CSMC 417

Computer Networks
Prof. Ashok K Agrawala

© 2017  Ashok Agrawala
Set 4
The Data Link Layer
Chapter 3

- Data Link Layer Design Issues
- Error Detection and Correction
- Elementary Data Link Protocols
- Sliding Window Protocols
- Example Data Link Protocols

Revised: August 2011
The Data Link Layer

Responsible for delivering frames of information over a single link

- Handles transmission errors and regulates the flow of data
Data Link Layer Design Issues

- Frames
- Possible services
- Framing methods
- Error control
- Flow control
Frames

Link layer accepts packets from the network layer, and encapsulates them into frames that it sends using the physical layer; reception is the opposite process.
Functions of the Data Link Layer

• Provide service interface to the network layer
• Dealing with transmission errors
• Regulating data flow
  • Slow receivers not swamped by fast senders
Possible Services

Unacknowledged connectionless service
  - Frame is sent with no connection / error recovery
  - Ethernet is example

Acknowledged connectionless service
  - Frame is sent with retransmissions if needed
  - Example is 802.11

Acknowledged connection-oriented service
  - Connection is set up; rare
Services Provided to Network Layer

(a) Virtual communication.
(b) Actual communication.
Services Provided to Network Layer (2)
Framing Methods

- Byte count
- Flag bytes with byte stuffing
- Flag bits with bit stuffing
- Physical layer coding violations
  - Use non-data symbol to indicate frame
Framing – Bit Oriented

(a) 0 1 1 0 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 0 0 1 0

(b) 0 1 1 0 1 1 1 1 1 1 0 1 1 1 1 1 0 1 1 1 1 1 0 1 0 0 1 0

(c) 0 1 1 0 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 0 0 1 0

**Bit stuffing**

(a) The original data.
(b) The data as they appear on the line.
(c) The data as they are stored in receiver’s memory after destuffing.
Bit Oriented Protocols

- Frame – a collection of bits
  - No Byte boundary
- SDLC – Synchronous Data Link Control
  - IBM
- HDLC – High-Level Data Link Control
  - ISO Standard

HDLC Frame Format
Framing – Bit stuffing

Stuffing done at the bit level:

- Frame flag has six consecutive 1s (not shown)
- On transmit, after five 1s in the data, a 0 is added
- On receive

```
Data bits: 011011111111111111111010
```

```
Transmitted bits with stuffing: 01101111110111111110111111111010
```

```
Stuffed bits: 0110111111011111111011111111110110010
```
Framing

• Break sequence of bits into a frame
  – Typically implemented by the network adaptor

• Sentinel-based
  – Delineate frame with special pattern (e.g., 01111110)

  – Problem: what if special patterns occurs within frame?
  – Solution: escaping the special characters
    • E.g., sender always inserts a 0 after five 1s
    • ... and receiver always removes a 0 appearing after five 1s
    • Bit Stuffing

  – Similar to escaping special characters in C programs
Byte-Oriented Protocols

• Frame – a collection of bytes.

• Examples
  – BISYNC – Binary Synchronous Communication – IBM
  – DDCMP – Digital Data Communication Message Protocol
  – PPP – Point-to-Point

• Sentinel Based – Use special character as marker
  – BISYNC
    • SYN and SOH
    • STX and ETX
    • DLE as escape character. - Character Stuffing
Framing

(a) A frame delimited by flag bytes.

(b) Four examples of byte sequences before and after stuffing.
Frame Structure

PPP Frame Format

BISYNC Frame Format
Framing (Continued)

- **Counter-based**
  - Include the payload length in the header
  - ... instead of putting a sentinel at the end
  - Problem: what if the count field gets corrupted?
    - Causes receiver to think the frame ends at a different place
  - Solution: catch later when doing error detection
    - And wait for the next sentinel for the start of a new frame

![DDCMP Frame Format](image)
Framing

A character stream.

(a) Without errors.

