Wired Communication

Pros
- Very reliable
  - For Ethernet, medium HAS TO PROVIDE a Bit Error Rate (BER) of $10^{-12}$ (one error for every trillion bits!)
    - Insulated wires; wires placed underground and in walls
    - Error Correction Techniques
  - Very high transfer rates - currently up to 100 Gbit/s
  - Long distance - Up to 40km in 10-Gbit/s Ethernet

Cons
- Expensive to set up infrastructure
- Infrastructure is fixed once set up
- No physical mobility
Wireless Communication

Pros
- Allows mobility
- Much cheaper and easier to deploy, change, and upgrade!

Cons
- Exposed (unshielded) medium
  - Susceptible to physical phenomena (interference)
  - Variable BER – Error correction may not suffice in all cases
- Slower data rates for wider distances
- Link layer, and higher-layers, designed for wired medium
  - E.g. TCP assumes loss = congestion
  - Difficult to “hide” underlying behavior
- Security: anyone in range hears transmission
Wireless

- FCC oversees all wireless communication
- Licensed Bands
  - Cellular phones, 3G, AM/FM radio, broadcast television, satellites, WiMax
  - Use of resources left to “owner” of band
- Unlicensed Bands
  - 802.11, Bluetooth, ZigBee, IR, WiMax
  - No license needed – free for all!
  - Restrictions to limit interference
    - Limit on transmission power
    - Spread spectrum communication

Unlicensed Bands
- 900 MHz
  - Industrial, Scientific and Medical (ISM)
- 2.4 GHz
- 5.4 GHz
- 10 – 66 GHz
Wireless Communication Standards (Alphabet Soup)

- Cellular (2G): GSM, CDMA, GPRS
- 3G: CDMA2000, W-CDMA, EDGE
- 4G: WiMAX, LTE
- IEEE 802.11
  - A: 5.0Ghz band, max 54Mbps
  - B: 2.4Ghz band, max 11Mbps
  - G: 2.4Ghz, max 54Mbps
  - N: 2.4/5Ghz, max 600Mbps
  - Many other versions
- IEEE 802.15 – lower power wireless
  - 802.15.1: 2.4Ghz, max 2.1 Mbps (Bluetooth)
  - 802.15.4: 2.4Ghz, max 250 Kbps (Sensor Networks)
Wireless Link Characteristics

- **200 Mbps**: 802.11n
- **54 Mbps**: 802.11a,g
- **5–11 Mbps**: 802.11b
- **4 Mbps**: 802.11a,g point-to-point
- **WiMAX**
- **UMTS/WCDMA-HSDPA, CDMA2000-1xEVDO**
- **3G enhanced**
- **UMTS/WCDMA, CDMA2000**
- **2G**
- **IS-95, CDMA, GSM**

- **Indoor**: 10–30m
- **Outdoor**: 50–200m
- **Mid range outdoor**: 200m–4Km
- **Long range outdoor**: 5Km–20Km
Challenges of wireless

- **Path loss**
  - Signal attenuation as a function of distance
  - Signal-to-noise ratio (SNR—Signal Power/Noise Power) decreases, make signal unrecoverable

- **Multipath propagation**
  - Signal reflects off surfaces, effectively causing self-interference

- **Internal interference (from other users)**
  - Hosts within range of each other collide with one another’s transmission

- **External interference**
  - Microwave is turned on and blocks your signal
Path Loss

- Signal power attenuates by about $\sim r^2$ factor for omni-directional antennas in free space
  - $r$ is the distance between the sender and the receiver
- The exponent in the factor is different depending on placement of antennas
  - Less than 2 for directional antennas
  - Faster attenuation
  - Exponent > 2 when antennas are placed on the ground
  - Signal bounces off the ground and reduces the power of the signal
Multipath Effects

- Signals bounce off surfaces and interfere with one another
- What if signals are out of phase?
  - Orthogonal signals cancel each other and nothing is received!
What is a Wireless “Link”?
What is a Wireless “Link”? 
Wireless Bit Errors

