Wireless Networks

Key Reference:

Peterson and Davie, "Computer Networks: A Systems Approach", 4th, 5th Edition, Morgan Kaufmann
(except slide 27 and 31)

Wireless Links

- Wireless links transmit electromagnetic signals
  - Radio, microwave, infrared
- Wireless links all share the same "wire" (medium)
  - The challenge is to share it efficiently without unduly interfering with each other
  - Most of this sharing is accomplished by dividing the "wire" along the dimensions of frequency and space
- Exclusive use of a particular frequency in a particular geographic area may be allocated to an individual entity such as a corporation
  - These allocations are determined by government agencies such as FCC (Federal Communications Commission) in USA

Band Allocation and Uses

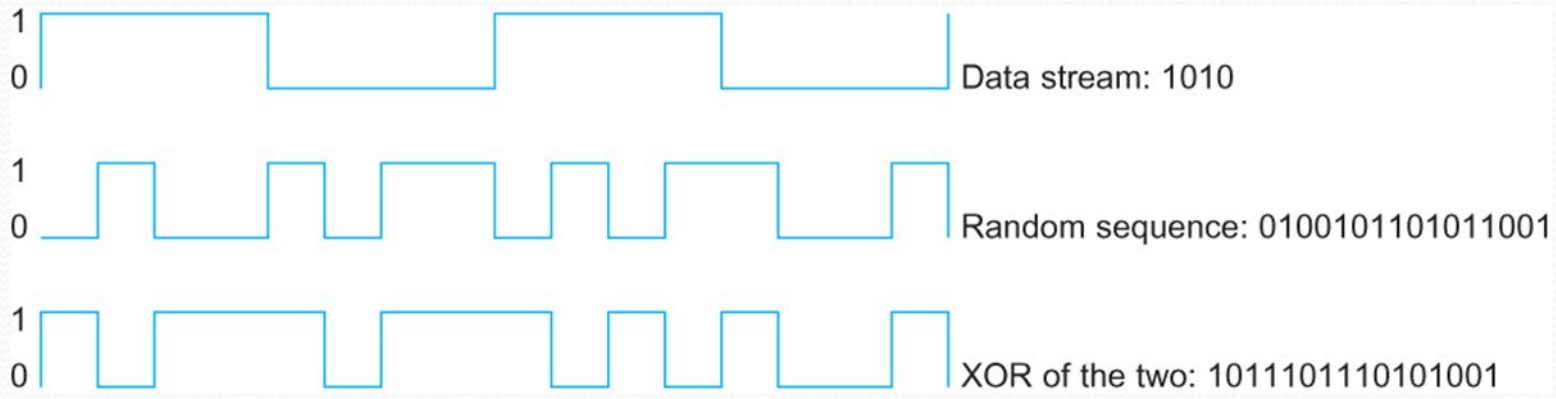
- Specific bands (frequency) ranges are allocated to certain uses
- Some bands are reserved for government use
- Other bands are reserved for uses such as AM radio, FM radio, televisions, satellite communications, and cell phones
- Specific frequencies within these bands are then allocated to individual organizations for use within certain geographical areas.
- Finally, there are several frequency bands set aside for "license exempt" usage (Bands in which a license is not needed)
- Devices that use license-exempt frequencies are still subject to certain restrictions
  - The first is a limit on transmission power
    - This limits the range of signal, making it less likely to interfere with another signal
    - For example, a cordless phone might have a range of about 100 feet.
  - The second is the use of spread spectrum technique

Spread Spectrum Techniques

- The idea is to spread the signal over a wider frequency band
  - So as to minimize the impact of interference from other devices
  - Originally designed for military use
  - Frequency hopping
  - Direct sequence
- ***Frequency hopping***
  - Transmitting signal over a random sequence of frequencies
    - First transmitting at one frequency, then a second, then a third…
    - The sequence of frequencies is not truly random, instead computed algorithmically by a pseudorandom number generator
    - The receiver uses the same algorithm as the sender, initializes it with the same seed, and is able to hop frequencies in sync with the transmitter to correctly receive the frame

Direct Sequence Technique

- Represents each bit in the frame by multiple bits in the transmitted signal.
- For each bit the sender wants to transmit
  - It actually sends the exclusive OR of that bit and *n* random bits
- The sequence of random bits is generated by a pseudorandom number generator known to both the sender and the receiver.
- The transmitted values, known as an ***n*-bit chipping code**, spread the signal across a frequency band that is *n* times wider
- Example: 4 bit chipping sequence

