CSCD 433/533
Advanced Networking

Lecture 6

Wireless LAN Components and Characteristics

Winter 2017

Some Material in these slides from J.F Kurose and K.W. Ross

Introduction

Reading: Chapter 4.4, Tanenbaum – Wireless Lans

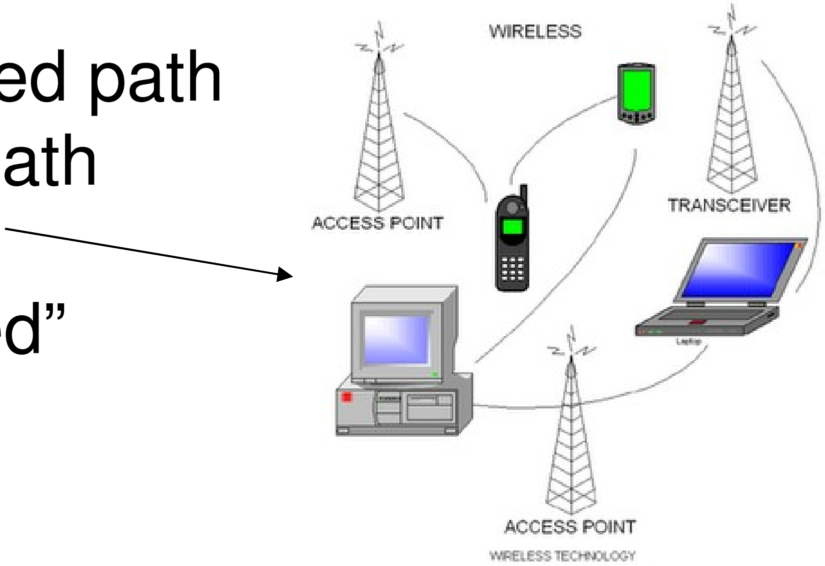
- Overview of Wireless
  - Signals
  - Transmission
  - Wireless Characteristics
- Identify components of wireless LAN networks
- Functions of Wireless 802.11 networks
- Services of 802.11

Wireless Signals

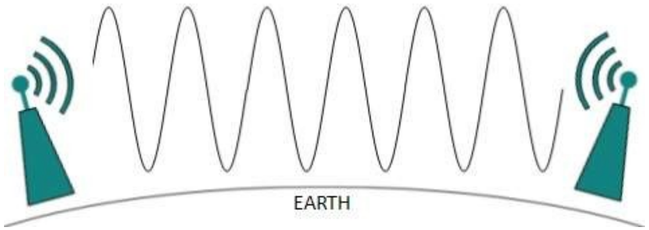
- Signals carried through the air by electromagnetic Waves
- Wireless spectrum varies between 9 KHz and 300 GHz
- Most WLAN's use 2.4 GHz or 5 GHz

Wireless Transmission

- Wired and wireless share many characteristics
  - Use the same Layer 3 - network and higher protocols
- However transmission through air vs. physical wires creates major differences
  - There is a lack of a fixed path
  - Air provides no fixed path for signals to follow, signals are “unguided”



Wireless Transmission

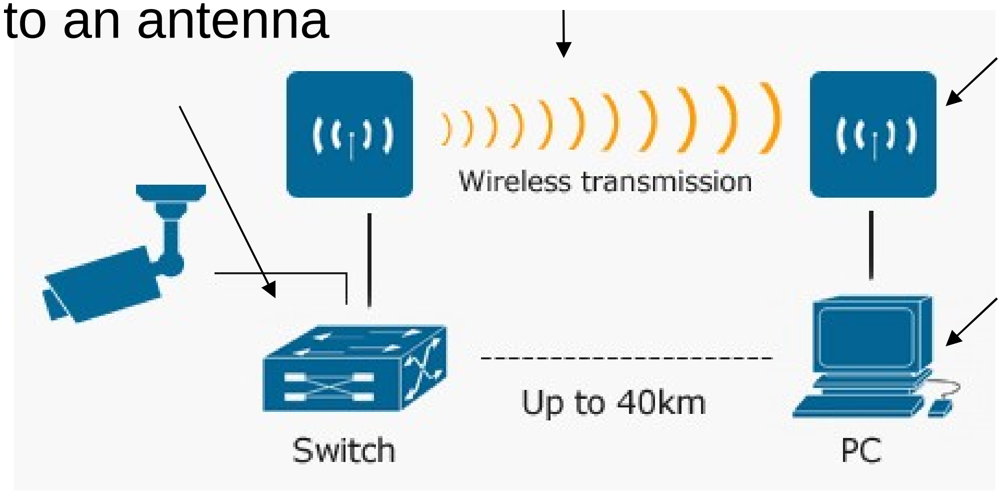


Wireless signals are transmitted, received and controlled differently than wired signals

1. Electronic signals travel from transmitter to an antenna
2. Emits signal as a series of electromagnetic waves at large in the air
3. Signal propagates through air until destination
4. Another antenna accepts signal, receiver converts it back to current

Both antennas must be tuned to same frequency

Wireless Transmission



Electromagnetic Waves

Transmitter to an antenna

Antenna accepts signal

receiver converts it back to current

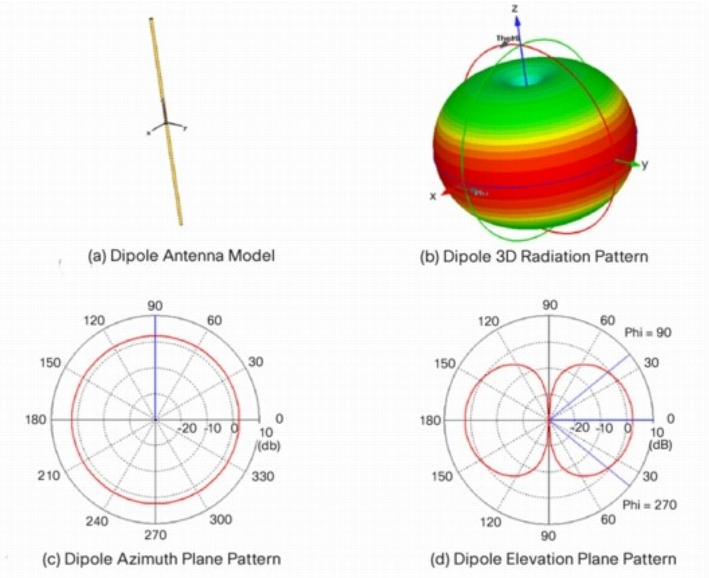
Antennas

- Each type of wireless technology uses a specific type of antenna
  - Antennas differ by power output, frequency and radiation pattern
  - The radiation pattern describes relative strength of an antenna
  - Two types are
    - **Omnidirectional**
    - **Directional**

Omnidirectional Antenna

- An omnidirectional antenna is a transmitting or receiving antenna that radiates or intercepts radio-frequency (RF) electromagnetic fields equally well in all horizontal directions - flat, two-dimensional (2D) geometric plane
- And, donut-like in 3D plane
- Most WiFi antennas are Omni

2-D Plane →



(a) Dipole Antenna Model

(b) Dipole 3D Radiation Pattern

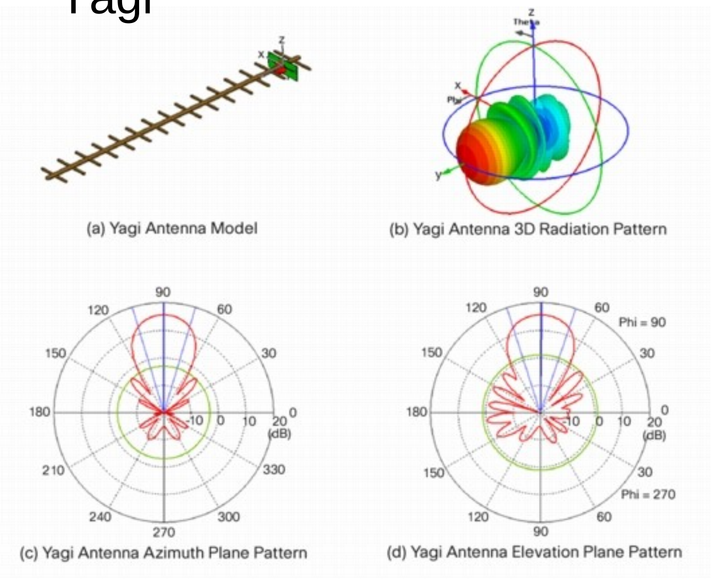
(c) Dipole Azimuth Plane Pattern

(d) Dipole Elevation Plane Pattern

Directional Antenna

- A **directional** antenna or **beam** antenna is an antenna which radiates or receives greater power in specific directions allowing for increased performance and reduced interference from unwanted sources

Yagi



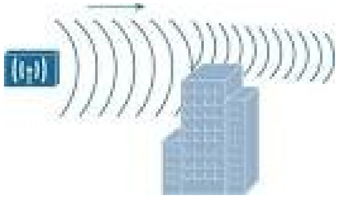
(a) Yagi Antenna Model

(b) Yagi Antenna 3D Radiation Pattern

(c) Yagi Antenna Azimuth Plane Pattern

(d) Yagi Antenna Elevation Plane Pattern

Signal Propagation



- Ideally wireless signal travels in a straight line from transmitter to receiver
- Yet, wireless signals do not usually follow a straight line
- When signal hits obstacle, signal may pass through object, be absorbed by object or may be subject to:

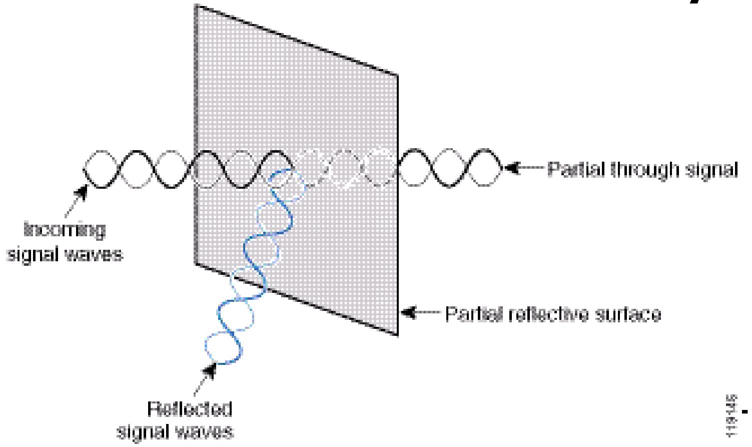
Reflection, Diffraction or Scattering

Anyone had trouble with obstacles and wireless?