- The lower the SNR (Signal/Noise) the higher the Bit Error Rate (BER)
- How can we deal with this?
  - Make the signal stronger
- Why is this not always a good idea?
  - Increased signal strength requires more power
  - Increases the interference range of the sender, so you interfere with more nodes around you
- Error correction can correct some problems
Spread Spectrum

- **Direct Sequence Spread Spectrum**
  - Spread the signal over a wider frequency band than required
  - Originally designed to thwart jamming
  - Original 802.11 uses 83 MHz in 2.4 GHz band

- **Frequency-Hopped Spread Spectrum**
  - Uses 80 1MHz sub-bands in 2.4 GHz band
  - Transmit over a random sequence of frequencies
Spread Spectrum

- **Direct Sequence Spread Spectrum**
  - Spread the signal over a wider frequency band than required
  - Originally designed to thwart jamming
  - Original 802.11 uses 83 MHz in 2.4 GHz band

- **Frequency-Hopped Spread Spectrum**
  - Uses 80 1MHz sub-bands in 2.4 GHz band
  - Transmit over a random sequence of frequencies

**Frequency hopping had many inventors**

- 1942: actress Hedy Lamarr and composer George Antheil patented Secret Communications System
  - Piano-roll to change between 88 frequencies, and was intended to make radio-guided torpedoes harder for enemies to detect or to jam
- The patent was rediscovered in the 1950s during patent searches when private companies independently developed Code Division Multiple Access, a civilian form of spread-spectrum
Direct Sequence Spread Spectrum

- Spread Spectrum
  - For each bit, send XOR of that bit and n random bits
  - Random sequence is known to both sender and receiver
  - Called n-bit chipping code (802.11 uses 11-bit code)

Data stream: 1010
Random sequence: 0100101101011001
XOR of the two: 1011101110101001
Current Wireless Technologies

- **IEEE 802.11**
  - Wireless LAN (WLAN)
  - MAC layer based on Ethernet
    - Originally called “wireless Ethernet”

<table>
<thead>
<tr>
<th></th>
<th>Max Rate</th>
<th>Frequency</th>
<th>Range</th>
<th>Energy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pre-802.11</td>
<td>2 Mbps</td>
<td>900 Mhz</td>
<td>100 m</td>
<td>100 mW</td>
</tr>
<tr>
<td>IEEE 802.11b</td>
<td>11 Mbps</td>
<td>2.4 GHz</td>
<td>35/150 m</td>
<td>100 mW</td>
</tr>
<tr>
<td>IEEE 802.11g</td>
<td>54 Mbps</td>
<td>2.4 GHz</td>
<td>35/150 m</td>
<td>100 mW</td>
</tr>
<tr>
<td>IEEE 802.11a</td>
<td>54 Mbps</td>
<td>5 GHz</td>
<td>10 /120 m</td>
<td>100 mW</td>
</tr>
<tr>
<td>IEEE 802.11n</td>
<td>600 Mbps</td>
<td>2.4/5 GHz</td>
<td>70 /250 m</td>
<td>100 mW</td>
</tr>
</tbody>
</table>
IEEE 802.11 - Physical Layer

- **IEEE 802.11 b**
  - Direct Sequence Spread Spectrum
    - Uses 83 MHz in 2.4 GHz band
    - Spread the signal over a wider frequency band than required
    - Originally designed to prevent jamming
  - 3 orthogonal channels

- **IEEE 802.11 g**
  - Frequency-Hopped Spread Spectrum
    - Uses 80 1MHz sub-bands in 2.4 GHz band
    - Transmit over a random sequence of frequencies
      - Hop 10 times a second
    - Originally designed to avoid snooping
  - 3 orthogonal channels
IEEE 802.11 - Physical Layer