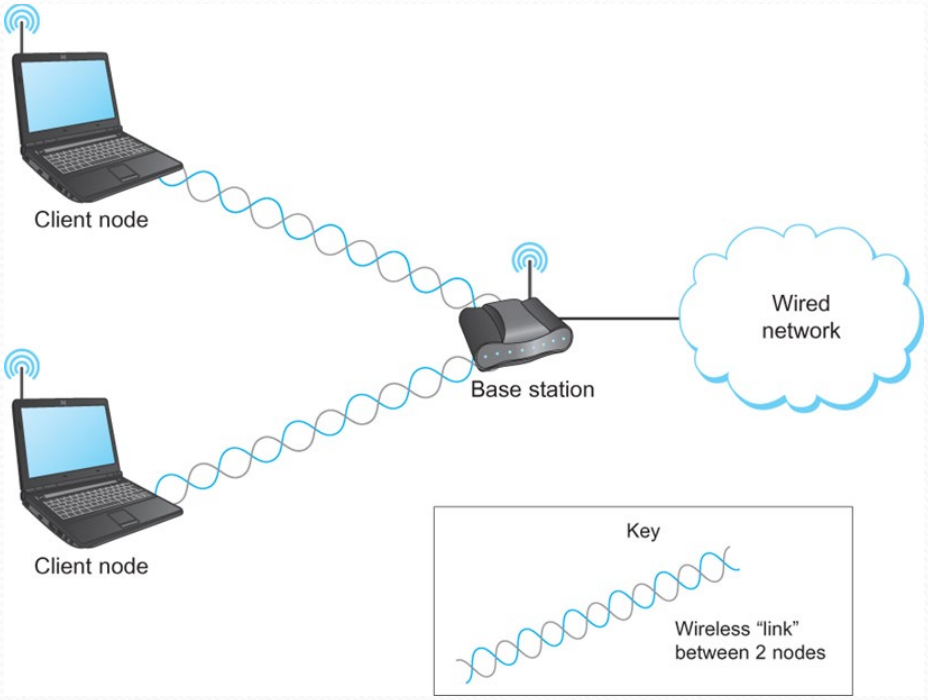


Wireless Technologies

- Wireless technologies differ in a variety of dimensions
  - How much bandwidth they provide
  - How far apart the communication nodes can be
- Some prominent wireless technologies
  - Bluetooth (802.15.1)
    - 2 Mbps, 10 m
  - Wi-Fi (802.11)
    - Few hundreds of Mbps, a few Gbps, 100m
  - 3G cellular wireless
    - few Mbps, tens of kilometers
  - 4G cellular wireless
    - Hundreds of Mbps, tens of kilometers

Wireless Links

- Mostly widely used wireless links today are usually asymmetric
  - Two end-points are usually different kinds of nodes
    - One end-point usually has no mobility, but has wired connection to the Internet (known as base station)
    - The node at the other end of the link is often mobile

