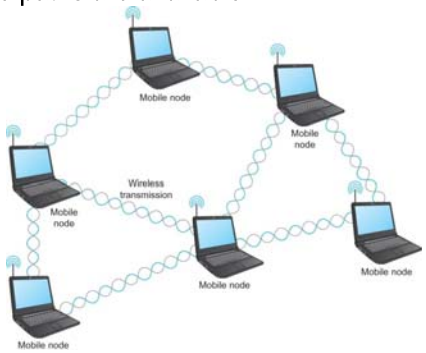
Wireless Links

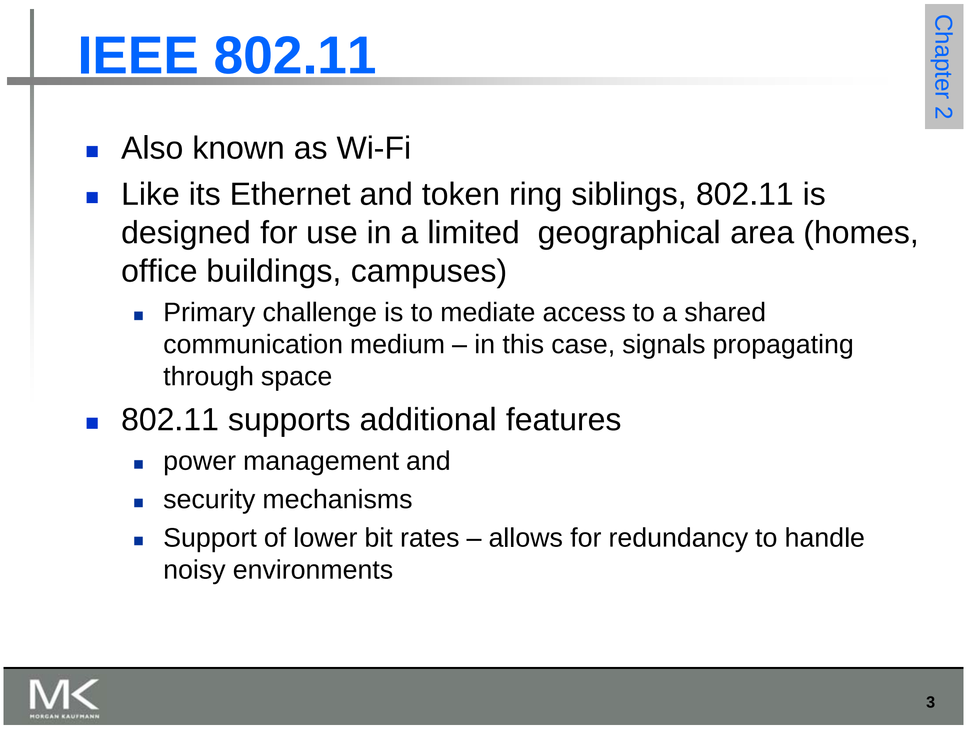
- Wireless communication supports point-to-multipoint communication
- Communication between non-base (client) nodes is routed via the base station
- Three levels of mobility for clients
  - No mobility: the receiver must be in a fix location to receive a directional transmission from the base station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

Wireless Links

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



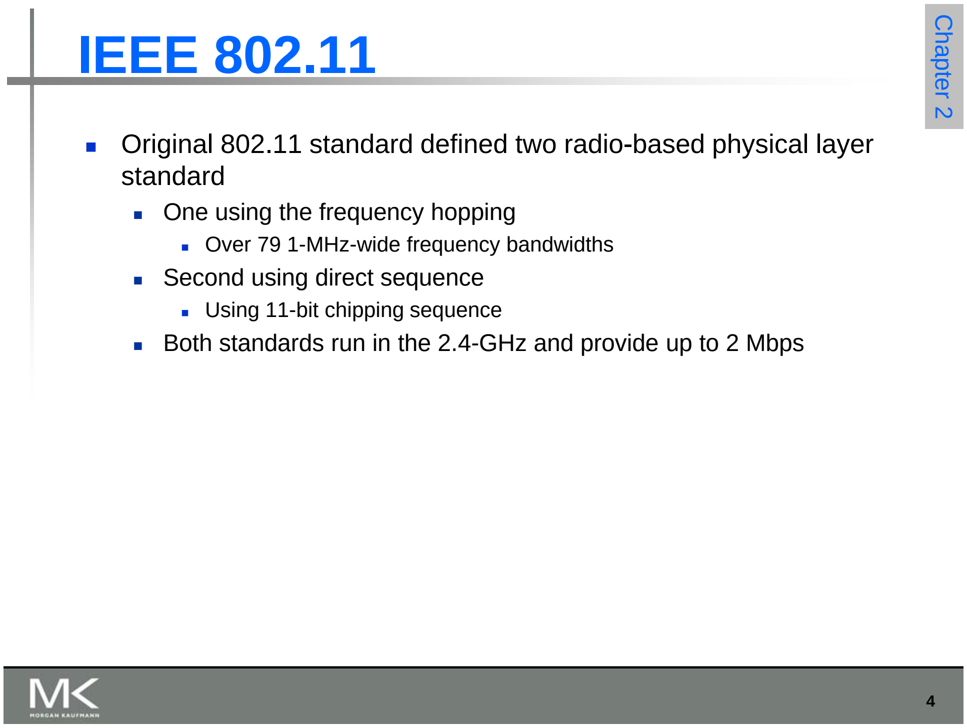
A wireless ad-hoc or mesh network



IEEE 802.11

Chapter 2

- Also known as Wi-Fi
- Like its Ethernet and token ring siblings, 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
  - Support of lower bit rates – allows for redundancy to handle noisy environments



IEEE 802.11

Chapter 2

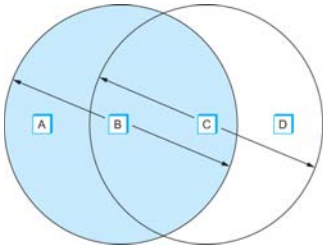
- Original 802.11 standard defined two radio-based physical layer standard
  - One using the frequency hopping
    - Over 79 1-MHz-wide frequency bandwidths
  - Second using direct sequence
    - Using 11-bit chipping sequence
  - Both standards run in the 2.4-GHz and provide up to 2 Mbps