Signal Reflection

- Wave encounters an obstacle and reflects or bounces back – towards source
- Signal bounces off objects whose size is large compared with signal wavelength

  Walls, floors, ceilings and the earth
- Some objects reflect more easily like metals

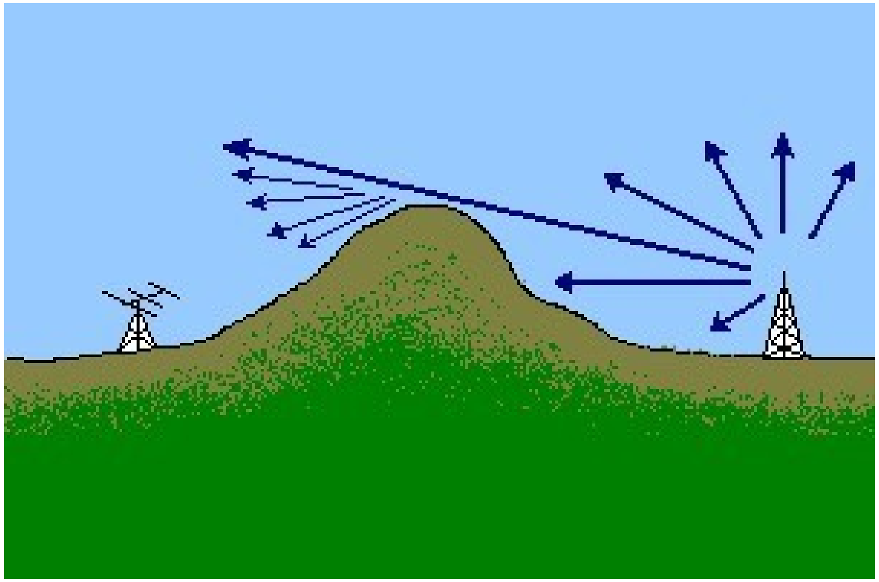


Signal Diffraction

- Signal splits into secondary waves when it encounters an obstacle.
- Waves then continue in direction they were traveling
- Objects with sharp edges, corners walls, desks create diffraction

Signal Diffraction

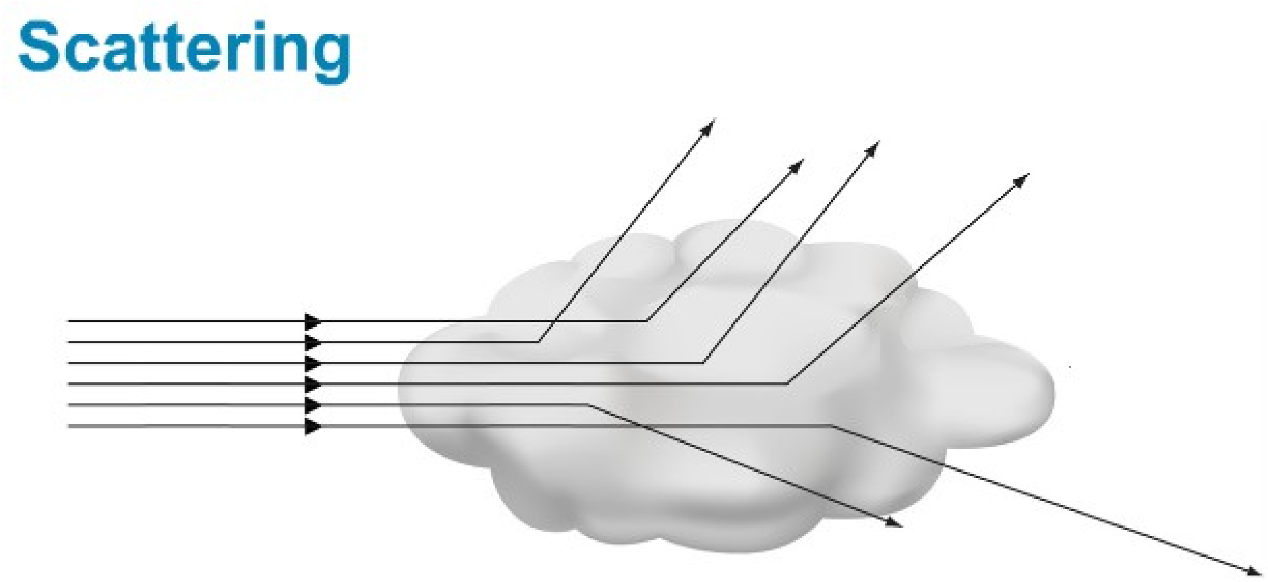
Receiver in shadow of hill may actually benefit from hill diffracting signal



Signal Scattering

- Scattering occurs when wireless encounters small objects compared to signal wavelength
  - Chairs, books, computers cause scattering
  - Outdoors, rain, mist, hail and snow can cause scattering

Signal Scattering



Interference

- Line noise distorts wired signals and Interference affects wireless
- Electromagnetic interference affects wireless signals because there is no shielding, only air
- Especially affects signals traveling in areas where there are other wireless devices
- Probably have seen this with your own wireless devices

802.11 Specifics

802.11 WLAN Networks

- 802.11 network is comprised of several components and services

- Wireless Station
- Access Point
- Communication Medium (Air)
- Wireless infrastructure

We will define these ...

802.11 WLAN Networks

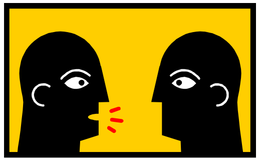
- Wireless Base Station
  The station (STA) is most basic component of wireless network
  - A station is any device that contains functionality of 802.11 protocol
    - Typically 802.11 functions implemented in hardware and software of network interface card (NIC)
    - A station could be laptop PC, handheld device, or a phone
    - Stations can be mobile, portable, or stationary
    - Stations can communicate with each other or an access point
    - All stations support 802.11 services
    - Stations also called Clients

802.11 WLAN Networks

- A Wireless Access Point (AP)
- Networking device equipped with wireless LAN network adapter acts as bridge between STA's and traditional wired network
- An access point Contains
  - At least one interface that connects wireless AP to an existing wired network (such as an Ethernet backbone)
  - Radio equipment with which it creates wireless connections with wireless clients
  - IEEE 802.1D bridging software, so can act as transparent bridge between wireless and wired LAN segments

Where is Access Point located in most homes?

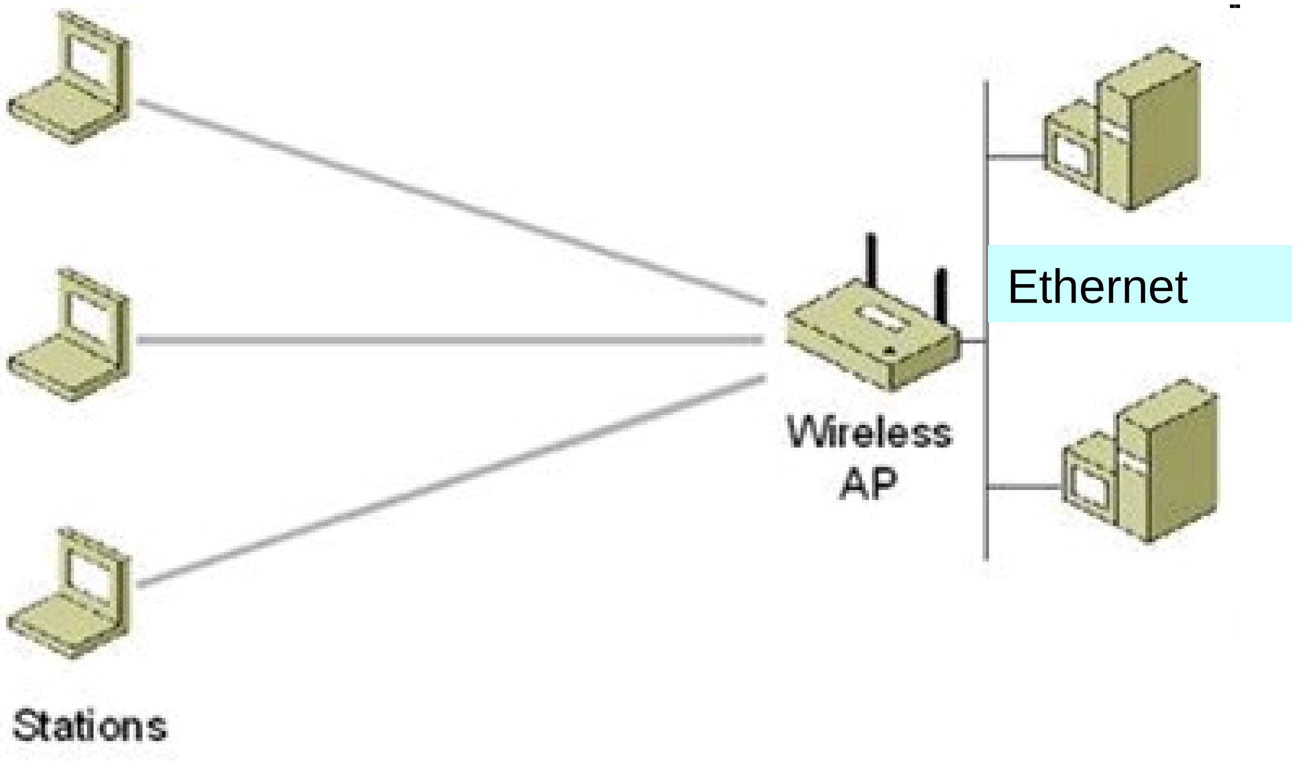
802.11 WLAN Networks



- Medium (Air)
  - Air is conduit by which information flows between computer devices and wireless infrastructure
  - Communication through wireless network is similar to talking to someone
  - As you move farther apart, it's more difficult to hear each other
  - What affects wireless signal strength or loss of strength?
  - Quality of transmission, depends on obstructions in air that either lessen or scatter strength and range of signals
    - Rain, snow, smog, and smoke are elements that impair propagation of wireless communications signals
    - A heavy downpour of rain can limit signal range by 50 percent while its raining
    - Placement affects strength, walls, large objects in the way

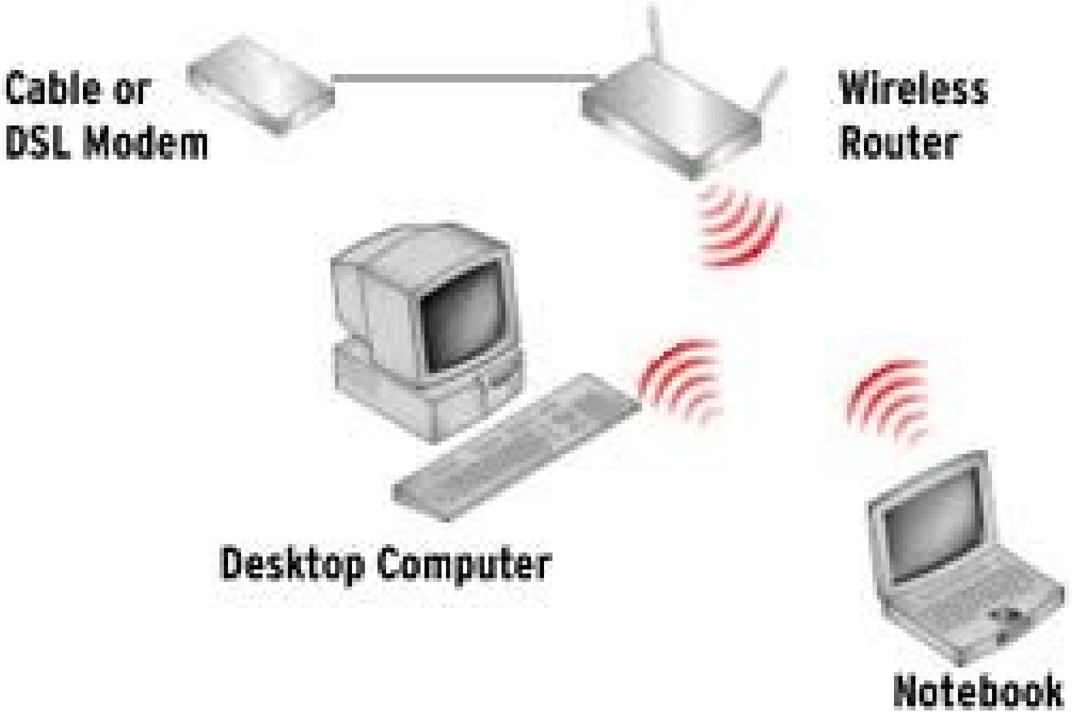
802.11 WLAN Networks

Typical picture of 802.11 LAN – Business Setting



Typical Home Setup

Many computers, one connection ...