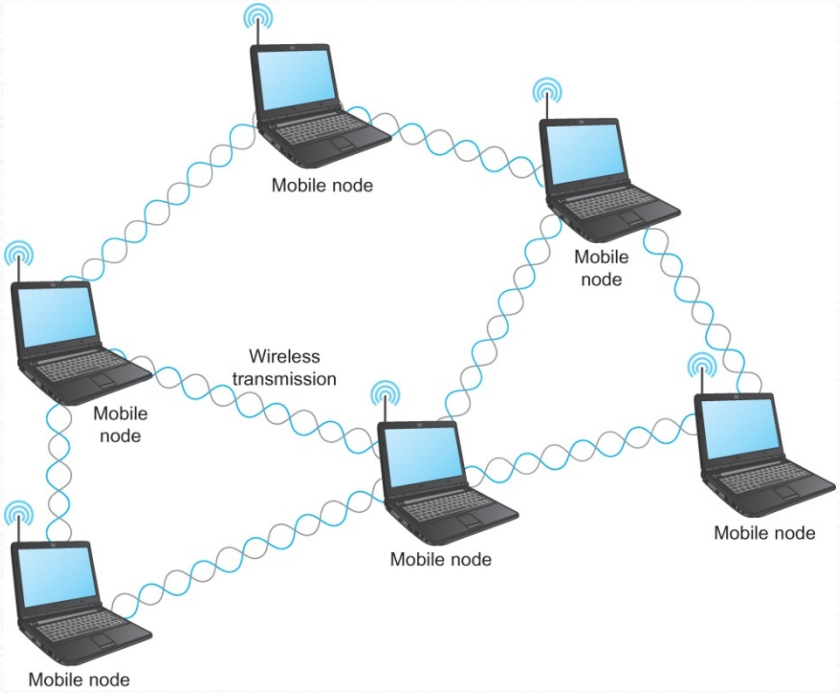


Mobility of nodes

- Wireless communication supports point-to-multipoint communication
- Communication between non-base (client) nodes is routed via the base station
- Different levels of mobility for clients
  - No mobility: the receiver must be in a fix location to receive a directional transmission from the base station
    - initial version of WiMAX (Worldwide Interoperability for Microwave Access)
  - Mobility is within the range of a base (Bluetooth)
  - Mobility between bases (Cell phones and Wi-Fi)

Wireless Mesh Network

- Mesh or Ad-hoc network
  - Nodes are peers
  - Messages may be forwarded via a chain of peer nodes



A wireless ad-hoc or mesh network

IEEE 802.11

- Also known as Wi-Fi
- Like Ethernet and token LAN, 802.11 is designed for use in a limited geographical area (homes, office buildings, campuses)
  - Primary challenge is to mediate access to a shared communication medium – in this case, signals propagating through space
- 802.11 supports additional features
  - power management and
  - security mechanisms

IEEE 802.11

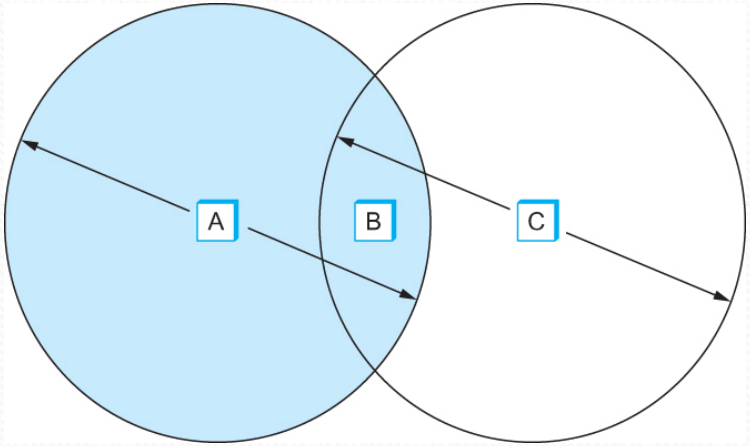
- Original 802.11 standard defined two radio-based physical layer standard
  - One using the frequency hopping
    - Over 79 1-MHz-wide frequency bandwidths
  - Second using direct sequence
    - Using 11-bit chipping sequence
  - Both standards run in the 2.4-GHz and provide up to 2 Mbps
- Then physical layer standard 802.11b was added
  - Using a variant of direct sequence 802.11b provides up to 11 Mbps
  - Uses license-exempt 2.4-GHz band
- Then came 802.11a, up to 54 Mbps using OFDM (orthogonal FDM)
  - 802.11a runs on license-exempt 5-GHz band
- Then came 802.11g which is backward compatible with 802.11b (Uses 2.4 GHz band, OFDM and delivers up to 54 Mbps)
- 802.11 n, improves on 802.11g, 2.4 GHz band, up to a few hundred Mbps, multiple antenna MIMO (multiple input multiple output) technique
- 802.11 ac, improves on 802.11n, 5 GHz band, up to a few Gbps, MIMO

802.11 Multiple Access

- CSMA/CA
- CS (Carrier Sense)
  - Sense before starts transmission, don't collide with ongoing transmissions
- No Collision Detection
  - Received signals are weak (due to fading); difficult to sense collision
  - Not possible to detect all collisions
    - Eg.: Hidden node problem (discussed later)
- Collision Avoidance (CA)
  - How to avoid collisions?

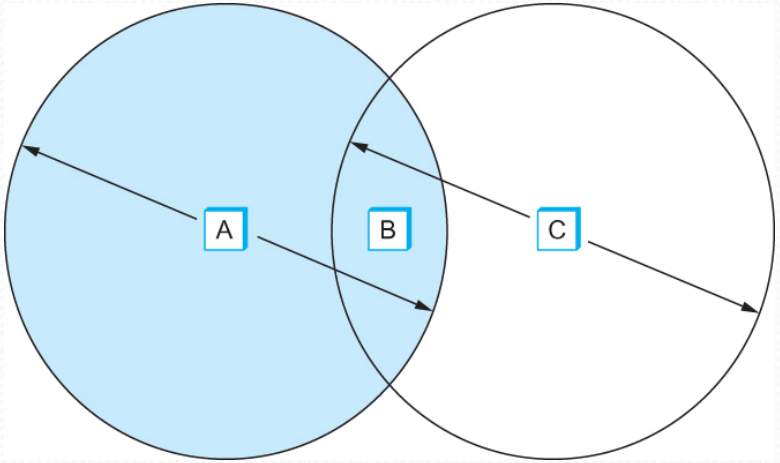
Hidden Node Problem

- Consider the situation in the following figure where each node is able to send and receive signals that reach just the nodes to its immediate left and right as shown in Figure
  - B can exchange frames with A and C
  - C can reach B but not A
  - A can reach B but not C