IEEE 802.11

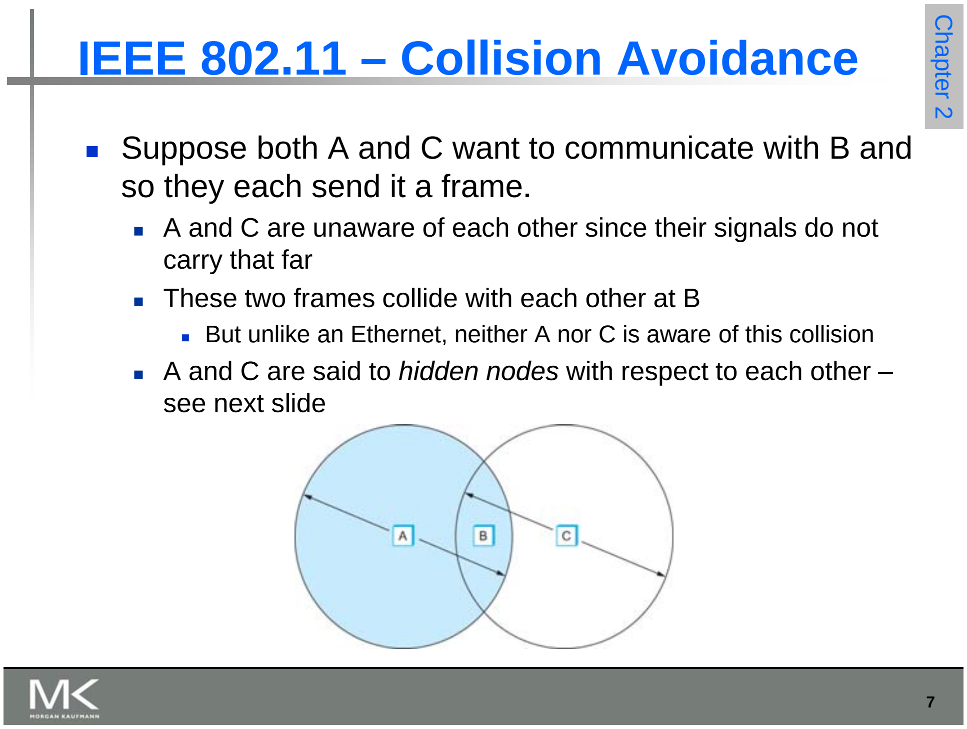
- Then physical layer standard 802.11b was added
  - Using a variant of direct sequence 802.11b provides up to 11 Mbps
  - Uses license-exempt 2.4-GHz band
- Then came 802.11a which delivers up to 54 Mbps using OFDM (Orthogonal FDM)
  - 802.11a runs on license-exempt 5-GHz band – less interference
  - Almost limited to line of sight due to signal absorption
- Then came 802.11g which is backward compatible with 802.11b
  - Uses 2.4 GHz band, OFDM and delivers up to 54 Mbps
- Most recent standard is 802.11n which delivers up to 600 Mbps
  - Uses multiple antennas – MIMO (multiple input multiple output)

IEEE 802.11 – Collision Avoidance

- Consider the situation in the following 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



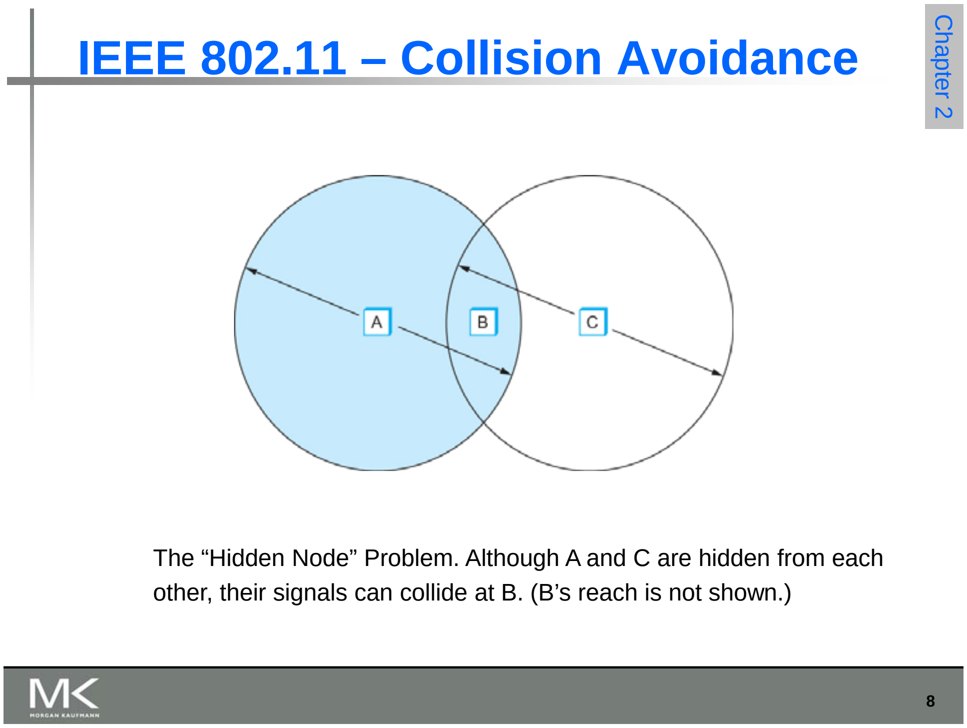
Example of a wireless network



IEEE 802.11 – Collision Avoidance

Chapter 2

- 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 – see next slide



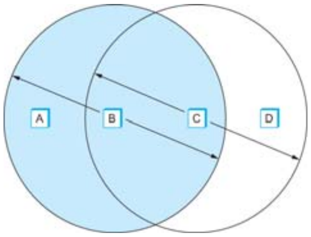
IEEE 802.11 – Collision Avoidance

Chapter 2

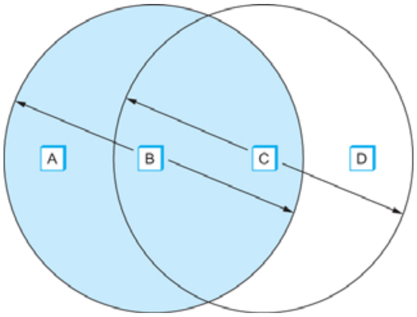
The “Hidden Node” Problem. Although A and C are hidden from each other, their signals can collide at B. (B’s reach is not shown.)