802.11 Operating Modes

- IEEE 802.11 defines two basic operating modes for an 802.11 network
  - Ad hoc mode
  - Infrastructure mode

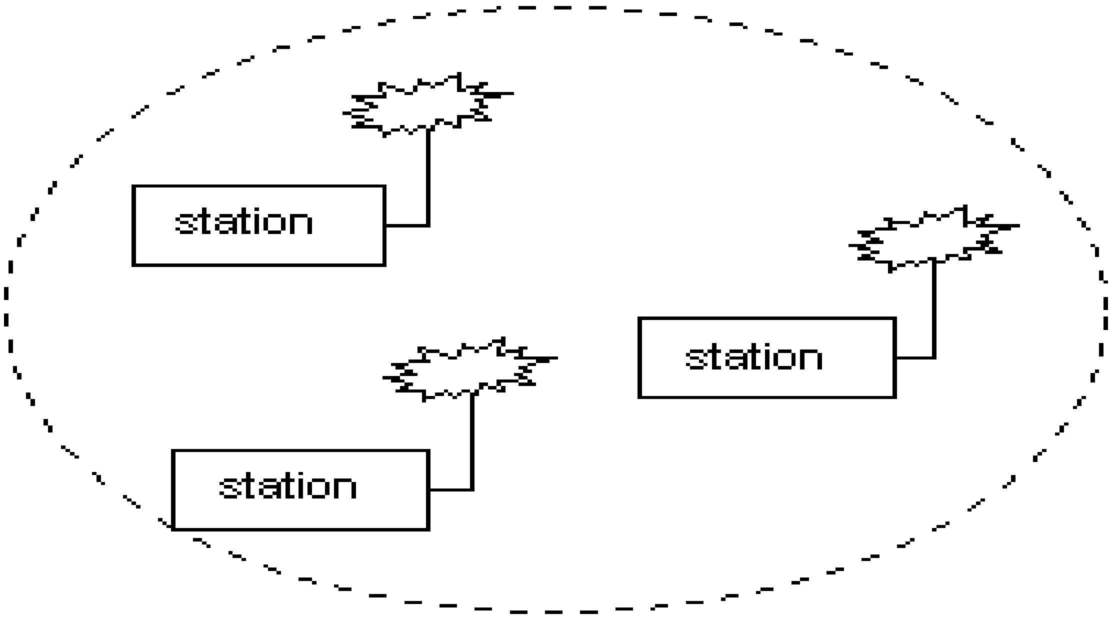
- Ad Hoc Mode
- In ad hoc mode, wireless clients communicate directly with each other without use of wireless AP or wired network

802.11 Operating Modes

- Ad hoc Mode is also called peer-to-peer mode
  - Wireless clients in ad hoc mode form an **Independent Basic Service Set (IBSS)**
    - Two or more wireless clients who communicate directly without use of wireless AP
  - Ad hoc mode used to connect wireless clients together
    - When there is no wireless AP
    - When wireless AP rejects an association due to failed authentication
    - When wireless client is explicitly configured to use ad hoc mode

802.11 Operating Modes

- In an IBSS, mobile stations communicate directly with each other
- Every mobile station may not be able to communicate with every other station due to range limitations
- No relay functions in an IBSS therefore all stations need to be within range of each other and communicate directly



Independent Basic Service Set (IBSS)

802.11 Operating Modes

- Ad hoc Mode
  - Smallest possible network is two stations
  - May be set up for a short time and specific purpose
    - Example: Meeting where all participants create an IBSS to share data
    - When meeting ends, IBSS is dissolved

802.11 Operating Modes

- Infrastructure mode
  - Usual way wireless networks set up
  - At least one wireless AP and one wireless client
  - Wireless client uses wireless AP to access resources of traditional wired network
  - Wired network is typically Ethernet LAN in business setting, or Ethernet + cable or DSL modem in home network

802.11 Operating Modes

- Infrastructure Mode
  - A single wireless AP supporting one or multiple wireless clients is

    Basic Service Set (BSS)

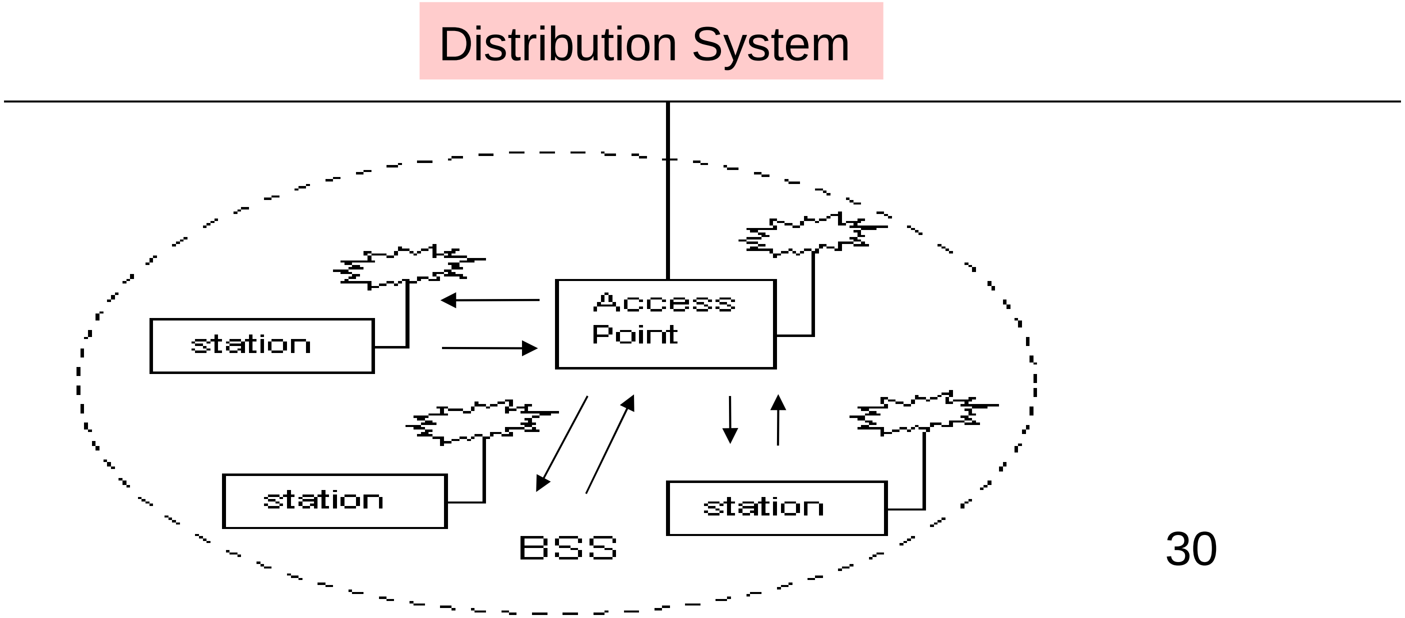
  - A set of two or more wireless APs connected to the same wired network is

    Extended Service Set (ESS)

    - An ESS is single logical network segment (also known as a subnet), and is identified by its SSID
    - More on ESS later …

Infrastructure Basic Service Set

- An Infrastructure Basic Service Set is BSS with an Access Point (AP)
- Access Point provides local relay function for BSS
- All stations in BSS communicate with access point and no longer communicate directly. All frames are relayed between stations by access point



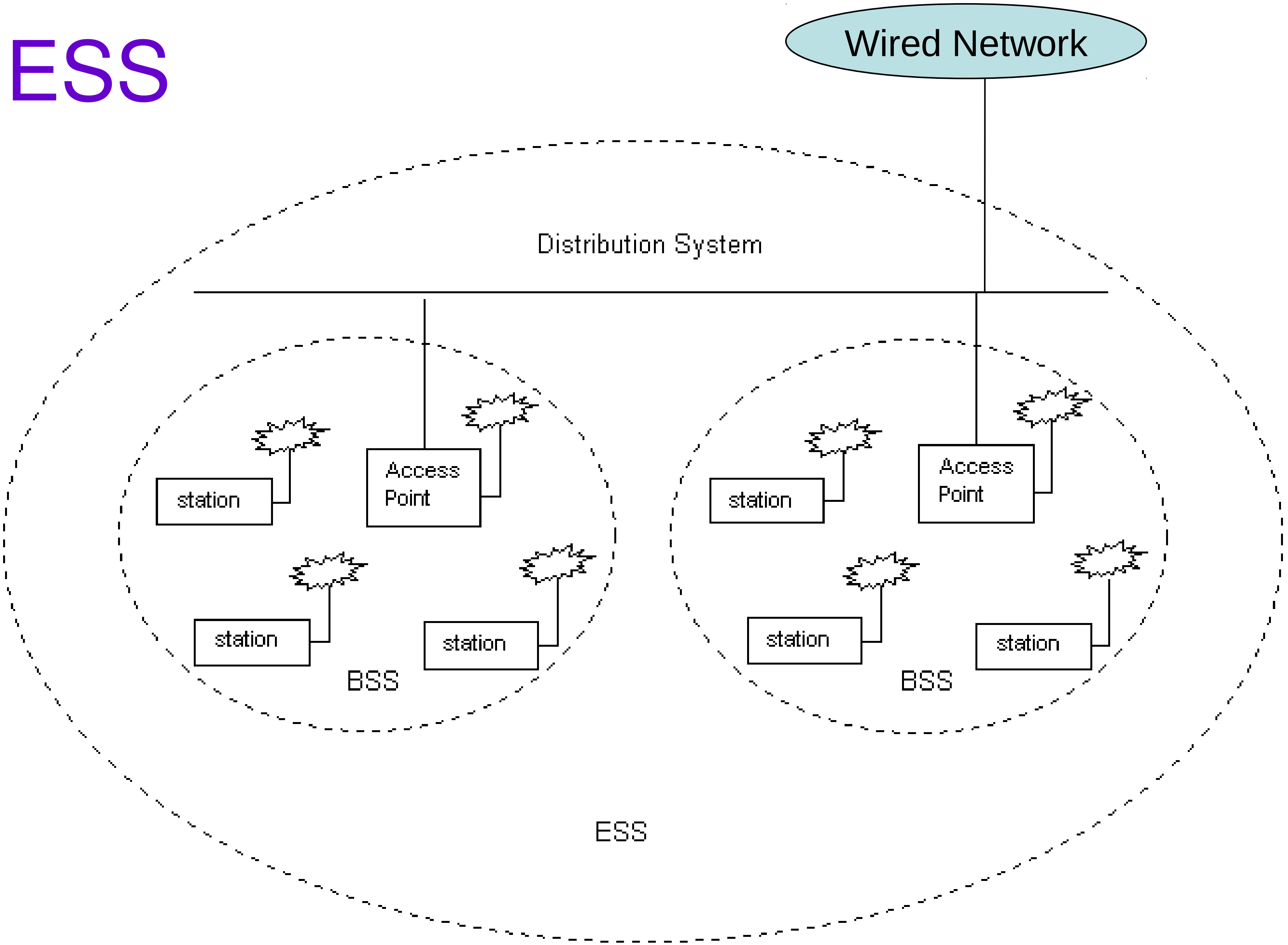
Infrastructure Basic Service Set

- BSS
  - Logical concept that groups STA’s with single AP
  - All STA’s use same channel
  - No limit is placed on number of STA’s that can associate to an AP
  - Larger geographic areas need a different configuration …