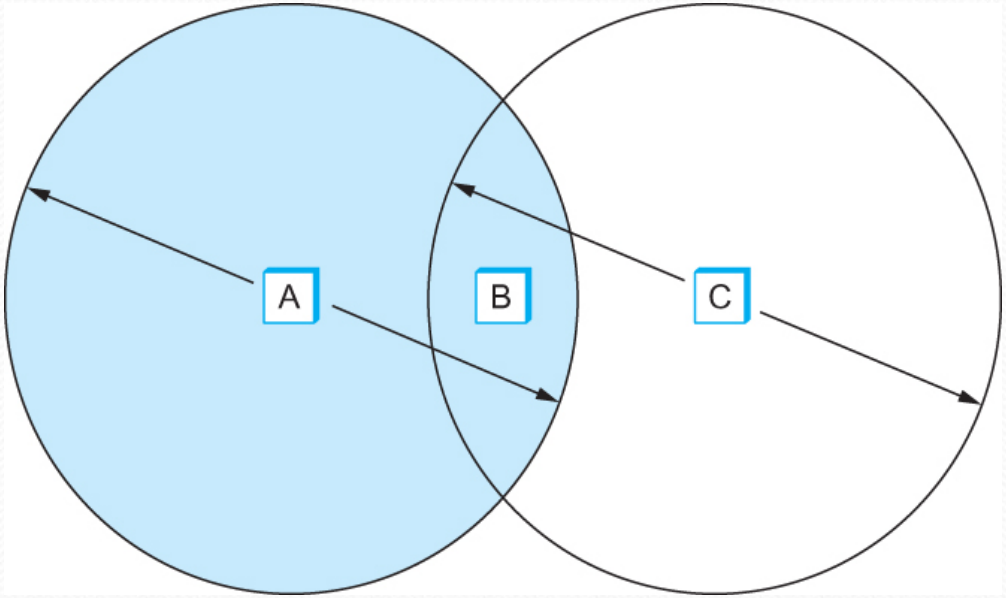


Hidden Node Problem

- Suppose both A and C want to communicate with B and so they each send it a frame.
  - A and C are unaware of each other since their signals do not carry that far
  - These two frames collide with each other at B
    - But unlike an Ethernet, neither A nor C is aware of this collision
  - A and C are said to *hidden nodes* with respect to each other