IEEE 802.11 – Collision Avoidance

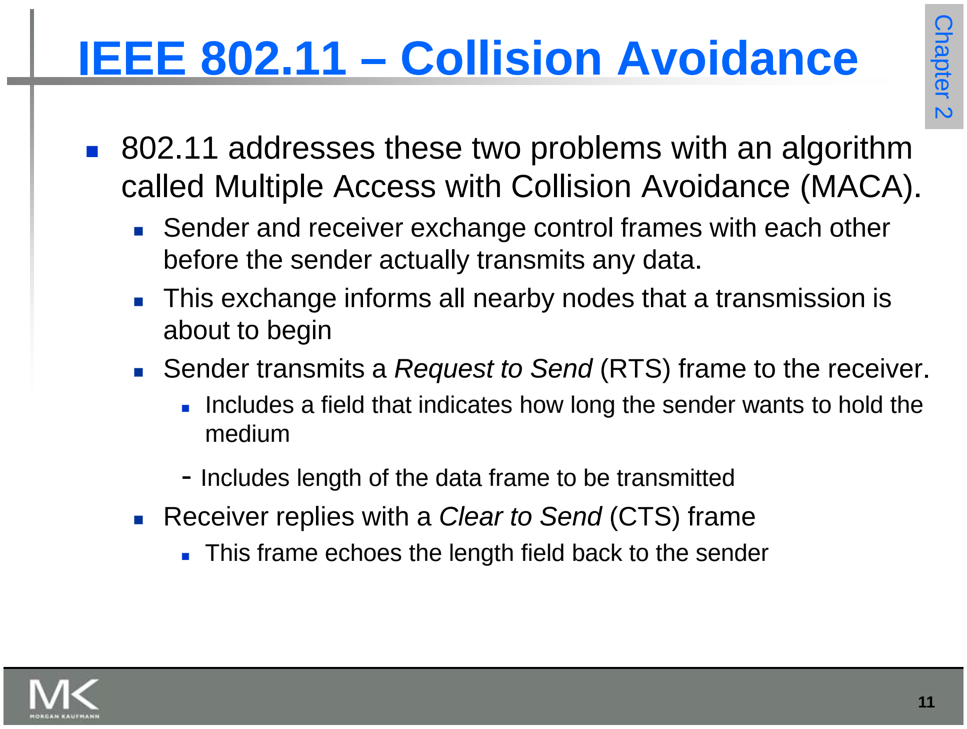
- Another problem called *exposed node* problem occurs
  - Suppose B is sending to A. Node C is aware of this communication because it hears B's transmission.
  - It would be a mistake for C to conclude that it cannot transmit to anyone just because it can hear B's transmission.
  - Suppose C wants to 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.



IEEE 802.11 – Collision Avoidance



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.)

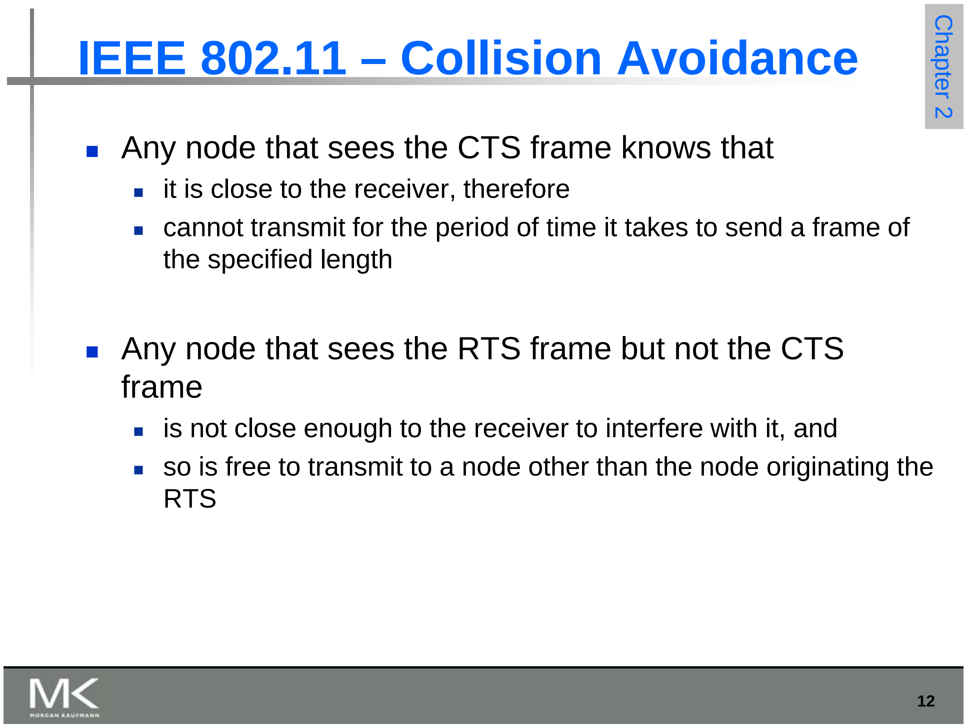


IEEE 802.11 – Collision Avoidance

Chapter 2

- 802.11 addresses these two problems with an algorithm called Multiple Access with Collision Avoidance (MACA).
  - 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.
    - Includes a field that indicates how long the sender wants to hold the medium
    - Includes length of the data frame to be transmitted
  - Receiver replies with a *Clear to Send* (CTS) frame
    - This frame echoes the length field back to the sender

