CSE 291: Wireless and Communication in the Internet of Things
Networking Speedrun

Pat Pannuto, UC San Diego
ppannuto@ucsd.edu
Today’s Goals

• Introduce OSI layer model of communication

• Refresh how services find each other, operate

• Overview of concerns for the Physical and Data link layers
  – Speak the “lingo” of wireless communication
  – Present technology aspects that we will return to in specific protocols

• Describe Medium Access Control mechanisms
Outline

• OSI Layers

• "The Upper Layers"

• Physical Layer

• Data Link Layer
Communication layers

- Application
- Presentation
- Session
- Transport
- Network
- Data Link
- Physical

What goes on at each of these?
**OSI model of communication layers**

- **Transport**
  - How to form connections between computers
  - TCP and UDP
- **Network**
  - How to send packets between networks
  - IP
- **Data Link**
  - How to send frames of data
  - Ethernet, WiFi
- **Physical**
  - How to send individual bits
  - Ethernet, WiFi
Protocols are “layered”

• Headers for each layer of communication wrap data
  – Data is wrapped with header for the network to make a packet
  – Packet is wrapped with header for the link to make a frame

![Diagram of Internet Packet and Ethernet Frame](image-url)
Protocols are “layered”

• Headers for each layer of communication wrap data
  – Data is wrapped with header for the network to make a packet
  – Packet is wrapped with header for the link to make a frame
# Transmitting data between networks

**LAN1**

1. Data

**internet packet**

2. Data PH

**LAN1 frame**

3. Data PH FH1

**Host A**

protocol software

**LAN1 adapter**

**Router**

**LAN1 adapter**

4. Data PH FH1

**LAN2 adapter**

5. Data PH FH2

**LAN2**

**Host B**

protocol software

**LAN2 adapter**

6. Data PH FH2

7. Data PH

8. Data

PH: Internet packet header
FH: LAN frame header
Model != reality

- Wireless protocols don’t always split between layers cleanly
  - Usually explain parts of physical, data link, and possibly upper layers
- Model still helps conceptualize stack-up though
Layering for IoT (joke) (kind of)

MQTT is a publish/subscribe message broker.
Outline

• OSI Layers

• “The Upper Layers”

• Physical Layer

• Data Link Layer
ALL the layers

• A ‘famous’ interview question
  – “What happens when you type google.com into your browser’s address bar and press enter?”
  – https://github.com/alex/what-happens-when
Let’s look at the internet part of the internet

• **IP layer**
  – Describes the overall goal
    • Packets from Mason Hall <---> Google

• **Link layer (Ethernet)**
  – Describes individual links
    • Packets from my computer <---> Mason Hall Router

• **Routing**
  – Using ethernet building blocks to get packets from one IP to another
Addressing

• How to solve the routing problem?
  – I need to know how to get data from me to you

• How does the post office work?
  – I know where you live (your address)
    • Zip Code
    • City
    • Street
    • House Number
    • Name
Addressing

• Your computer moves all the time
  – Home, school, Starbucks...
Addressing - *Intranet and Internet*

• **In general, network operators don’t change that often**

• **Solution:**
  – Tie IP addresses to network operators
  – Assign computers IPs as they join networks

• **Key Point:**
  – Networks “own” a block of IP address space
  – “The Internet” is a network of networks
A campus-scale example

- Let’s assume each building is its own network, with its own pool of IPs
Getting an IP from `your building’s network`

• The 1st Floor Mason Hall router "owns" 141.217.68.0-255
  — This is notated as 141.211.68.0/24
  — The first 24 bits "matter"

• Your computer "owns" 141.211.68.100
  — 141.217.68.100/32, usually omit the /32

• Trivia: The University of Michigan owns 141.211.0.0/14
Aside: Who owns what?
https://ipinfo.io/AS7377

AS7377
University of California, San Diego • ucsd.edu

AS7377 – University of California, San Diego

<table>
<thead>
<tr>
<th>Country</th>
<th>United States</th>
</tr>
</thead>
<tbody>
<tr>
<td>Website</td>
<td>ucsd.edu</td>
</tr>
<tr>
<td>Hosted domains</td>
<td>964</td>
</tr>
<tr>
<td>Number of IPs</td>
<td>12,855,552</td>
</tr>
<tr>
<td>ASN type</td>
<td>Education</td>
</tr>
<tr>
<td>Allocated</td>
<td>25 years ago on Nov 25, 1996</td>
</tr>
</tbody>
</table>
Identifying your computer?