(b) With one error.
Clock-Based Framing (SONET)

• Clock-based
  – Make each frame a fixed size
  – No ambiguity about start and end of frame
  – But, may be wasteful

• Synchronous Optical Network (SONET)
  – Slowest speed link STS-1 – 51.84 Mbps (810*8*8K)
  – Frame – 9 rows of 90 bytes
    • First 3 bytes of each row are overhead
    • First two bytes of a frame contain a special bit pattern – to mark the start of the frame – check for it every 810 bytes
Sonet Frame
Three STS-1 frames to one STS-3 frame
Flow Control

Prevents a fast sender from out-pacing a slow receiver

- Receiver gives feedback on the data it can accept
- Rare in the Link layer as NICs run at “wire speed”
  - Receiver can take data as fast as it can be sent

Flow control is a topic in the Link and Transport layers.
Sliding Window Protocols

- Sliding Window concept »
- One-bit Sliding Window »
- Go-Back-N »
- Selective Repeat »
Error Control

Error control repairs frames that are received in error

- Requires errors to be detected at the receiver
- Typically retransmit the unacknowledged frames
- Timer protects against lost acknowledgements

Detecting errors and retransmissions are next topics.
Error Detection and Correction

Error codes add structured redundancy to data so errors can be either detected, or corrected.

Error correction codes:

- Hamming codes
- Binary convolutional codes
- Reed-Solomon and Low-Density Parity Check codes
  - Mathematically complex, widely used in real systems

Error detection codes:

- Parity
- Checksums
- Cyclic redundancy codes
Error Detection

• Errors are unavoidable
  – Electrical interference, thermal noise, etc.

• Error detection
  – Transmit extra (redundant) information
  – Use redundant information to detect errors
  – Extreme case: send two copies of the data
  – Trade-off: accuracy vs. overhead

• Techniques for detecting errors
  – Parity checking
  – Checksum
  – Cyclic Redundancy Check (CRC)
Error Detection Techniques

• Parity check
  – Add an extra bit to a 7-bit code
  – Odd parity: ensure an odd number of 1s
    • E.g., 0101011 becomes 01010111
  – Even parity: ensure an even number of 1s
    • E.g., 0101011 becomes 01010110

• Two Dimensional Parity
Error Bounds – Hamming distance

Code turns data of $n$ bits into codewords of $n+k$ bits

Hamming distance is the minimum bit flips to turn one valid codeword into any other valid one.

- Example with 4 codewords of 10 bits ($n=2$, $k=8$):
  - 0000000000, 0000011111, 1111100000, and 1111111111
  - Hamming distance is 5

Bounds for a code with distance:
- $2d+1$ – can correct $d$ errors (e.g., 2 errors above)
- $d+1$ – can detect $d$ errors (e.g., 4 errors above)
Error Detection – Parity (1)

Parity bit is added as the modulo 2 sum of data bits
- Equivalent to XOR; this is even parity
- Ex: 1110000 $\rightarrow$ 11100001
- Detection checks if the sum is wrong (an error)

Simple way to detect an odd number of errors
- Ex: 1 error, 11100101; detected, sum is wrong
- Ex: 3 errors, 11011001; detected sum is wrong
- Ex: 2 errors, 11101101; not detected, sum is right!
- Error can also be in the parity bit itself
- Random errors are detected with probability $\frac{1}{2}$
Error Detection – Parity (2)

Interleaving of N parity bits detects burst errors up to N

- Each parity sum is made over non-adjacent bits
- An even burst of up to N errors will not cause it to fail
Two Dimensional Parity

![Two Dimensional Parity Diagram](image)
Error Detection – Checksums

Checksum treats data as N-bit words and adds N check bits that are the modulo $2^N$ sum of the words

- Ex: Internet 16-bit 1s complement checksum

Properties:

- Improved error detection over parity bits
- Detects bursts up to N errors
- Detects random errors with probability $\frac{1}{2^N}$
- Vulnerable to systematic errors, e.g., added zeros
Checksum

• Checksum
  – Treat data as a sequence of 16-bit words
  – Compute a sum of all the 16-bit words, with no carries
  – Transmit the sum along with the packet
Internet Checksum Algorithm

