EEC-484/584 Computer Networks

Lecture 9

Wenbing Zhao

wenbing@ieee.org

(Lecture nodes are based on materials supplied by Dr. Louise Moser at UCSB and Prentice-Hall)

Outline

- Review
  - Multiple access protocols
- IEEE 802 Standards
  - Ethernet, wireless LAN, and wireless MAN
- Reminder: Midterm #1, Oct 5 Wednesday
  - Chapters 1-4
  - Closed book, closed notes

Multiple Access Protocols

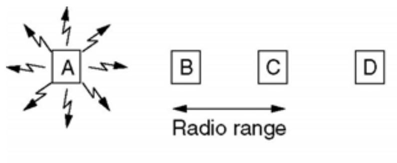
- ALOHA
  - Pure Aloha and slotted Aloha
- Carrier Sense Multiple Access Protocols
  - (1,p,0)-persistant CSMA; CSMA/CD
- Collision-Free Protocols
  - Bitmap protocol, binary countdown
- Limited-Contention Protocols
  - Adaptive tree walk protocol
- Wavelength Division Multiple Access Protocols
- Wireless LAN Protocols (MACA, MACAW)

Wireless LAN Protocols

- Special problems
  - When receiver within range of two active transmitters, resulting signals garbled and useless (assume CDMA not used)
  - Not all stations within range of each other
  - Walls etc. impact range of each station
  - **What matters is interference at receiver**
    - Sender needs to know whether there's activity around the receiver

Hidden Station Problem

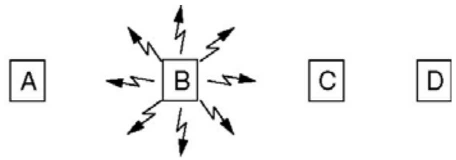
- A transmits to B,
- C out of range of A, thinks OK to transmit to B
- C transmits to B, interference occurs at B



(a)

Exposed Station Problem

- B transmits to A
- C sense transmission, concludes can't send to D, when it could have



Multiple Access with Collision Avoidance

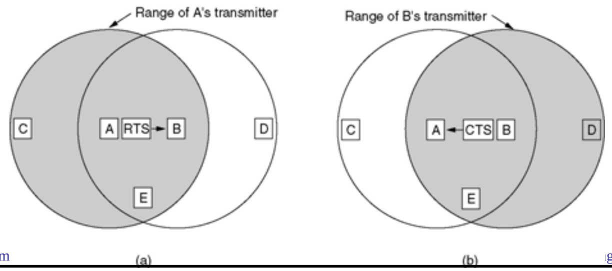
- Idea:
  - Sender gets receiver to output short frame
  - Stations near receiver detect this and avoid transmitting themselves

Multiple Access with Collision Avoidance

- MACA protocol
  - A sends Request to Send (RTS) to B containing length of data frame to follow
  - B replies with Clear to Send (CTS) to A containing length in RTS
  - When A receives CTS, A sends data frame
  - Collision can occur (for RTS), use exponential backoff

MACA

- Any station (e.g., C,E) hearing RTS is close to A, must keep quite until B finishes sending CTS
- Any station (e.g., D,E) hearing CTS is close to B, must keep quite until A finish sending data frame



MACAW

- Extension of MACA
  - Uses ack frame after each successful data frame
  - Carrier sense to avoid station's transmitting RTS when nearby station is doing so
  - Exponential backoff for each data stream rather than for each station
  - Congestion mechanism

IEEE 802 Standards

- IEEE 802 standards for LAN and MAN
  - 802.3 – Ethernet
  - 802.11 – Wireless LAN
  - 802.15 – Bluetooth
  - 802.16 – Wireless MAN
  - 802.2 – Logical link control sublayer
    - 802.3 and 802.11 converge on 802.2