• Every network card has its own MAC address
  – IPs are (somewhat) dynamic, “owned” by local networks
  – MACs are hardware and static, “owned” by specific computers
    • Manufacturers own blocks of MACs, “spend” them each time they make a device

• “Connecting” to a network
  – Your computer leases an IP from the local network
  – Only the local router knows your MAC, everyone else sees your IP
    • [n.b. this overview ignores NATs, which are commonplace today]
How to get across campus?
Only go up as far as you need

141.211.68.100/32 (you)
- Go to umich.edu
- Go to 141.211.13.224
- 141.211.68.100/32 ≠ 141.211.13.244
- Forward request to owning router (141.211.68.0/8)

141.211.68.0/24 (Mason Hall router)
- 141.211.68.0/24 ≠ 141.211.13.244
- Forward request to owning router (141.211.60.0/11)

141.211.60.0/21 (Central Campus Buildings)
- 141.211.60.0/21 ≠ 141.211.13.244
- Forward request to owning router (141.211.0.0/14)

141.211.0.0/14 (University of Michigan)
- 141.211.0.0/14 = 141.211.13.244
- Lookup and pass request down

141.211.13.0/24 (Fleming Administration Building)
- 141.211.13.0/8 = 141.211.13.244
- Lookup MAC and route to umich.edu server

141.211.13.244/32
- Replies (and routing process reverses)
How to get across the country?
No central authority of whole of address space...
Routing – "Adaptive"
Routing – Promises

• The current architecture promises:
  – If it is possible, your packet will reach its destination

• And **nothing more**
  – Can we make packets pick the fastest route every time?
Routing – Speed?

- 1.0.0.0/8
- 2.0.0.0/8
- 3.0.0.0/8
- 4.0.0.0/8
- 5.0.0.0/8
- 10.0.0.0/8
- 10.0.0.0/8
- 10.0.0.0/8
- 10.0.0.0/8
- 10.0.0.0/8

- 10ms
- 20ms
- 50ms

Map of the United States with nodes labeled with subnets and delays in milliseconds.
Who route?

- Often, this is done
- This causes:
  - Pakistan
  - Sweeden
Routing – Congestion

- 1.0.0.0/8
- 2.0.0.0/8
- 3.0.0.0/8
- 4.0.0.0/8
- 5.0.0.0/8
- 10.0.0.0/8

- 20.0.0.0/8

- 50ms
- 10ms
- 20ms
- 100ms
Routing – Congestion + Time
Routing – Congestion + Time
Routing – Other considerations [pre-2010, hah!]

• Most ethernet packets have a Maximum Transmission Unit (MTU) of 1500 bytes
• The fastest routers run at 10 GB/s

\[
\frac{1500 \text{ bytes/packet}}{1073741824 \text{ bytes/second}} \approx 1.4\times 10^{-6} \text{ seconds/packet}
\]

• A 1 GHz processor can only do ~1000 instructions / packet
• Tables must fit in cache
  – Memory accesses would cost ~100 instructions each
Some Perspective: North America (in June, 1999)
Some Perspective: The Internet
So how does the Internet of Things fit into the Internet?

- “IP is the Narrow Waist of the Internet”
  - **IP is Dead, Long Live IP for Wireless Sensor Networks**
- A recurring theme in this class:
  - How does this actually attach to the Internet
    - Physically [hello Hue Hub, Wyze Hub, August Hub, ...]
    - Logically [are BLE devices really part of the IoT?]
Outline

• OSI Layers

• ”The Upper Layers”

• Physical Layer

• Data Link Layer
Physical Layer

• How bits are transmitted
  – Wireless makes this entirely different from wired cases

• Important considerations
  – Signal strength
  – Modulation
  – Frequency
Wireless is a shared medium

• Wired communication has signals confined to a conductor
  – Copper or fiber
  – Guides energy to destination
  – Protects signal from interference

• Wireless communication is inherently broadcast
  – Energy is distributed in space
  – Signals must compete with other signals in same frequency band
Increasing network capacity is challenging

• Wired networks just add more wires
  – Buses are many signals in parallel to send more data