- IEEE 802.11 a
  - Orthogonal Frequency Division Multiplexing (OFDM)
  - 13 orthogonal channels
- IEEE 802.11 n
  - Works on both 802.11a and 802.11g spectrum
  - MIMO – Multi-input, Multi-output antenna
    - Up to 4 antenna
IEEE 802.11 - Physical Layer

Channel Rate vs. Signal strength

- All versions of IEEE 802.11 can reduce the rate to increase the signal strength
  - IEEE 802.11 b 1, 2, 5.5, 11 Mbps
  - IEEE 802.11 a, g 6, 9, 12, 18, 24, 36, 48, or 54 Mbps

- Increased range → lower signal → lower rate
IEEE 802.11 Extensions

- IEEE 802.11e
  - Enhancements: QoS, including packet bursting
- IEEE 802.11i
  - Enhanced security
- IEEE 802.11p
  - WAVE - Wireless Access for the Vehicular Environment
- IEEE 802.11s
  - ESS Mesh Networking
- IEEE 802.11u
  - Interworking with non-802 networks (for example, cellular)
- IEEE 802.11 ac
  - Provides high throughput in the 5 GHz band
  - Wider RF bandwidth, more streams (up to 8), and high-density modulation (up to 256 QAM)
Current Wireless Technologies

- BlueTooth – IEEE 802.15.1
  - Originally designed as a cable replacement technology
  - Master/Slave configuration
  - Piconets

<table>
<thead>
<tr>
<th></th>
<th>Max Rate</th>
<th>Frequency</th>
<th>Range</th>
<th>Energy</th>
</tr>
</thead>
<tbody>
<tr>
<td>BlueTooth</td>
<td>3 Mbps</td>
<td>2.4 GHz</td>
<td>100 m</td>
<td>100 mW</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>10 m</td>
<td>2.5 mW</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>1 m</td>
<td>1 mW</td>
</tr>
</tbody>
</table>
BlueTooth

- **Physical Layer**
  - Frequency-Hopped Spread Spectrum
    - Uses 79 1MHz sub-bands in 2.4 GHz band
    - Transmit over a random sequence of frequencies
      - Hop 1600 times a second
    - 5 orthogonal sub-hopping sets

- **MAC Layer**
  - Slotted
    - Managed by the master
    - Single slot packet
      - Max data rate of 172Kbps
    - Multislot frames
      - Support higher rates of 721Kbps
Current Wireless Technologies

- **ZigBee – IEEE 802.15.4**
  - Low power, short range
    - Sensor networks
    - Personal area networks

<table>
<thead>
<tr>
<th>Max Rate</th>
<th>Frequency</th>
<th>Range</th>
<th>Energy</th>
</tr>
</thead>
<tbody>
<tr>
<td>ZigBee (IEEE 802.15.4)</td>
<td>250 kbps</td>
<td>2.4 GHz</td>
<td>10 - 100 m</td>
</tr>
<tr>
<td></td>
<td>40 Kbps</td>
<td>915 MHz</td>
<td>10 - 100 m</td>
</tr>
<tr>
<td></td>
<td>20 Kbps</td>
<td>868 MHz</td>
<td>10 - 100 m</td>
</tr>
</tbody>
</table>
ZigBee

- Physical Layer
  - Direct Sequence Spread Spectrum
    - 2.4 GHz – 16 orthogonal channels
    - 915 MHz – 10 orthogonal channels
    - 868 MHz – 1 channel

- MAC Layer
  - CSMA/CA
  - Battery Life Extension (BLE) mode
    - Limit the back-off exponent to max 2
Current Wireless Technologies

- **InfraRed**
  - Directional

<table>
<thead>
<tr>
<th></th>
<th>Max Rate</th>
<th>Frequency</th>
<th>Range</th>
<th>Energy</th>
</tr>
</thead>
<tbody>
<tr>
<td>InfraRed – IrDA</td>
<td>9600 bps – 16 Mbps</td>
<td>&lt; 1 m</td>
<td>Low</td>
<td></td>
</tr>
</tbody>
</table>
Current Wireless Technologies