Extended Service Set (ESS)

- ESS’s extend coverage of larger networks by chaining BSS’s together with backbone network
  - An extended service set is set of infrastructure BSS’s, where access points communicate amongst themselves to forward traffic from one BSS to another
  - All BSS’s configured to be part of same ESS
    - All AP’s are given Same SSID
    - Example: Wi-EWU or Wi-EWUguest

ESS


Wired Network
Distribution System
station
Access Point
station
station
BSS
station
Access Point
station
station
BSS
ESS

Extended Service Set (ESS)

- ESS is highest level of abstraction supported by 802.11 networks
  - AP's in ESS operate together so that outside world uses station's MAC address for communication
    - Doesn't matter what it's location in ESS
    - AP associated with Station delivers data
  - Besides delivery of data to STA's, ESS's
    - Do load balancing on channels
    - Automatic fail-over if AP goes down
    - Physical roaming between BSS's in same ESS

ESS and Network Transparency

- Final Comment on ESS Abstraction
- Network equipment outside of Extended Service Set views ESS and all of its mobile stations as a single MAC-layer network where all stations are physically stationary
- Thus, ESS hides mobility of mobile stations from everything outside ESS
- This level of indirection allows existing network protocols that have no concept of mobility to operate correctly with a wireless LAN

802.11 Distribution System

802.11 Distribution System

- Interfaces
  - An AP has three interfaces:
    1. Ethernet Interface (portal)
       - Connects AP or organization's network backbone
       - Also, historical distribution system for 802.11
    2. Radio Interface
       - Enables communication between AP and STA's
       - Radio Interface's MAC address is BSS's unique hardware identifier – called BSSID

802.11 Distribution System

- Interfaces continued

    3. Serial interface

        - Typically managed via HTTP interface or SSH secure command line interface
        - If not, AP’s local serial port provides an alternative command line interface

  - Note: Smaller (cheaper) AP’s also function as broadband routers and typically don’t have a serial interface

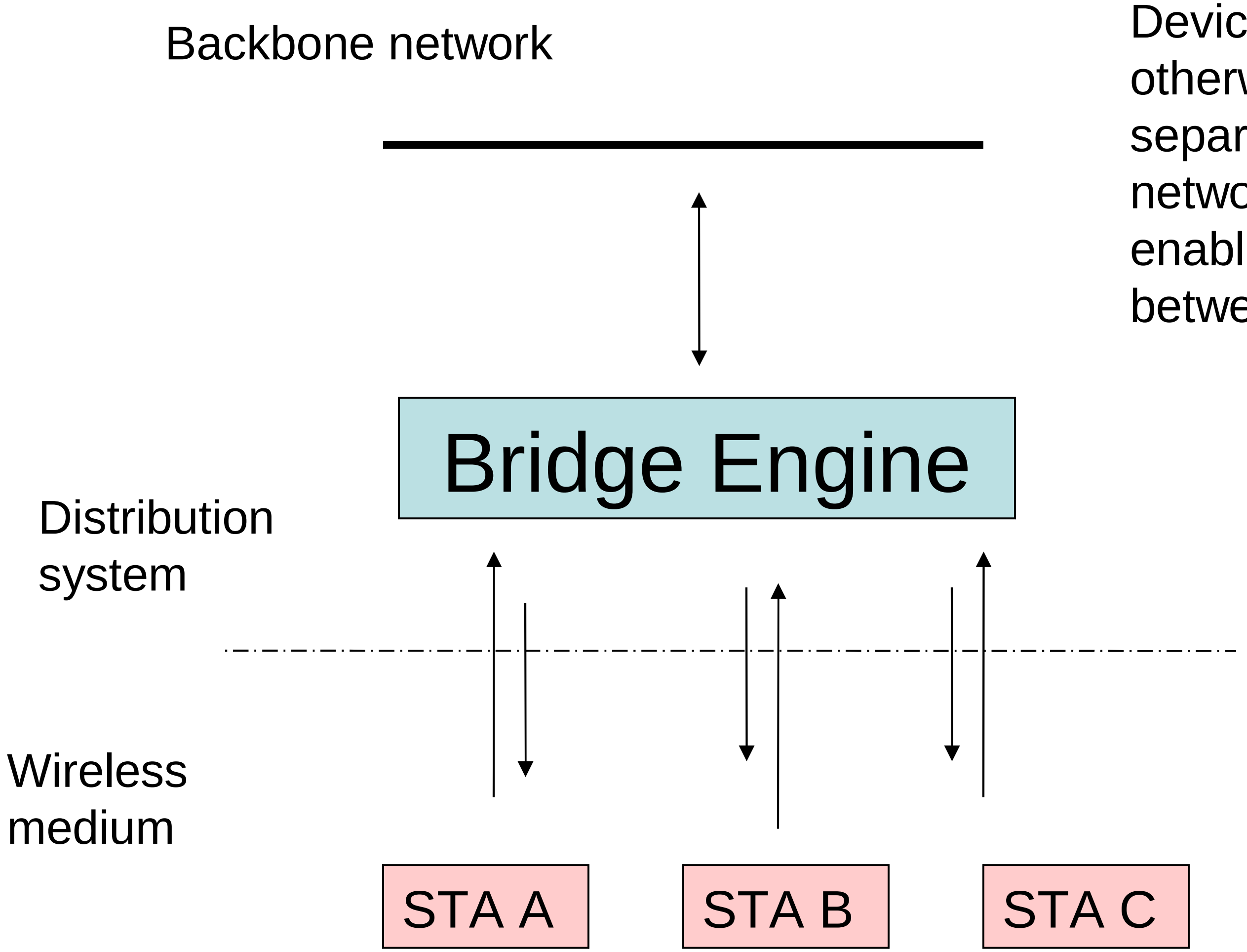
802.11 Distribution System

- Logical component of 802.11 used to forward frames to their destination STA's
- Most commercial products, on market distribution system medium is:
  - Typically Ethernet, wired network
  - Also, can be wireless distribution system (WDS)
    - Wireless bridge can be used to quickly connect two physical locations

802.11 WLAN Networks

- Distribution System
- In IEEE 802.11, distribution system is not necessarily a network
  - Nor does standard place any restrictions on how distribution system is implemented
  - Only on services it must provide
  - Services discussed next …

Distribution System



What is a bridge?

Device joins two otherwise separate computer networks together to enable communication between them.

Distribution Services

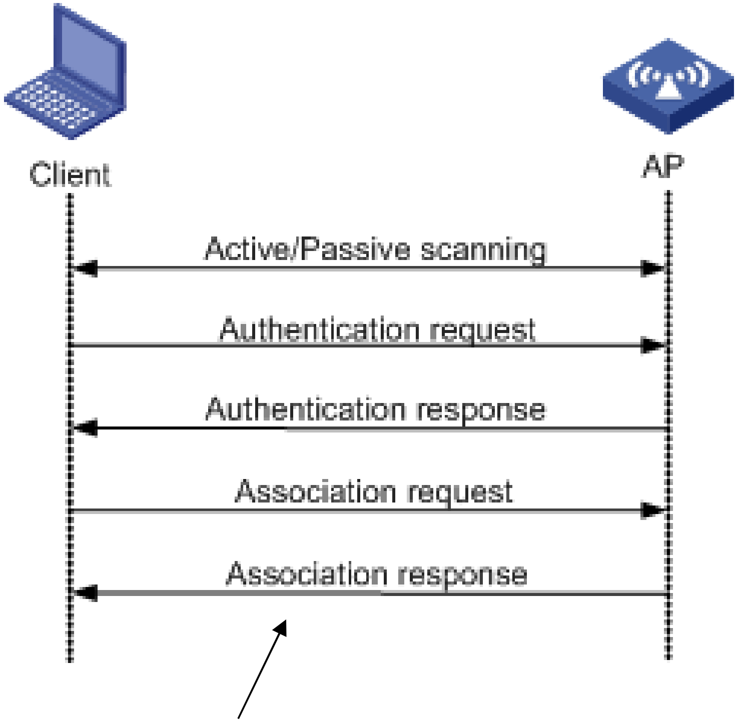
- Distribution services provide functionality across a distribution system
  - Typically, access points provide distribution **services**
- Distribution services and functions detailed below include:
  - Distribution System Services
    - Association, disassociation, re-association, distribution, and integration
  - Station Services
    - Authentication, Deauthentication, Privacy and Packet delivery

Examine these in more detail

Association

- The association service used to make logical connection between mobile station and an access point
  - Each station must be **associated** with an access point before it can send data through access point into distribution system
  - Connection is necessary in order for distribution system to know where and how to deliver data to mobile station
- Mobile station invokes association service once and only once, typically when station enters BSS
- Each station can associate with one access point though Access Point can associate with multiple stations

Association Service



Client sends an Association Request
AP sends back an Association Response

Disassociation

- The disassociation service is used
  - To force mobile station to terminate association with an access point or
  - Mobile station to inform an access point that it no longer requires services of distribution system

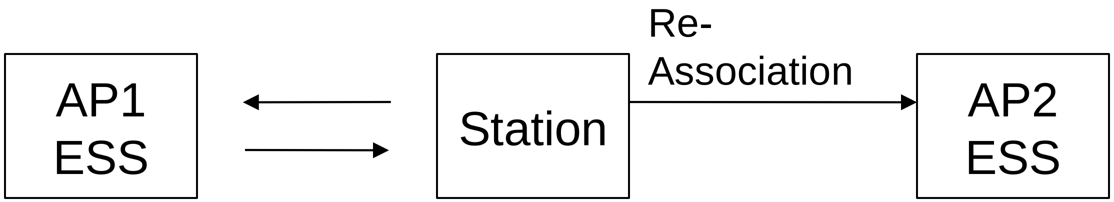
- When station becomes disassociated, it must begin a new association to communicate with an access point again

  An AP may force station or stations to disassociate because of resource restraints, AP is shutting down or being removed from network for a variety of reasons

- When a mobile station knows that it will no longer require services of an access point, it may invoke disassociation service to notify AP that connection services of AP no longer required

Re-association

- Re-Association enables station to change its current association with an access point
  - Re-association service similar to association service, except it includes information about AP with which mobile station has been previously associated
  - A mobile station will use **re-association** service repeatedly as it moves throughout ESS,
    - Loses contact with AP with which it is associated, and
    - Needs to become associated with a new AP



Re-association

- By using re-association service, a mobile station provides information to AP to which it will be associated and information pertaining to AP which it will be disassociated
- Allows newly associated AP to contact previously associated AP to obtain frames that may be waiting there for delivery to mobile station as well as other information that may be relevant to the new association

The mobile station always initiates re-association.