11



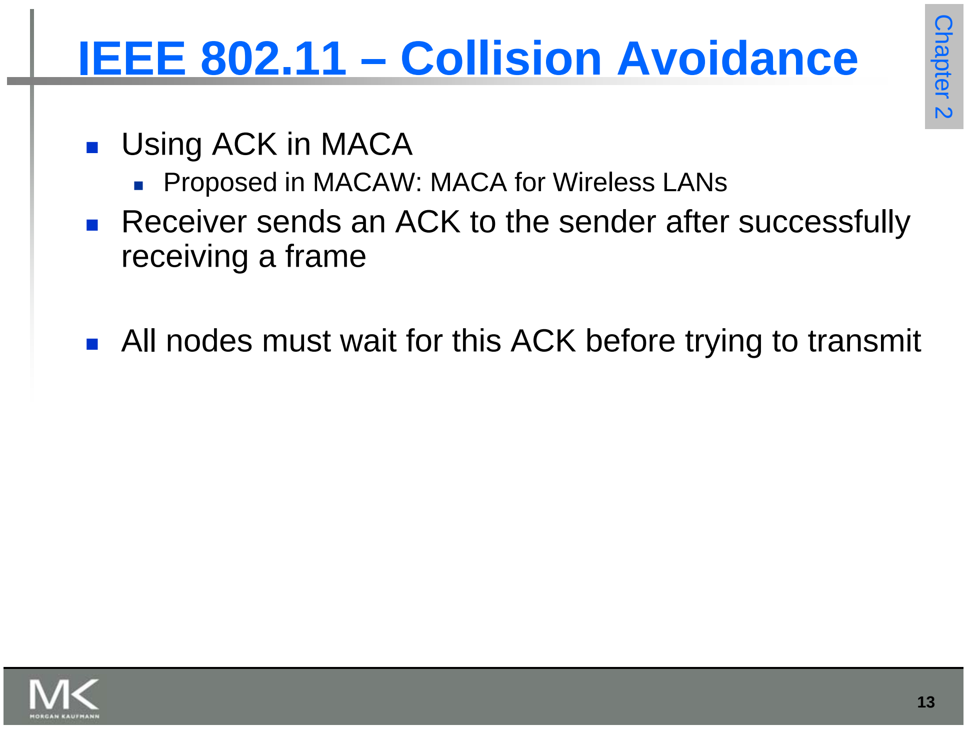
IEEE 802.11 – Collision Avoidance

Chapter 2

- 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

- 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 to a node other than the node originating the RTS

12

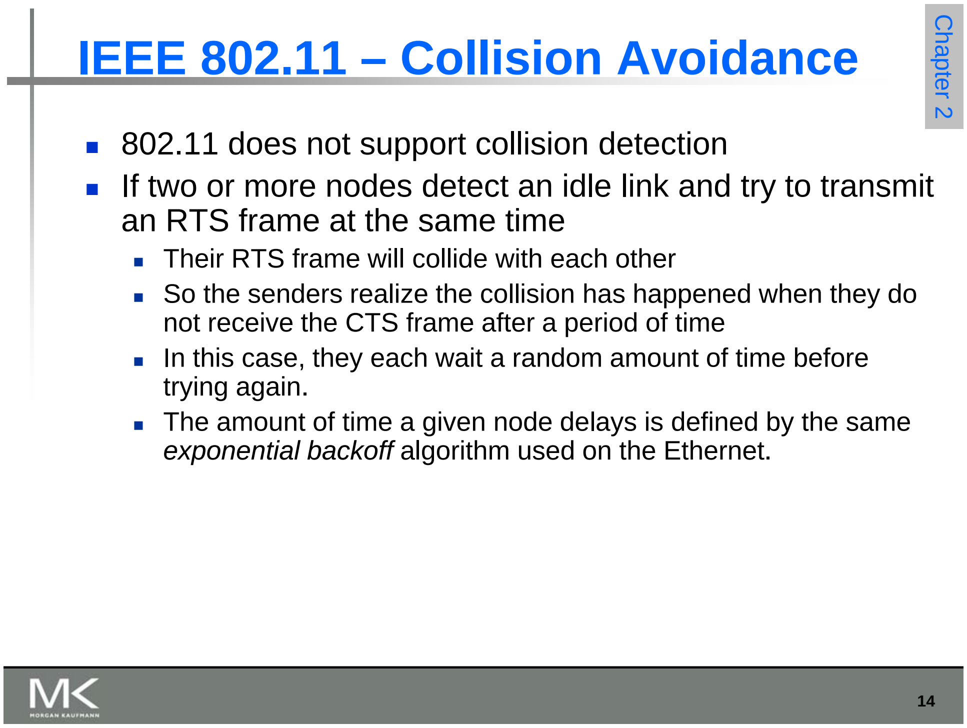


IEEE 802.11 – Collision Avoidance

Chapter 2

- 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

13

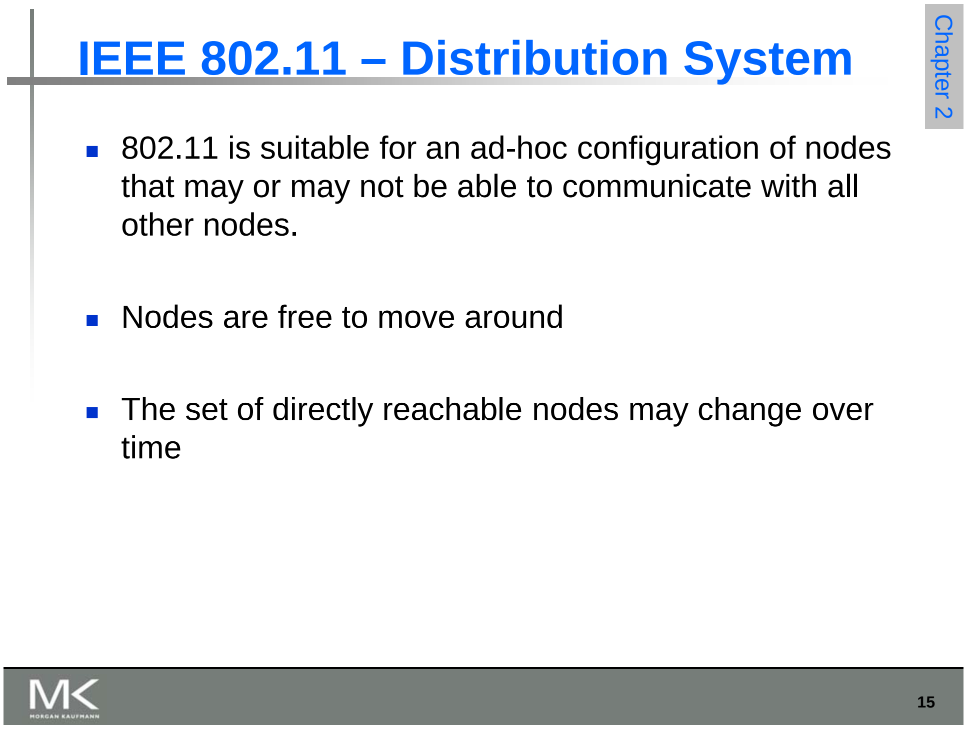


IEEE 802.11 – Collision Avoidance

Chapter 2

- 802.11 does not support collision detection
- 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
  - 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.