- RFID
  - Passive technology
  - Used for inventory control

<table>
<thead>
<tr>
<th></th>
<th>Max Rate</th>
<th>Frequency</th>
<th>Range</th>
<th>Energy</th>
</tr>
</thead>
<tbody>
<tr>
<td>RFID – Near Field</td>
<td></td>
<td></td>
<td>&lt; 10 cm</td>
<td>Self-powered</td>
</tr>
<tr>
<td>RFID – Far Field</td>
<td></td>
<td></td>
<td>&lt; 3 m</td>
<td>Self-powered</td>
</tr>
</tbody>
</table>
RFID Basics
- Reader powers the “tag”
- Antenna “captures” the energy for a response
- Simple MAC
  - All tags respond
- Contention-based MAC
  - Use ALOHA or Tree-splitting algorithm to avoid collisions

Near field
- Magnetic induction
  - Range < 10 cm

Far field
- Electromagnetic wave capture
  - Range < 3 m
Current Wireless Technologies

- **WiMAX – IEEE 802.16**
  - Wireless Metropolitan Area Networks (WMAN)
  - May require line-of-sight (LOS)

<table>
<thead>
<tr>
<th></th>
<th>Max Rate</th>
<th>Frequency</th>
<th>Range</th>
<th>Energy</th>
</tr>
</thead>
<tbody>
<tr>
<td>WiMAX – LOS</td>
<td>70 Mbps</td>
<td>10-66 GHz</td>
<td>50 km</td>
<td>Very high</td>
</tr>
<tr>
<td>WiMAX Non-LOS</td>
<td></td>
<td>2-11 GHz</td>
<td></td>
<td>Very high</td>
</tr>
</tbody>
</table>
Communication Characteristics

- Rate
  - Defines the communication speeds
- Frequency
  - Defines the behavior in the physical environment
- Range
  - Defines the physical communication area
- Power
  - Defines the cost in terms of energy
Communication Characteristics

- **Rate**
  - Defines the communication speeds
  - Channel Bandwidth
    - Defined by the specifications of the technology
  - Available Bandwidth
    - Defined by the current use of the communication channel
      - Channel competition – MAC layer
      - Bandwidth competition – Transport layer

- **Which is better?**
  - IEEE 802.11a or IEEE 802.11b
Communication Characteristics

- Frequency/signal characteristics
  - Defines the behavior in the physical environment
    - Does the signal go through walls?
    - Is the signal susceptible to multipath fading?
  - Challenge
    - Many technologies use the same frequency

- Which is better?
  - Environment: a home with WiFi and cordless phones
  - Bluetooth or 802.11?
Communication Characteristics

- **Range**
  - Defines the physical communication area
  - May be affected by buildings, walls, people
  - May be affected by distance

- **Which is better?**
  - InfraRed or ZigBee?
Communication Characteristics

- **Power**
  - Defines the cost in terms of energy
  - Power can be adapted to save energy
    - Inversely affects range

- Which is better?
  - IEEE 802.11g or ZigBee?
Medium Access Control

- IEEE 802.11
  - A physical and multiple access layer standard for wireless local area networks (WLAN)

Ad Hoc Network: no servers or access points

Client Server Network
Medium Access Control

- Wireless channel is a shared medium
- Need access control mechanism to avoid interference
- Why not CSMA/CD?
Ethernet MAC Algorithm

- Listen for carrier sense before transmitting
- Collision: What you hear is not what you sent!
CSMA/CD in WLANs?