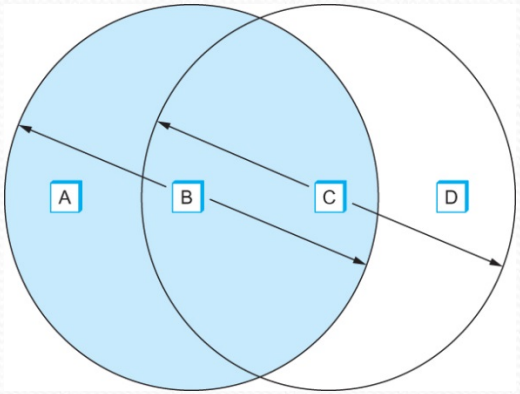
Hidden Node Problem



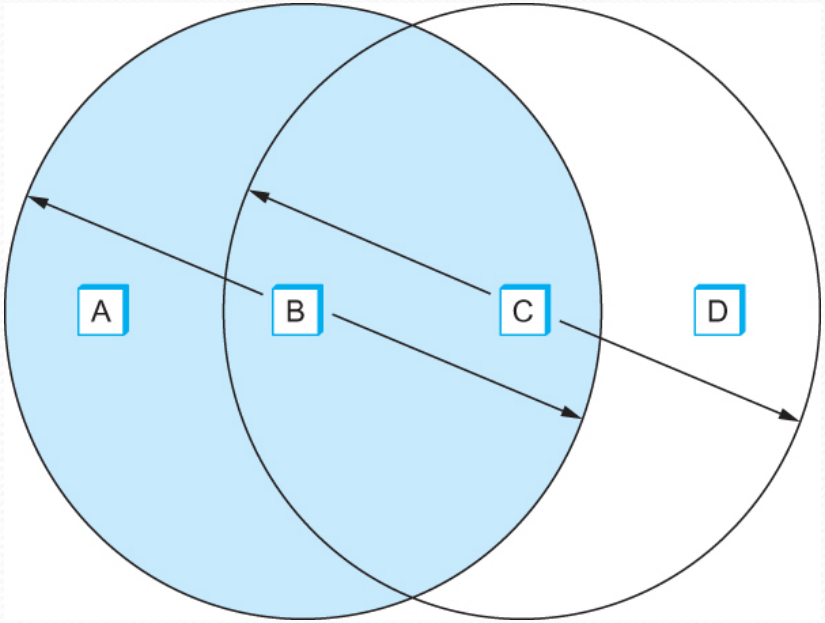
The “Hidden Node” Problem. Although A and C are hidden from each other, their signals can collide at B. (B’s reach is not shown.)

Exposed Node Problem

- Consider the situation in the figure where each of four nodes is able to send and receive signals that reach just the nodes to its immediate left and right
  - For example, B can exchange frames with A and C, but it cannot reach D; C can reach B and D but not A
- *Exposed node* problem occurs
  - Suppose B is sending to A. Node C is aware of this communication because it hears B's transmission.
  - It would be a mistake for C to conclude that it cannot transmit to anyone just because it can hear B's transmission.
  - Suppose C wants to transmit to node D.
  - This is not a problem since C's transmission to D will not interfere with A's ability to receive from B.



Exposed Node Problem



Exposed Node Problem. Although B and C are exposed to each other's signals, there is no interference if B transmits to A while C transmits to D. (A and D's reaches are not shown.)

IEEE 802.11 – Collision Avoidance

- 802.11 addresses these two problems (hidden node, exposed node) with an algorithm called Multiple Access with Collision Avoidance (MACA).
- Key Idea
  - Sender and receiver exchange control frames with each other before the sender actually transmits any data.
  - This exchange informs all nearby nodes that a transmission is about to begin
  - Sender transmits a *Request to Send* (RTS) frame to the receiver.
    - The RTS frame includes a field that indicates how long the sender wants to hold the medium
      - Length of the data frame to be transmitted
  - Receiver replies with a *Clear to Send* (CTS) frame
    - This frame echoes this length field back to the sender

IEEE 802.11 – Collision Avoidance

- Any node that sees the CTS frame knows that
  - it is close to the receiver, therefore
  - cannot transmit for the period of time it takes to send a frame of the specified length
  - See the hidden node problem example
- Any node that sees the RTS frame but not the CTS frame
  - is not close enough to the receiver to interfere with it, and
  - so is free to transmit (not to receive?)
  - See the exposed node problem example

IEEE 802.11 – Collision Avoidance

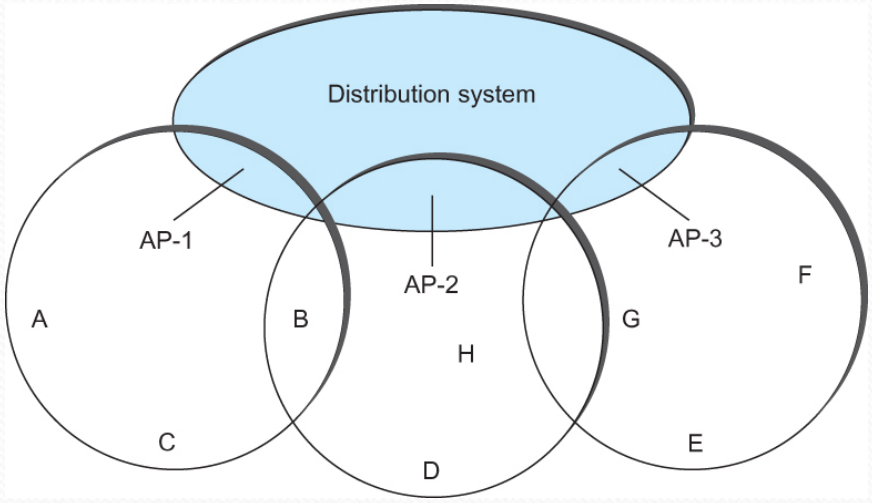
- Using ACK in MACA
  - Proposed in MACAW: MACA for Wireless LANs
- Receiver sends an ACK to the sender after successfully receiving a frame
- All nodes must wait for this ACK before trying to transmit
- If two or more nodes detect an idle link and try to transmit an RTS frame at the same time
  - Their RTS frame will collide with each other
- 802.11 does not support collision detection
  - So the senders realize the collision has happened when they do not receive the CTS frame after a period of time
  - In this case, they each wait a random amount of time before trying again.
  - The amount of time a given node delays is defined by the same *exponential backoff* algorithm used on the Ethernet.