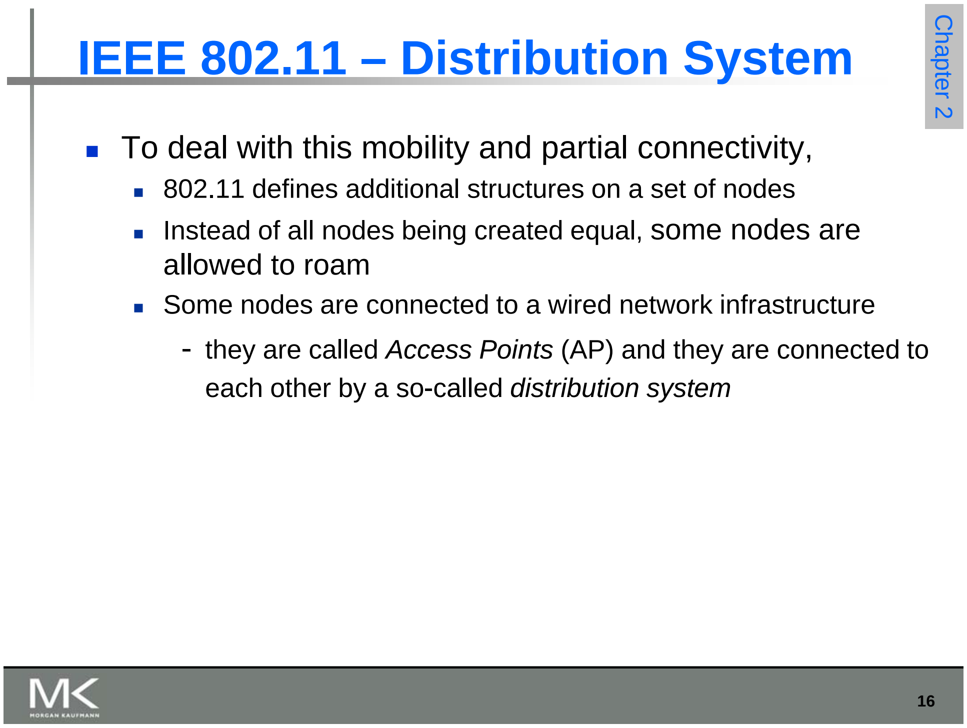
14



IEEE 802.11 – Distribution System

Chapter 2

- 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



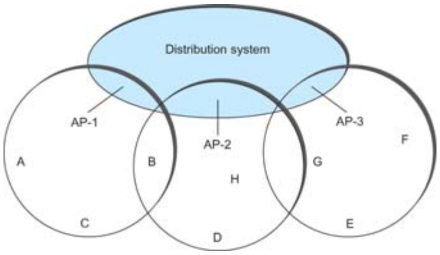
IEEE 802.11 – Distribution System

Chapter 2

- 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 nodes 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*

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 APIs playing the same role as a base station
- The distribution network runs at the link layer of the ISO architecture
- Distribution network could be ethernet

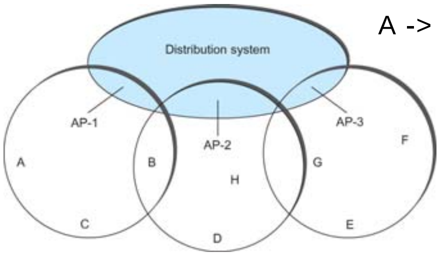


Access points connected to a distribution network

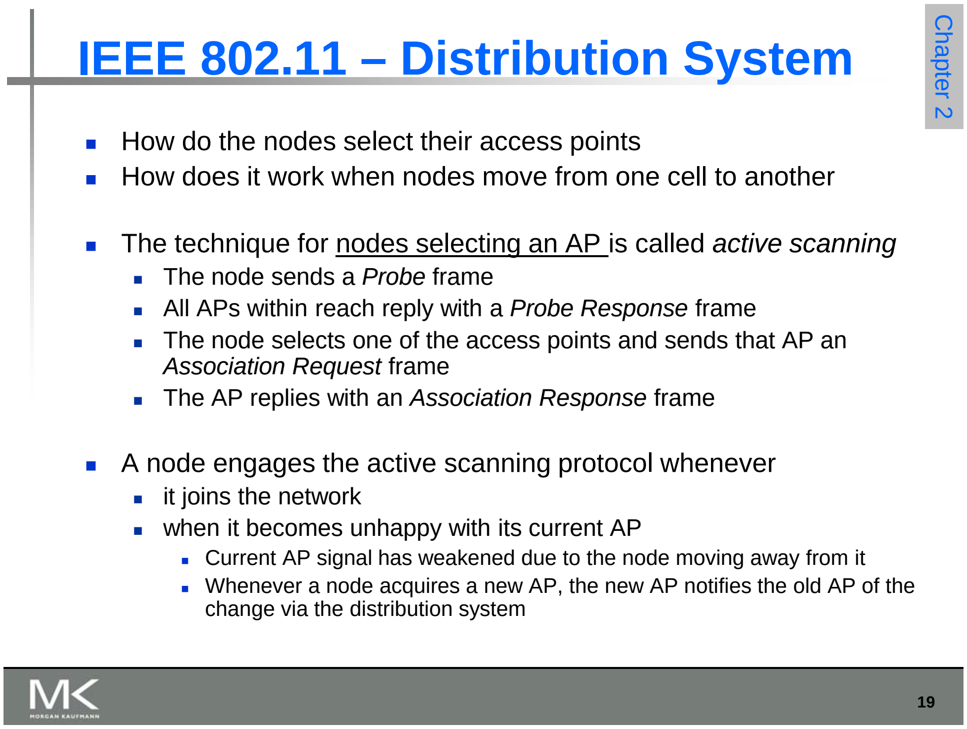
IEEE 802.11 – Distribution System

- Although two nodes can communicate directly with each other if they are within reach of each other, the idea behind this configuration is
  - Each nodes 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