Distribution

- Distribution is primary service used by an 802.11 station
- A station uses distribution service every time it sends MAC frames across distribution system
- Distribution service provides distribution with enough information to determine proper destination BSS for MAC frame

  Association services (association, re-association, and disassociation) provide necessary information for distribution service to operate

Comment

- Distribution within distribution system does not necessarily involve any additional features outside of the association services, though a station must be associated with an access point for the distribution service to forward frames properly

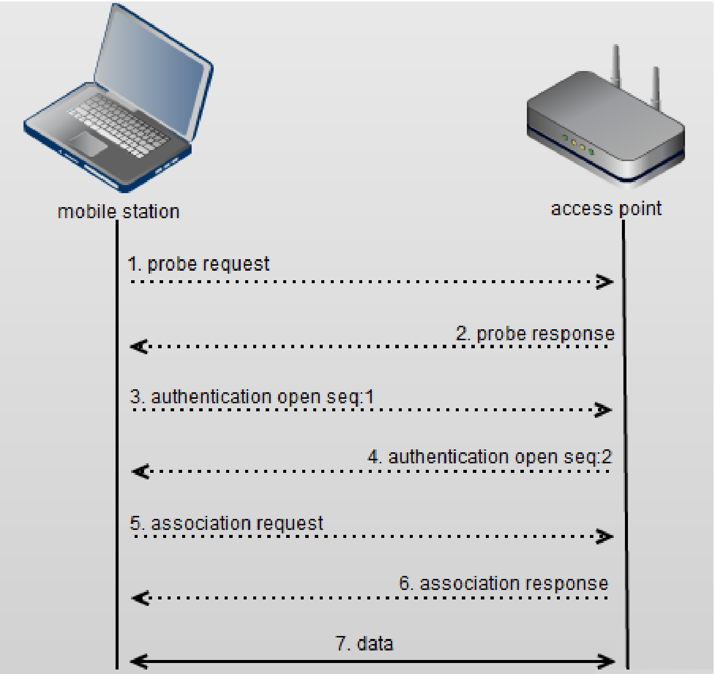
Integration

- Integration service connects 802.11 WLAN to other LANs, including one or more wired LANs or 802.11 WLANs
  - A portal performs the integration service.
  - The portal is an abstract architectural concept that typically resides in an AP though it could be part of a separate network component entirely.

    The integration service translates 802.11 frames to frames that may traverse another network, and vice versa

Authentication

- The Authentication service provides ability to control access to the LAN
  - If two stations want to communicate with each other, they first identify each other
  - This is done in ESSs as well as in IBSSs
  - This service provides only link-level authentication mechanism
  - Authentication at the low level is typically allowed, set to “open”
  - In the association step, encryption and other privacy settings occur



Deauthentication and Privacy

- The deauthentication service is invoked whenever an existing authentication is to be terminated

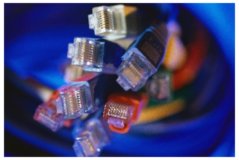
- Privacy is obtained by executing "Wired Eqivalent Privacy" (WEP) – old or WPA2 algorithms, all data frames (and some authentication management frames) are encrypted
- This occurs during association

MAC Service Data Unit (MSDU)

- Stations provide the MSDU (or packets) delivery service.
  - Responsible for getting data to actual endpoints
  - More on this later …

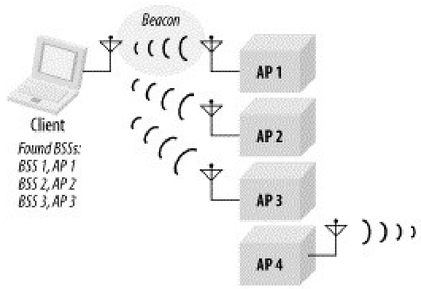
Basic Network Operation Example

802.11 Network Operation



- Wireless adapter is turned on, it scans wireless frequencies for wireless APs and other wireless clients
- Scanning is like **listening**, wireless adapter listens on all channels for beacon frames sent by wireless AP's and other wireless clients
  - Two types of scanning:
    - Active and Passive

802.11 Network Operation

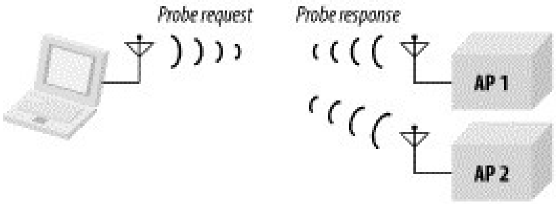


WLAN Passive Scanning

- Passive scanning
  - Adapter will tune to every RF channel, note information discovered about each AP
  - APs send beacon frames every 100ms
  - While adapter is scanning a channel, receives beacon frames from AP
  - Adapter notes signal strength of beacon frame and proceeds to scan other channels, also encryption type and data rate supported
  - Once scanning of RF channels is complete, adapter decides on AP to associate to

AP with strongest beacon signal, compatible data rate and supported encryption

802.11 Network Operation



WLAN active scanning

- Active scanning
  - Adapter will send probe request frames on all RF channels
  - An AP receiving probe requests sends probe responses
  - Adapter decides what AP to associate with based on information in probe response frame
    - Information is same as in passive scanning, signal strength, data rate and encryption

802.11 Network Operation

- After scanning,
  - Wireless adapter chooses a wireless AP with which to associate
  - Selection is made by using Service Set Identifier (SSID) of wireless network and wireless AP with best signal strength (highest SNR) given data rate and encryption is compatible
- Next,
  - First the authentication process is done, to identify the laptop to the AP, this has to happen before association
  - Wireless client switches to channel of chosen wireless AP and negotiates use of a logical wireless point-to-point connection
- Known as association

802.11 Network Operation

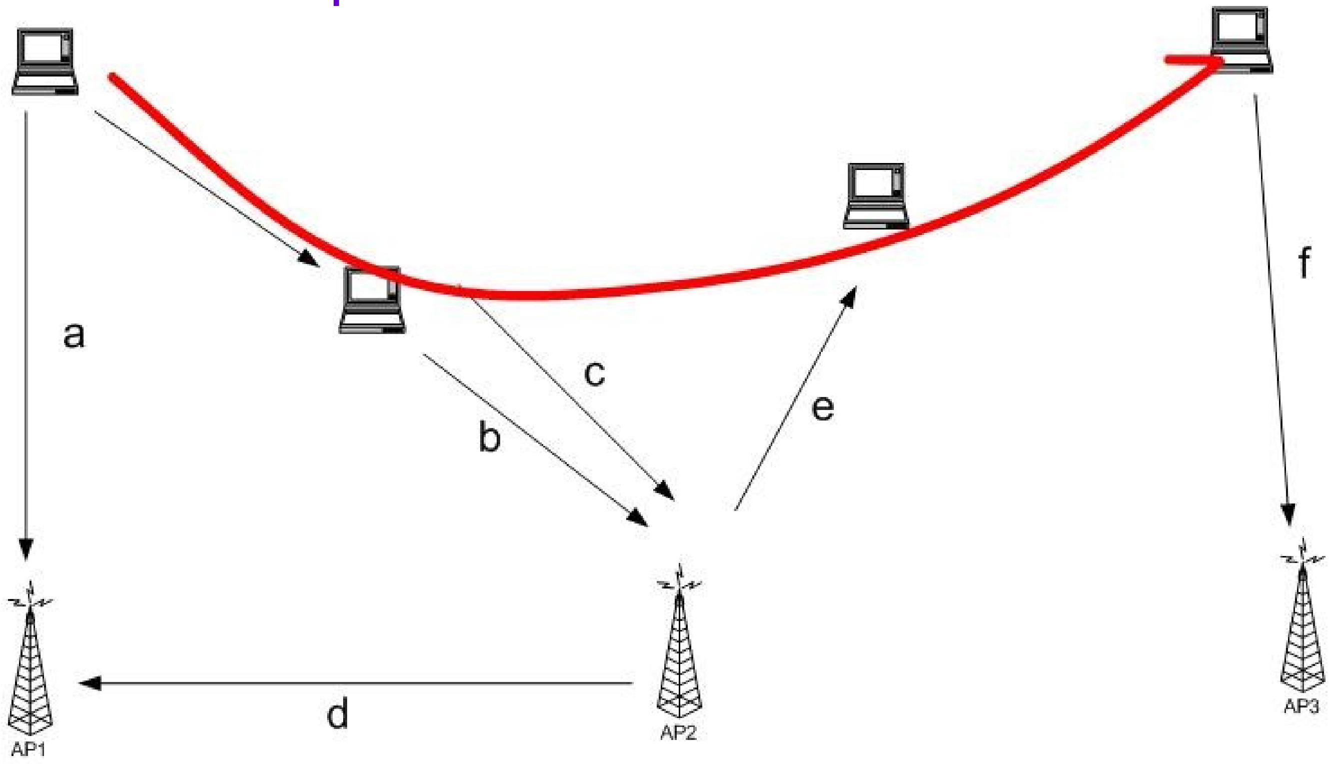
- If signal strength of wireless AP is too low,
- error rate too high, or
- instructed by the operating system
  (in the case of Windows, every 60 seconds),

- Wireless client scans for other wireless APs for a stronger signal to the same wireless network
- If found,
  - Wireless client switches to the channel of that wireless AP
- Known as reassociation

802.11 Network Operation

- Reassociation with a different wireless AP occurs for many reasons
  - Signal can weaken because wireless client moves away from wireless AP or wireless AP becomes congested with too much other traffic or interference
  - Wireless client, by switching to another wireless AP, can distribute the load over other wireless APs, increasing the performance for other wireless clients
- As a wireless client moves its physical location
  - Can associate and reassociate from one wireless AP to another, maintaining a continuous connection during physical relocation

802.11 Network Operation



(a) ---- The station finds AP1, it will authenticate and associate.

(b) ---- As the station moves, it may pre-authenticate with AP2.

(c) ---- When the association with AP1 is no longer desirable, it may reassociate with AP2.

(d) ---- AP2 notify AP1 of the new location of the station, terminates the previous association with AP1.

(e) ---- At some point, AP2 may be taken out of service. AP2 would disassociate the associated stations.

(f) ---- The station find another access point and authenticate and associate.

