Chapter 3: Data Link Layer

Raj Jain

Raj Jain is now at
Washington University in Saint Louis
Jain@cse.wustl.edu
http://www.cse.wustl.edu/~jain/

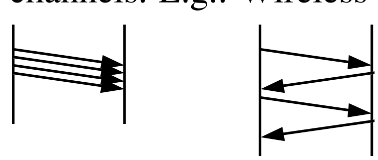
- Datalink layer design issues
- Error detection and correction
- Simple datalink protocols
- Sliding window protocols
- Example datalink protocols

Data Link Layer Design Issues

- Services provided to the Network Layer
- Framing
- Error Control
- Flow Control

Datalink Layer Services

- Unacknowledged connectionless service
  - No acks, no connection
  - Error recovery up to higher layers
  - For low error-rate links or voice traffic
- Acknowledged connectionless service
  - Acks improve reliability
  - For unreliable channels. E.g.: Wireless Systems



Datalink Services (Cont)

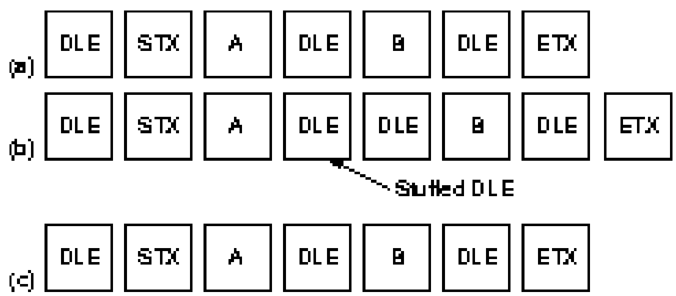
- Acknowledged connection-oriented service
  - Equivalent of reliable bit-stream
  - Connection establishment
  - Packets Delivered In-Order
  - Connection Release
  - Inter-Router Traffic

Framing

- Framing = How to break a bit-stream into frames
- Need for framing: Error Detection/Control work on chunks and not on bit streams of data
- Framing methods:
  - Timing : risky. No network guarantees.
  - Character count: may be garbled by errors
  - Character stuffing: Delimit frame with special characters
  - Bit stuffing: delimit frame with bit pattern
  - Physical layer coding violations

Character Stuffing

- Delimit with DLE STX or DLE ETX character flags
- Insert 'DLE' before accidental 'DLE' in data
- Remove stuffed character at destination

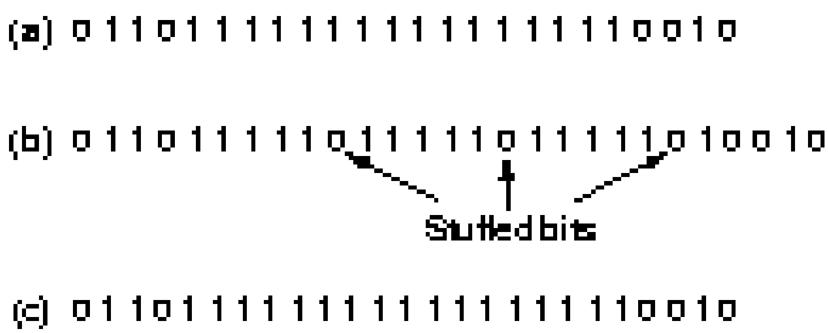


The Ohio State University | Fig 3-4 | Raj Jain

7

Bit Stuffing

- Delimit with special bit pattern (bit flags)
- Stuff bits if pattern appears in data
- Remove stuffed bits at destination



The Ohio State University | Fig 3-5 | Raj Jain

8

Physical Coding Violations

- On networks having coding redundancy on physical medium

The Ohio State University Raj Jain

9

Error Control

- Error Control = Deliver frames without error, in the proper order to network layer
- Error control Mechanisms:
  - Ack/Nak: Provide sender some feedback about other end
  - Time-out: for the case when entire packet or ack is lost
  - Sequence numbers: to distinguish retransmissions from originals

The Ohio State University Raj Jain

10

Flow Control

- Flow Control = Sender does not flood the receiver, but maximizes throughput
- Sender throttled until receiver grants permission

Error Detection and Correction

- Transmission errors: common on local loops, wireless links
- Single bit-errors vs Burst Errors
- n-bit codeword = m message bits + r check bits
- Hamming Distance = number of bit positions in which two code words differ
- Distance D code = minimum hamming distance between any two code words written in the code
- To detect d errors, distance d+1 code required
- To correct d errors, distance 2d+1 code required

Error-Correcting Codes

- Enough redundant information in a frame to detect and correct the error
- Lower limit on number of check bits to correct 1 error: $(m+r+1) <= 2^r$
- Hamming's method: (corrects 1-bit errors)
  - Bit positions in powers of 2 (1,2,4 ...) = check bits
  - Other bit positions data
  - Every bit included in several parity computations (See text)

