CWNA Guide to Wireless LANs, 3rd ed.

Chapter 7: WLAN Management and Architectures

Objectives

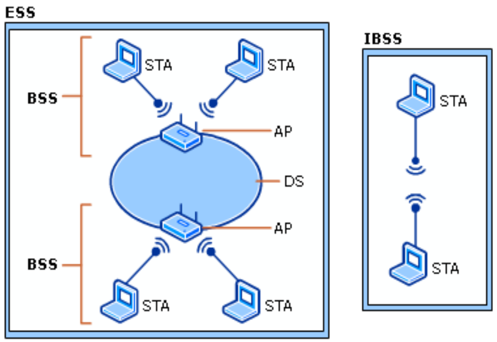
- Describe the functions of an autonomous access point architecture
- Explain the characteristics and features of a controller-based architecture
- Describe the difference between multiple- and single-channel architecture models
- Explain what a wireless network management system is and how it functions
- Describe the characteristics of basic and enhanced power management technologies

Autonomous Access Point Architectures

- Most common WLAN architecture is one with a "stand-alone" AP
  - These APs are known as *autonomous access points*
- All of the "intelligence" for wireless management, authentication, and encryption is contained within the AP
  - Because everything is self-contained they are also called *fat access points*
- Autonomous access point architectures include network connectivity with lots of features

Network Connectivity

- Network connectivity of WLANs depends on its type of service set
- Three WLAN service set configurations:
  - BSS
  - ESS
  - IBSS



- ESS is composed of two or more BSS networks
  - Distributed WLAN architecture: multiple APs form a non-centralized network through a wireless connection

Feature Sets

- Features found in APs vary
  - Many are designed to enhance the configuration, installation, and management of the AP

- Typical feature sets:
  - Ability to add 5-GHz 802.11a support to a 2.5-GHz 802.11g AP
  - Built-in security and manageability features
  - External antenna connection
  - Support for Wireless Distribution Systems (WDS)
  - Support for large numbers of wireless stations
  - Auto network connect and dynamic rate shifting

Feature Sets

- Typical feature sets (continued):
  - Power over Ethernet (PoE) options
  - Diversity radio antenna
  - Security to limit unauthorized stations access to network resources
  - Adjustable transmit power
  - Ability to configure parameters, run diagnostics, and monitor performance from anywhere on the network using a Web browser
  - Support for standards-based management protocols

Quality of Service (QoS)

- Distributed Coordination Function (DCF) does not work well for real-time, time-dependent traffic
- **Quality of Service (QoS):** Capability to prioritize different types of frames
- QoS has become increasingly important due to widespread adoption of Voice over IP (VoIP)
- **Wi-Fi Multimedia (WMM):** Modeled after wired network QoS prioritization scheme
  - Released in 2004 by the Wi-Fi Alliance

Quality of Service (QoS)

WMM Access Category	Description
WMM Voice Priority	The highest priority; facilitates multiple high-quality voice calls
WMM Video Priority	Prioritizes video traffic higher than regular data traffic but not as high as voice traffic
WMM Best Effort Priority	Includes traffic from applications that are not time sensitive
WMM Background Priority	Includes low-priority traffic, such as file transfers or print jobs

Table 7-1 Wi-Fi Multimedia (WMM)

Quality of Service (QoS)

- **IEEE 802.11e-2005** : released in 2005
  - Based on the hybrid coordination function (HCF)
  - Two access mechanisms:
    - Enhanced Distributed Channel Access (EDCA)
      - Four access categories (AC)
    - Hybrid Coordination Function Controlled Channel Access (HCCA)
    - Uses polling along with centralized scheduling controlled by the AP

Wireless Virtual LANs (VLANs)

- **VLAN**: a logical grouping of network devices within a larger physical network
  - Example: a VLAN group might consist of all accounting employees even if they are in different buildings
  - Switch is required for correct operation
- Wireless VLANs do not require any additional network hardware
  - SSID can be used to separate users on the network
  - APs that support wireless VLANs may support 16 or more multiple SSIDs (and thus multiple VLANs)