A -> AP-1 -> AP-3 -> E



Access points connected to a distribution network



IEEE 802.11 – Distribution System

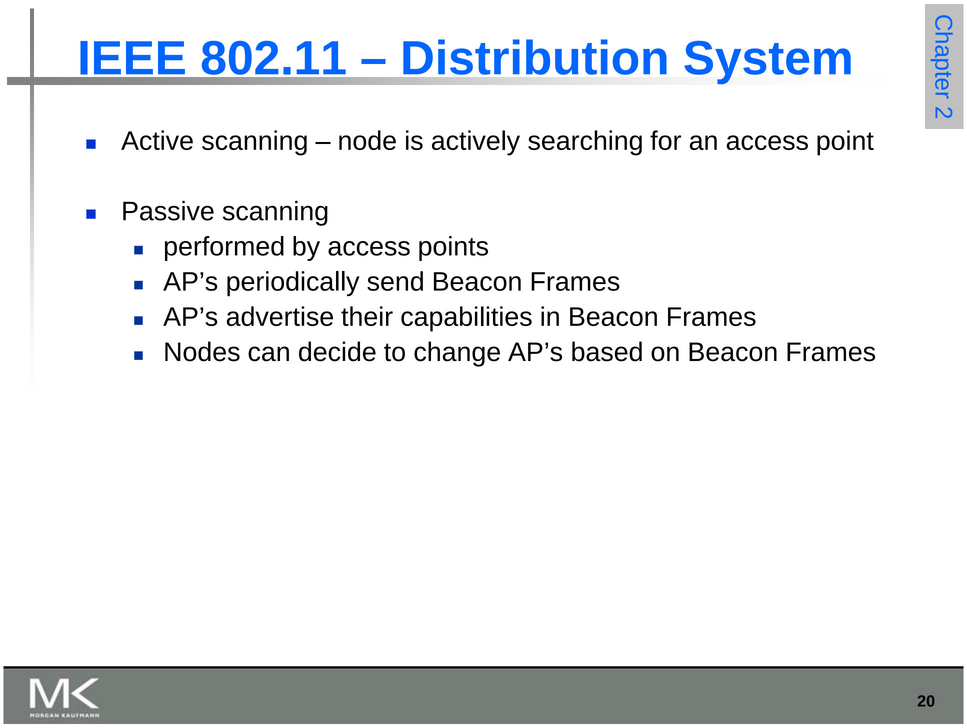
Chapter 2

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

- The technique for nodes selecting an AP is called *active 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 the active scanning protocol whenever
  - it joins the network
  - when it becomes unhappy with its current AP
    - Current AP signal 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

19



IEEE 802.11 – Distribution System

Chapter 2

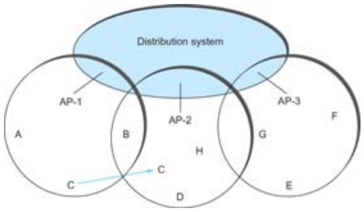
- Active scanning – node is actively searching for an access point

- Passive scanning
  - performed by access points
  - AP's periodically send Beacon Frames
  - AP's advertise their capabilities in Beacon Frames
  - Nodes can decide to change AP's based on Beacon Frames

20

IEEE 802.11 – Distribution System

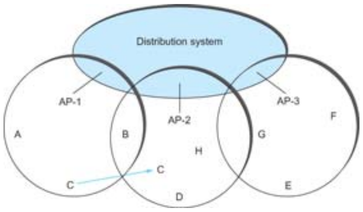
- Consider the situation shown in the following figure when node C moves from the cell serviced by AP-1 to the cell serviced by AP-2.
- As it moves, it sends *Probe* frames, which eventually result in *Probe Responses* from AP-2.
- At some point, C prefers AP-2 over AP-1 , and so it associates itself 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

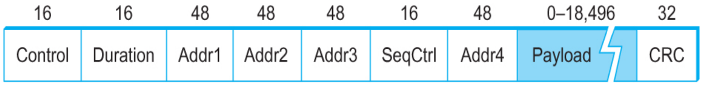
- APs also periodically send a *Beacon* frame that advertises the capabilities of the access point; these include the transmission rate supported by the AP
  - This is called *passive scanning*
  - A node can change to this AP based on the *Beacon* frame simply by sending it an *Association Request*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



Node Mobility

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 an RTS or CTS frame or being used by the scanning algorithm
    - A pair of 1 bit fields : called **ToDS** and **FromDS**

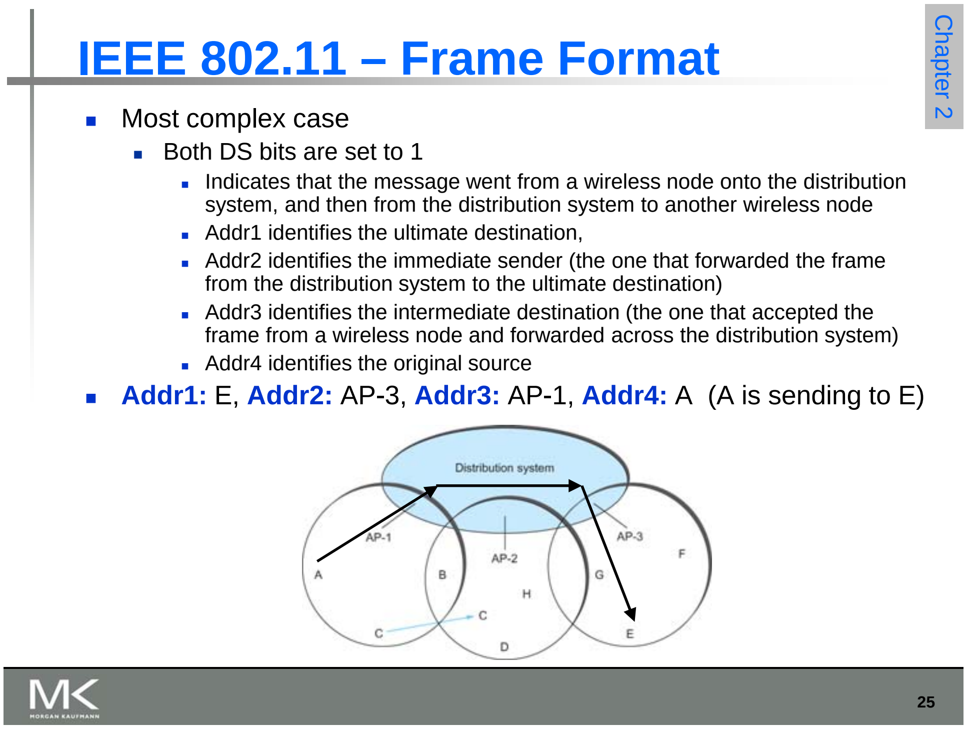


16	16	48	48	48	16	48	0–18,496	32
Control	Duration	Addr1	Addr2	Addr3	SeqCtrl	Addr4	Payload	CRC