Burst Error Correction

- Arrange code words as matrix
- Transmit one column at a time
- Uses kr check bits to immunize blocks of km data bits to single burst error of length k or less

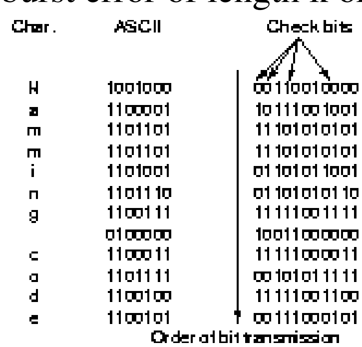


Fig 3-6

Error-Detecting Codes

- Enough redundant information in a frame to detect error
- Request retransmission from source to correct the error
- Parity checks
- Cyclic Redundancy Code (CRC) checks

Check Digit Method

- Make number divisible by 9

Example: 823 is to be sent

1. Left-shift: 8230
2. Divide by 9, find remainder: 4
3. Subtract remainder from 9: 9-4=5
4. Add the result of step 5 to step 1: 8235
5. Check that the result is divisible by 9.

Detects all single-digit errors: 7235, 8335, 8255, 8237

Detects several multiple-digit errors: 8765, 7346

Does not detect some errors: 7335, 8775, ...

Modulo 2 Arithmetic

```
  1111     11001          1100
 +1010   ×    11     11  | 10101
 -----   --------        / 11
  0101     11001          ----
          11001            x11
          ---------         11
          101011           ----
                            x00
                             00
                            ----     010   2
                             x01     011   3
                              00     ----  --
                             ----    001   1  Mod 2
                              x1     101   5  Binary
```


Cyclic Redundancy Check (CRC)

- **Binary Check Digit Method**
- Make number divisible by P=110101 (n+1=6 bits)

Example: M=1010001101 is to be sent

1. Left-shift M by n bits 2^nM= 101000110100000
2. Divide 2^nM by P, find remainder: R=01110
3. Subtract remainder from P
4. Add the result of step 2 to step 1 : T=101000110101110
5. Check that the result T is divisible by P.

Modulo 2 Division

```
             Q=1101010110
P=110101)101000110100000=2^nM
                 110101
                  111011
                  110101
                   011101
                   000000
                    111010
                    110101
                     011111
                     000000
                      111110
                      110101
                       010110
                       000000
                        101100
                        110101
                         110010
                         110101
                          001110
                          000000
                           01110 = R
```


Checking At The Receiver

```
         1101010110
110101)101000110101110
         110101
          111011
          110101
           011101
           000000
            111010
            110101
             011111
             000000
              111110
              110101
               010111
               000000
                101111
                110101
                 110101
                 110101
                  00000
```

Polynomial Representation

- Number the bits 0, 1, ..., from <u>right</u>
  $b_n b_{n-1} b_{n-2} \ldots b_3 b_2 b_1 b_0$
  $b_n x^n + b_{n-1} x^{n-1} + b_{n-2} x^{n-2} + \ldots + b_3 x^3 + b_2 x^2 + b_1 x + b_0$
- Example:
  543210
  ↓↓↓↓↓
  $110101 = x^5+x^4+x^2+1$
  $1101\ 1001\ 0011 = x^{11}+x^{10}+x^8+x^7+x^4+x+1$
  11 10 9 8 1 0

The Ohio State University Raj Jain

21

Cyclic Redundancy Check (CRC)

Polynomial Division Method

Make $T(x)$ divisible by $P(x) = x^5+x^4+x^2+1$ (Note: n=5)

Example: M=1010001101 is to be sent
$M(x) = x^9+x^7+x^3+x^2+1$

1. Multiply M(x) by x^n, $x^nM(x) = x^{14}+x^{12}+x^8+x^7+x^5+$ ....
2. Divide $x^nM(x)$ by $P(x)$, find remainder:
   $R(x)$=01110=x^3+x^2+x

The Ohio State University Raj Jain

22

CRC (Cont)

- 3. Add the remainder $R(x)$ to $x^nM(x)$:
  $T(x)= x^{14}+x^{12}+x^8+x^7+x^5+x^3+x^2+x$
- 4. Check that the result $T(x)$ is divisible by $P(x)$.
- Transmit the bit pattern corresponding to $T(x)$:
  101000110101110

The Ohio State University Raj Jain

23

Popular CRC Polynomials

- CRC-12: $x^{12}+x^{11}+x^3+x^2+x+1$
- CRC-16: $x^{16}+x^{15}+x^2+1$
- CRC-CCITT: $x^{16}+x^{12}+x^5+1$
- CRC-32: Ethernet, FDDI, ...
  $x^{32}+x^{26}+x^{23}+x^{22}+x^{16}+x^{12}+x^{11}$
  $+x^{10}+x^8+x^7+x^5+x^4+x^2+x+1$