• Consider data as a sequence of 16-bit integers
• Add them together using 16-bit one’s complement arithmetic
• Take 1’s complement of the sum
• That is the checksum
Cyclic Redundancy Check

• Have to maximize the probability of detecting the errors using a small number of additional bits.
• Based on powerful mathematical formulations – theory of finite fields
• Consider \((n+1)\) bits as \(n\) degree polynomial
• Message \(M(x)\) represented as polynomial
• Divisor \(C(x)\) of degree \(k\)
• Send \(P(x)\) as \((n+1)\) bits +\(k\) bits such that \(P(x)\) is exactly divisible by \(C(x)\)

\[
C(x) = x^3 + x^2 + 1
\]

\[
M(x) = x^7 + x^4 + x^3 + x^1
\]
CRC Basis

• Use modulo 2 arithmetic
• Any Polynomial $B(x)$ can be divided by a divisor polynomial $C(x)$ if $B(x)$ is of higher degree than $C(x)$
• Any polynomial $B(x)$ can be divided once by a divisor polynomial $C(x)$ if they are of the same degree
• The remainder obtained when $B(x)$ is divided by $C(x)$ is obtained by subtracting $C(x)$ from $B(x)$
• To subtract $C(x)$ from $B(x)$ we simply perform the exclusive-OR operation on each pair of matching coefficients.
CRC Basis

1. Multiply $M(x)$ by $x^k$, i.e. add $k$ zeros at the end of the message. Call this $T(x)$
2. Divide $T(x)$ by $C(x)$
3. Subtract the remainder from $T(x)$

- Message sent – 1001101010 101
Cyclic Redundancy Check

• All single bit errors – if \( x^k \) and \( x^0 \) terms are nonzero
• All double-bit errors – as long as \( C(x) \) has a factor with at least three terms
• Any odd number of errors as long as \( C(x) \) has \( (x+1) \) as a factor
• Any burst error of length \( k \) bits
## Common CRC Polynomials

<table>
<thead>
<tr>
<th>CRC</th>
<th>C(x)</th>
</tr>
</thead>
<tbody>
<tr>
<td>CRC-8</td>
<td>$x^8 + x^2 + x^1 + 1$</td>
</tr>
<tr>
<td>CRC-10</td>
<td>$x^{10} + x^9 + x^5 + x^4 + x^1 + 1$</td>
</tr>
<tr>
<td>CRC-12</td>
<td>$x^{12} + x^{11} + x^3 + x^2 + 1$</td>
</tr>
<tr>
<td>CRC-16</td>
<td>$x^{16} + x^{15} + x^2 + 1$</td>
</tr>
<tr>
<td>CRC-CCITT</td>
<td>$x^{16} + x^{12} + x^5 + 1$</td>
</tr>
<tr>
<td>CRC-32</td>
<td>$x^{32} + x^{26} + x^{23} + x^{22} + x^{16} + x^{12} + x^{11} + x^{10} + x^8 + x^7 + x^5 + x^4 + x^2 + x^1 + 1$</td>
</tr>
</tbody>
</table>
Error Detection – CRCs (1)

- Adds bits so that transmitted frame viewed as a polynomial is evenly divisible

Start by adding 0s to frame and try dividing

Offset by any reminder to make it evenly divisible
Error Detection – CRCs (2)

Based on standard polynomials:

- Ex: Ethernet 32-bit CRC is defined by:
  \[ x^{32} + x^{26} + x^{23} + x^{22} + x^{16} + x^{12} + x^{11} + x^{10} + x^{8} + x^{7} + x^{5} + x^{4} + x^{2} + x^{1} + 1 \]

- Computed with simple shift/XOR circuits

Stronger detection than checksums:

- E.g., can detect all double bit errors
- Not vulnerable to systematic errors
Error Correction – Hamming code

Hamming code gives a simple way to add check bits and correct up to a single bit error:

- Check bits are parity over subsets of the codeword
- Recomputing the parity sums (syndrome) gives the position of the error to flip, or 0 if there is no error

(11, 7) Hamming code adds 4 check bits and can correct 1 error
Error-Correcting Codes

Use of a Hamming code to correct burst errors.