Frame Format

IEEE 802.11 – Frame Format

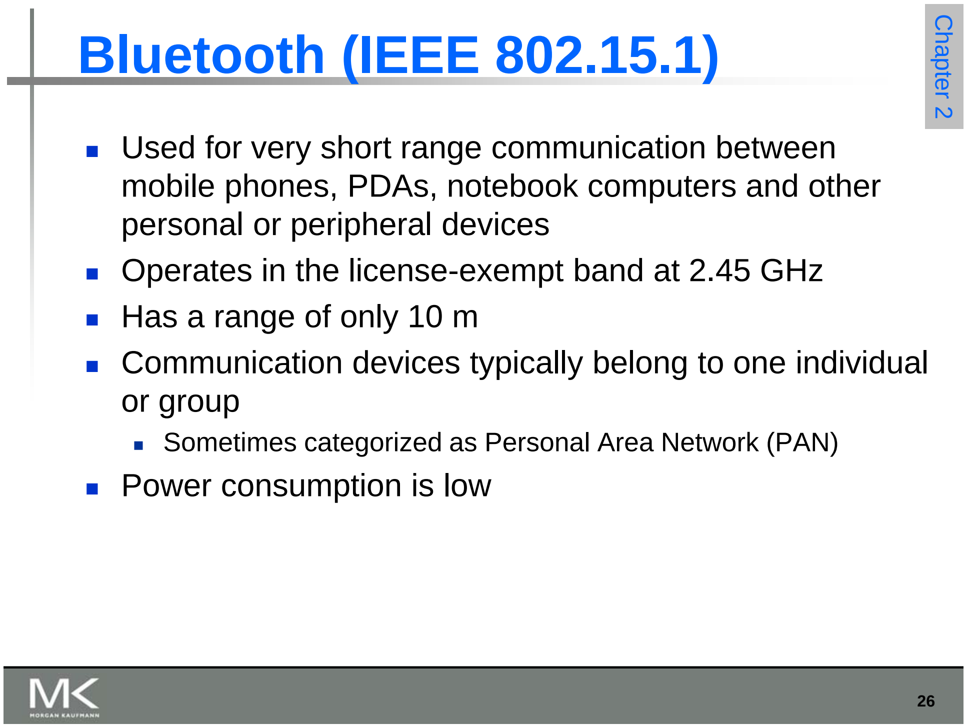
- Frame contains four addresses
- How these addresses are interpreted depends on the settings of the **ToDS** and **FromDS** bits in the frame's Control field
- This is to account for the possibility that the frame had to be forwarded across the distribution system which would mean that,
  - the original 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

Chapter 2

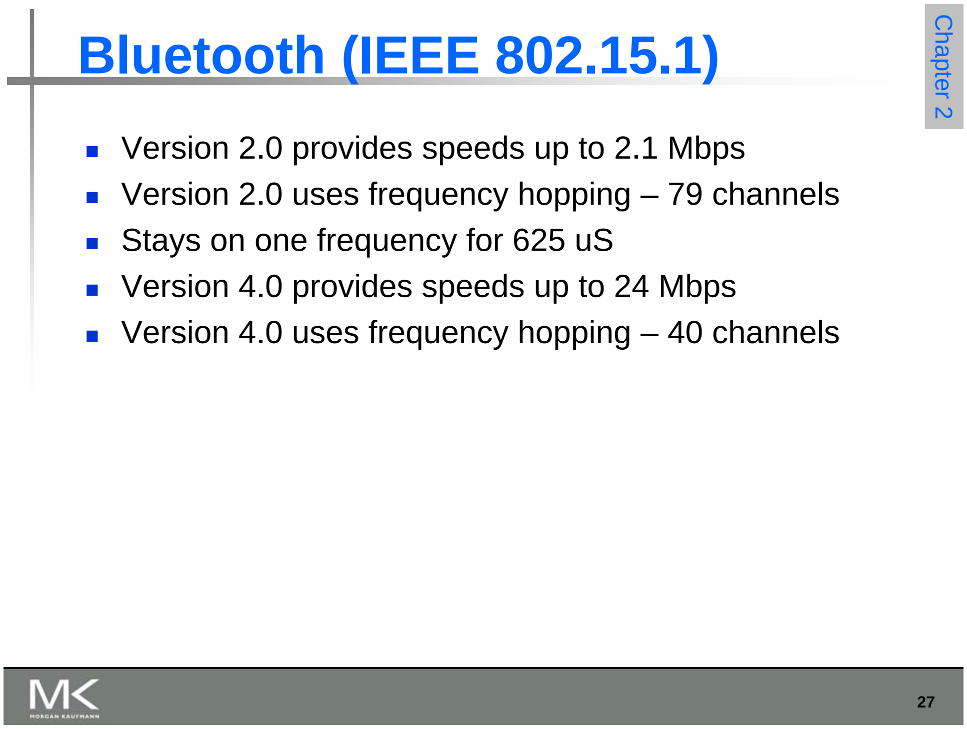
- Most complex case
  - Both DS bits are set to 1
    - Indicates that the message went from a wireless node onto the distribution system, and then from the distribution system to another wireless node
    - Addr1 identifies the ultimate destination,
    - Addr2 identifies the immediate sender (the one 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
- **Addr1:** E, **Addr2:** AP-3, **Addr3:** AP-1, **Addr4:** A (A is sending to E)



Bluetooth (IEEE 802.15.1)