Ethernet

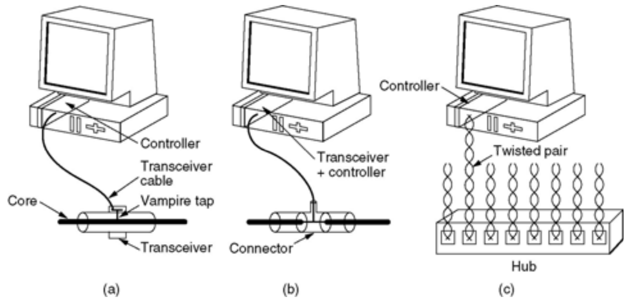
- Ethernet Cabling
- Manchester Encoding
- The Ethernet MAC Sublayer Protocol
- The Binary Exponential Backoff Algorithm
- Ethernet Performance
- Switched Ethernet
- Fast Ethernet
- Gigabit Ethernet
- IEEE 802.2: Logical Link Control
- Retrospective on Ethernet

Ethernet Cabling

- The most common kinds of Ethernet cabling
  - 10Base5 – think Ethernet, taps every 2.5 meters
  - 10Base2 – thin Ethernet, uses BNC connectors to form T-junctions
  - 10Base-T – twisted pair

Name	Cable	Max. seg.	Nodes/seg.	Advantages
10Base5	Thick coax	500 m	100	Original cable; now obsolete
10Base2	Thin coax	185 m	30	No hub needed
10Base-T	Twisted pair	100 m	1024	Cheapest system
10Base-F	Fiber optics	2000 m	1024	Best between buildings

Ethernet Cabling



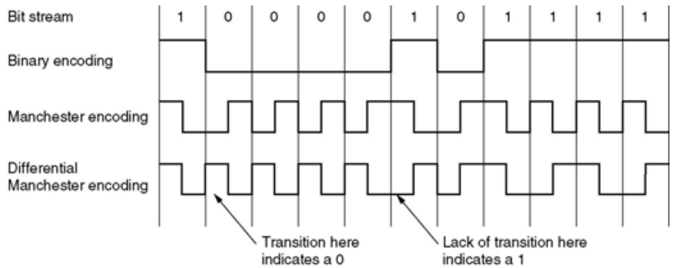
10Base5 10Base2 10Base-T

Ethernet Cabling

- **Transceiver** – handles carrier detection and collision detection
  - When collision detected, puts special invalid signal on cable so other transceivers also know collision occurred
- **Repeater** – connects multiple cables, receives, amplifies, retransmits signals in both directions

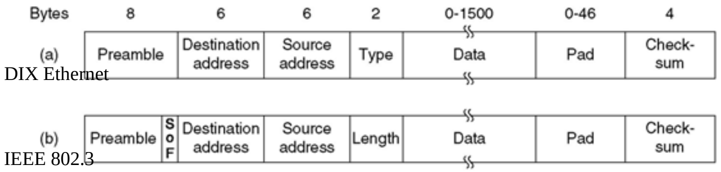
Manchester Encoding

- Binary encoding
  - Hard to distinguish 0 bit (0-volt) from idle (0-volt)
  - Requires clocks of all stations synchronized
- Manchester encoding and differential Manchester encoding



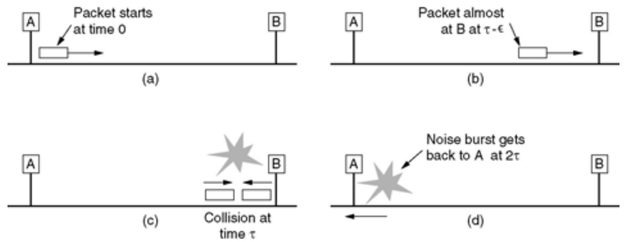
Ethernet MAC Sublayer Protocol

- Uses 1-persistent CSMA/CD
- Frame formats
  - Preamble – allows receiver's clock to synchronize with sender's clock
  - Destination address – highest order bit: 0 individual, 1 multicast; all 1's broadcast
  - Pad – used to produce valid frame >= 64 bytes
  - Checksum – 32-bit hash code of data, cyclic redundancy check



Ethernet MAC Sublayer Protocol

- Why imposing a minimum frame length?
  - Ensure the sender can detect collision if it happens
    - All frames must still take more than 2τ to send so that transmission is still taking place when the noise burst gets back to the sender