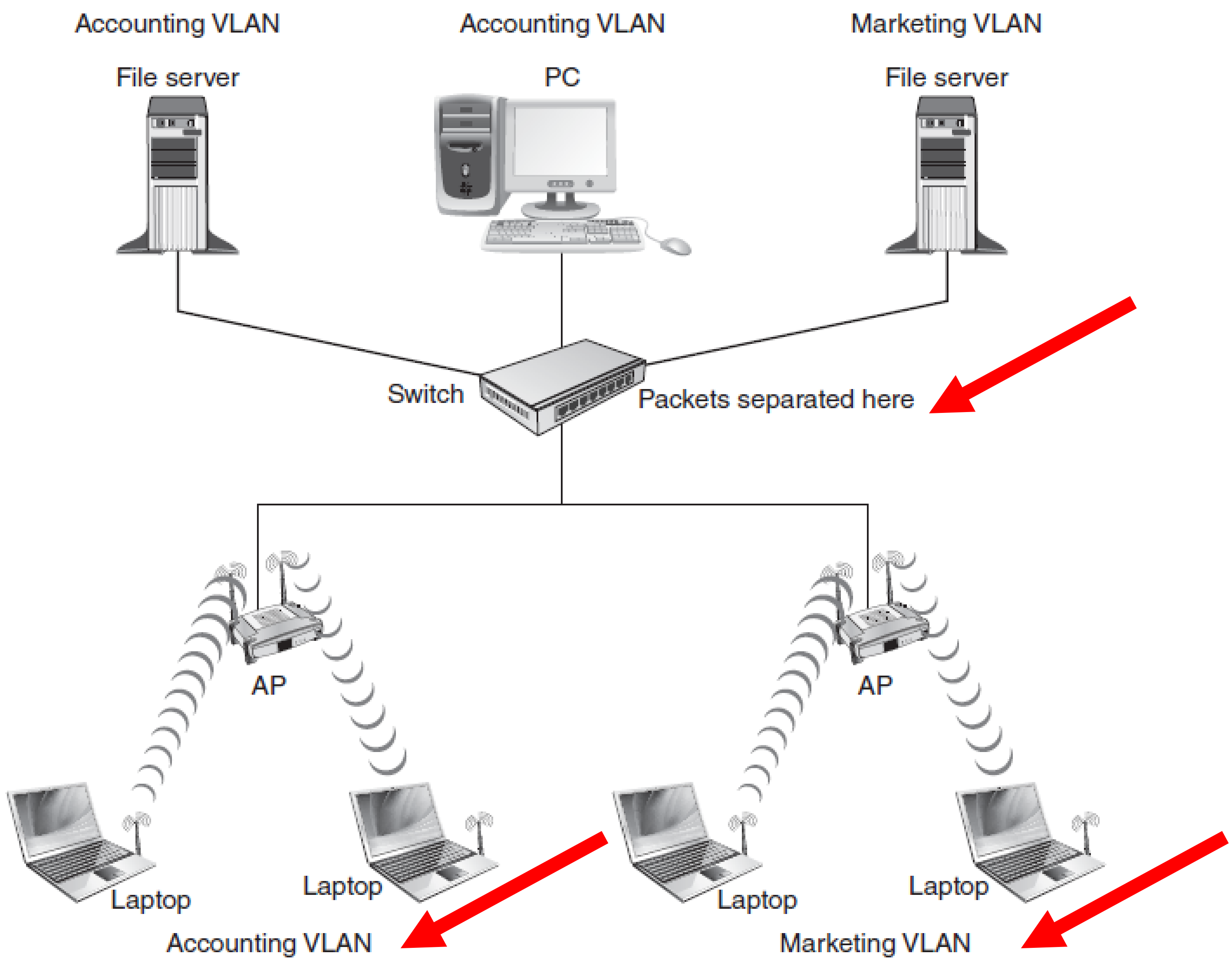


Figure 7-1 Packets separated at switch

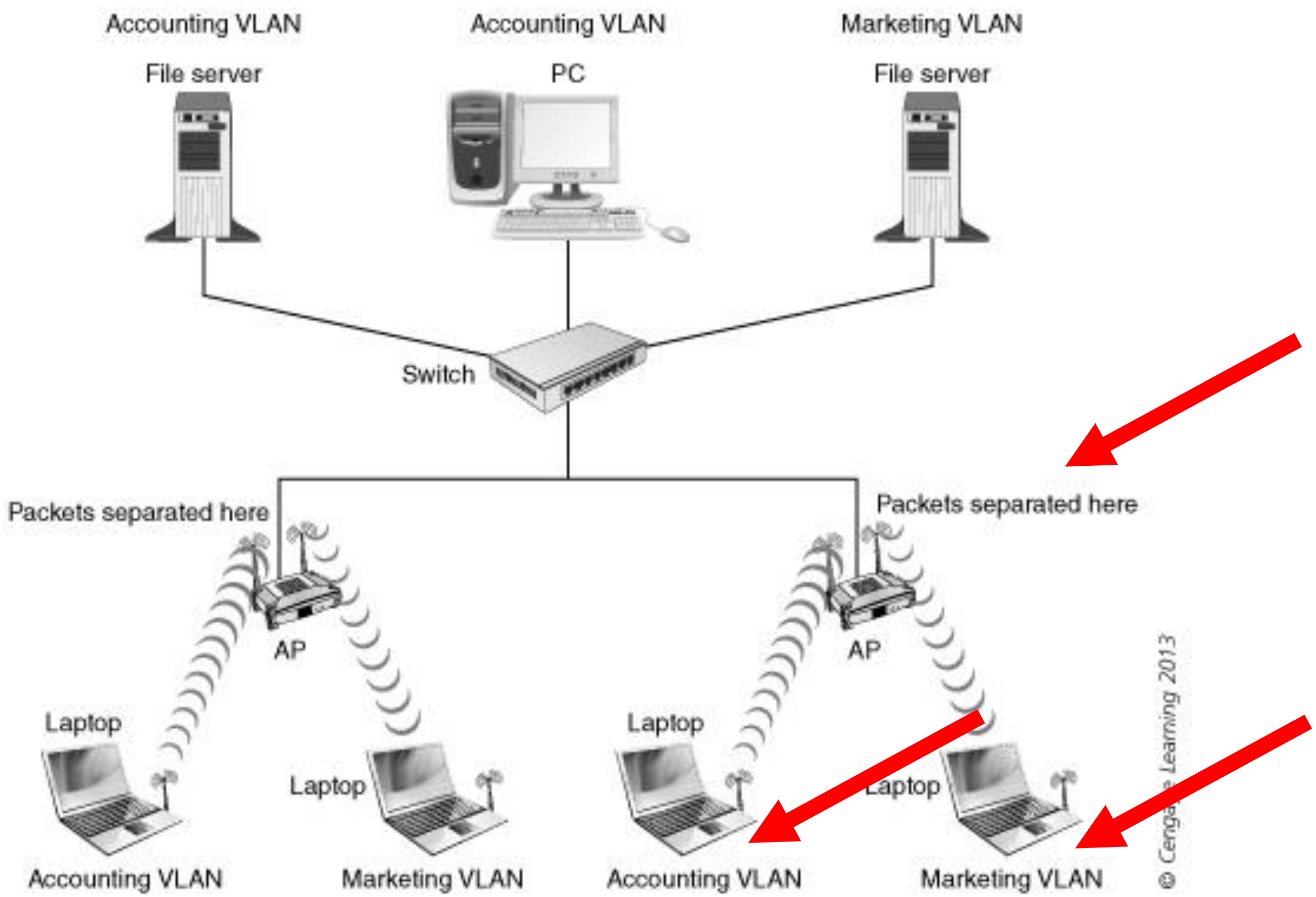


Figure 7-2 Packets separated at AP

Advantages and Limitations

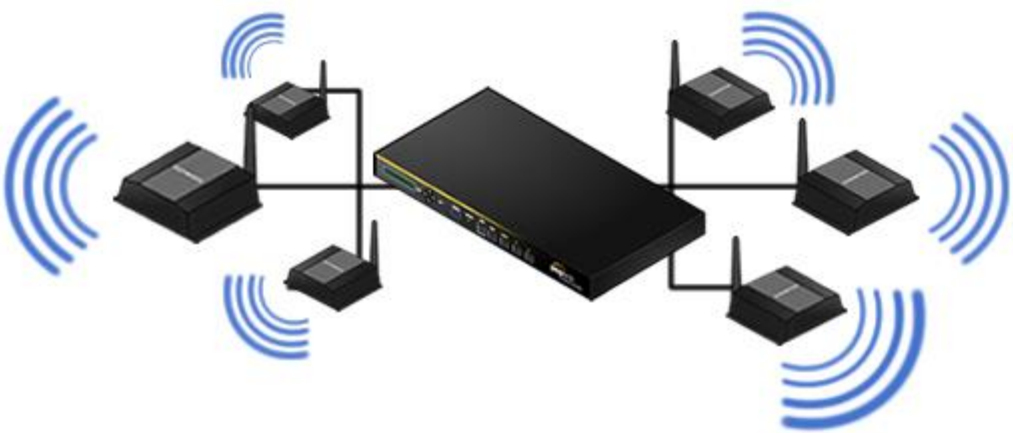
- Advantages of autonomous access point architecture:
  - Offer QoS, wireless VLANs and other options
  - Scalability is straightforward and unlimited

