Data Link Layer


Reference: *Computer Networks: A Systems Approach*. Larry Peterson, Bruce Davie, Morgan Kaufmann
Introduction

• Hosts and routers: nodes
• Communication channels that connect adjacent nodes along communication path: links
  • Wired links
  • Wireless links
  • LANs
• Layer-2 packet: frame, encapsulates datagram

• Data-link layer has responsibility of transferring datagram from one node to physically adjacent node over a link
Introduction

• Datagram transferred by different link protocols over different links
  • Example: Ethernet on first link
    Frame relay on intermediate links
    802.11 on last link

• Each link protocol provides different services
  • Example: May or may not provide reliable data transfer over link
Link Layer Services

• Framing, link access
  • Encapsulate datagram into frame, adding header, trailer
  • Channel access if shared medium
  • MAC addresses used in frame headers to identify source, destination
    • Different from IP address!

• Reliable delivery between adjacent nodes
  • We learned how to do this already (chapter 3)!
  • Seldom used on low bit-error link (fiber, some twisted pair)
  • Wireless links: high error rates
    • Q: why both link-level and end-end reliability?
Link Layer Services

- **Flow control**
  - Pacing between adjacent sending and receiving nodes

- **Error detection**
  - Errors caused by signal attenuation, noise.
  - Receiver detects presence of errors:
    - Signals sender for retransmission or drops frame

- **Error correction**
  - Receiver identifies *and corrects* bit error(s) without resorting to retransmission

- **Half-duplex and full-duplex**
  - With half duplex, nodes at both ends of link can transmit, but not at same time
Implementation

• In each and every host
• Link layer implemented in adaptor (aka network interface card NIC) or on a chip
  • implements link, physical layer
    • Ethernet card
    • 802.11 card
    • Ethernet chipset
• Attaches into system buses of host
• Combination of hardware, software, firmware
Adaptors Communicating

- Sending side
  - Encapsulates datagram in frame
  - Adds error checking bits, rdt, flow control, etc.
- Receiving side
  - Looks for errors, reliable data transfer, flow control, etc.
  - Extracts datagram, passes to upper layer at receiving side
Link Layer

✓ Error detection, correction
• Multiple access protocols
• LANs
  • Addressing, ARP
  • Ethernet
  • Switches
  • VLANS
• Link virtualization: MPLS
• Data center networking
Error Detection

• EDC = Error Detection and Correction bits (redundancy)
• D = Data protected by error checking, may include header fields
• Error detection not 100% reliable!
  • Protocol may miss some errors, but rarely
  • Larger EDC field yields better detection and correction
Parity Checking

Single bit parity:
Detect single bit errors

Two-dimensional bit parity:
Detect and correct single bit errors

0111000110101011 0
Internet Checksum

**Goal:** Detect errors (e.g. flipped bits) in transmitted packet (note: used at transport layer only)

**Sender:**
- Treat segment contents as sequence of 16-bit integers
- Checksum: addition (1’s complement sum) of segment contents
- Sender puts checksum value into UDP checksum field
Cyclic Redundancy Check

- More powerful error-detection coding
- View data bits, $D$, as a binary number
- Choose $r+1$ bit pattern (generator), $G$
- Goal: choose $r$ CRC bits, $R$, such that
  - $\langle D, R \rangle$ exactly divisible by $G$ (modulo 2)
  - Receiver knows $G$, divides $\langle D, R \rangle$ by $G$. If non-zero remainder: error detected!
  - Can detect all burst errors less than $r+1$ bits
- Widely used in practice (Ethernet, 802.11 WiFi, ATM)
Example: CRC

Want: \( D.2^r \text{ XOR } R = nG \)

Equivalently: \( D.2^r = nG \text{ XOR } R \)

Equivalently: If we divide \( D.2^r \) by \( G \), want remainder \( R \) to satisfy:

\[
R = \text{ remainder} \left[ \frac{D.2^r}{G} \right]
\]
Link Layer

- Error detection, correction
  ✓ Multiple access protocols
- LANs
  - Addressing, ARP
  - Ethernet
  - Switches
  - VLANS
- Link virtualization: MPLS
- Data center networking
Multiple Access Links & Protocols

Two types of links

- Point-to-point
  - PPP for dial-up access
  - Point-to-point link between Ethernet switch, host
- Broadcast (shared wire or medium)
  - Old-fashioned Ethernet
  - Upstream HFC
  - 802.11 wireless LAN
Multiple Access Protocols

• Single shared broadcast channel
• Two or more simultaneous transmissions by nodes: interference
  • Collision if node receives two or more signals at the same time

Multiple access protocol
• Distributed algorithm that determines how nodes share channel
  i.e. determine when node can transmit
• Communication about channel sharing must use channel itself
  • No out-of-band channel for coordination
Ideal Multiple Access Protocol

**Given:** broadcast channel of rate $R$ bps

**Desiderata**

- When one node wants to transmit, it can send at rate $R$.
- When $M$ nodes want to transmit, each can send at average rate $R/M$
- Fully decentralized
  - No special node to coordinate transmissions
  - No synchronization of clocks, slots
- Simple
MAC Protocols: Taxonomy

Three broad classes

• **Channel partitioning**
  • Divide channel into smaller pieces (time slots, frequency, code)
  • Allocate piece to node for exclusive use

• **Random access**
  • Channel not divided, allow collisions
  • Recover from collisions

• **Taking turns**
  • Nodes take turns, but nodes with more to send can take longer turns
Channel Partitioning MAC Protocols: TDMA

TDMA: time division multiple access

• Access to channel in rounds
• Each station gets fixed length slot (length = packet transmission time) in each round
• Unused slots go idle
• Example: 6-station LAN, 1,3,4 have packets to send, slots 2,5,6 idle
Channel Partitioning MAC Protocols: FDMA

FDMA: frequency division multiple access

• Channel spectrum divided into frequency bands
• Each station assigned fixed frequency band
• Unused transmission time in frequency bands go idle
• Example: 6-station LAN, 1,3,4 have packet to send, frequency bands 2,5,6 idle
Random Access Protocols

• When node has packet to send
  • Transmit at full channel data rate R.
  • No a priori coordination among nodes

• Two or more transmitting nodes \(\rightarrow\) “collision”,

• Random access MAC protocol specifies:
  • How to detect collisions
  • How to recover from collisions (e.g., via delayed retransmissions)

• Examples of random access MAC protocols:
  • Slotted ALOHA
  • ALOHA
  • CSMA, CSMA/CD, CSMA/CA
Acknowledgements

• The following materials have been used in preparation of this slide set:

   7th Edition
   James Kurose, Keith Ross
   Pearson
   2016

   5th Edition
   Larry Peterson, Bruce Davie
   Morgan Kaufmann
   2011