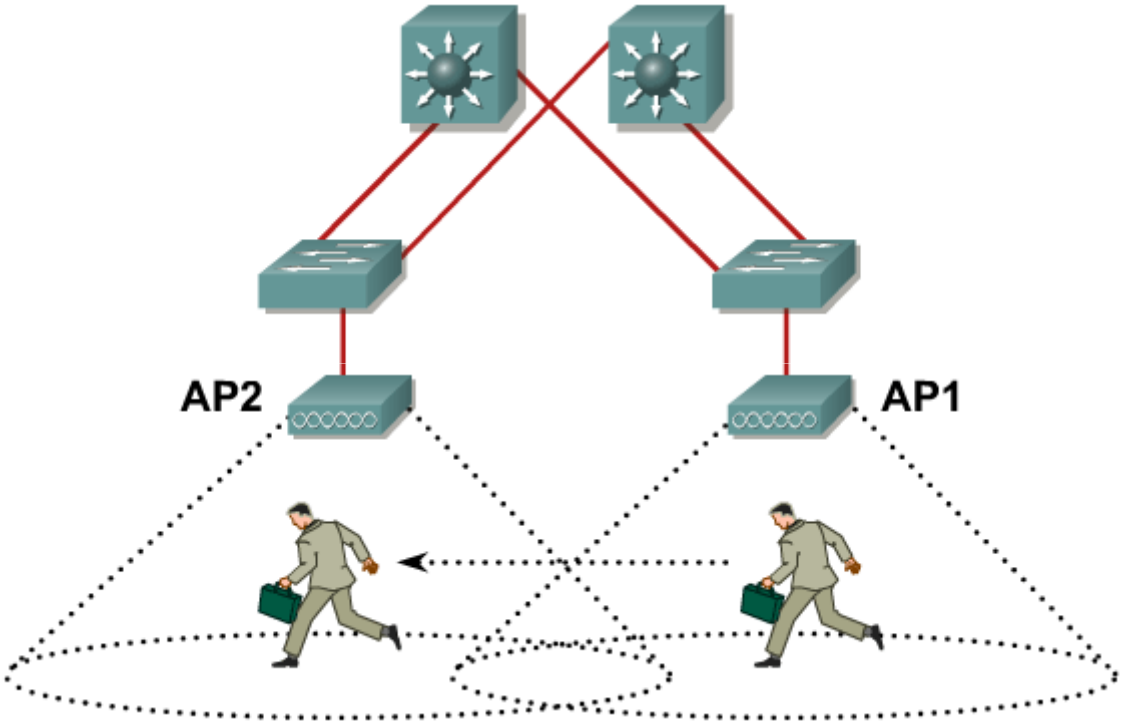
- Ad hoc mode
  - Independent Basic Service Set (IBSS)
    - Mobile clients connect directly without an intermediate AP.
- Infrastructure mode
  - Basic Service Set (BSS)
    - Mobile clients use a single AP for connecting to each other or to wired network resources.
  - Extended Services Set (ESS)
    - Two or more Basic Service Sets are connected by a common distribution system (DS).