• Wireless networks are harder
  – Adding more links just increases interference
  – Need to expand to different frequencies
Model of RF communication

• Energy that radiates spherically from an antenna

• Attenuation with distance
  – Density of energy reduces over time, distance
  – Signal strength is reduced, errors go up

• Two key features
  – Error rates depend on distance
  – Spatial reuse of frequencies
Signal strength is measured in decibels

- Power is measured in Watts or dBw or dBm
  - \( \text{Power}_{\text{dBw}} = 10 \times \log_{10}(\text{Power}_{\text{Watts}}) \)
  - \( \text{Power}_{\text{dBm}} = 10 \times \log_{10}(\text{Power}_{\text{milliwatts}}) \)

- dBm is most relevant to the IoT domain
  - 0 dBm equals 1 mW transmit power
  - Example
    - Max BLE transmit power for nRF52840: 8 dBm (6.31 mW)
    - Min BLE receive sensitivity for nRF52840: -95 dBm (316.2 fW)

- Rules of thumb: +3 dB is double the power, 10 dB is 10x power
Signal strength varies significantly across technologies

- dBm is most relevant to the IoT domain
  - 0 dBm equals 1 mW transmit power
  - Example
    • Max BLE transmit power for nRF52840: 8 dBm (6.31 mW)
    • Min BLE receive sensitivity for nRF52840: -95 dBm (316.2 fW)
  - Different example
    • SX127X LoRa transmit: 20 dBm (100 mW)
    • SX127X LoRa receive sensitivity: -148 dBm (1.6 attoWatt) “down to…”

- Rules of thumb: +3 dB is double the power, 10 dB is 10x power
Many factors affect the ability to actually receive data

- Here’s one more example, from DW1000 [ultra wideband transceiver]

### 3.4 Receiver Sensitivity Characteristics

\[ T_{\text{amb}} = 25 \, ^\circ\text{C}, \text{all supplies centered on typical values. 20 byte payload} \]

#### Table 6: Typical Receiver Sensitivity Characteristics

<table>
<thead>
<tr>
<th>Packet Error Rate</th>
<th>Data Rate</th>
<th>Typical Receiver Sensitivity</th>
<th>Units</th>
<th>Condition/Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>1%</td>
<td>110 kbps</td>
<td>-106</td>
<td>dBm/500 MHz</td>
<td>Carrier frequency offset \pm 1 ppm. Requires use of the “tight” Rx operating parameter set – see [2]</td>
</tr>
<tr>
<td>10%</td>
<td>110 kbps</td>
<td>-107</td>
<td>dBm/500 MHz</td>
<td>All measurements performed on Channel 5, PRF 16 MHz. Channel 2 is approximately 1 dB less sensitive</td>
</tr>
<tr>
<td>1%</td>
<td>110 kbps</td>
<td>-102</td>
<td>dBm/500 MHz</td>
<td>Carrier frequency offset \pm 10 ppm</td>
</tr>
<tr>
<td>1%</td>
<td>850 kbps</td>
<td>-101</td>
<td>dBm/500 MHz</td>
<td>Preamble 2048</td>
</tr>
<tr>
<td>6.8 Mbps</td>
<td>-93 (-97)</td>
<td>dBm/500 MHz</td>
<td>Preamble 256</td>
<td></td>
</tr>
<tr>
<td>10%</td>
<td>110 kbps</td>
<td>-106</td>
<td>dBm/500 MHz</td>
<td>Preamble 2048</td>
</tr>
<tr>
<td>10%</td>
<td>850 kbps</td>
<td>-102</td>
<td>dBm/500 MHz</td>
<td>Preamble 1024</td>
</tr>
<tr>
<td>6.8 Mbps</td>
<td>-94 (-98)</td>
<td>dBm/500 MHz</td>
<td>Preamble 256</td>
<td></td>
</tr>
</tbody>
</table>
Propagation degrades RF signals

• Attenuation in free space
  – Signals get weaker as they travel over long distances
  – Signal spreads out -> free space path loss

• Obstacles can weaken signal through absorption or reflection

• Important: distance is NOT the only signal strength loss
  – Free space path loss calculation will not give you accurate range for a signal
ITU model for Indoor Attenuation

\[ L = 20 \log_{10} f + N \log_{10} d + P_f(n) - 28 \]

where,

- \( L \) = the total path loss. Unit: decibel (dB).
- \( f \) = Frequency of transmission. Unit: megahertz (MHz).
- \( d \) = Distance. Unit: meter (m).
- \( N \) = The distance power loss coefficient.
- \( n \) = Number of floors between the transmitter and receiver.
- \( P_f(n) \) = the floor loss penetration factor.