Randomization and Binary Exponential Backoff

- Time divided into slots
  - Length of slot = 2τ = worst-case round-trip propagation time
  - To accommodate longest path, slot time = 512 bit times = 51.2 μsec
- Binary exponential backoff

Randomization and Binary Exponential Backoff

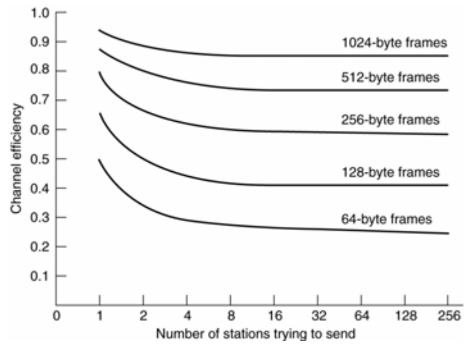
- After 1st collision, station picks 0 or 1 at random, waits that number of slots and tries again
- After 2nd collision, station picks 0,1,2,3 at random, waits that number of slots and tries again
- ....
- After *i*-th collision, station picks 0,1,…,2^i-1 at random, …
- If 10 <= *i* < 16, station picks 0,1,…,2^{10}-1 at random
- If *i*=16, controller reports failure to computer

Ethernet Performance

- Binary exponential backoff results in
  - Low delay when few stations collide
  - Reasonable delay for collision resolution when many stations collide
- Let F = frame length, B = network bandwidth L = cable length, c = signal propagation speed then channel efficiency = 1/(1 + 2BLe/cF)
  - As B or L increases, channel efficiency decreases for fixed F

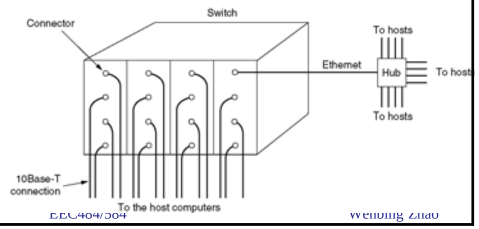
Ethernet Performance

- Efficiency of Ethernet at 10 Mbps with 512-bit slot times



Switched Ethernet

- Switch – contains a high-speed backplane and room for typically 4 to 32 plug-in line cards, each containing one to eight connectors
  - Possibly each card forms its own collision domain, or
  - Full-duplex operation if each input port is buffered – orders magnitude high throughput over 10Base5



Fast Ethernet

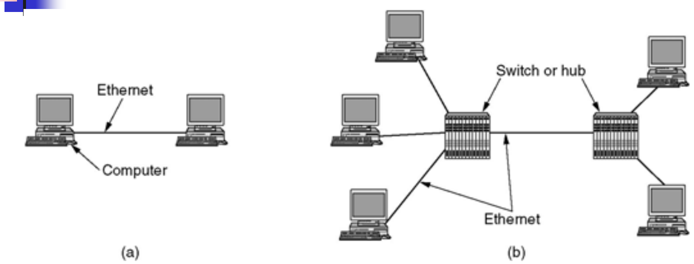
- IEEE standard 802.3u
  - Uses hubs instead of vampire tap or BNC connectors
  - Two kinds of interconnection devices
    - Hubs – all incoming lines (or those at same card) are logically connected, forming a single collision domain. Uses exponential backoff algorithm
    - Switches

Fast Ethernet Cabling

- 100Base-T4
  - 4 twisted pair (one to hub, one from hub, other two switchable)
  - Signal speed 25MHz, ternary signals (0,1,2), < 100m per segment
- 100Base-TX
  - 2 twisted pair
  - Signaling speed 125MHz, 4B5B coding (every 5 clock periods send 4 bits), < 100m per segment, full duplex
- 100Base-FX
  - 2 strands of multimode fiber, < 2000m per segment, full duplex

Name	Cable	Max. segment	Advantages
100Base-T4	Twisted pair	100 m	Uses category 3 UTP
100Base-TX	Twisted pair	100 m	Full duplex at 100 Mbps
100Base-FX	Fiber optics	2000 m	Full duplex at 100 Mbps; long runs