Roaming Through Wireless Cells



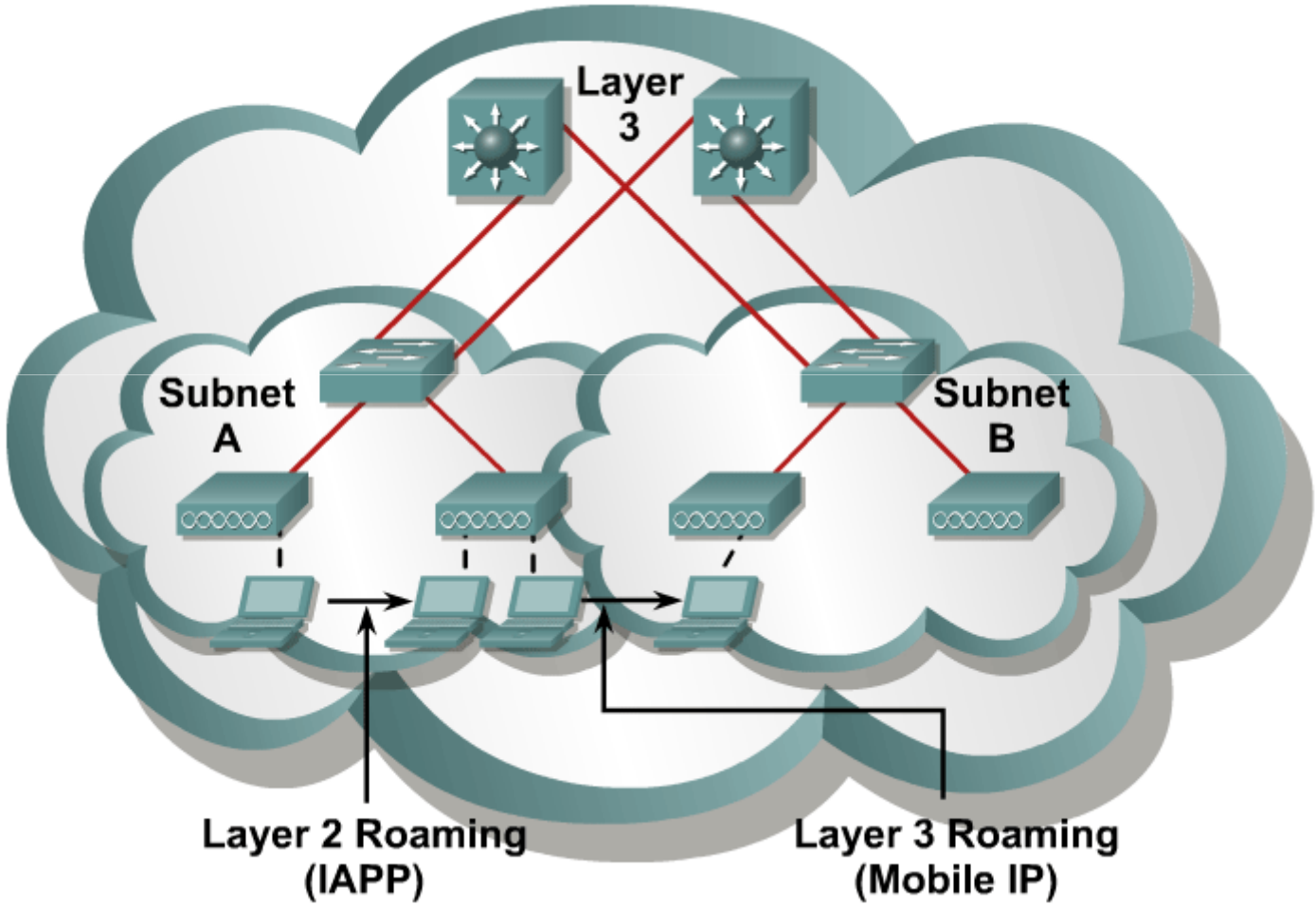
Client Roaming



- Maximum data retry count exceeded
- Too many beacons missed
- Data rate shifted
- Periodic intervals

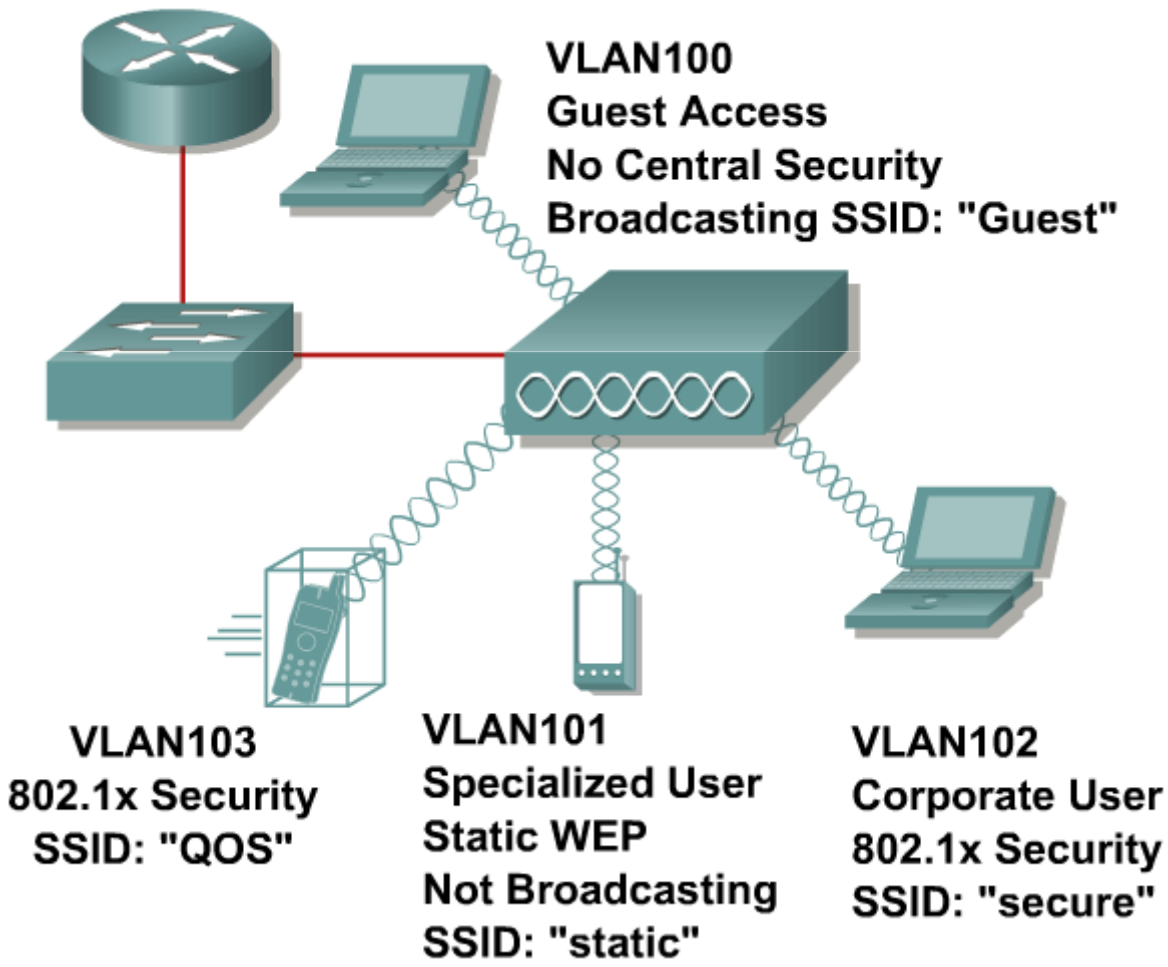
- Roaming without interruption requires the same SSID on all access points.