Even number of terms in the polynomial
⇒ Polynomial is divisible by 1+x
⇒ Will detect all odd number of bit errors

The Ohio State University Raj Jain

24

Errors Detected by CRC

- All single bit errors
- Any burst error of length n bits or less, n=degree of the polynomial
- Most larger burst errors P(undetected burst errors|error has occurred) = 2^{-n}
- Any odd number of errors if P(x) has 1+x as a factor, i.e., has even number of terms
- Any double bit errors as long as P(x) has a factor with 3 terms, e.g., $(1+x^4+x^9)(....)$

Elementary Data Link Protocols

- Unrestricted Simplex Protocol
  - Framing only
  - No error or flow control
- Simplex Stop-and-Wait
  - Send one packet
  - Wait for Ack before proceeding

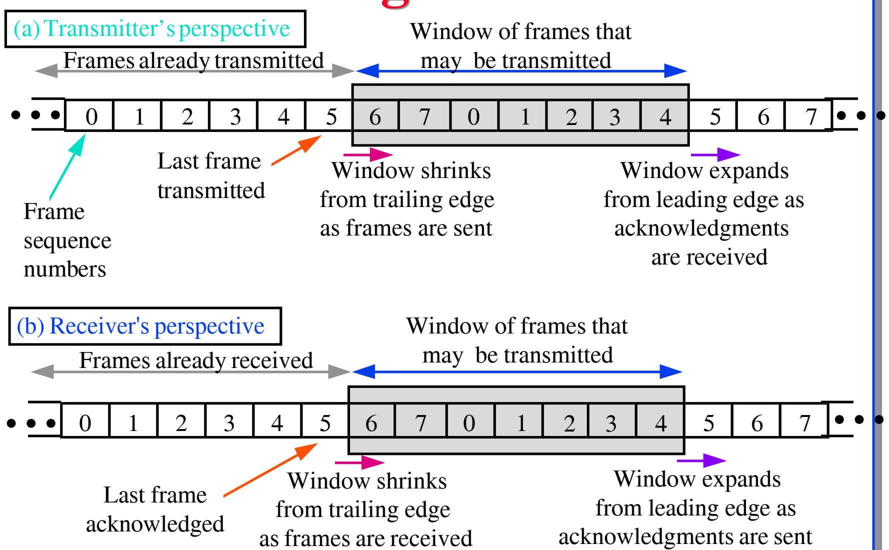
Elementary Datalinks (Cont)

- Simplex Protocol for a Noisy Channel
  - Automatic Repeat request (ARQ) protocols
  - Positive Ack
  - 1-bit sequence number in frames (not in acks)
  - Timeout to detect lost frames/acks
  - Retransmission
  - Can fail under early timeout conditions
- Full Duplex Communication
  - Piggybacking of acks

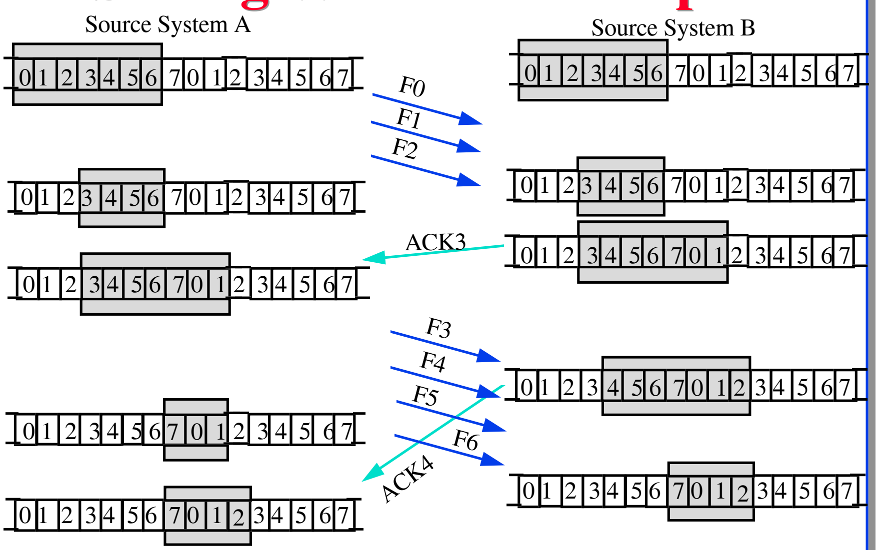
Sliding Window Protocols

- Window = Set of sequence numbers to send/receive
- Sender window
  - Sender window increases when ack received
  - Packets in sender window must be buffered at source
  - Sender window may grow in some protocols