Gigabit Ethernet



A two-station Ethernet

A multistation Ethernet

Gigabit Ethernet

- Two modes of operations
  - Full-duplex mode
    - Used when there is a central switch connected to computers
    - CSMA/CD is not used, max length of cable is determined by signal strength issues
  - Half-duplex mode
    - Used when a hub is used – for backward compatibility only
    - To ensure collision detection, must do to ensure
      - Carrier extension – hardware to add its own padding after normal frame to extend frame to 512 bytes
      - Or, frame bursting – allows a sender to transmit a concatenated sequence of multiple frames in a single transmission

Gigabit Ethernet

- Supports flow control
  - PAUSE frames are used
    - Tells how long to pause, in units of 512 nsec, can pause up to 33.6 msec
- Gigabit Ethernet cabling

Name	Cable	Max. segment	Advantages
1000Base-SX	Fiber optics	550 m	Multimode fiber (50, 62.5 microns)
1000Base-LX	Fiber optics	5000 m	Single (10 µ) or multimode (50, 62.5 µ)
1000Base-CX	2 Pairs of STP	25 m	Shielded twisted pair
1000Base-T	4 Pairs of UTP	100 m	Standard category 5 UTP

Gigabit Ethernet

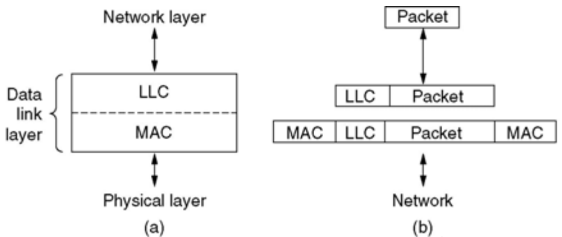
- Encoding rules for fibers
  - Manchester encoding is not used
  - 8B/10B was chosen
    - 8-bit byte is encoded on the fiber as 10bits
    - 1024 possible output codewords for each input byte
      - No codeword may have more than four identical bits in a row
      - No codeword may have more than six 0's or six 1's
      - Aim to keep the number of 0's and 1's as close to equal as possible, to maximize number of transitions to ease the sync issue

Gigabit Ethernet

- Encoding rules for 1000Base-T
  - Uses 4 cat5 twisted pairs to allow four symbols to be transmitted in parallel
  - Each symbol is encoded using one of five voltage levels, thus, there are 2 data bits per twisted pair, or 8 data bits per clock cycle
  - Clock runs at 125MHz, allowing a 1-Gbps operation

IEEE 802.2: Logical Link Control

- LLC – hides differences between various kinds of 802 networks by providing a single format and interface to the network layer
  - Closely based on HDLC protocol



Position of LLC Protocol formats

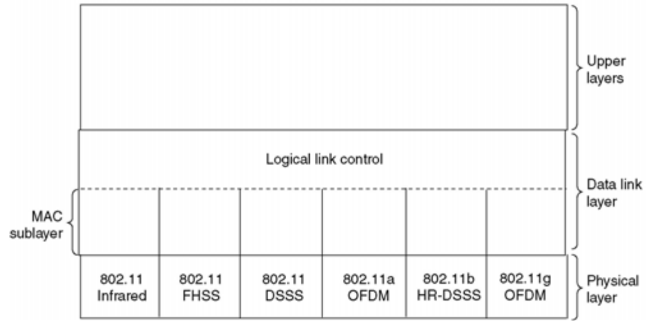
Retrospective on Ethernet

- Why Ethernet is so successful for so long?
  - It is simple and flexible.
    - Simple => reliable, cheap, easy to maintain
  - It interworks easily with TCP/IP
    - IP is connectionless protocol, so is the Ethernet
  - It has been able to evolve nicely

Wireless LANs – Mobile Ethernet

- The 802.11 Protocol Stack
- The 802.11 Physical Layer
- The 802.11 MAC Sublayer Protocol
- The 802.11 Frame Structure
- Services