Layer 2 vs. Layer 3 Roaming



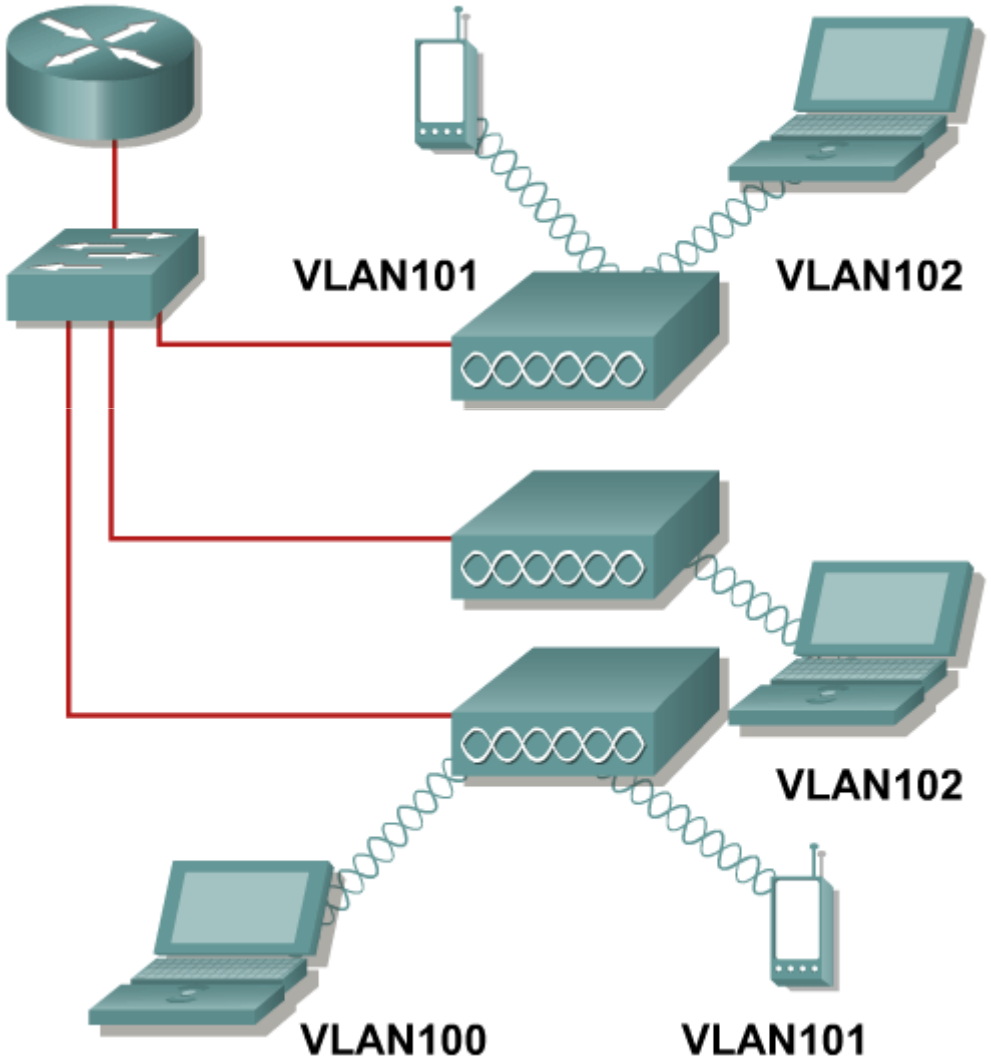
Wireless VLAN Support

- Multiple SSIDs
- Multiple security types
- Support for multiple VLANs from switches
- 802.1Q trunking protocol