- Models like this are more trustworthy less bad than FSPL
Frequency separation enables different wireless technologies to operate in operation.
Modulation

- Encoding digital data in an analog “carrier” signal

- Basic forms:
  - Amplitude-shift Keying (ASK)
    - Modify amplitude of carrier signal
  - Frequency-shift Keying (FSK)
    - Modify frequency of carrier signal
  - Phase-shift Keying (PSK)
    - Modify phase of carrier signal
Unlicensed bands are where IoT thrives

- 902 MHz – 928 MHz
  - LPWANs
- 2.4 GHz to 2.5 GHz
  - WiFi, BLE, Thread
- 5 GHz
  - Faster WiFi
- Cellular uses licensed bands at great cost
  - Why?
Unlicensed bands are where IoT thrives

- 902 MHz – 928 MHz
  - LPWANs
- 2.4 GHz to 2.5 GHz
  - WiFi, BLE, Thread
- 5 GHz
  - Faster WiFi

Cellular uses licensed bands at great cost
  - Why? No interference from other users
Frequency Hopping Spread Spectrum

- Transmitter hops through a sequence of transmit channels
  - Spend some “dwell time” on each channel before hopping again
  - Receiver must know the hopping pattern

![Diagram showing frequency hopping over time](image-url)
Sidebar: inventor of FHSS – Hedy Lamarr

• Actress and Inventor
  – Designed FHSS with George Antheil during WWII
  – Idea: torpedo control can’t be easily jammed if it jumps around

• https://en.wikipedia.org/wiki/Hedy_Lamarr#Inventor
Outline

• OSI Layers

• “The Upper Layers”

• Physical Layer

• Data Link Layer
Data Link Layer

• Framing
  – Combine arbitrary bits into a “packet” of data

• Logical link control
  – Manage transfer between transmitter and receiver
  – Error detection and correction

• Media access
  – Controlling which device gets to transmit next

• Inherently coupled to PHY and its decisions
Framing

• Typical packet structure
  – Preamble - Existence of packet and synchronization of clocks
  – Header - Addresses, Type, Length
  – Data - Payload plus higher layer headers (e.g. IP packet)
  – Trailer - Padding, CRC

<table>
<thead>
<tr>
<th>Preamble</th>
<th>Destination Address</th>
<th>Source Address</th>
<th>Type and Length</th>
<th>Data</th>
<th>CRC</th>
</tr>
</thead>
</table>

• Wireless considerations
  – Control information for Physical Layer
  – Ensure robustness for header
  – Explicit multi-hop routing
  – Possibly different data rates for different parts of packet
Error control: detection and recovery

• Detection: only detect errors
  – Make sure corrupted packets get discarded
  – Cyclical Redundancy Checks
    • Detect single bit errors
    • Detect “burst” errors of several contiguous bits

• Recovery: also try to recover from small bit errors
  – Forward error correction
  – Retransmissions
  – Far more important for wireless because the cost of transmission is higher
Medium Access Control

• How does a network determine which transmitter gets to transmit?

• Remember: the wireless medium is inherently broadcast
  – Two simultaneous transmitters may lose both packets
Analogy: wireless medium as acoustic

- How do we determine who gets to speak?
  - Two simultaneous speakers also lose both “transmissions”
Analogy: wireless medium as acoustic

• How do we determine who gets to speak?
  – Two simultaneous speakers also lose both “transmissions”

• Eye contact (or raise hand) -> out-of-band communication
• Wait until it’s quiet for some time -> carrier sense multiple access
• Strict turn order -> time division multiple access
• Just speak and hope it works -> ALOHA
• Everybody sing at different tones -> frequency division multiple access (stretching the metaphor)

• Others?
MAC protocol categorization

Medium Access Control Protocols

Contention-Based Protocols
- ALOHA
- CSMA

Contention-Free Protocols
- FDMA
- TDMA

Also, CDMA
ALOHA

• ALOHAnet (1971)
  – University of Hawaii – Norman Abramson
  – First demonstration of wireless packet network