- Most (if not all) radios are half-duplex
  - Listening while transmitting is not possible
- Collision might not occur at sender
  - Collision at receiver might not be detected by sender!
Wireless Ethernet - CSMA/CA

- **CS** – Carrier Sense
  - Nodes can distinguish between an idle and a busy link

- **MA** - Multiple Access
  - A set of nodes send and receive frames over a shared link

- **CA** – Collision Avoidance
  - Nodes use protocol to prevent collisions from occurring
IEEE 802.11 MAC Layer Standard

- Similar to Ethernet
- But consider the following:
Hidden Terminal Problem

- Node B can communicate with both A and C
- A and C cannot hear each other
- When A transmits to B, C cannot detect the transmission using the carrier sense mechanism
- If C transmits, collision will occur at node B
MACA Solution for Hidden Terminal Problem

- When node A wants to send a packet to node B
  - Node A first sends a Request-to-Send (RTS) to A
- On receiving RTS
  - Node A responds by sending Clear-to-Send (CTS)
  - provided node A is able to receive the packet
- When a node C overhears a CTS, it keeps quiet for the duration of the transfer
IEEE 802.11 MAC Layer Standard

- But we still have a problem
Exposed Terminal Problem

- B talks to A
- C wants to talk to D
- C senses channel and finds it to be busy
- C stays quiet (when it could have ideally transmitted)
MACA Solution for Exposed Terminal Problem

- Sender transmits Request to Send (RTS)
- Receiver replies with Clear to Send (CTS)
- Neighbors
  - See CTS - Stay quiet
  - See RTS, but no CTS - OK to transmit
IEEE 802.11 MAC Layer Standard

- **MACAW** – Multiple Access with Collision Avoidance for Wireless
  - Sender transmits Request to Send (RTS)
  - Receiver replies with Clear to Send (CTS)
  - Neighbors
    - See CTS
      - Stay quiet
    - See RTS, but no CTS
      - OK to transmit
  - Receiver sends ACK for frame
    - Neighbors stay silent until they hear ACK
Collisions

- Still possible
  - RTS packets can collide!

- Binary exponential backoff
  - Backoff counter doubles after every collision and reset to minimum value after successful transmission
  - Performed by stations that experience RTS collisions

- RTS collisions not as bad as data collisions in CSMA
  - Since RTS packets are typically much smaller than DATA packets
Reliability

- Wireless links are prone to errors
  - High packet loss rate detrimental to transport-layer performance
- Mechanisms needed to reduce packet loss rate experienced by upper layers
A Simple Solution to Improve Reliability - MACAW

- When node B receives a data packet from node A, node B sends an Acknowledgement (ACK)
- If node A fails to receive an ACK
  - Retransmit the packet
Revisiting the Exposed Terminal Problem

- **Problem**
  - Exposed terminal solution doesn't consider CTS at node C
  - With RTS-CTS, C doesn’t wait since it doesn’t hear A’s CTS
    - With B transmitting DATA, C can’t hear intended receiver’s CTS
    - C trying RTS while B is transmitting is useless
Revisiting the Exposed Terminal Problem - MACAW

- One solution
  - Have C use carrier sense before RTS

- Alternative
  - B sends DS (data sending) packet before DATA
    - Short packet lets C know that B received A’s CTS
    - Includes length of B’s DATA so C knows how long to wait
Deafness

For the scenario below

- Node A sends an RTS to B
  - While node C is receiving from D,
- Node B cannot reply with a CTS
  - B knows that D is sending to C
  - A keeps retransmitting RTS and increasing its own BO timeout
Request for RTS - MACAW

- Have B do contention on behalf of A
  - If B receives RTS for which it must defer CTS reply
  - Then B later sends RRTS to A when it can send
  - A responds by starting normal RTS-CTS
  - Others hearing RRTS defer long enough for RTS-CTS
Another MACAW Proposal

- This approach, however, does not work in the scenario below
  - Node B may not receive the RTS from A at all, due to interference with transmission from C

![Diagram showing interference in communication between nodes A, B, C, and D]
Broadcast/Multicast

Problem
- Basic RTS-CTS only works for unicast transmissions

For multicast
- RTS would get CTS from each intended receiver
- Likely to cause (many) collisions back at sender
Multicast - MACAW

- Sort-of solution
  - Don’t use CTS for multicast data

- Receivers recognize multicast destination in RTS
  - Don’t return CTS
  - Sender follows RTS immediately by DATA
  - After RTS, all receivers defer for long enough for DATA