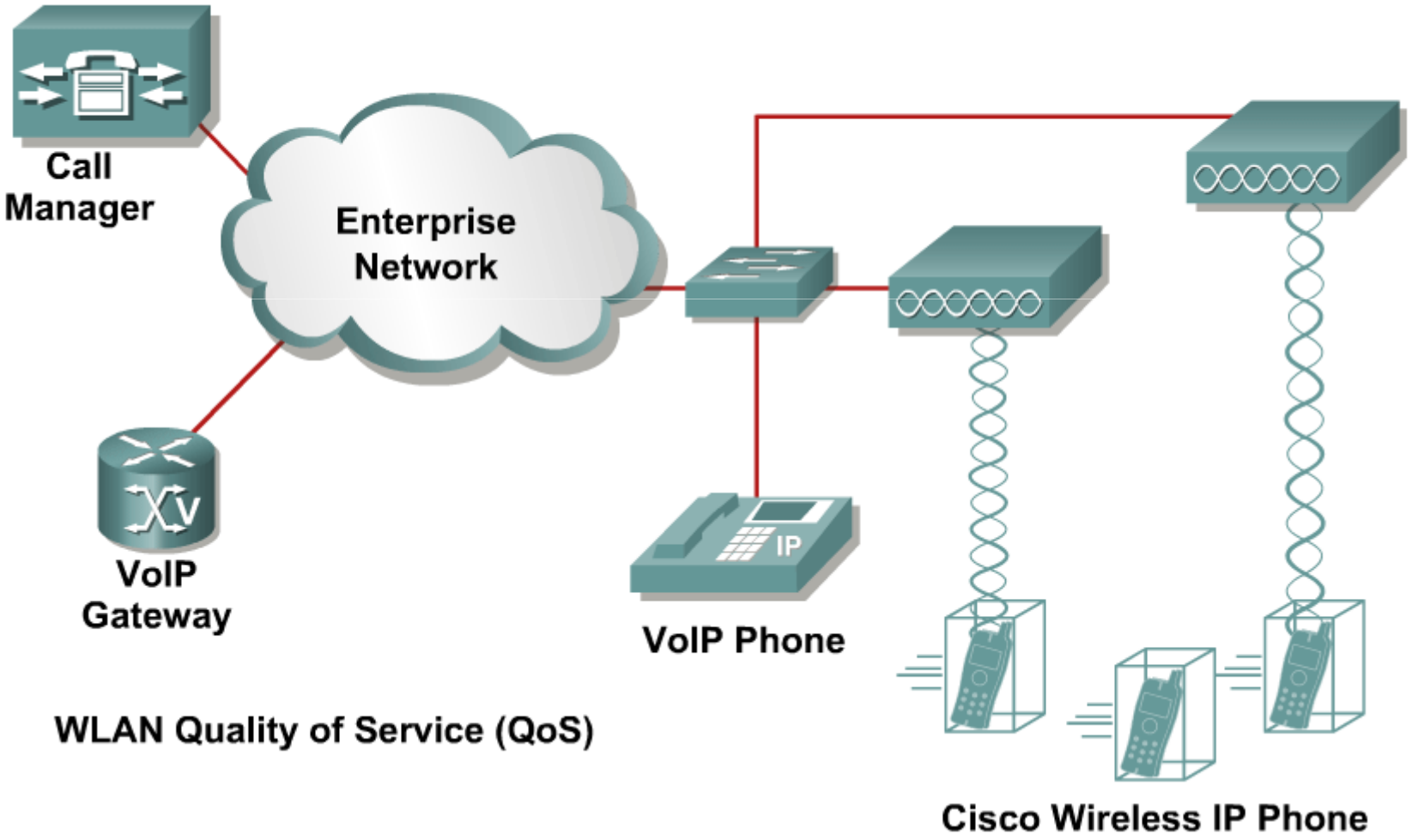


Wireless VLAN Support (Cont.)

- VLANs propagate across APs.
- VLAN numbers are unique.
- Autonomous access points handle up to 16 VLANs.