IEEE 802.11 – Distribution System

- 802.11 is suitable for an ad-hoc configuration of nodes that may or may not be able to communicate with all other nodes.
  - Nodes are free to move around
  - The set of directly reachable nodes may change over time
  - Adhoc vs. infrastructure wireless network; adhoc not studied here
- To deal with this mobility and partial connectivity,
  - 802.11 defines additional structures on a set of nodes
  - Instead of all nodes being created equal,
    - some nodes are allowed to roam
    - some are connected to a wired network infrastructure
      - they are called *Access Points* (AP) and they are connected to each other by a so-called *distribution system*
    - Infrastructure wireless LAN: communication thru APs; APs are interconnected by Ethernet switches or IP routers

IEEE 802.11 – Distribution System

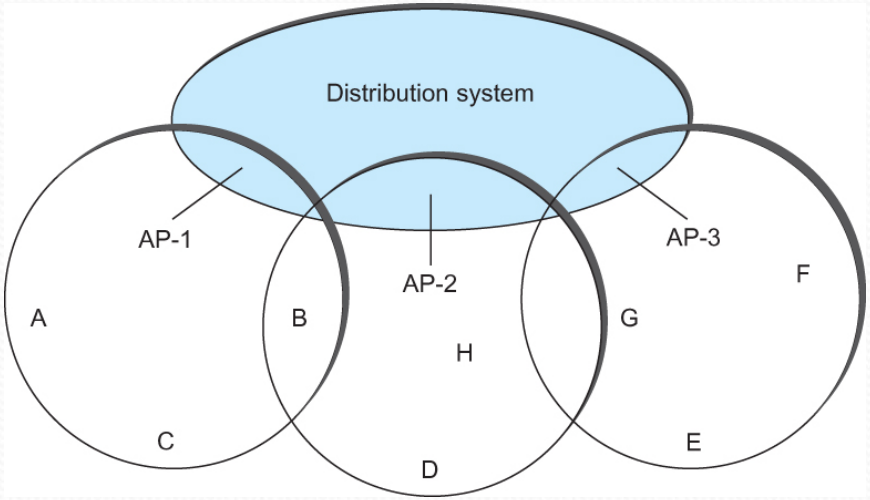
- Following figure illustrates a distribution system that connects three access points, each of which services the nodes in the same region
- Each of these regions is analogous to a cell in a cellular phone system with the APs playing the same role as a base station
- The distribution network runs at layer 2 of the ISO architecture



Access points connected to a distribution network

IEEE 802.11 – Distribution System

- Although two nodes can communicate directly with each other if they are within reach of each other, the idea behind this configuration is
  - Each node associates itself with one access point
  - For node A to communicate with node E, A first sends a frame to its AP-1 which forwards the frame across the distribution system to AP-3, which finally transmits the frame to E



Access points connected to a distribution network

IEEE 802.11 – Distribution System (Scanning)

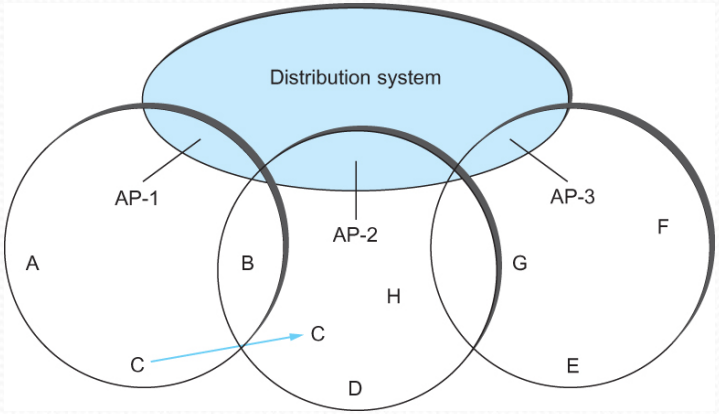
- How do the nodes select their access points
- How does it work when nodes move from one cell to another