Windows Example

- For example, a wireless client is assigned an IP address when it connects to first wireless AP
  - When wireless client roams within an ESS, it creates wireless connection with another wireless AP, Does IP Address change?
  - No. It keeps same IP address since wireless APs are on the same logical subnet
  - ESS abstraction allows this to happen
  - When it roams to different ESS, IP address needs to change

Windows Example continued

- Wireless client behavior affects whether it needs another IP or not
  - For Windows wireless clients, a reassociation is interpreted as a media disconnect/connect event
  - This causes Windows to perform a DHCP renewal for the TCP/IP protocol
    - For reassociations within ESS, DHCP renewal refreshes current IP address
    - For client reassociations with AP across an ESS boundary, the DHCP renewal process obtains a new IP address that is relevant for logical IP subnet of the new ESS

Summary

- Presented a high level view of wireless in general
- 802.11 operation specifically
  - Network operation and client association
  - 802.11 networks provide basic services including association, disassociation, re-association, distribution, integration plus privacy, authentication and MSDU delivery
- Overview of how services work
- Next more details – frames

Finish

- Chapter 4.4, Tanenbaum – Wireless Lans

CSCD 433/533 Advanced Networking

Lecture 6

Wireless LAN Components and Characteristics

Winter 2017

Some Material in these slides from J.F Kurose and K.W. Ross

Introduction

Reading: Chapter 4.4, Tanenbaum – Wireless Lans

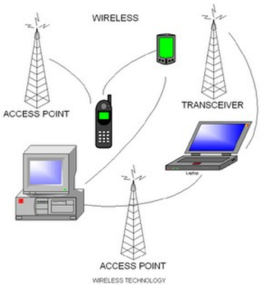
- Overview of Wireless
  - Signals
  - Transmission
  - Wireless Characteristics
- Identify components of wireless LAN networks
- Functions of Wireless 802.11 networks
- Services of 802.11

Wireless Signals

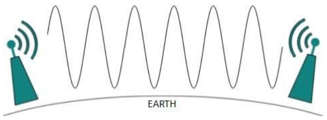
- Signals carried through the air by electromagnetic Waves
- Wireless spectrum varies between 9 KHz and 300 GHz
- Most WLAN's use 2.4 GHz or 5 GHz

Wireless Transmission

- Wired and wireless share many characteristics
  - Use the same Layer 3 - network and higher protocols
- However transmission through air vs. physical wires creates major differences
  - There is a lack of a fixed path
  - Air provides no fixed path
    for signals to follow,
    signals are “unguided”



Wireless Transmission

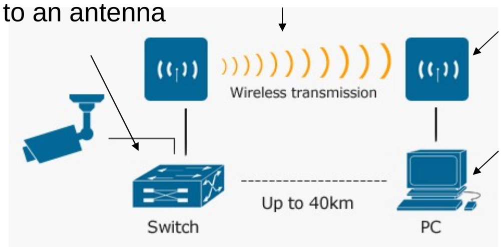


Wireless signals are transmitted, received and controlled differently than wired signals

1. Electronic signals travel from transmitter to an antenna
2. Emits signal as a series of electromagnetic waves at large in the air
3. Signal propagates through air until destination
4. Another antenna accepts signal, receiver converts it back to current

Both antennas must be tuned to same frequency

Wireless Transmission



Electromagnetic Waves

Transmitter to an antenna

Antenna
accepts signal

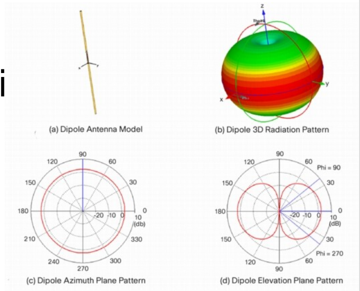
receiver converts
it back to current

Antennas

- Each type of wireless technology uses a specific type of antenna
  - Antennas differ by power output, frequency and radiation pattern
  - The radiation pattern describes relative strength of an antenna
  - Two types are
    - **Omnidirectional**
    - **Directional**

Omnidirectional Antenna

- An omnidirectional antenna is a transmitting or receiving antenna that radiates or intercepts radio-frequency (RF) electromagnetic fields equally well in all horizontal directions - flat, two-dimensional (2D) geometric plane
- And, donut-like in 3D plane
- Most WiFi antennas are Omni



(a) Dipole Antenna Model

(b) Dipole 3D Radiation Pattern

(c) Dipole Azimuth Plane Pattern

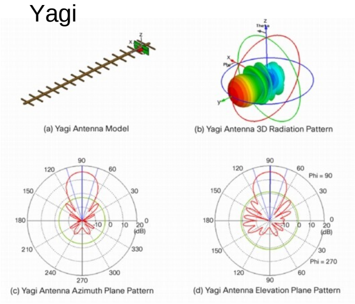
(d) Dipole Elevation Plane Pattern

2-D Plane →

Directional Antenna

- A **directional** antenna or **beam** antenna is an antenna which radiates or receives greater power in specific directions allowing for increased performance and reduced interference from unwanted sources

Yagi



(a) Yagi Antenna Model

(b) Yagi Antenna 3D Radiation Pattern

(c) Yagi Antenna Azimuth Plane Pattern

(d) Yagi Antenna Elevation Plane Pattern

Signal Propagation

- Ideally wireless signal travels in a straight line from transmitter to receiver
- Yet, wireless signals do not usually follow a straight line
- When signal hits obstacle, signal may pass through object, be absorbed by object or may be subject to:

Reflection, Diffraction or Scattering

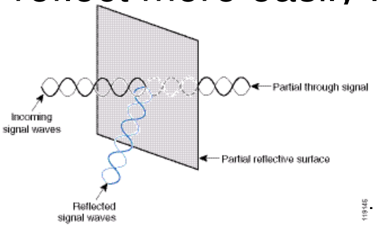
Anyone had trouble with obstacles and wireless?

Signal Reflection

- Wave encounters an obstacle and reflects or bounces back – towards source
- Signal bounces off objects whose size is large compared with signal wavelength

  Walls, floors, ceilings and the earth

- Some objects reflect more easily like metals

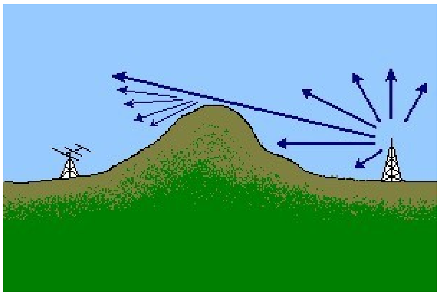


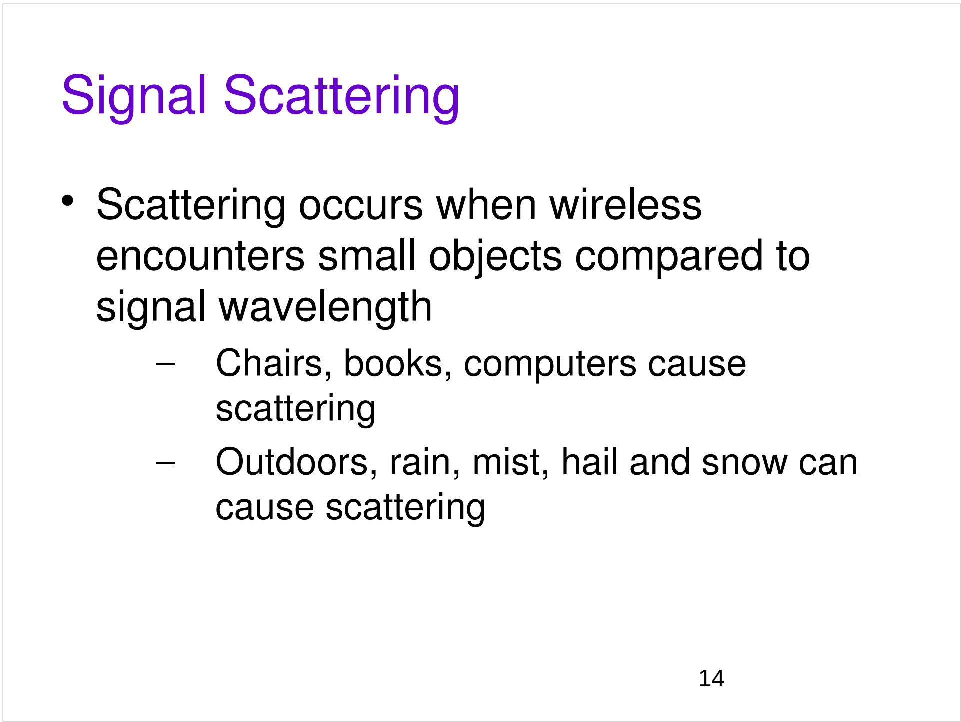
Signal Diffraction

- Signal splits into secondary waves when it encounters an obstacle.
- Waves then continue in direction they were traveling
- Objects with sharp edges, corners walls, desks create diffraction

Signal Diffraction

Receiver in shadow of hill may actually benefit from hill diffracting signal

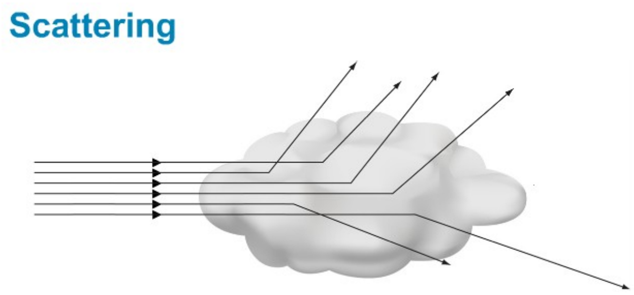




Signal Scattering

- Scattering occurs when wireless encounters small objects compared to signal wavelength
  - Chairs, books, computers cause scattering
  - Outdoors, rain, mist, hail and snow can cause scattering

Signal Scattering



Interference

- Line noise distorts wired signals and Interference affects wireless
- Electromagnetic interference affects wireless signals because there is no shielding, only air
- Especially affects signals traveling in areas where there are other wireless devices
- Probably have seen this with your own wireless devices

IEEE 802.11™

802.11 Specifics

802.11 WLAN Networks

- 802.11 network is comprised of several components and services

- Wireless Station
- Access Point
- Communication Medium (Air)
- Wireless infrastructure

We will define these ...

802.11 WLAN Networks

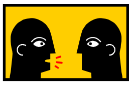
- Wireless Base Station
  The station (STA) is most basic component of wireless network
  - A station is any device that contains functionality of 802.11 protocol
    - Typically 802.11 functions implemented in hardware and software of network interface card (NIC)
    - A station could be laptop PC, handheld device, or a phone
    - Stations can be mobile, portable, or stationary
    - Stations can communicate with each other or an access point
    - All stations support 802.11 services
    - Stations also called Clients

802.11 WLAN Networks

- A Wireless Access Point (AP)
- Networking device equipped with wireless LAN network adapter acts as bridge between STA's and traditional wired network
- An access point Contains
  - At least one interface that connects wireless AP to an existing wired network (such as an Ethernet backbone)
  - Radio equipment with which it creates wireless connections with wireless clients
  - IEEE 802.1D bridging software, so can act as transparent bridge between wireless and wired LAN segments

Where is Access Point located in most homes?