Enterprise Voice Architecture

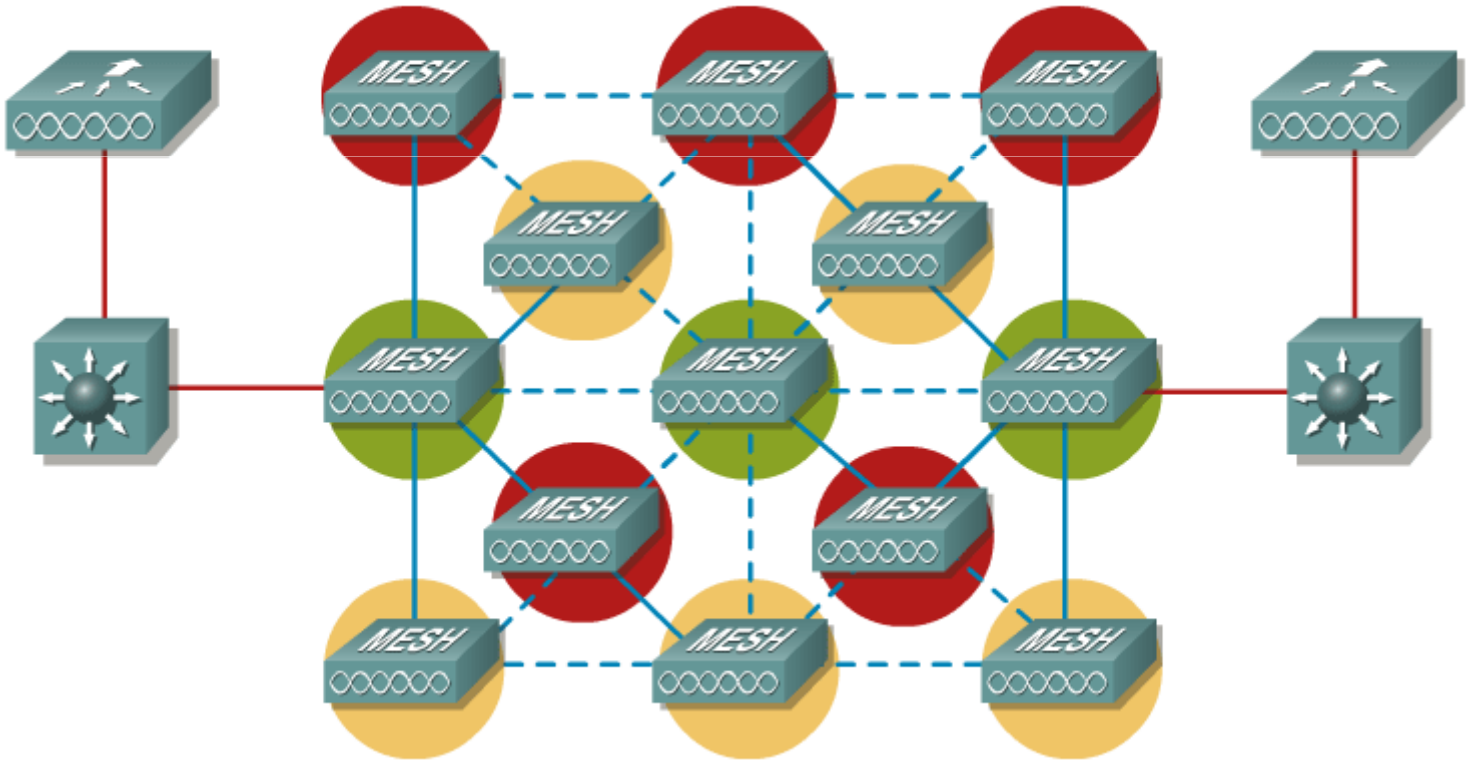


Autonomous or Lightweight?

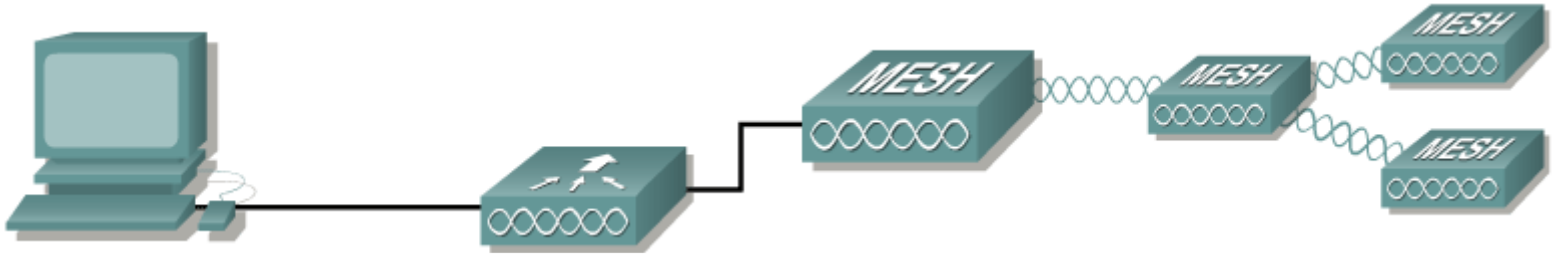
- Most Cisco wireless access points/bridges are available as **autonomous** or **lightweight** devices.
- Lightweight APs use Lightweight Access Point Protocol (LWAPP) and must have a LAN controller to function within the network.
- Autonomous APs can be configured via Cisco IOS or may operate with the CiscoWorks Wireless LAN Solution Engine (WLSE).
- Most Cisco autonomous APs can be software upgraded to function as lightweight APs.
- The Cisco Networking Academy FWL course focused on autonomous APs.