<table>
<thead>
<tr>
<th>Char.</th>
<th>ASCII</th>
<th>Check bits</th>
</tr>
</thead>
<tbody>
<tr>
<td>H</td>
<td>1001000</td>
<td>001100010000</td>
</tr>
<tr>
<td>a</td>
<td>1100001</td>
<td>101110010001</td>
</tr>
<tr>
<td>m</td>
<td>1101101</td>
<td>1110101010101</td>
</tr>
<tr>
<td>m</td>
<td>1101101</td>
<td>1110101010101</td>
</tr>
<tr>
<td>i</td>
<td>1101001</td>
<td>01101011001</td>
</tr>
<tr>
<td>n</td>
<td>1101110</td>
<td>01101010110</td>
</tr>
<tr>
<td>g</td>
<td>1100111</td>
<td>01111001111</td>
</tr>
<tr>
<td>c</td>
<td>0100000</td>
<td>10011000000</td>
</tr>
<tr>
<td>o</td>
<td>1100011</td>
<td>11111000011</td>
</tr>
<tr>
<td>d</td>
<td>1100100</td>
<td>11111001110</td>
</tr>
<tr>
<td>e</td>
<td>1100101</td>
<td>00111000101</td>
</tr>
</tbody>
</table>

Order of bit transmission
Error Correction – Convolutional codes

Operates on a stream of bits, keeping internal state

- Output stream is a function of all preceding input bits
- Bits are decoded with the Viterbi algorithm

Popular NASA binary convolutional code (rate = $\frac{1}{2}$) used in 802.11
Link-Layer Services

- **Encoding**
  - Representing the 0s and 1s

- **Framing**
  - Encapsulating packet into frame, adding header, trailer
  - Using MAC addresses, rather than IP addresses

- **Error detection**
  - Errors caused by signal attenuation, noise.
  - Receiver detecting presence of errors

- **Error correction**
  - Receiver correcting errors without retransmission

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

- Link layer implemented in adaptor (network interface card)
  - Ethernet card, PCMCI card, 802.11 card

- Sending side:
  - Encapsulates datagram in a frame
  - Adds error checking bits, flow control, etc.

- Receiving side
  - Looks for errors, flow control, etc.
  - Extracts datagram and passes to receiving node
Elementary Data Link Protocols

- Link layer environment »
- Utopian Simplex Protocol »
- Stop-and-Wait Protocol for Error-free channel »
- Stop-and-Wait Protocol for Noisy channel »
Link layer environment (1)

Commonly implemented as NICs and OS drivers: network layer (IP) is often OS
Link layer environment (2)

- Link layer protocol implementations use library functions
  - See code (protocol.h) for more details

<table>
<thead>
<tr>
<th>Group</th>
<th>Library Function</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network layer</td>
<td>from_network_layer(&amp;packet)</td>
<td>Take a packet from network layer to send</td>
</tr>
<tr>
<td></td>
<td>to_network_layer(&amp;packet)</td>
<td>Deliver a received packet to network layer</td>
</tr>
<tr>
<td></td>
<td>enable_network_layer()</td>
<td>Let network cause “ready” events</td>
</tr>
<tr>
<td></td>
<td>disable_network_layer()</td>
<td>Prevent network “ready” events</td>
</tr>
<tr>
<td>Physical layer</td>
<td>from_physical_layer(&amp;frame)</td>
<td>Get an incoming frame from physical layer</td>
</tr>
<tr>
<td></td>
<td>to_physical_layer(&amp;frame)</td>
<td>Pass an outgoing frame to physical layer</td>
</tr>
<tr>
<td>Events &amp; timers</td>
<td>wait_for_event(&amp;event)</td>
<td>Wait for a packet / frame / timer event</td>
</tr>
<tr>
<td></td>
<td>start_timer(seq_nr)</td>
<td>Start a countdown timer running</td>
</tr>
<tr>
<td></td>
<td>stop_timer(seq_nr)</td>
<td>Stop a countdown timer from running</td>
</tr>
<tr>
<td></td>
<td>start_ack_timer()</td>
<td>Start the ACK countdown timer running</td>
</tr>
<tr>
<td></td>
<td>stop_ack_timer()</td>
<td>Stop the ACK countdown timer</td>
</tr>
</tbody>
</table>
Protocol Definitions