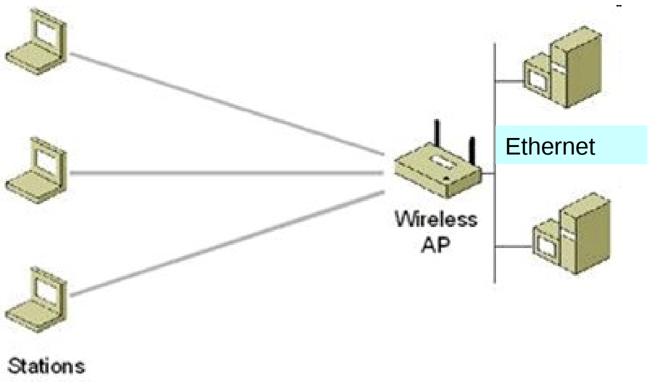
802.11 WLAN Networks



- Medium (Air)
  - Air is conduit by which information flows between computer devices and wireless infrastructure
  - Communication through wireless network is similar to talking to someone
  - As you move farther apart, it's more difficult to hear each other
  - What affects wireless signal strength or loss of strength?
  - Quality of transmission, depends on obstructions in air that either lessen or scatter strength and range of signals
    - Rain, snow, smog, and smoke are elements that impair propagation of wireless communications signals
    - A heavy downpour of rain can limit signal range by 50 percent while its raining
    - Placement affects strength, walls, large objects in the way

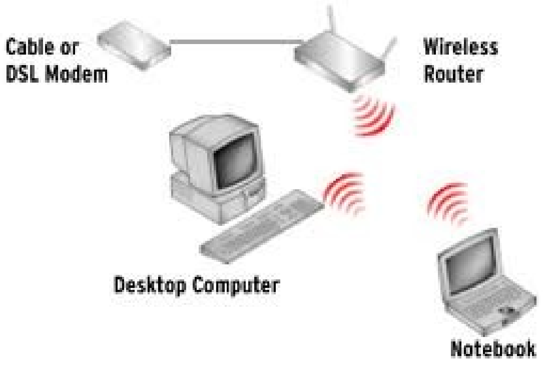
802.11 WLAN Networks

Typical picture of 802.11 LAN – Business Setting



Typical Home Setup

Many computers, one connection ...



802.11 Operating Modes

- IEEE 802.11 defines two basic operating modes for an 802.11 network
  - Ad hoc mode
  - Infrastructure mode

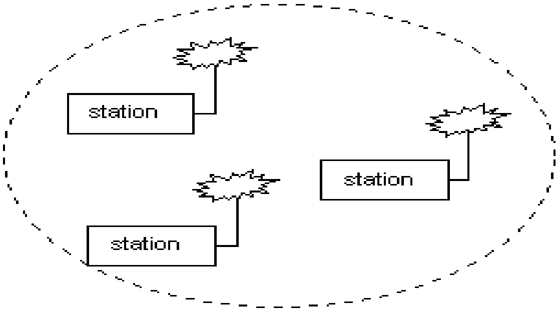
- Ad Hoc Mode
- In ad hoc mode, wireless clients communicate directly with each other without use of wireless AP or wired network

802.11 Operating Modes

- Ad hoc Mode is also called peer-to-peer mode
  - – Wireless clients in ad hoc mode form an **Independent Basic Service Set (IBSS)**
    - Two or more wireless clients who communicate directly without use of wireless AP
  - – Ad hoc mode used to connect wireless clients together
    - When there is no wireless AP
    - When wireless AP rejects an association due to failed authentication
    - When wireless client is explicitly configured to use ad hoc mode

802.11 Operating Modes

- In an IBSS, mobile stations communicate directly with each other
- Every mobile station may not be able to communicate with every other station due to range limitations
- No relay functions in an IBSS therefore all stations need to be within range of each other and communicate directly



Independent Basic Service Set (IBSS)

802.11 Operating Modes

- Ad hoc Mode
  - Smallest possible network is two stations
  - May be set up for a short time and specific purpose
    - Example: Meeting where all participants create an IBSS to share data
    - When meeting ends, IBSS is dissolved

802.11 Operating Modes

- Infrastructure mode
  - Usual way wireless networks set up
  - At least one wireless AP and one wireless client
  - Wireless client uses wireless AP to access resources of traditional wired network
  - Wired network is typically Ethernet LAN in business setting, or Ethernet + cable or DSL modem in home network

802.11 Operating Modes

- Infrastructure Mode
  - A single wireless AP supporting one or multiple wireless clients is

    Basic Service Set (BSS)

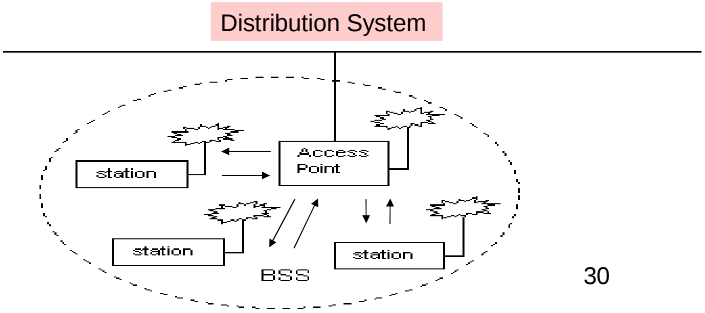
  - A set of two or more wireless APs connected to the same wired network is

    Extended Service Set (ESS)

    - An ESS is single logical network segment (also known as a subnet), and is identified by its SSID
    - More on ESS later …

Infrastructure Basic Service Set

- An Infrastructure Basic Service Set is BSS with an Access Point (AP)
- Access Point provides local relay function for BSS
- All stations in BSS communicate with access point and no longer communicate directly. All frames are relayed between stations by access point



Distribution System

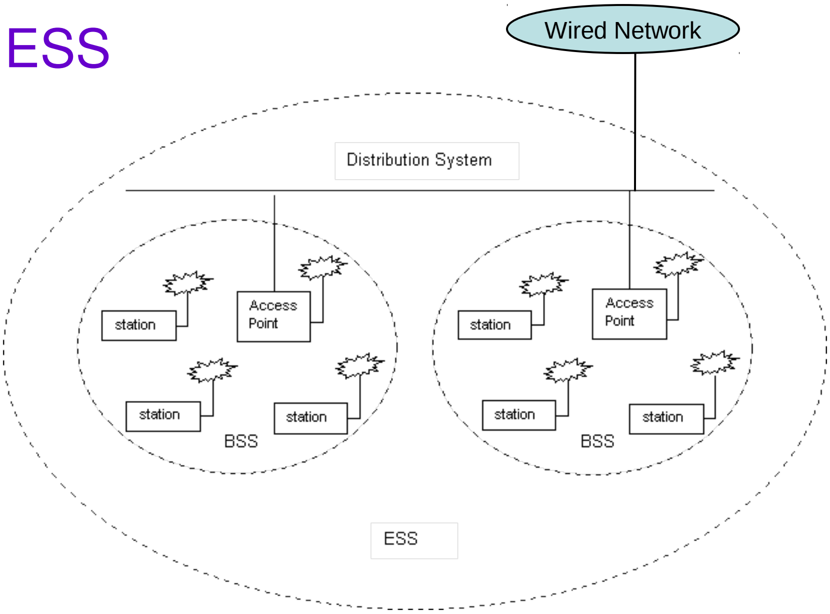
Infrastructure Basic Service Set

- BSS
  - Logical concept that groups STA’s with single AP
  - All STA’s use same channel
  - No limit is placed on number of STA’s that can associate to an AP
  - Larger geographic areas need a different configuration …

Extended Service Set (ESS)

- ESS's extend coverage of larger networks by chaining BSS's together with backbone network
  - An extended service set is set of infrastructure BSS's, where access points communicate amongst themselves to forward traffic from one BSS to another
  - All BSS's configured to be part of same ESS
    - All AP's are given Same SSID
    - Example: Wi-EWU or Wi-EWUguest

ESS


Wired Network
Distribution System
station
Access Point
station
station
BSS
station
Access Point
station
station
BSS
ESS

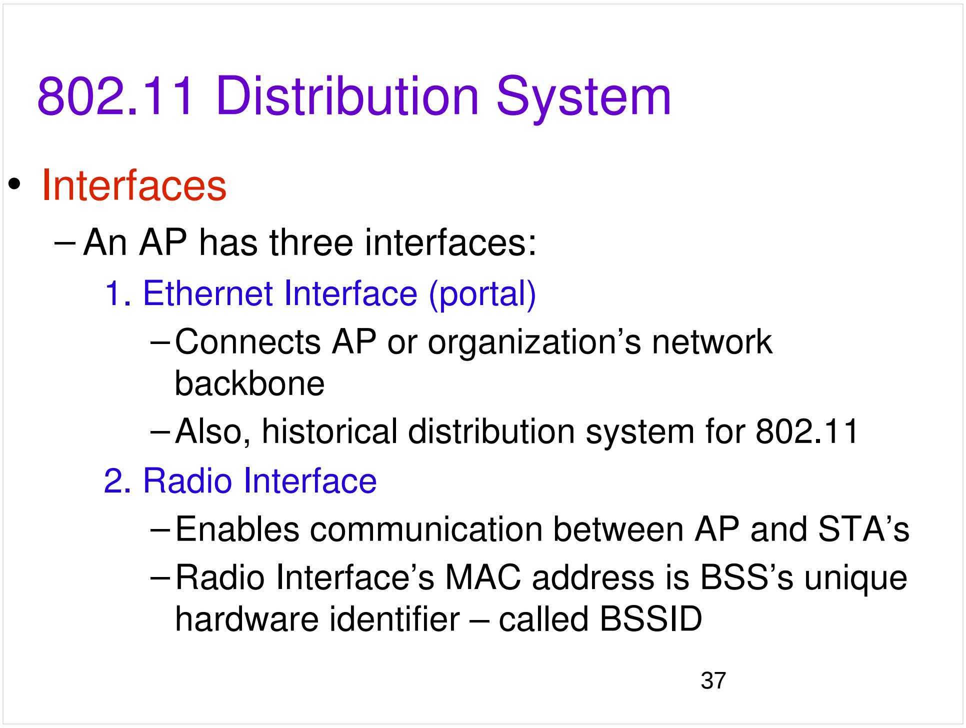
Extended Service Set (ESS)

- ESS is highest level of abstraction supported by 802.11 networks
  - AP’s in ESS operate together so that outside world uses station’s MAC address for communication
    - Doesn’t matter what it’s location in ESS
    - AP associated with Station delivers data
  - Besides delivery of data to STA’s, ESS’s
    - Do load balancing on channels
    - Automatic fail-over if AP goes down
    - Physical roaming between BSS’s in same ESS

ESS and Network Transparency

- Final Comment on ESS Abstraction
- Network equipment outside of Extended Service Set views ESS and all of its mobile stations as a single MAC-layer network where all stations are physically stationary
- Thus, ESS hides mobility of mobile stations from everything outside ESS
- This level of indirection allows existing network protocols that have no concept of mobility to operate correctly with a wireless LAN

802.11 Distribution System



802.11 Distribution System

- Interfaces
  - An AP has three interfaces:
    1. Ethernet Interface (portal)
       - Connects AP or organization’s network backbone
       - Also, historical distribution system for 802.11
    2. Radio Interface
       - Enables communication between AP and STA’s
       - Radio Interface’s MAC address is BSS’s unique hardware identifier – called BSSID

802.11 Distribution System

- Interfaces continued
  3. Serial interface
     - Typically managed via HTTP interface or SSH secure command line interface
     - If not, AP’s local serial port provides an alternative command line interface

  - Note: Smaller (cheaper) AP’s also function as broadband routers and typically don’t have a serial interface

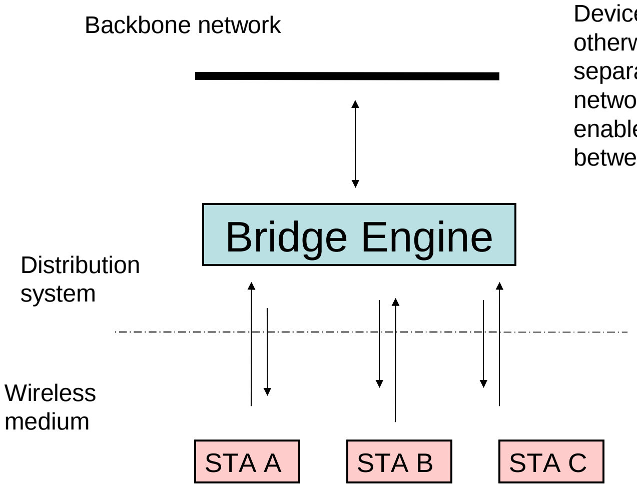
802.11 Distribution System

- Logical component of 802.11 used to forward frames to their destination STA’s
- Most commercial products, on market distribution system medium is:
  - – Typically Ethernet, wired network
  - – Also, can be wireless distribution system (WDS)
    - Wireless bridge can be used to quickly connect two physical locations

802.11 WLAN Networks

- Distribution System
- In IEEE 802.11, distribution system is not necessarily a network
  - Nor does standard place any restrictions on how distribution system is implemented
  - Only on services it must provide
  - Services discussed next …

Distribution System



What is a bridge?