Wireless Mesh Networking

- In a mesh network topology, devices are connected with redundant connections between nodes.



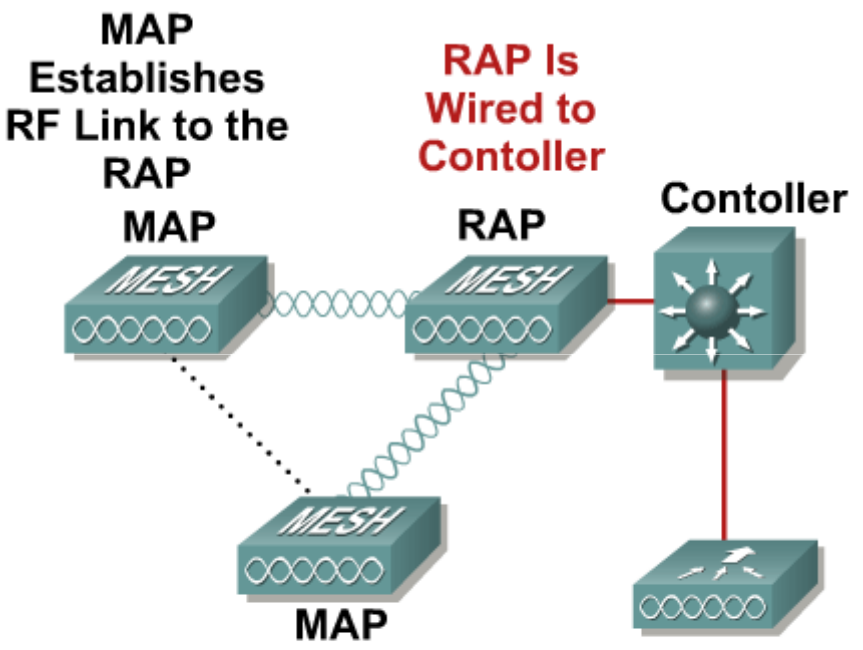
Wireless Mesh Solution Components



Cisco Wireless Control Systems	Cisco Wireless LAN Controller	Root Access Point "RAP"	Mesh Access Point "MAP"
• Wireless Mesh management system • Enables network-wide policy configuration and device management • Supports SNMP and Syslog	• Links the wireless Mesh APs to the wired network • Handles RF algorithms and optimization • Seamless L3 mobility • Provides security and mobility mgt	• Serves as "Root" or "Gateway" AP to the wired network • Typically located on roof-tops or towers • Connects up to 32 "Pole-top" APs using 802.11a	• Provides 802.11b/g client access • Connects to Root AP via 802.11a • Takes AC or DC power; PoE capable • Ethernet port for connecting peripheral devices