Procedure	Description	Limitation
Layer 2 Roaming	Seamless station roaming across APs	Must install and configure new AP and may need to reconfigure some existing APs
Layer 3 Roaming	Station roaming across separate subnets	Not possible with autonomous APs; may need to implement Mobile IP
Management	Adjust configuration settings as necessary	Must visit each AP to change settings; no centralized management possible
Load Balancing	Equalize number of stations across multiple APs so that all APs have manageable loads	Must be done on a manual basis; cannot automatically spread load across multiple APs

Table 7-2 Autonomous access point architecture limitations

Controller-Based Architectures

- Controller-based architectures: rely upon a wireless LAN controller (WLC) at the heart of the network
  - WLC can be centrally configured, the settings can then be automatically distributed to all APs
- APs used in controller-based architectures are different from APs used in an autonomous access point WLAN



Access Points

- There are three main types of APs found in a controller-based architecture
  - Lightweight APs (thin access points)
  - Mesh APs
  - Captive portal APs

Lightweight APs

- Lightweight AP: does not contain management and configuration functions
  - Only have simplified radios for wireless communication and a media converter for accessing the wired network

- Split MAC: division in which lightweight APs only handle the real-time layer functions while MAC functionality is processed by the WLC

- Benefit to lightweight APs is a decrease in the total cost of ownership (TCO)
  - TCO: total cost of ownership includes acquisition, setup, support, ongoing maintenance, service, and all operating expenses

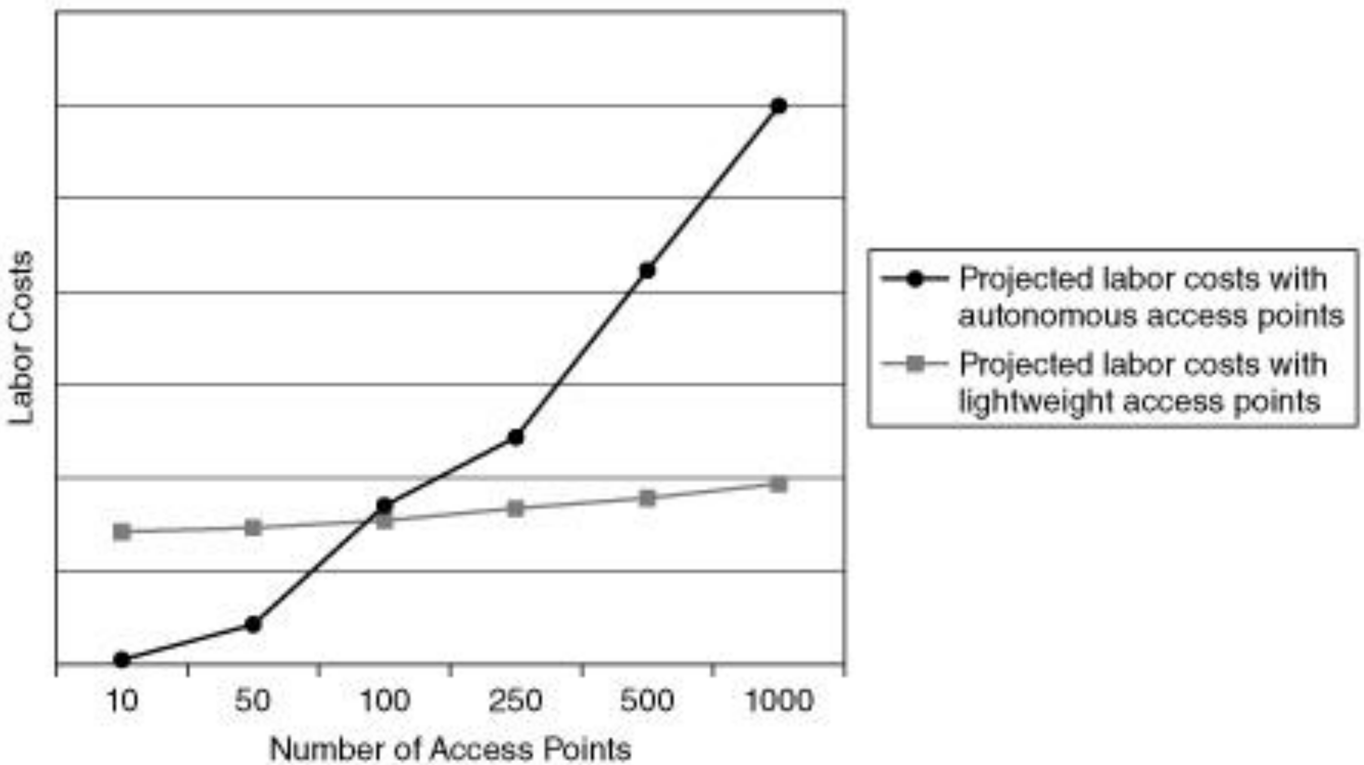
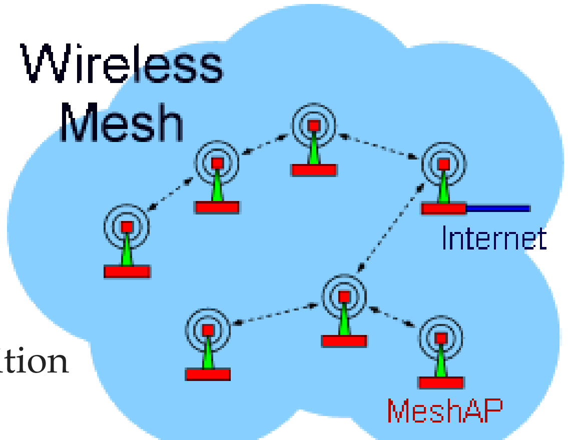


Figure 7-3 Autonomous AP vs. lightweight AP labor costs

Lightweight Mesh APs

- *Mesh access point*: communicates with the next closes mesh access point
  – does not have to be connected by a cable to the existing wired network
  – Only one mesh access point must be physically connected to the wired network

- **Lightweight mesh AP**: a mesh AP that is centrally configured and managed through a WLC



Captive Portal APs

- Captive portal AP: uses a standard Web browser to provide information, give the wireless user the opportunity to agree to a policy, or present valid login credentials
  - Typically used for public WLAN access
  - Usually requires the user to read and accept an *Acceptable Use Policy (AUP)*
- Captive portal AP is not a required part of a controller-base architecture, however, this is the architecture in which it is often found