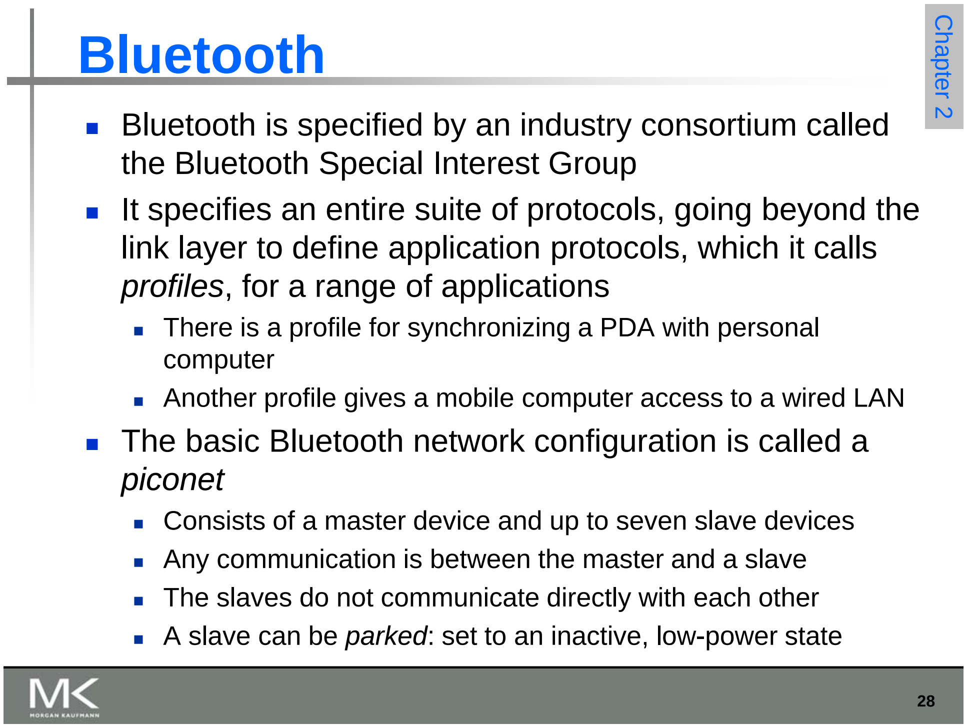
Chapter 2

- Used for very short range communication between mobile phones, PDAs, notebook computers and other personal or peripheral devices
- Operates in the license-exempt band at 2.45 GHz
- Has a range of only 10 m
- Communication devices typically belong to one individual or group
  - Sometimes categorized as Personal Area Network (PAN)
- Power consumption is low



Bluetooth (IEEE 802.15.1)

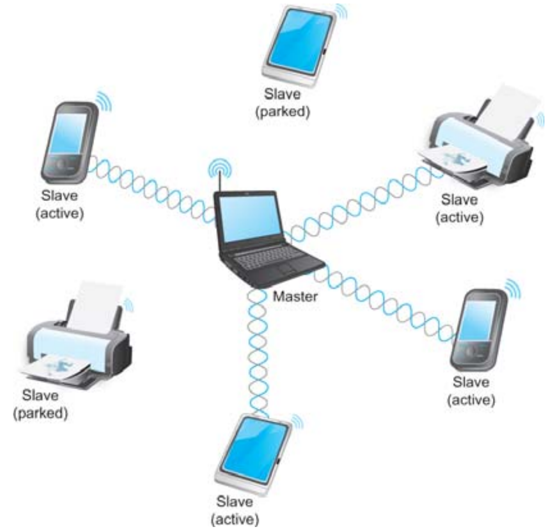
- Version 2.0 provides speeds up to 2.1 Mbps
- Version 2.0 uses frequency hopping – 79 channels
- Stays on one frequency for 625 uS
- Version 4.0 provides speeds up to 24 Mbps
- Version 4.0 uses frequency hopping – 40 channels



Bluetooth

- Bluetooth is specified by an industry consortium called the Bluetooth Special Interest Group
- It specifies an entire suite of protocols, going beyond the link layer to define application protocols, which it calls *profiles*, for a range of applications
  - There is a profile for synchronizing a PDA with personal computer
  - Another profile gives a mobile computer access to a wired LAN
- The basic Bluetooth network configuration is called a *piconet*
  - Consists of a master device and up to seven slave devices
  - Any communication is between the master and a slave
  - The slaves do not communicate directly with each other
  - A slave can be *parked*: set to an inactive, low-power state

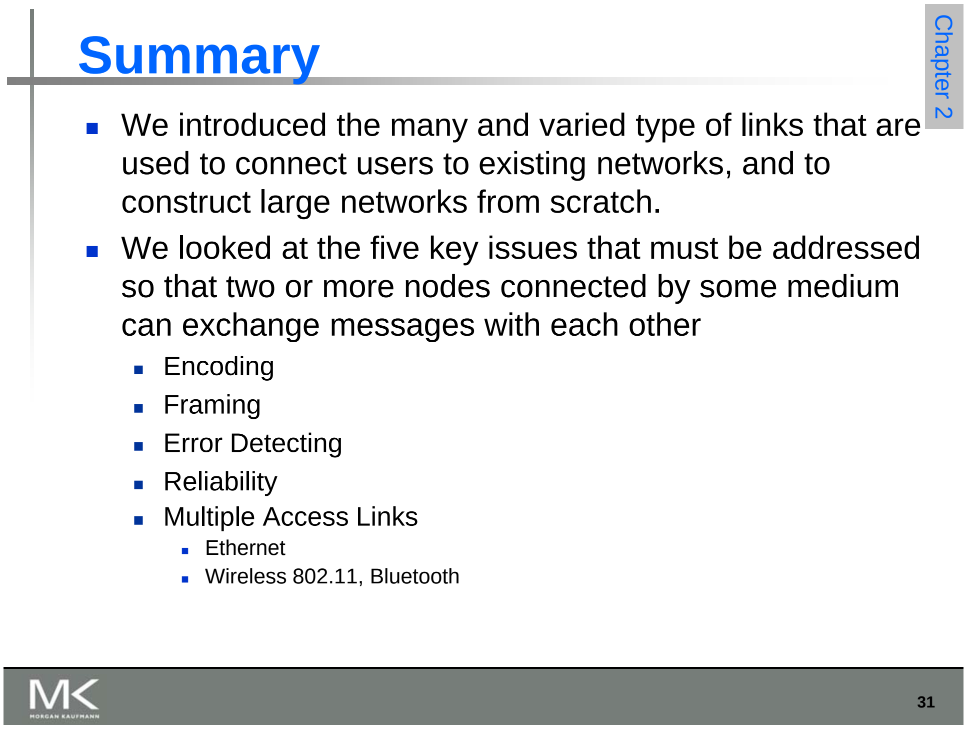
Bluetooth



A Bluetooth Piconet

ZigBee

- ZigBee is a new technology that competes with Bluetooth
- Devised by the ZigBee alliance and standardized as IEEE 802.15.4
- It is designed for situations
  - where the bandwidth requirements are low and
  - power consumption must be very low to give very long battery life – good for sensors
  - 10-100 meters with line of site
- Transfer rate is 250 kbps
- It is also intended to be simpler and cheaper than Bluetooth, making it financially feasible to incorporate in cheaper devices such as a wall switch that wirelessly communicates with a ceiling-mounted fan



Chapter 2

Summary

- We introduced the many and varied type of links that are used to connect users to existing networks, and to construct large networks from scratch.
- We looked at the five key issues that must be addressed so that two or more nodes connected by some medium can exchange messages with each other
  - Encoding
  - Framing
  - Error Detecting
  - Reliability
  - Multiple Access Links
    - Ethernet
    - Wireless 802.11, Bluetooth

MK MORGAN KAUFMANN

31