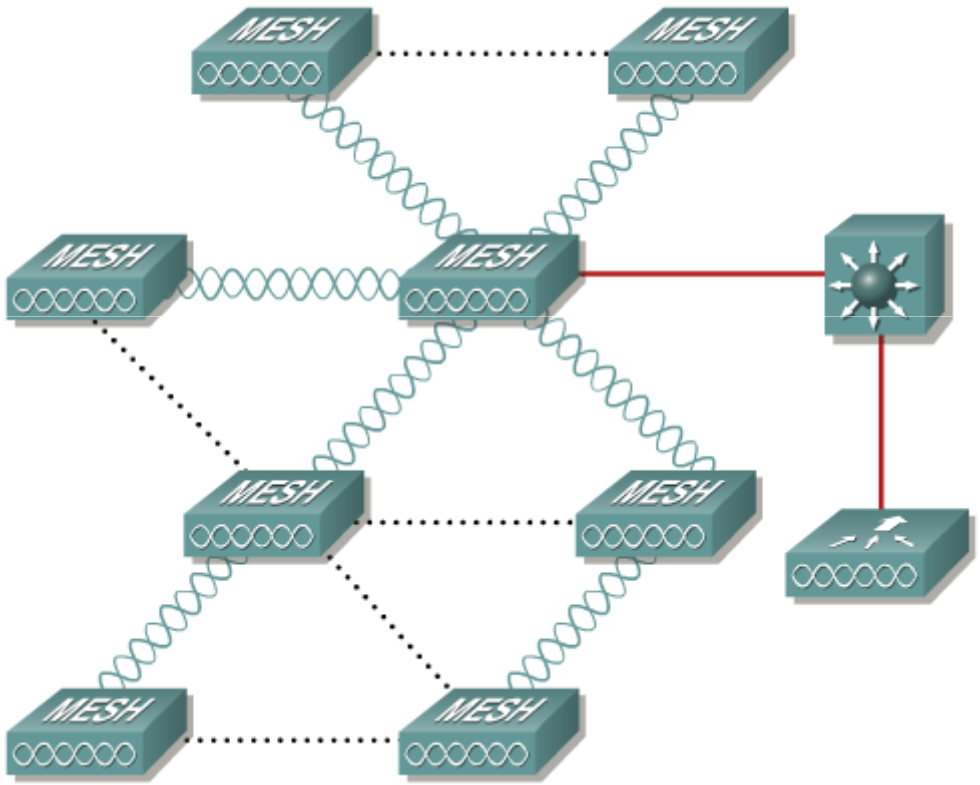
Mesh AP Roles

- Mesh APs automatically establish connection to Controller
  - Root AP (RAP) via wired connection
  - Mesh AP (MAP) via self-configuring backhaul connection
- Mesh AP uses Cisco's Adaptive Wireless Path Protocol "AWPP" to establish best path to the Root AP
- AP authenticates to Controller and downloads configuration and radio parameters



Ethernet Port Can Be Enabled on MAPs for Bridging or to Support Wired Devices Such as a Cameras

Adaptive Wireless Path Protocol (AWP)



- Adaptive Wireless Path (AWP) protocol establishes an optimal path to root.
- Each access point carries feasible successor or successors if topology or link health changes.
- AWP uses a “parent sticky” value to mitigate route flaps.

Why Mesh Technology?

Enterprise Mesh
Moving Indoor Wi-Fi Outside

- **Universities and healthcare**
  - Extending Wi-Fi coverage throughout the entire campus
- **Hospitality**
  - Outdoor mesh can open up new hospitality markets (EMEA)
- **Manufacturing—shipping and receiving**
  - Inventory applications, hand-held scanner, RFID, etc.
- **Wireless bridging**
  - P2P/P2MP links between buildings

Municipal Mesh
State, County and City

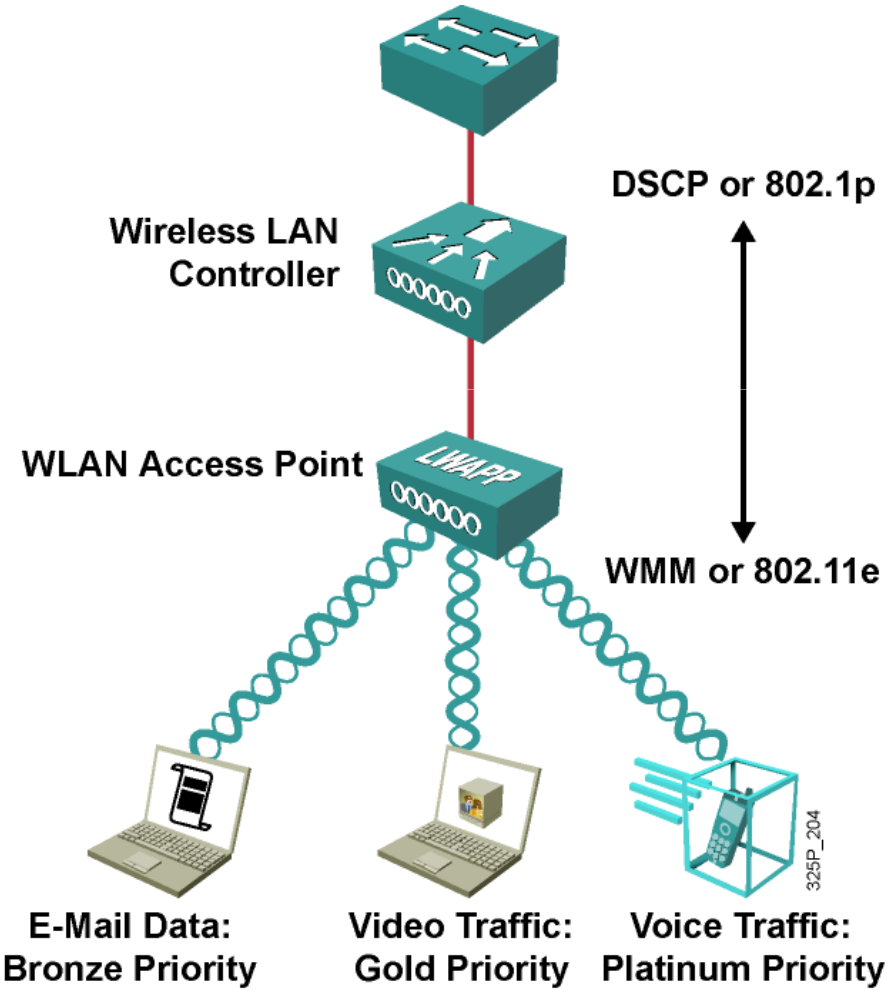
- **Public safety/homeland defense**
  - Police, fire and 1st responders
  - Wireless infrastructure, vehicles and clients
- **Wireless access for fixed applications**
  - Video surveillance, sensors
- **Public service**
  - Hot Spot access for city workers, utilities, inspectors
- **Digital divide and economic development**
  - Wi-Fi broadband access in under-served communities