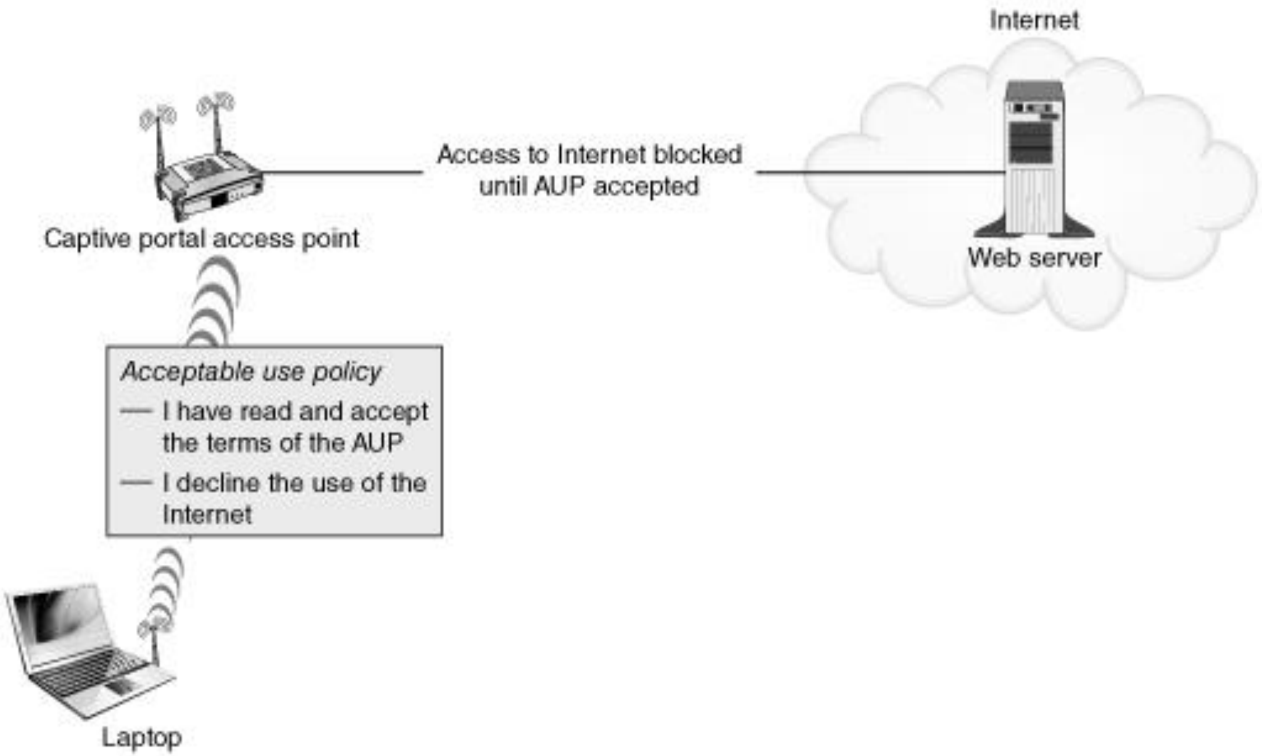


Figure 7-4 Captive portal AP

https://www.youtube.com/watch?v=ZFTgI-2gWsI

Wireless LAN Controllers (WLCs)

- A WLC is very similar to a switch on a wired network
  - WLC is sometimes called a wireless switch

- An enhanced feature of a WLC is network placement. A WLC can be placed at either:
  - Core layer: backbone of the network
  - Distribution layer: also called the workgroup layer because devices at this layer ensure frames are routed between subnets
  - Access layer: where client nodes connect to the network (hubs and switches are located here)