The 802.11 Protocol Stack



The 802.11 Physical Layer

- Infrared
  - Uses transmission at 0.85 or 0.95 microns, speeds allowed: 1 Mbps and 2Mbps
  - Encoding scheme for 1 Mbps
    - A group of 4 bits encoded as 16-bit codeword containing 15 0's and a single 1 – Gray code
    - Gray code has property that a small error in time sync leads to only a single bit error in output
  - Encoding scheme for 2 Mbps
    - Takes 2 bits and produces a 4-bit codeword, also with only a single 1
  - Not popular due to low bandwidth

The 802.11 Physical Layer

- FHSS – frequency hopping spread spectrum
  - Uses 79 channels, each 1-MHz wide, starting at low end of 2.4-GHz ISM band
  - A pseudorandom number generator is used to produce the sequence of frequencies hopped to
    - as long as all stations use the same seed to the random number generator and stay synced in time, they will hop to the same frequencies simultaneously
  - Dwell time – amount of time spent at each frequency
    - Adjustable but must be < 400 msec
  - Advantages
    - Provides a modicum of security
    - Resists to multipath fading
    - Insensitive to radio interference
  - Disadvantage – low bandwidth

The 802.11 Physical Layer

- DSSS – direct sequence spread spectrum
  - Restricted to 1 or 2 Mbps
  - Similar to CDMA
    - Each bit is transmitted as 11 chips, using a Barker sequence
    - Uses phase shift modulation at 1 Mbaud

The 802.11 Physical Layer

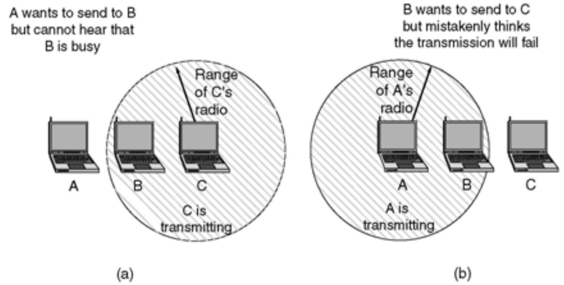
- OFDM – orthogonal frequency division multiplexing
  - Used in 802.11a, delivers up to 54 Mbps in wider 5-GHz band
  - 52 frequency band, 48 for data, 4 for sync
  - Transmission are present on multiple frequencies at the same time, it is also considered a form of spread spectrum
  - A complex encoding system is used,
    - Based on phase-shift modulation for speeds up to 18 Mbps
    - Based on QAM for higher speed
    - At 54 Mbps, 216 data bits are encoded into 288-bit symbols

The 802.11 Physical Layer

- HR-DSSS – high rate direct sequence spread spectrum
  - Used in 802.11b
  - Uses 11 million chips per sec to achieve 11 Mbps in 2.4GHz band
  - Data rates supported are 1,2,5.5, and 11 Mbps
    - For slow rates (1 or 2 Mbps), using phase shift modulation
    - For higher rates, runs at 1.375 Mbaud, with 4 and 8 bits per baud, using Walsh/Hadamard codes
- 802.11g uses OFDM, operates in 2.4GHz band
  - In theory it can operate at up to 54 Mbps

The 802.11 MAC Sublayer Protocol

- Problems must be addressed



The hidden station problem   The exposed station problem

The 802.11 MAC Sublayer Protocol

- Operation modes
  - PCF – point coordination function
    - Uses base station to control all activity in its cell
    - Optional feature
  - DCF – distributed coordination function
    - No central control, similar to Ethernet
    - Uses CSMA/CA, in turn, has two operation modes
      - Stations sense channel, if idle, transmit, does not sense while transmitting
      - Based on MACAW and uses virtual channel sensing