Device joins two otherwise separate computer networks together to enable communication between them.

Distribution Services

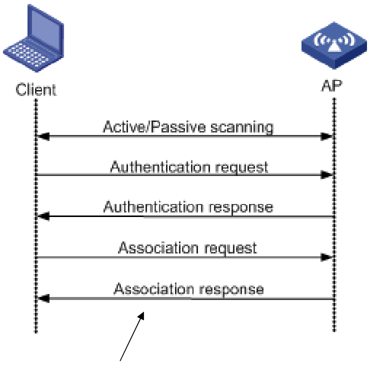
- Distribution services provide functionality across a distribution system
  - Typically, access points provide distribution **services**
- Distribution services and functions detailed below include:
  - Distribution System Services
    - Association, disassociation, re-association, distribution, and integration
  - Station Services
    - Authentication, Deauthentication, Privacy and Packet delivery

Examine these in more detail

Association

- The association service used to make logical connection between mobile station and an access point
  - Each station must be **associated** with an access point before it can send data through access point into distribution system
  - Connection is necessary in order for distribution system to know where and how to deliver data to mobile station
- Mobile station invokes association service once and only once, typically when station enters BSS
- Each station can associate with one access point though Access Point can associate with multiple stations

Association Service



Client sends an Association Request
AP sends back an Association Response

Disassociation

- The disassociation service is used
  - To force mobile station to terminate association with an access point or
  - Mobile station to inform an access point that it no longer requires services of distribution system

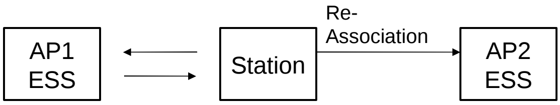
- When station becomes disassociated, it must begin a new association to communicate with an access point again

  An AP may force station or stations to disassociate because of resource restraints, AP is shutting down or being removed from network for a variety of reasons

- When a mobile station knows that it will no longer require services of an access point, it may invoke disassociation service to notify AP that connection services of AP no longer required

Re-association

- Re-Association enables station to change its current association with an access point
  - Re-association service similar to association service, except it includes information about AP with which mobile station has been previously associated
  - A mobile station will use **re-association** service repeatedly as it moves throughout ESS,
    - Loses contact with AP with which it is associated, and
    - Needs to become associated with a new AP



Re-association

- By using re-association service, a mobile station provides information to AP to which it will be associated and information pertaining to AP which it will be disassociated
- Allows newly associated AP to contact previously associated AP to obtain frames that may be waiting there for delivery to mobile station as well as other information that may be relevant to the new association

  The mobile station always initiates re-association.

Distribution

- Distribution is primary service used by an 802.11 station
- A station uses distribution service every time it sends MAC frames across distribution system
- Distribution service provides distribution with enough information to determine proper destination BSS for MAC frame

  Association services (association, re-association, and disassociation) provide necessary information for distribution service to operate

Comment

- Distribution within distribution system does not necessarily involve any additional features outside of the association services, though a station must be associated with an access point for the distribution service to forward frames properly

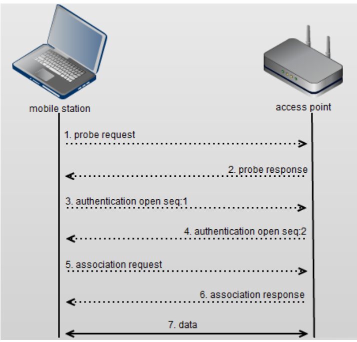
Integration

- Integration service connects 802.11 WLAN to other LANs, including one or more wired LANs or 802.11 WLANs
  - A portal performs the integration service.
  - The portal is an abstract architectural concept that typically resides in an AP though it could be part of a separate network component entirely.

    The integration service translates 802.11 frames to frames that may traverse another network, and vice versa

Authentication

- The Authentication service provides ability to control access to the LAN
  - If two stations want to communicate with each other, they first identify each other
  - This is done in ESSs as well as in IBSSs
  - This service provides only link-level authentication mechanism
  - Authentication at the low level is typically allowed, set to “open”
  - In the association step, encryption and other privacy settings occur



Deauthentication and Privacy

- The deauthentication service is invoked whenever an existing authentication is to be terminated

- Privacy is obtained by executing "Wired Eqivalent Privacy" (WEP) – old or WPA2 algorithms, all data frames (and some authentication management frames) are encrypted
- This occurs during association

MAC Service Data Unit (MSDU)

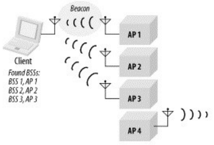
- Stations provide the MSDU (or packets) delivery service.
  - Responsible for getting data to actual endpoints
  - More on this later …

Basic Network Operation Example

802.11 Network Operation

- Wireless adapter is turned on, it scans wireless frequencies for wireless APs and other wireless clients
- Scanning is like **listening**, wireless adapter listens on all channels for beacon frames sent by wireless AP's and other wireless clients
  - Two types of scanning:
    - Active and Passive

802.11 Network Operation

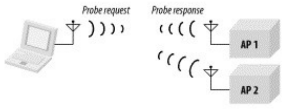


WLAN Passive Scanning

- Passive scanning
  - Adapter will tune to every RF channel, note information discovered about each AP
  - APs send beacon frames every 100ms
  - While adapter is scanning a channel, receives beacon frames from AP
  - Adapter notes signal strength of beacon frame and proceeds to scan other channels, also encryption type and data rate supported
  - Once scanning of RF channels is complete, adapter decides on AP to associate to

AP with strongest beacon signal, compatible data rate and supported encryption

802.11 Network Operation



WLAN active scanning

- Active scanning
  - Adapter will send probe request frames on all RF channels
  - An AP receiving probe requests sends probe responses
  - Adapter decides what AP to associate with based on information in probe response frame
    - Information is same as in passive scanning, signal strength, data rate and encryption

802.11 Network Operation

- After scanning,
  - Wireless adapter chooses a wireless AP with which to associate
  - Selection is made by using Service Set Identifier (SSID) of wireless network and wireless AP with best signal strength (highest SNR) given data rate and encryption is compatible
- Next,
  - First the authentication process is done, to identify the laptop to the AP, this has to happen before association
  - Wireless client switches to channel of chosen wireless AP and negotiates use of a logical wireless point-to-point connection
- Known as association

802.11 Network Operation

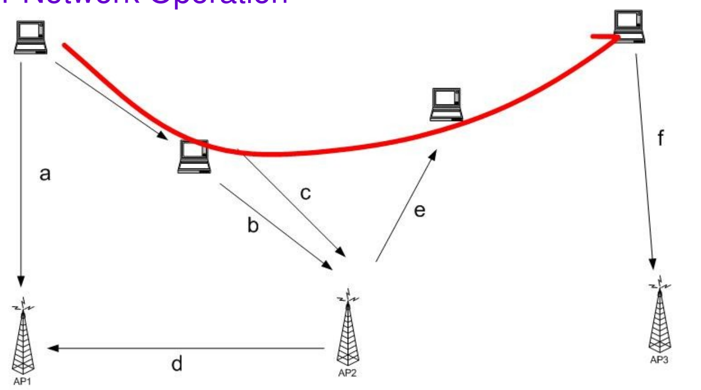
- – If signal strength of wireless AP is too low,
- – error rate too high, or
- – instructed by the operating system
  (in the case of Windows, every 60 seconds),

- Wireless client scans for other wireless APs for a stronger signal to the same wireless network
- If found,
  - – Wireless client switches to the channel of that wireless AP
- Known as reassociation

802.11 Network Operation

- Reassociation with a different wireless AP occurs for many reasons
  - Signal can weaken because wireless client moves away from wireless AP or wireless AP becomes congested with too much other traffic or interference
  - Wireless client, by switching to another wireless AP, can distribute the load over other wireless APs, increasing the performance for other wireless clients
- As a wireless client moves its physical location
  - Can associate and reassociate from one wireless AP to another, maintaining a continuous connection during physical relocation

802.11 Network Operation



(a) ---- The station finds AP1, it will authenticate and associate.

(b) ---- As the station moves, it may pre-authenticate with AP2.

(c) ---- When the association with AP1 is no longer desirable, it may reassociate with AP2.

(d) ---- AP2 notify AP1 of the new location of the station, terminates the previous association with AP1.

(e) ---- At some point, AP2 may be taken out of service. AP2 would disassociate the associated stations.

(f) ---- The station find another access point and authenticate and associate.

Windows Example

- For example, a wireless client is assigned an IP address when it connects to first wireless AP
  - When wireless client roams within an ESS, it creates wireless connection with another wireless AP, Does IP Address change?
  - No. It keeps same IP address since wireless APs are on the same logical subnet
  - ESS abstraction allows this to happen
  - When it roams to different ESS, IP address needs to change

Windows Example continued

- Wireless client behavior affects whether it needs another IP or not
  - For Windows wireless clients, a reassociation is interpreted as a media disconnect/connect event
  - This causes Windows to perform a DHCP renewal for the TCP/IP protocol
    - For reassociations within ESS, DHCP renewal refreshes current IP address
    - For client reassociations with AP across an ESS boundary, the DHCP renewal process obtains a new IP address that is relevant for logical IP subnet of the new ESS

Summary

- Presented a high level view of wireless in general
- 802.11 operation specifically
  - Network operation and client association
  - 802.11 networks provide basic services including association, disassociation, re-association, distribution, integration plus privacy, authentication and MSDU delivery
- Overview of how services work
- Next more details – frames

Finish

- Chapter 4.4, Tanenbaum – Wireless Lans