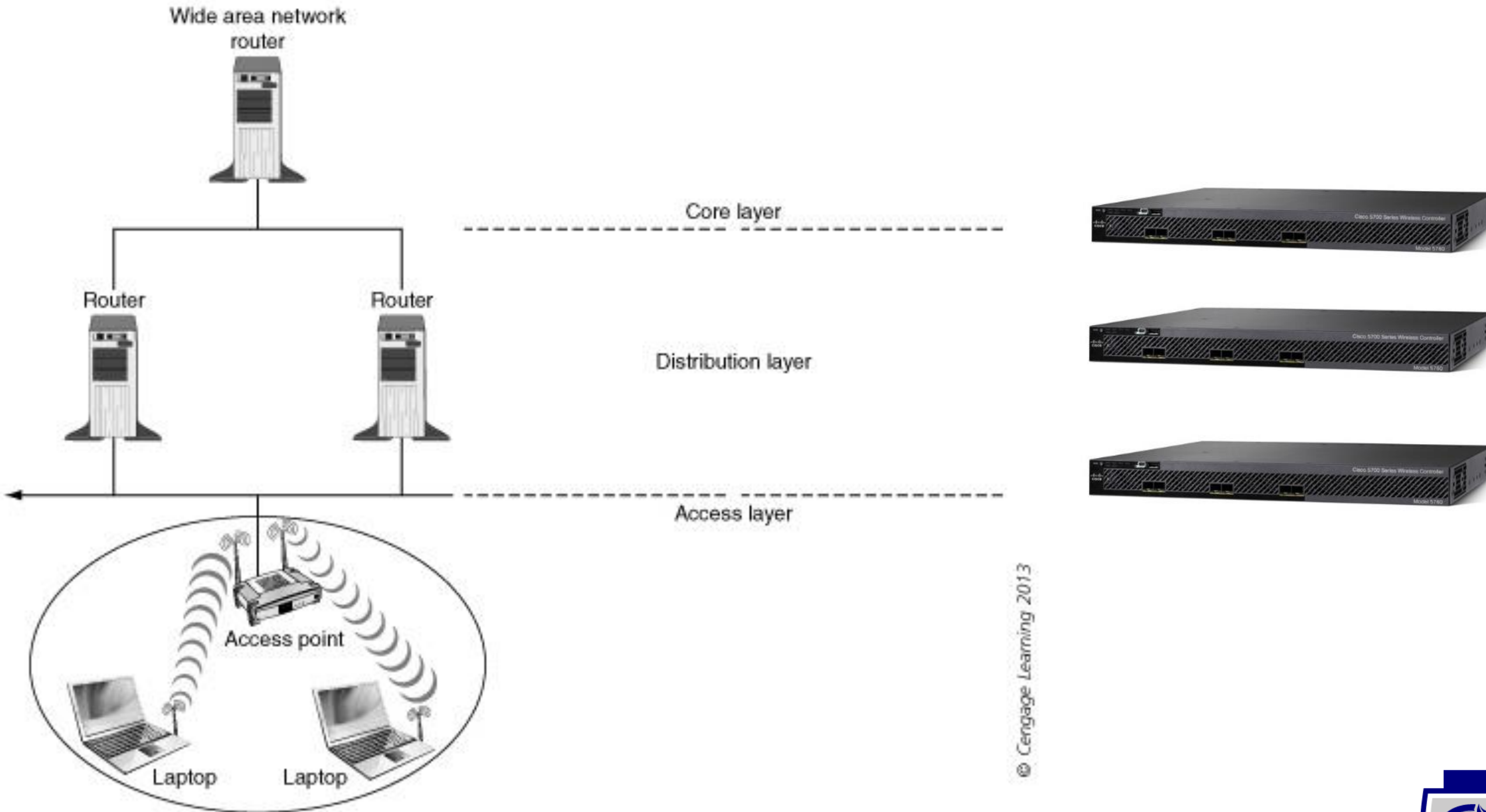
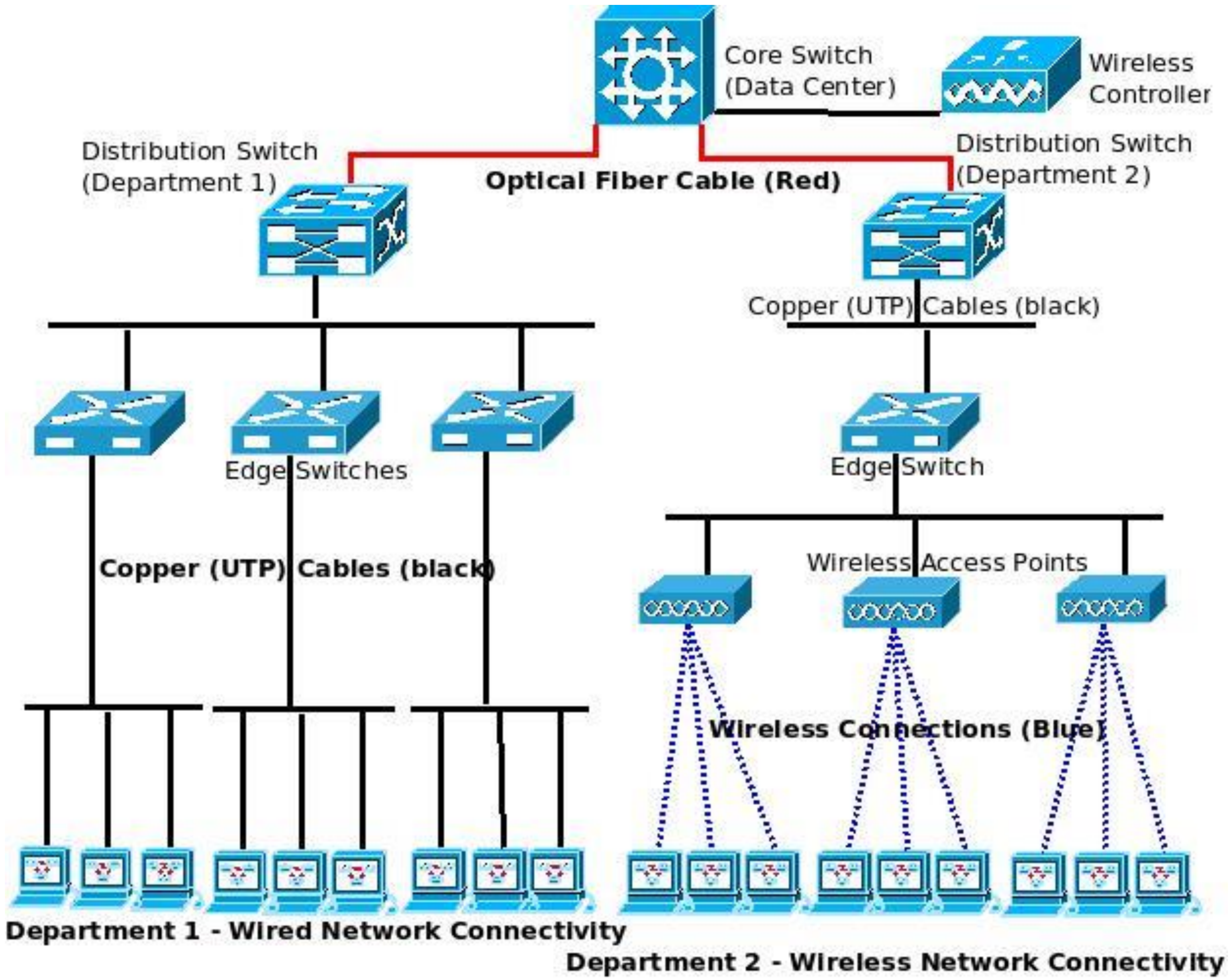


Figure 7-5 Network functional layers

Wireless LAN Controllers (WLCs)



Wireless LAN Controllers (WLCs)

- Another feature of a WLC is network connectivity
  - WLCs offer automated tools that can help predict the best locations for APs

- Other WLC features include:
  - WLAN profiles: set of specific configurations that can be applied to different wireless stations
  - Multiple BSSIDs
  - Scalability: allows for wireless network growth
  - Client roaming: allows stations to roam even to different subnets

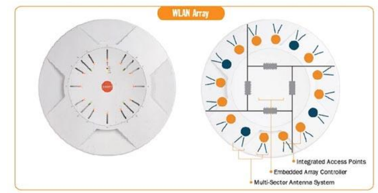
Wireless LAN Controllers (WLCs)

- Disadvantages to the controller-based architecture:
  - Currently, all devices are proprietary
    - IETF (Internet Engineering Task Force) and CAPWAP (Control and Provisioning of Wireless Access Points) are working on developing a protocol that will allow any vendor's WLC to communicate with any lightweight AP
  - Many WLC products still do not provide true convergence of the wired and wireless networks

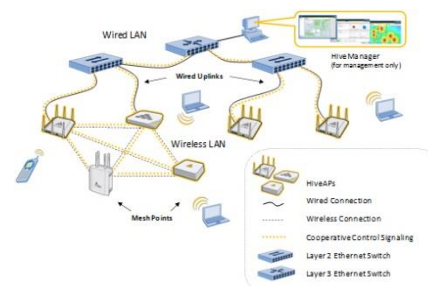
http://www.cisco.com/c/en/us/products/wireless/buyers-guide.html#~controllers

Other Architectures

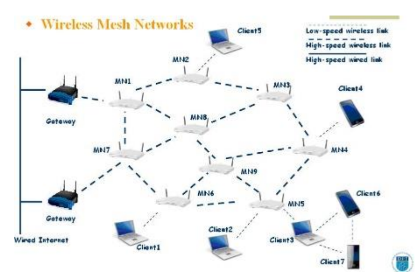
- Other types of WLAN architectures:
  - WLAN arrays