• Rules
  1. If you have data to send, send it

• Two (or more) simultaneous transmissions will collide and be lost
  – Wait a duration of time for an acknowledgement
  – If transmission was lost, try sending again “later”
    • Want some kind of exponential backoff scheme here
Packet collisions

• Each packet transmission has a window of vulnerability
  – Twice the on-air duration of a packet
  – Transmissions during the packet are bad
  – Transmissions before packet can also be bad

![Diagram showing time and packet collisions]
### Slotted ALOHA

- Split time into synchronized “slots”
- Any device can transmit whenever it has data
  - But it must transmit at the start of a slot
  - And its transmission cannot be longer than a slot
  - Removes half of the possibilities for collisions!
    - At the cost of some synchronization method
ALOHA throughput

- It can be shown that traffic maxes out at
  - ALOHA: 18.4%
  - Slotted ALOHA: 36.8%

- Assuming Poisson distribution of transmission attempts

- Slotted throughput is double because the "before" collisions can no longer occur
Capture effect

• Actually, two packets at once isn’t *always* a total loss
  – The louder packet can still sometimes be heard if loud enough

• How much louder?
  – Ballpark 12-14 dB

• When does this work?
  – Depends on the radio hardware
  – Louder packet first almost always works
  – Louder packet second *sometimes* works
**CSMA/CA – Carrier Sense Multiple Access with Collision Avoidance**

- First listen for a duration and determine if anyone is transmitting
  - If idle, you can transmit
  - If busy, wait and try again later

- “listen before send”

- Can be combined with notion of slotting
  - If current slot is idle, transmit in next slot
  - If current slot is busy, follow some algorithm to try again later
CSMA/CD – CSMA with Collision Detection

- Detect collisions during your own transmission
  - Works great on wired mediums (Ethernet, I2C)
  - Somewhere between challenging and impossible for wireless
- Transmit and receive are usually done with the same antenna
  - Receiving while transmitting would be drowned out by transmission
- Remember: TX at 8 dBm, RX at -95 dBm

On the Feasibility of Collision Detection in Full-Duplex 802.11 Radio

Dept. of Info. Eng., University of Wisconsin-Madison

Abstract—Full-duplex radios are thanks to recent advances in technology and hardware. Network features and chip level MAC layer. The literature provides some approaches to solving collisions, but is the dominating factor. Some of these approaches, however, mostly focus on centralized, distributed, and multi-hop communication. While the main approaches are to reduce collision rates, it is more important to identify potential candidations in full-duplex systems. We show that, if MAC layer can be added, and could largely standardize the use of CSMA/CD, it is possible to identify a collision during transmission.

CSMA/CD: Collision Avoidance

- CSMA with Collision Detection
- Transmits data packet, listens for collisions
- If no collisions detected, transmits
- Otherwise, back off for a random amount of time

CSMA/CD: Collision Detection

- Detects collisions during your own transmission
- Works great on wired mediums (Ethernet, I2C)
- Somewhere between challenging and impossible for wireless
- Transmit and receive are usually done with the same antenna
- Receiving while transmitting would be drowned out by transmission
- Remember: TX at 8 dBm, RX at -95 dBm

Concise Paper: Semi-Synchronous Channel Access for Full-Duplex Wireless Networks

Xiaofeng Xie and Xin Yu Zhang
University of Wisconsin-Madison
Email: {xiaofeng.xie, xinyu.zhang}@engr.wisc.edu

Throughput Analysis of CSMA With Imperfect Collision Detection in Full-Duplex-Enabled WLAN

Megumi Kaneko

Abstract—As an alternative to carrier sensing (CSMA) with collision avoidance in half-duplex wireless local area network (WLAN) that incurs heavy control overhead, full-duplex WLANs enabling wireless collision detection (WCD) by simultaneous carrier sensing and data transmission are gathering tremendous interest. Although CSMA with perfect WCD leads to large throughput enhancements, actual performances highly depend on the wireless environment, user distributions, and resulting collision patterns. Hence, we derive the achievable system throughput accounting for imperfect WCD, and evaluate the throughput gains that can be expected from CSMA with imperfect WCD over conventional random access protocols.

