Data-link Layer I

Dmitri Loguinov
Texas A&M University

April 24, 2024
Homework #4

- ICMP header:

```cpp
class ICMPHeader{
    public:
        u_char type; /* ICMP packet type */
        u_char code; /* ICMP type subcode */
        u_short checksum; /* checksum */
        u_short ID; /* usually process ID */
        u_short seq; /* sequence */
};
```

- Received ICMP pkts are delivered to all open ICMP sockets (since ICMP has no port numbers)
  - Routers will echo your entire IP packet in their TTL expired messages
  - Use the ID field to distinguish your pkts from junk
Homework #4

- TTL Expired pkt structure:

<table>
<thead>
<tr>
<th>Layer</th>
<th>Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP header (20 bytes)</td>
<td></td>
</tr>
<tr>
<td>ICMP reply header (8 bytes)</td>
<td></td>
</tr>
<tr>
<td>Original IP header (20 bytes)</td>
<td></td>
</tr>
<tr>
<td>Original ICMP header (8 bytes)</td>
<td></td>
</tr>
</tbody>
</table>

- Find out whether the ID field in the 4-th header matches your ID
Homework #4

• Other things to consider:
  – If your checksums are incorrect, the packet will likely be dropped and you won’t get a reply
  – If your firewall is enabled to block all incoming traffic, the kernel will not deliver ICMP packets

• In some Windows configurations, you must be admin to open ICMP sockets

• Mores caveats – read the handout!
  – UAC needs to be disabled or VS run as administrator
  – Custom in-bound firewall rules
  – Batch mode requires pinging the target before tracing
  – Hard limits on trace delay in batch mode
Link Layer

5.1 Introduction and services
5.2 Error detection and correction
5.3 Multiple access protocols
5.4 Link-Layer Addressing
5.5 Ethernet
5.6 Hubs and switches
Summary
**Link Layer: Introduction**

**Terminology:**
- Hosts and routers are **nodes**
- Communication channels that connect adjacent nodes are **layer-3 links**
  - Wired or wireless
- Each link may contain multiple layer-2 devices (e.g., switches)

*Data-link layer has responsibility of transferring IP datagram from one node to adjacent node over a single link.*
Link Layer Services

• Framing:
  – Add header, trailer to IP packet
  – Data-link addresses (completely independent of IP addresses) used in frame headers to identify source, dest

• Link access:
  – Channel access if shared medium

• Flow control:
  – Pacing between adjacent sending and receiving nodes

• Error detection:
  – Errors caused by signal attenuation, noise
  – Receiver detects presence of errors and signals data-link layer of adjacent node for retransmission or drops frame
**Link Layer Services**

- **Forward Error Correction (FEC):**
  - Receiver identifies *and corrects* bit error(s) without resorting to retransmission

- **Reliable delivery (rdt) between adjacent nodes**
  - Rdt 3.0 is a common technique (chapter 3)
  - Seldom used on low bit error links (fiber, twisted pair), but may be implemented in wireless networks

- **More terminology**
  - In *half-duplex* mode, nodes at both ends of link can transmit, but not at the same time
  - In *full-duplex*, bidirectional transfer happens concurrently
5.1 Introduction and services
5.2 Error detection and correction
5.3 Multiple access protocols
5.4 Link-Layer Addressing
5.5 Ethernet
5.6 Hubs and switches
Summary
Multiple Access Links and Protocols

Two types of links:

- **Point-to-point, e.g.:**
  - PPP for dial-up and DSL access
  - Dedicated cable between Ethernet switch and host

- **Broadcast (shared wire/medium):**
  - Traditional Ethernet
  - Upstream HFC (hybrid fiber coax)
  - 802.11 wireless LAN, satellite
Multiple Access Protocols

• Assume a single shared broadcast channel

• Two or more simultaneous transmissions by nodes is called interference or collision
  ▪ Receiver cannot discern packets when multiple signals are jammed together

Link access protocol

• Distributed algorithm that determines how nodes share channel

• Communication about channel sharing must use the channel itself!
  ▪ No out-of-band channel for coordination

• MAC (Media Access Control) layer = data-link layer = layer 2
Ideal Multiple Access Protocol

Desired properties

1. Single node can achieve full channel rate C (high utilization without competition)
2. When N nodes want to transmit, each can send at average rate C / N (fairness and high utilization during competition)
3. Fully decentralized:
   - No special node to coordinate transmissions
   - No synchronization of clocks
4. Simple
MAC Protocols: Taxonomy

Three broad classes:

- **Channel Partitioning**
  - Divide channel into smaller “pieces” (time slots, frequency, wavelengths)
  - 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 may take longer turns
TDMA: time division multiple access

- Access to channel in “rounds” (time frames)
  - Each station gets fixed length slot in each round (1/N of frame time to each node), unused slots go idle
- Example: 6-device LAN

- Maximum throughput for a single user is $C / N$, which is far from ideal!
**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-device LAN
Random Access Protocols

• When node has packet to send
  – Transmit at full channel data rate $C$
  – No \textit{a-priori} coordination among nodes

• Two or more transmitting nodes cause collision
  – All involved packets are useless, must be retransmitted

• \textbf{Random access MAC protocol} specifies:
  – How to detect collisions
  – How to recover from collisions (e.g., via delayed retransmission)

• \textbf{Examples of random access MAC protocols}:
  – Slotted ALOHA
  – CSMA, CSMA/CD