- The technique for selecting an AP is called *scanning*
  - The node sends a *Probe* frame
  - All APs within reach reply with a *Probe Response* frame
  - The node selects one of the access points and sends that AP an *Association Request* frame
  - The AP replies with an *Association Response* frame

- A node engages this protocol whenever
  - it joins the network, as well as
  - when it becomes unhappy with its current AP
    - This might happen, for example, because the signal from its current AP has weakened due to the node moving away from it
    - Whenever a node acquires a new AP, the new AP notifies the old AP of the change via the distribution system

IEEE 802.11 – Distribution System (Scanning)

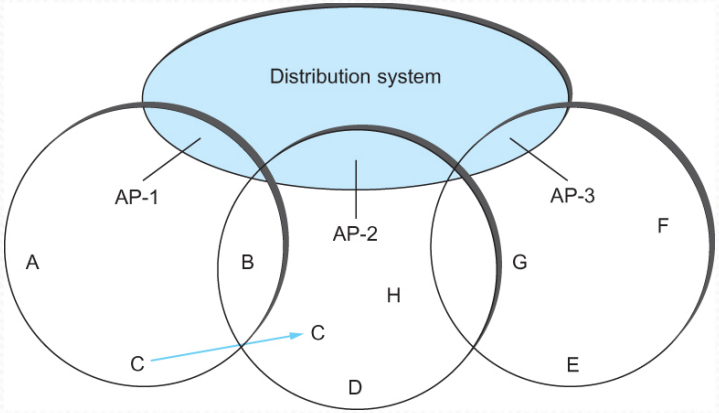
- Consider the situation shown in the following figure when node C moves from the cell serviced by AP-1 to the cell serviced by AP-2.
- As it moves, it sends *Probe* frames, which eventually result in *Probe Responses* from AP-2.
- At some point, C prefers AP-2 over AP-1 , and so it associates itself with that access point.
  - This is called *active scanning* since the node is actively searching for an access point



Node Mobility

IEEE 802.11 – Distribution System (Scanning)

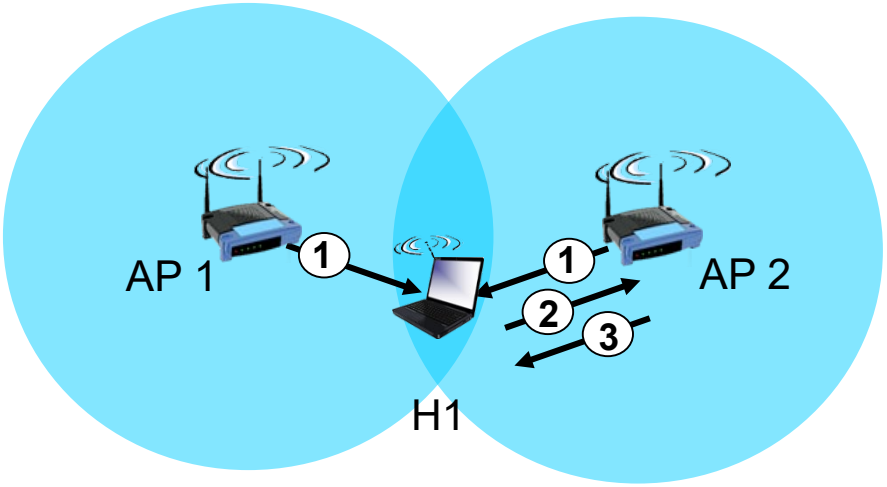
- APs also periodically send a *Beacon* frame that advertises the capabilities of the access point; these include the transmission rate supported by the AP
  - This is called *passive scanning*
  - A node can change to this AP based on the *Beacon* frame simply by sending it an *Association Request* frame back to the access point.

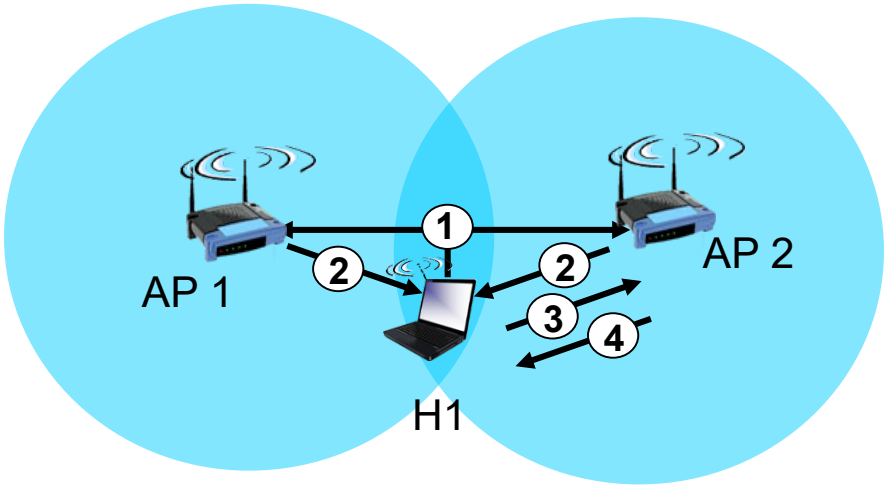


Node Mobility

802.11: passive/active scanning (Illustration)