I. INTRODUCTION

Wireless Local Area Networks (WLANs) are facing severe congestion problems due to the exponential growth of mobile data traffic. To cope with these issues, Mult-Input Multi-Output (MIMO) antenna techniques have improved the achievable data rates at the Physical (PHY) layer. However, the conventional MAC layer is based on Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) [1], imposing heavy overhead for retransmission control to resolve packet collisions. This is due to the Half-Duplex (HD) operation of current WLAN systems, where a main reason is that a collision detected at the transmitter does not necessarily imply a collision at the receiver due to the nature of wireless channels such as large small-scale fading. Second, detecting simultaneous transmissions among one’s own transmission is very challenging, as the transmitter’s self-interference signal power is several orders of magnitude higher than that of collision signals to be detected. Thus, a number of PHY layer WCD schemes have been proposed [7], [8]. A MIMO-based scheme is designed in [7] for detecting an interfering preamble signal at one of the transmit antennas, and a self-interference canceler is designed in [8] which enables the transmitter to detect simultaneous transmissions even under very high self-interference. Such schemes allow the UTs to detect potential collisions during transmission, and hence to immediately revert to the retransmission process without any delay, leading to large throughput improvements compared to CSMA/CA [3]. Note that [3] assumed an ideal WCD where any collision can be perfectly detected at the transmitter. In [9], the impact of interference on full-duplex transmitter-receiver pairs in ad-hoc mode was analyzed. However, self-interference was not considered. In [4]-[6], full-duplex MAC protocols performing simultaneous carrier sensing and data transmission based on energy detection of the carrier sensing signal are proposed. However, the analysis overlooks the PHY layer overhead required for WCD and only considers the collision between two users, so that if one senses correctly, everybody else does too, which is not true in more than three colliding users.
Hidden terminal problem

Device A

Device B

Device C
CSMA with RTS/CTS

• Hidden terminal problem means that two transmitters might never be able to detect each other’s transmissions

• A partial solution
  – When channel is idle, transmitter sends a short Request To Send (RTS)
  – Receiver will send a Clear To Send (CTS) to only one node at a time
  – RTS collisions are faster and less wasteful than hidden terminal collisions
  – Downside: overhead is high for waiting for CTS when contention is low
Contention-free access control protocols

• Goal: split up communication such that devices will not conflict

• Can be predetermined or reservation-based
  – Devices might request to join the schedule and be given a slot
    • Devices lose their slot if it goes unused for some amount of time
    • Reservations often occur during a dedicated CSMA contention slot
  – Assignment of schedules can be complicated

• Really efficient at creating a high-throughput network
  – Assuming they are all following the same protocol
  – Otherwise, interference can be very problematic
FDMA – Frequency Division Multiple Access

• Split transmissions in frequency
  – Different carrier frequencies are independent
  – Fundamentally how RF spectrum is split

• Technically, each device uses a separate, fixed frequency
  – Walkie-talkies

• Conceptually, how RF channels work
  – WiFi networks pick different bands
  – 802.15.4 picks a channel to communicate on
TDMA – Time Division Multiple Access

• Split transmissions in time
  – Devices share the same channel

• Splits time into fixed-length windows
  – Each device is assigned one or more windows
  – Can build a priority system here with uneven split among devices

• Requires synchronization between devices
  – Often devices must listen periodically to resynchronize
  – Less efficient use of slots reduce synchronization
    • Large guard windows. E.g. 1.5 second slot for a 1 second transmission
CDMA - Code Division Multiple Access

• Split transmissions in ‘codes’
  – Not new; original applications in radar and early satellite communications

• Analogy: Multiple speakers in the same room all in different languages
  – [The human brain is crazy good at ignoring what it doesn’t understand 😊]

• Requires signal power coordination
  – [everyone needs to speak ~the same volume]
  – Can be hard in uncontrolled / dynamic environments

• Also can be more performant with highly synchronized clocks
  – i.e. if the code clock is known to both devices; intractable in mobile settings
Real-world protocol access control

- **ALOHA**
  - BLE advertisements
  - Unlicensed LPWANs: Sigfox, LoRaWAN

- **CSMA**
  - WiFi (slotted, CSMA/CA)

- **TDMA**
  - BLE connections
  - Cellular LPWANs: LTE-M and NB-IoT

- **CDMA**
  - Most modern cellular networks
Next Time: How does your Internet work?

- What can you learn about the network around you?
- Play with Wireshark
- Protocol analysis, introspection