#define MAX_PKT 1024
/* determines packet size in bytes */
typedef enum {false, true} boolean;
/* boolean type */
typedef unsigned int seq_nr;
/* sequence or ack numbers */
typedef struct {unsigned char data[MAX_PKT];} packet;
/* packet definition */
typedef enum {data, ack, nak} frame_kind;
/* frame_kind definition */
typedef struct {
    frame_kind kind;
    seq_nr seq;
    seq_nr ack;
    packet info;
} frame;
/* frames are transported in this layer */
/* what kind of a frame is it? */
/* sequence number */
/* acknowledgement number */
/* the network layer packet */

Continued →

Some definitions needed in the protocols to follow.
These are located in the file protocol.h.
Protocol Definitions (ctd.)

Some definitions needed in the protocols to follow. These are located in the file protocol.h.
**Utopian Simplex Protocol**

An optimistic protocol (p1) to get us started

- Assumes no errors, and receiver as fast as sender
- Considers one-way data transfer

```c
void sender1(void)
{
    frame s;
    packet buffer;

    while (true) {
        from_network_layer(&buffer);
        s.info = buffer;
        to_physical_layer(&s);
    }
}
```

```c
void receiver1(void)
{
    frame r;
    event_type event;

    while (true) {
        wait_for_event(&event);
        from_physical_layer(&r);
        to_network_layer(r.info);
    }
}
```

Sender loops blasting frames

- That’s it, no error or flow control ...

Receiver loops eating frames
Flow Control
Reliable Transmission

• Transfer frames without errors
  – Error Correction
  – Error Detection
  – Discard frames with error
• Acknowledgements and Timeouts
• Retransmission
• ARQ – Automatic Repeat Request
Stop and Wait with 1-bit Seq No
Stop and Wait Protocols

• Simple
• Low Throughput
  – One Frame per RTT
• Increase throughput by having more frames in flight
  – Sliding Window Protocol
Stop and Wait

Duplicate Frames
Stop and Wait Protocol

- http://www.cs.stir.ac.uk/~kjt/software/comms/jasper/ABP.html
- http://www.cs.stir.ac.uk/~kjt/software/comms/jasper/ABRA.html
Stop-and-Wait – Error-free channel

Protocol (p2) ensures sender can’t outpace receiver:

- Receiver returns a dummy frame (ack) when ready
- Only one frame out at a time – called stop-and-wait
- We added flow control!

```c
void sender2(void)
{
    frame s;
    packet buffer;
    event_type event;

    while (true) {
        from_network_layer(&buffer);
        s.info = buffer;
        to_physical_layer(&s);
        wait_for_event(&event);
    }
}
```

```c
void receiver2(void)
{
    frame r, s;
    event_type event;
    while (true) {
        wait_for_event(&event);
        from_physical_layer(&r);
        to_network_layer(&r.info);
        to_physical_layer(&s);
    }
}
```

Sender waits to for ack after passing frame to physical layer

Receiver sends ack after passing frame to network layer
ARQ (Automatic Repeat reQuest) adds error control
- Receiver acks frames that are correctly delivered
- Sender sets timer and resends frame if no ack

For correctness, frames and acks must be numbered
- Else receiver can’t tell retransmission (due to lost ack or early timer) from new frame
- For stop-and-wait, 2 numbers (1 bit) are sufficient
Stop-and-Wait – Noisy channel (2)

Sender loop (p3):

Send frame (or retransmission)
Set timer for retransmission
Wait for ack or timeout

If a good ack then set up for the next frame to send (else the old frame will be retransmitted)
Stop-and-Wait – Noisy channel (3)

Receiver loop (p3):

- Wait for a frame
- If it’s new then take it and advance expected frame
- Ack current frame
Example Data Link Protocols