  - Cooperative control

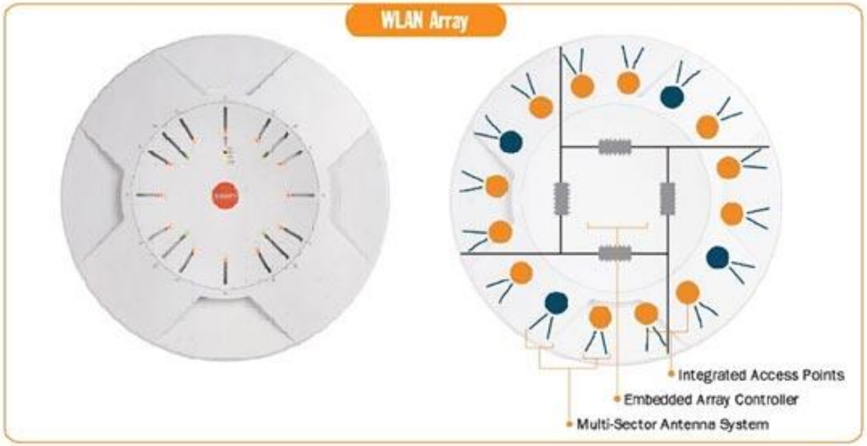


  - Mesh networks



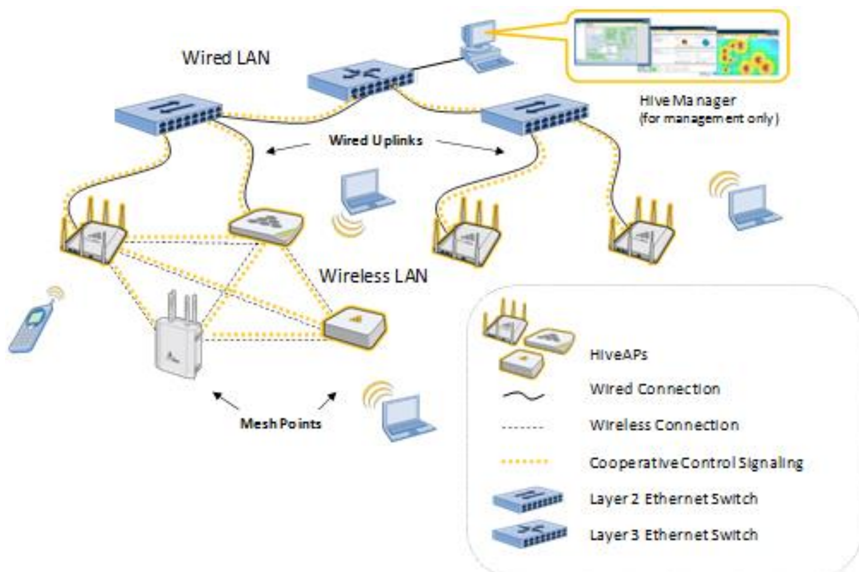
WLAN Arrays

- **WLAN array**: a proprietary product that contains a WLC that can be directly connected to as many as 16 integrated APs (IAPs)
  - The IAPs are arranged in a circular configuration around the WLC
  - Each IAP provides a separate RF channel of highly directional coverage
  - Channels are physically adjacent and can form a multichannel region of coverage around the WLAN array



Cooperative Control

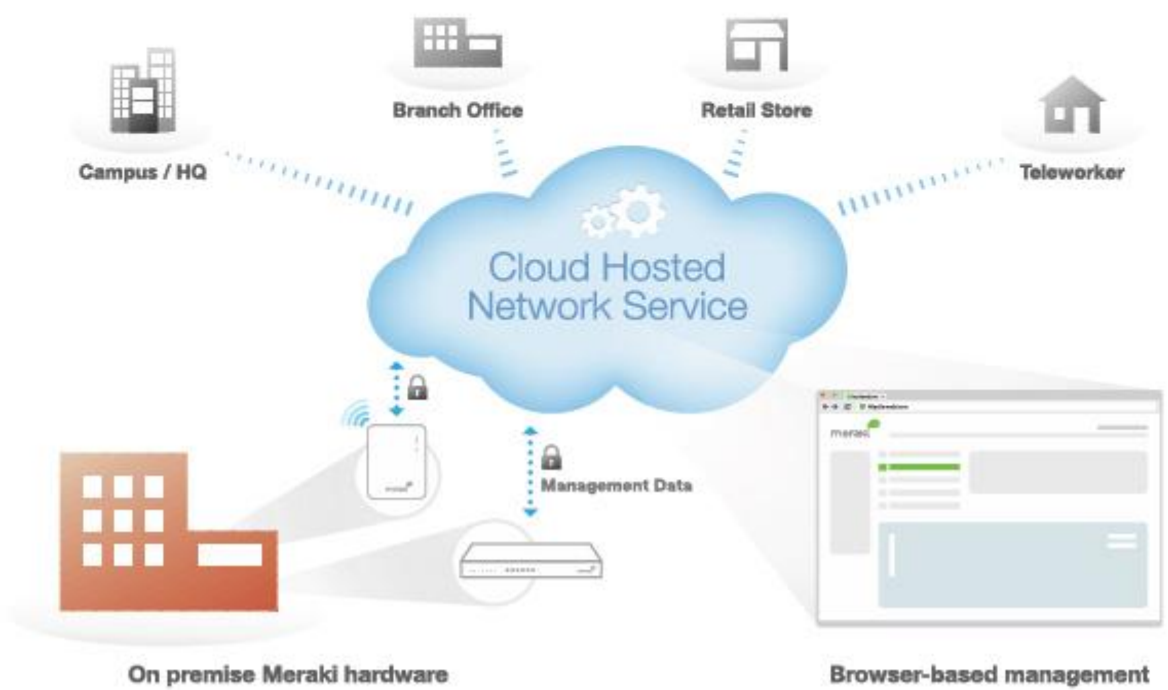
- **Cooperative control**: wireless LAN architecture that enables APs to communicate and coordinate with each other without a WLC
  - Each AP contains the capabilities of a WLC
- *HiveAP*: a special cooperative control autonomous AP
  - Multiple HiveAPs can be organized into groups (hives) that share control information between other HiveAPs to enable roaming, security, and load balancing