Source: J.F. Kurose and K. W. Ross, "Computer Networking: A Top-Down Approach"





passive scanning:

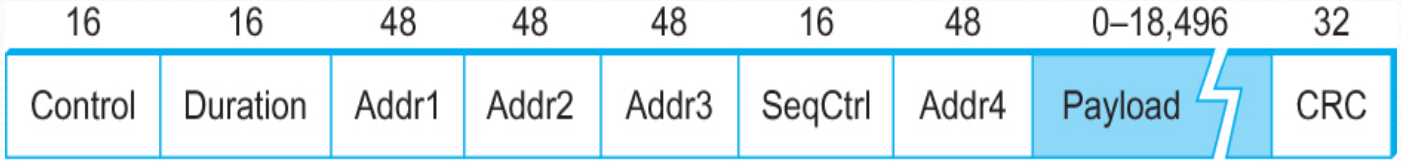
(1) beacon frames sent from APs
(2) association Request frame sent: H1 to selected AP
(3) association Response frame sent from selected AP to H1

active scanning:

(1) Probe Request frame broadcast from H1
(2) Probe Response frames sent from APs
(3) Association Request frame sent: H1 to selected AP
(4) Association Response frame sent from selected AP to H1

IEEE 802.11 – Frame Format

- Source and Destinations addresses: each 48 bits
- Data: up to 2312 bytes
- CRC: 32 bit
- Control field: 16 bits
  - Contains three subfields (of interest)
    - 6 bit **Type** field: indicates whether the frame is data, an RTS or CTS frame or being used by the scanning algorithm
    - A pair of 1 bit fields : called **ToDS** and **FromDS**
- Duration: reserve the channel for the specified duration



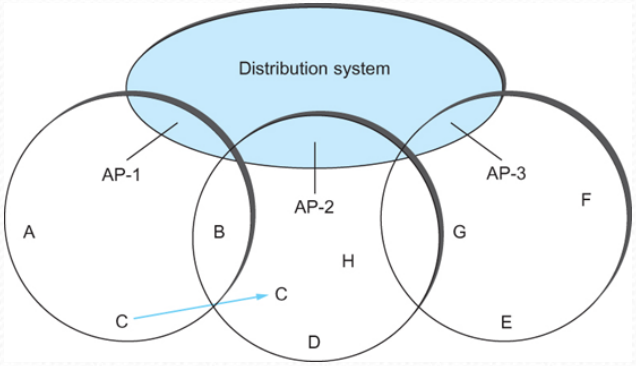
Frame Format

IEEE 802.11 – Frame Format

- Frame contains four addresses
- How these addresses are interpreted depends on the settings of the **ToDS** and **FromDS** bits in the frame's Control field
- This is to account for the possibility that the frame had to be forwarded across the distribution system which would mean that,
  - the original sender is not necessarily the same as the most recent transmitting node
- Same is true for the destination address
- Simplest case
  - When one node is sending directly to another, both the DS bits are 0, Addr1 identifies the target node, and Addr2 identifies the source node

IEEE 802.11 – Frame Format

- Most complex case
  - Both DS bits are set to 1
    - Indicates that the message went from a wireless node onto the distribution system, and then from the distribution system to another wireless node
  - With both bits set,
    - Addr1 identifies the ultimate destination,
    - Addr2 identifies the immediate sender (the one that forwarded the frame from the distribution system to the ultimate destination)
    - Addr3 identifies the intermediate destination (the one that accepted the frame from a wireless node and forwarded across the distribution system)
    - Addr4 identifies the original source
- Example: A sends to E (See Figure in slide 23)
- Addr1: E, Addr2: AP-3, Addr3: AP-1, Addr4: A



802.11 frame: addressing (example)

H1 sends and IP packet thru Internet: H1 needs to send to R1 interface

Source: J.F. Kurose and K. W. Ross, "Computer Networking: A Top-Down Approach"