The 802.11 MAC Sublayer Protocol

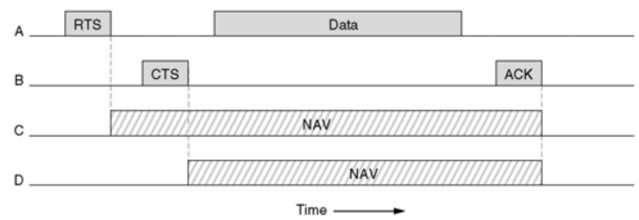
- The use of virtual channel sensing using CSMA/CA
  - A wants to send to B. C is a station within range of A. D is a station within range of B but not within range of A
  - A sends an RTS to B, B grants request and sends a CTS
  - Upon receipt of CTS, A sends its frame and starts an ACK timer
  - Upon correct receipt of the data frame, B responds with an ACK frame
  - If A's ACK timer expires before the ACK gets back to it the whole protocol is run again

The 802.11 MAC Sublayer Protocol

- View points of C and D
  - C is within range of A
    - It desist from transmitting if receive the RTS frame
    - It can estimate how long the sequence will take, including the final ACK
      - It asserts a kind of virtual channel busy for itself, indicated by NAV (network allocation vector)
  - D is within range of B
    - It also asserts the NAV signal for itself if it receives the CTS

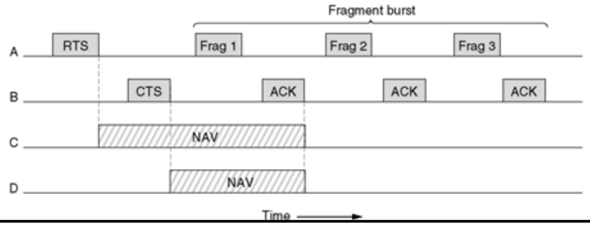
The 802.11 MAC Sublayer Protocol

- DCF and MACAW operation mode



The 802.11 MAC Sublayer Protocol

- Coping with noisy channel
  - Frames are fragmented into smaller pieces, each with its own checksum
  - Each fragment is individually numbered and acked using a stop-and-wait protocol
  - Once the channel has been acquired using RTS and CTS, multiple fragments can be sent in a row. Sequence of fragments is called a fragment burst



The 802.11 MAC Sublayer Protocol

- PCF mode
  - Base station broadcasts a beacon frame periodically (10 to 100 times per second).
    - The beacon frame contains system parameters, such as hopping sequences and dwell times, clock sync etc.
    - It also invites new stations to sign up for polling service
    - A station is guaranteed a fraction of bandwidth

The 802.11 Interframe Spacing

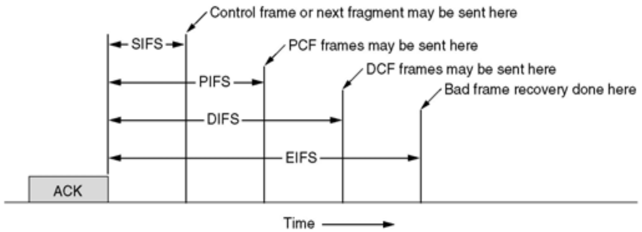
- DCF and PCF can coexist in same cell
- It works by carefully defining the interframe time interval
- After a frame has been sent, a certain amount of dead times is required before any station may send a frame

The 802.11 Interframe Spacing

- Four different intervals are defined
  - SIFS – Short InterFrame Spacing
    - Allows the parties in a single dialog the chance to go first, e.g., letting receiver to send CTS in response to a RTS
  - PIFS – PCF InterFrame Spacing
    - Allows a station sending a data frame to finish its frame without anyone else getting in the way
  - DIFS – DCF InterFrame Spacing
    - Any station may attempt to acquire the channel to send a new frame
  - EIFS – Extended InterFrame Spacing
    - Used only by a station that has just received a bad or unknown frame to report the bad frame

The 802.11 Interframe Spacing

- Four different interframe spacing



The 802.11 Frame Structure

- The 802.11 data frame

802.11 Services

- Distribution services
  - Association
    - For stations to connect to base stations
  - Disassociation
  - Reassociation
    - To facilitate a station to move between cells, allows a station to change its preferred base station
  - Distribution
    - Determines how to route frames sent to the base station, local, or forward through wired network
  - Integration
    - Translates from 802.11 format to the format required by the destination network