Cloud Management

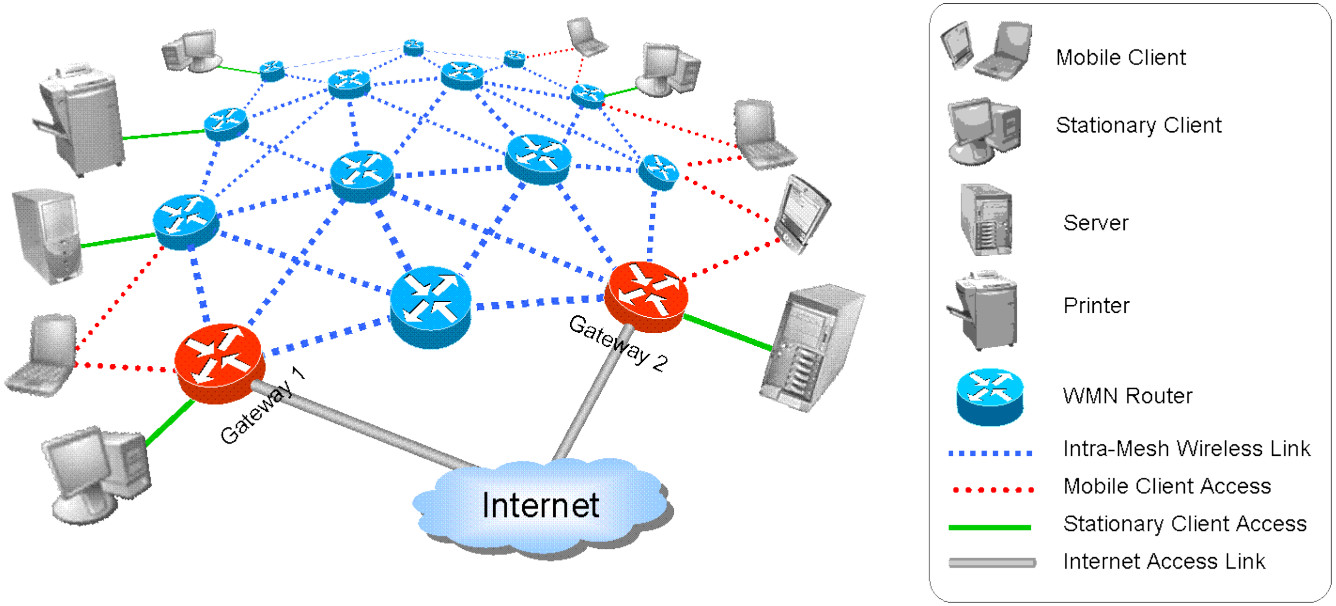
- **Cloud management**: connecting wireless devices together using the Internet in order to remotely manage them
  - Diagnostic tests can be run
  - Updates can be applied

- Cloud management helps reduce cost
  - Because devices can be managed remotely there is no need for multiple support teams for each location



Wireless Mesh Networks

- **Wireless Mesh Network (WMN)**: when multiple mesh access points communicate between themselves
  - Mesh access point does not have to be individually connected by a cable to an existing wired network
  - Only one of the mesh access point in a WMN must be physically connected to the wired network



Multiple-Channel Architecture vs. Single-Channel Architecture Models

- Two architecture models for WLANs:
  - Multiple-channel architecture
  - Single-channel architecture
- Each approach has their own respective applications

Multiple-Channel Architecture (MCA)

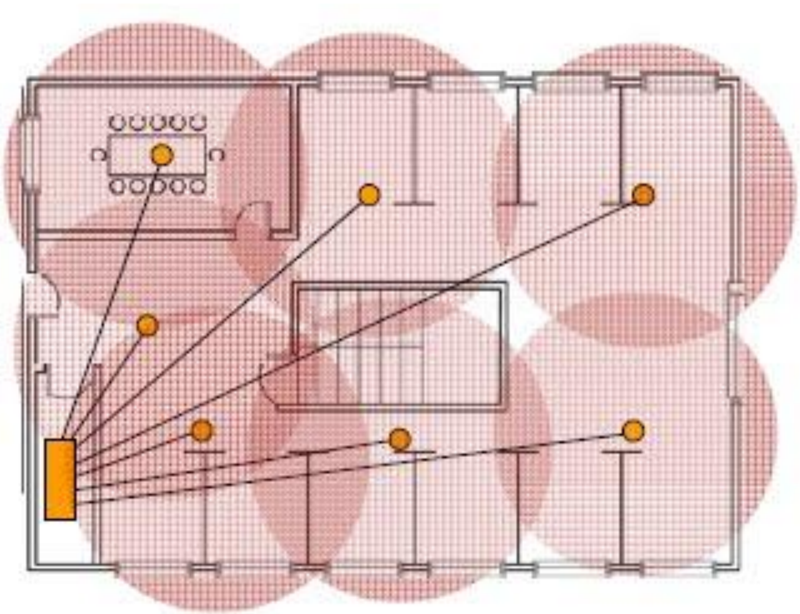
- **Multiple-Channel Architecture (MCA)**: a wireless architecture in which more than one channel is used in the wireless network
  - Cochannel interference: reduced throughput caused as a result of all of the APs set to same channel
  - MCA helps to eliminate this interference

- **Micro-cell architecture**: creates small areas of coverage
  - Helps to minimize adjacent channel interference and makes WLAN more scalable

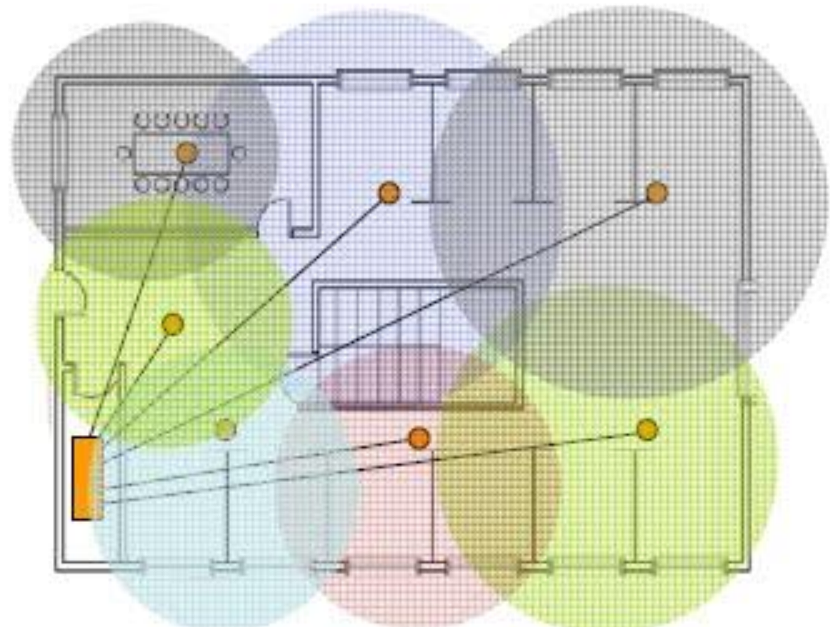
Single-Channel Architecture (SCA)

- **Single-channel architecture (SCS)**: all of the APs use the same channel
  - Each AP has overlapping coverage that forms a continuous region on a single channel
- Advantages:
  - Smoother handoffs
  - Easy setup – all APs are set to the same RF channel
  - Cochannel interference is no longer an issue
  - SCA provides more network information in order to make informed decisions
- Channel stacking: allows for increased capacity by having more than one SCA operating in an area

SCA vs MCA



Single channel architectures increase client contention and co-channel interference



Self-tuning multi-channel architectures reduce client contention and co-channel interference

Wireless Network Management Systems (WNMS)

- **Wireless network management system (WNMS)**: set of hardware/software that can be used to provide management of a wireless network
  - Includes configuration management
  - Deployment
  - Troubleshooting

Wireless Network Management Systems (WNMS)

- Typical features of a WNMS:
  - **Configuration management**: new or updated configurations can be "pushed" out to wireless devices
  - **Firmware/Software distribution**: can be distributed to all devices from a central management facility
  - **Intelligent scheduling**: updates can be scheduled to occur late at night or on the weekends
  - **User and device monitoring**: allows for monitoring historical information and use special diagnostic information to address problems