- Helps, but doesn’t fully solve problem
  - Like normal CSMA, only those in range of sender will defer
  - Others in range of receiver will not defer
IEEE 802.11 Wireless MAC

- Distributed and centralized MAC components
  - Distributed Coordination Function (DCF)
  - Point Coordination Function (PCF)
- DCF suitable for multi-hop ad hoc networking
- DCF is a Carrier Sense Multiple Access/Collision Avoidance (CSMA/CA) protocol
IEEE 802.11 DCF

- Uses RTS-CTS exchange to avoid hidden terminal problem
  - Any node overhearing a CTS cannot transmit for the duration of the transfer
- Uses ACK to achieve reliability
- Any node receiving the RTS cannot transmit for the duration of the transfer
  - To prevent collision with ACK when it arrives at the sender
  - When B is sending data to C, node A keeps quite
IEEE 802.11 CSMA/CA

- Nodes stay silent when carrier sensed
  - Physical carrier sense
  - Virtual carrier sense
    - Network Allocation Vector (NAV)
    - NAV is updated based on overheard RTS/CTS/DATA/ACK packets, each of which specified duration of a pending transmission

- Backoff intervals used to reduce collision probability
IEEE 802.11 Physical Carrier Sense

Interference range

Carrier sense range

Transmit range

Packet
IEEE 802.11 Virtual Carrier Sense

RTS = Request-to-Send

Pretending a circular range
IEEE 802.11 Virtual Carrier Sense

NAV = remaining duration to keep quiet

RTS = Request-to-Send

NAV = 10
IEEE 802.11 Virtual Carrier Sense

CTS = Clear-to-Send
IEEE 802.11 Virtual Carrier Sense

CTS = Clear-to-Send

CTS

A  B  C  D  E  F

NAV = 8
IEEE 802.11 Virtual Carrier Sense

- DATA packet follows CTS

Diagram:

A → B → C → D → E → F

DATA

Spring 2012 © CS 438 Staff, University of Illinois
IEEE 802.11 Virtual Carrier Sense

- Successful data reception acknowledged using ACK
IEEE 802.11

Reserved area
Interframe Spacing

- Interframe spacing
  - Plays a large role in coordinating access to the transmission medium

- Varying interframe spacings
  - Creates different priority levels for different types of traffic!

- 802.11 uses 4 different interframe spacings

![Diagram showing interframe spacings: DIFS, PIFS, SIFS, medium busy, contention, next frame, direct access if medium is free ≥ DIFS]
IEEE 802.11 - CSMA/CA

- Sensing the medium
- If free for an Inter-Frame Space (IFS)
  - Station can start sending (IFS depends on service type)
- If busy
  - Station waits for a free IFS, then waits a random back-off time (collision avoidance, multiple of slot-time)
- If another station transmits during back-off time
  - The back-off timer stops (fairness)
Types of IFS

- **SIFS**
  - Short interframe space
  - Used for highest priority transmissions
  - RTS/CTS frames and ACKs

- **DIFS**
  - DCF interframe space
  - Minimum idle time for contention-based services (> SIFS)
Types of IFS

- **PIFS**
  - PCF interframe space
  - Minimum idle time for contention-free service (>SIFS, <DIFS)

- **EIFS**
  - Extended interframe space
  - Used when there is an error in transmission
IEEE 802.11 - Competing Stations

Station 1

Station 2

Station 3

Station 4

Station 5

packet arrival at MAC

medium not idle (frame, ack etc.)

elapsed backoff time

residual backoff time
Backoff Interval

- When transmitting a packet, choose a backoff interval in the range $[0, CW]$
  - CW is contention window
- Count down the backoff interval when medium is idle
  - Count-down is suspended if medium becomes busy
- When backoff interval reaches 0, transmit RTS
DCF Example