802.11 Services

- Intracell services
  - Authentication
    - Identify the stations
  - Deauthentication
  - Privacy
    - Handles encryption and decryption
  - Data Delivery
    - Modeled after Ethernet, higher layers must deal with detecting and correcting errors

Broadband Wireless

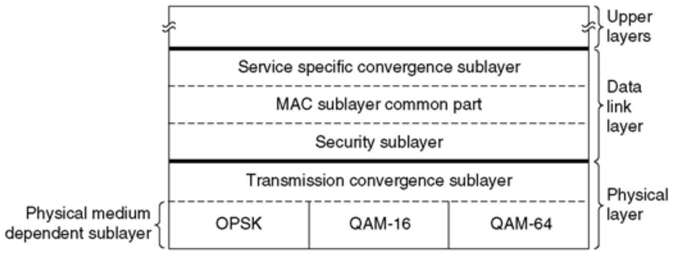
- Motivation – standardize wireless local loop
- Comparison of 802.11 and 802.16
- The 802.16 Protocol Stack
- The 802.16 Physical Layer
- The 802.16 MAC Sublayer Protocol
- The 802.16 Frame Structure

Comparison of 802.11 and 802.16

- Similarity – both are designed to provide high-bandwidth wireless communications
- Differences
  - 802.16 – provides service to buildings
    - Not mobile
    - Many computers
    - Can sustain higher cost => better radio
    - Uses full-duplex
    - Much longer distance, higher bandwidth, operates in 10-66 GHz ranges, quality of service
    - Directional
  - 802.11 - Mobile Ethernet

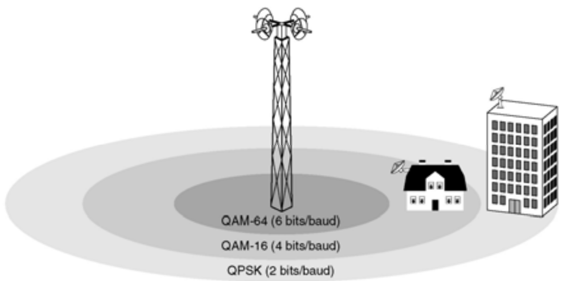
The 802.16 Protocol Stack

- The 802.16 Protocol Stack.



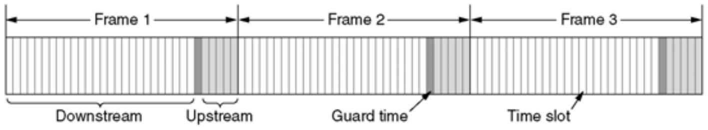
The 802.16 Physical Layer

- Uses millimeter waves, 10-66 GHz range
- Uses multiple antennas, each pointing at a different sector
- Bandwidth available is reduced for longer distances



The 802.16 Physical Layer

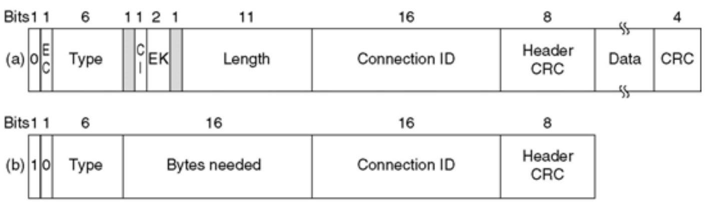
- Uses available spectrum efficiently
  - FDD – frequency division duplexing
  - TDD – time division duplexing
    - Downstream gets more time slots, base station in control
    - Can pack multiple MAC frames back-to-back in a single physical transmission
    - Uses Hamming codes to do forward error correction



The 802.16 MAC Sublayer Protocol

- Service Classes
  - Constant bit rate service
    - Bandwidth determined at connection time
  - Real-time variable bit rate service
    - Base station polls subscribers at fixed interval for bandwidth needed by each subscriber
  - Non-real-time variable bit rate service
    - Bases station polls often, but not with fixed interval
  - Best efforts service
    - No polling, subscribers of same class contend for bandwidth
- All services are connection-oriented

The 802.16 Frame Structure



(a) A generic frame. (b) A bandwidth request frame.