Power Management

- When laptop is part of a WLAN, must remain "awake" in order to receive network transmissions
  - Original IEEE 802 standard assumes stations always ready to receive network messages
- **Power management:** Allows mobile devices to conserve battery life without missing transmissions
  - Transparent to all protocols
  - Will not interfere with normal network functions
- Power management is divided into two categories: basic power management and enhanced power management techniques

Basic Power Management

- Steps of power save mode:
  - A station sends a frame to the AP notifying it that it will go into power save mode after this transmission
  - AP records that the station is in power save mode
  - As AP receives frames specifically for that station, it temporarily stores those frames **(buffering)**
  - At prescribed times, the AP will send out a beacon frame to all stations that will switch stations to active mode to receive the frame
    - Frame contains a list of stations that have buffered information waiting for them
    - List is known as a **traffic indication map (TIM)**

Basic Power Management

- Steps of power save mode (continued):
  - If a station learns from the TIM that buffered frames are waiting for it, that station will request the AP to have those frames forwarded
    - If it has no buffered frames then it can return to power save mode
- When a station in power save mode must receive a frame intended for all stations the AP will send a special TIM called a **delivery traffic indication message (DTIM)**
  - All stations will change to active mode to receive

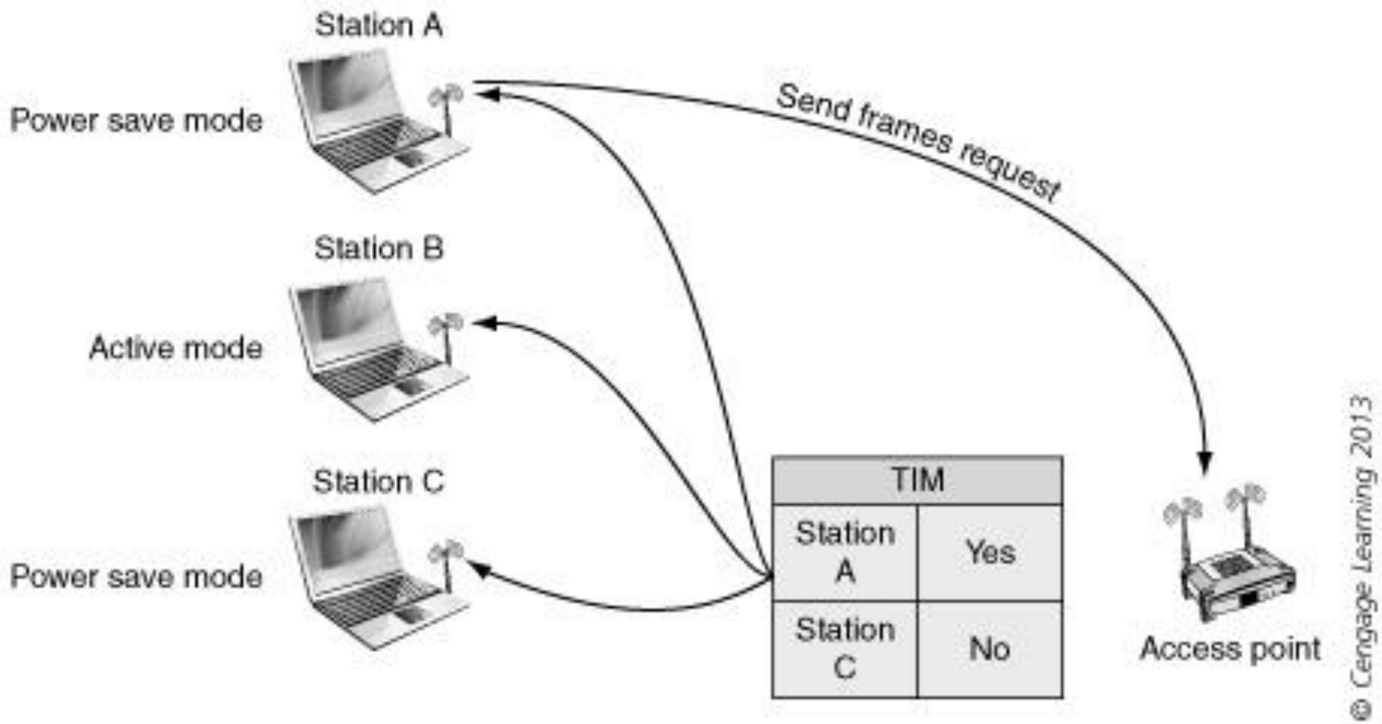


Figure 7-7 Request for frames

Basic Power Management

- Power management for IBSS:
  - **Ad hoc traffic indication message (ATIM) window:** Time at which all stations must be awake
    - Wireless device sends beacon to all other devices
      - Devices that previously attempted to send a frame to a sleeping device will send ATIM frame indicating that receiving device has data to receive and must remain awake

Enhanced Power Management

- **Unscheduled Automatic Power Save Delivery (U-APSD)**: a technology in which whenever the AP sees a frame coming from the station it will immediately release any frames it has been holding for that station

- **U-APSD** improves the efficiency in two ways:
  - It increases the amount of time that a station can be in power save mode
  - It decreases the number of frames that a station must send and receive in order to download stored frames on the AP

Enhanced Power Management

- **Power Save Multi-Poll (PSMP)**: an enhanced power management technology that can have either a scheduled or unscheduled component

- **Scheduled Power Save Multi-Poll (S-PSMP)**: allows an AP to send a transmission schedule to one or more stations in a WLAN
  - Schedule shows when that station will be in active mode as well as when they are allowed to begin transmitting

Enhanced Power Management

- Spatial Multiplexing Power Save (SMPS): an enhanced power management technology that turns off MIMO radios
  - Can be used with IEEE 802.11n devices using Multiple-Input Multiple-Output (MIMO)

Summary

- The most common type of wireless architecture is an autonomous access point architecture
- There are several enhanced features in this type of architecture: Quality of Service (QoS) and wireless virtual LANs (VLANS)
- A controller-based architecture uses a wireless LAN controller (WLC) to manage and provide configuration services to the WLAN
- There are three types of controller-based architecture access points: lightweight APs, lightweight mesh APs, and captive portal APs

Summary

- There are three other types of WLANs: a WLAN array, cooperative control, and wireless mesh networks
- A multiple-channel architecture, or MCA, has more than one channel in the wireless network
- In a single-channel architecture, or SCA, all APs use the same channel and each AP has overlapping coverage that forms a continuous region on a single channel
- A wireless network management system (WNMS) is a set of hardware/software that can be used to manage a wireless network

Summary

- Power management allows a station to be in either active or power save mode
- Power management is transparent to all protocols and applications so that it will not interfere with normal network functions
- Power management is divided into two categories: basic power management and enhanced power management techniques