Service Provider
Managed Wi-Fi Services

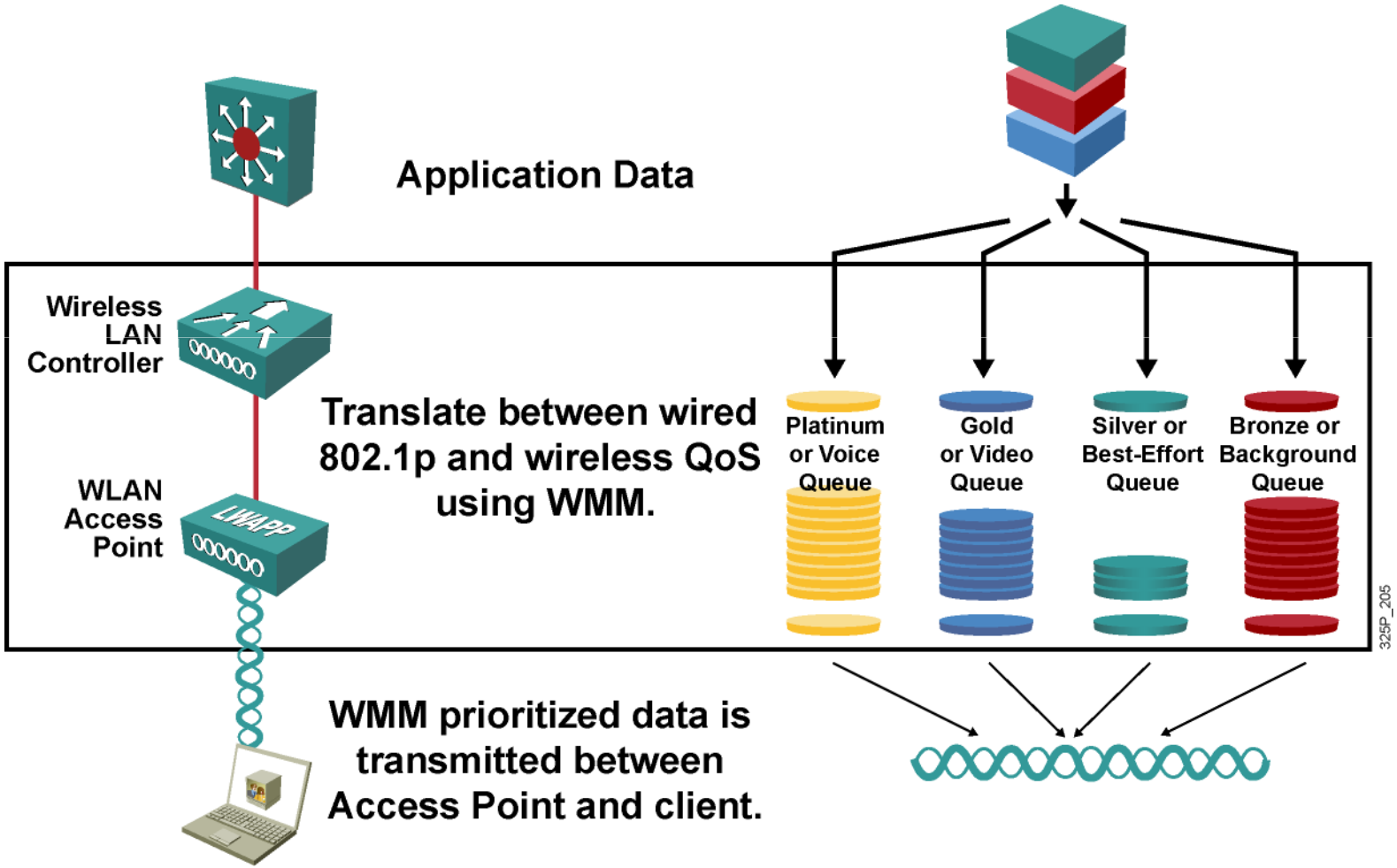
- **“Hot Zones”**
  - Extend the existing “Hot Spots” into “Hot Zones” covering high traffic outdoor areas
- **Wireless ISPs**
  - Competitive last-mile access providers using Wi-Fi for broadband service
- **Cable operators**
  - Extend the network offering beyond the cable plant

The Need for QoS in Wireless LANs

- WLANs use collision *avoidance* rather than collision *detection*, which is used by Ethernet LANs.
- Wired LANs use DSCP or 802.1p to provide QoS. These do not work in a WLAN.
- 802.11e is an extension of 802.11 that provides more consistent, quality RF transmission for voice and video.



WLAN QoS Queuing Overview



WLAN QoS RF Backoff Timing