- Packet over SONET
- PPP (Point-to-Point Protocol)
- ADSL (Asymmetric Digital Subscriber Loop)
Packet over SONET

Packet over SONET is the method used to carry IP packets over SONET optical fiber links

- Uses PPP (Point-to-Point Protocol) for framing

![Diagram showing protocol stacks and PPP frames over SONET payloads]
Packet over SONET (1)

Packet over SONET. (a) A protocol stack. (b)
Packet over SONET (2)

PPP Features
1. Separate packets, error detection
2. Link Control Protocol
3. Network Control Protocol
PPP (1)

PPP (Point-to-Point Protocol) is a general method for delivering packets across links

- Framing uses a flag (0x7E) and byte stuffing
- “Unnumbered mode” (connectionless unacknowledged service) is used to carry IP packets
- Errors are detected with a checksum

<table>
<thead>
<tr>
<th>Bytes</th>
<th>1</th>
<th>1</th>
<th>1</th>
<th>1 or 2</th>
<th>Variable</th>
<th>2 or 4</th>
<th>1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Flag</td>
<td>01111110</td>
<td>Address</td>
<td>11111111</td>
<td>Control</td>
<td>00000011</td>
<td>Protocol</td>
<td>Payload</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>0x21</td>
<td>for IPv4</td>
<td>IP packet</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
A link control protocol brings the PPP link up and down
## PPP – Point to Point Protocol (3)

<table>
<thead>
<tr>
<th>Name</th>
<th>Direction</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure-request</td>
<td>I → R</td>
<td>List of proposed options and values</td>
</tr>
<tr>
<td>Configure-ack</td>
<td>I ← R</td>
<td>All options are accepted</td>
</tr>
<tr>
<td>Configure-nak</td>
<td>I ← R</td>
<td>Some options are not accepted</td>
</tr>
<tr>
<td>Configure-reject</td>
<td>I ← R</td>
<td>Some options are not negotiable</td>
</tr>
<tr>
<td>Terminate-request</td>
<td>I → R</td>
<td>Request to shut the line down</td>
</tr>
<tr>
<td>Terminate-ack</td>
<td>I ← R</td>
<td>OK, line shut down</td>
</tr>
<tr>
<td>Code-reject</td>
<td>I ← R</td>
<td>Unknown request received</td>
</tr>
<tr>
<td>Protocol-reject</td>
<td>I ← R</td>
<td>Unknown protocol requested</td>
</tr>
<tr>
<td>Echo-request</td>
<td>I → R</td>
<td>Please send this frame back</td>
</tr>
<tr>
<td>Echo-reply</td>
<td>I ← R</td>
<td>Here is the frame back</td>
</tr>
<tr>
<td>Discard-request</td>
<td>I → R</td>
<td>Just discard this frame (for testing)</td>
</tr>
</tbody>
</table>
ADSL (1)

Widely used for broadband Internet over local loops

- ADSL runs from modem (customer) to DSLAM
PPP data is sent in AAL5 frames over ATM cells:

- ATM is a link layer that uses short, fixed-size cells (53 bytes); each cell has a virtual circuit identifier.

AAL5 frame is divided into 48 byte pieces, each of which goes into one ATM cell with 5 header bytes.
High-Level Data Link Control

Frame format for bit-oriented protocols.

<table>
<thead>
<tr>
<th>Bits</th>
<th>8</th>
<th>8</th>
<th>8</th>
<th>≥0</th>
<th>16</th>
<th>8</th>
</tr>
</thead>
<tbody>
<tr>
<td>011111110</td>
<td>Address</td>
<td>Control</td>
<td>Data</td>
<td>Checksum</td>
<td>011111110</td>
<td></td>
</tr>
</tbody>
</table>
High-Level Data Link Control (2)

Control field of
(a) An information frame.
(b) A supervisory frame.
(c) An unnumbered frame.
The Data Link Layer in the Internet

User's home

PC

Client process using TCP/IP

Modem

Internet provider's office

Modems

Dial-up telephone line

TCP/IP connection using PPP

Router

Routing process
End

Chapter 3