B1 = 25
B2 = 20

B1 = 5
B2 = 15

B2 = 10

B1 and B2 are backoff intervals at nodes 1 and 2

CW = 31
Backoff Interval

- The time spent counting down backoff intervals is a part of MAC overhead
- Large CW
  - Large backoff intervals
  - Can result in larger overhead
- Small CW
  - Larger number of collisions (when two nodes count down to 0 simultaneously)
Backoff Interval

- The number of nodes attempting to transmit simultaneously may change with time
  - Some mechanism to manage contention is needed

- IEEE 802.11 DCF
  - Contention window CW is chosen dynamically depending on collision occurrence
Binary Exponential Backoff in DCF

- When a node fails to receive CTS in response to its RTS, it increases the contention window
  - $cw$ is doubled (up to an upper bound)
- When a node successfully completes a data transfer, it restores $cw$ to $CW_{\min}$
  - $cw$ follows a sawtooth curve
**Fairness Issue**

- Many definitions of fairness plausible
- Simplest definition
  - All nodes should receive equal bandwidth

Two flows
Fairness Issue

- Assume that initially, A and B both choose a backoff interval in range [0,31] but their RTSs collide
- Nodes A and B then choose from range [0,63]
  - Node A chooses 4 slots and B choose 60 slots
  - After A transmits a packet, it next chooses from range [0,31]
  - It is possible that A may transmit several packets before B transmits its first packet

Two flows
Fairness Issue

- Unfairness occurs when one node has backed off much more than some other node

MACAW Solution

- When a node transmits a packet
  - Append the cw value to the packet
  - all nodes hearing that CW value use it for their future transmission attempts
Channelization of spectrum

- Typically, available frequency spectrum is split into multiple channels
- Some channels may overlap

<table>
<thead>
<tr>
<th>Channels</th>
<th>Frequency (MHz)</th>
<th>Frequency (GHz)</th>
</tr>
</thead>
<tbody>
<tr>
<td>3 channels</td>
<td>26 MHz, 100 MHz</td>
<td>2.45 GHz, 5.25 GHz</td>
</tr>
<tr>
<td>8 channels</td>
<td>200 MHz, 150 MHz</td>
<td>5.8 GHz</td>
</tr>
<tr>
<td>4 channels</td>
<td>250 MHz, 500 MHz, 1000 MHz</td>
<td>24.125 GHz, 61.25 GHz, 122.5 GHz</td>
</tr>
</tbody>
</table>
Preventing Collisions Altogether

- Frequency Spectrum partitioned into several channels
  - Nodes within interference range can use separate channels
  - Now A can send to B while C sends to D without any interference!
  - Aggregate Network throughput doubles
Using Multiple Channels

- **802.11: AP’s on different channels**
  - Usually manually configured by administrator
  - Automatic Configuration may cause problems

- **Most cards have only 1 transceiver**
  - Not Full Duplex: Cannot send and receive at the same time

- **Multichannel MAC Protocols**
  - Automatically have nodes negotiate channels
    - Channel coordination amongst nodes is necessary
    - Introduces negotiation and channel-switching latency that reduce throughput
Wireless Multihop Networks

- Vehicular Networks
  - Delay Tolerant (batch) sending over several hops carry data to a base station

- Common in Sensor Network for periodically transmitting data
  - Infrastructure Monitoring
    - E.g., structural health monitoring of the Golden Gate Bridge

- Multihop networking for Internet connection sharing
  - Routing traffic over several hops to base station connected to Internet
Multi-Hop Wireless Networks

In an ideal world …
Multi-Hop Wireless Networks

- In an ideal world …
Multi-Hop Wireless Networks

Reality check …

Problem 1
- Node A can’t use both links at the same time
Reality check...

Problem 2
  - Can’t use both links at the same time

Multi-Hop Wireless Networks

Overlap at A
Hidden and exposed terminals
Problem 3
- Lots of contention for the channels
- Everyone wants to send

RTS/CTS helps with contention but wastes resources
Reality check …

Problem 4
- TCP uses ACKS and bidirectional channels
- Even more contention!