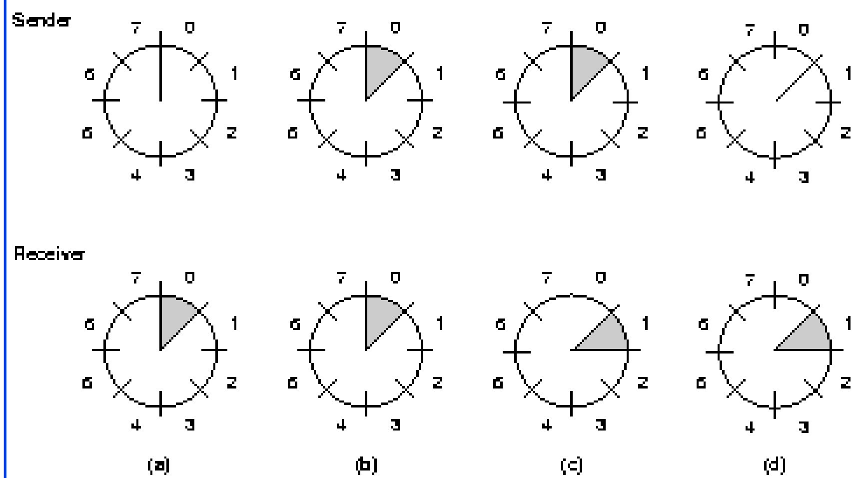
Sliding Window



Sliding Window: Example



Sliding Window: Example



Sliding Window (Cont)

- Receiver window
  - Packets outside window discarded
  - Window advances when sequence number = low edge of window received
  - Receiver window always constant
- Sender transmits W frames before blocking (pipelining)

One-Bit Sliding Window

- Stop and Wait + error control
- Piggybacked acks
- Acks sent instantly
- Packets may be resent to accommodate immediate piggybacking
- Acks contain sequence number
- Peculiar case: when both sides start simultaneously

One-Bit: Example

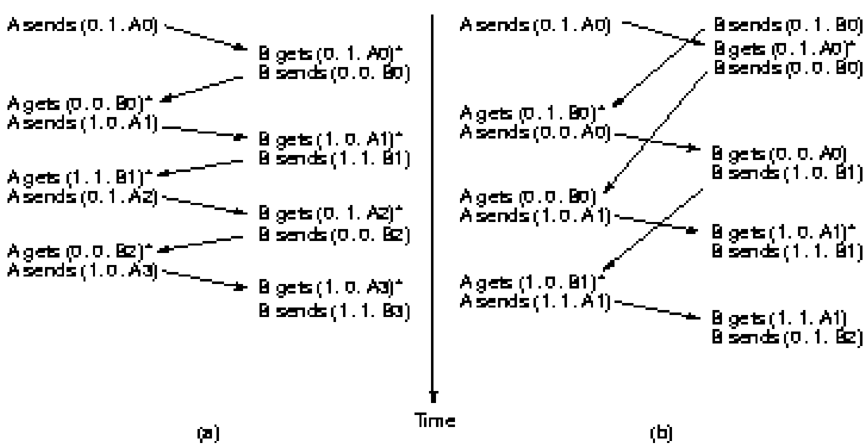


Fig 3-14

Go Back n

- Round trip propagation + transmission time not negligible
- Stop and Wait not efficient
- Sliding Window + Retransmit all packets starting from earliest unacked packet
- Acks are cumulative
- Ack the latest packet (N) if all packets (< N) are received.
- Can waste a lot of bandwidth if error rate high

Go Back n: Example

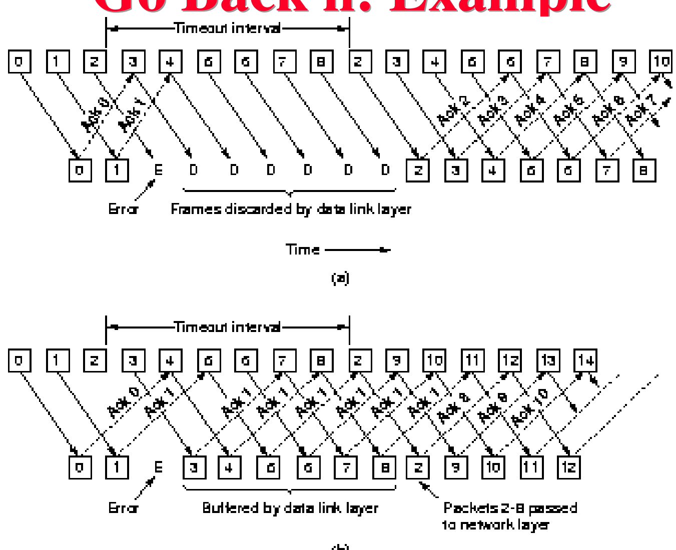


Fig 3-15

Go Back n (Cont)

- Out-of-order buffering not mandatory at destination
- Maximum Window = Sequence Number Space - 1
- N timers or 1 timer may be used

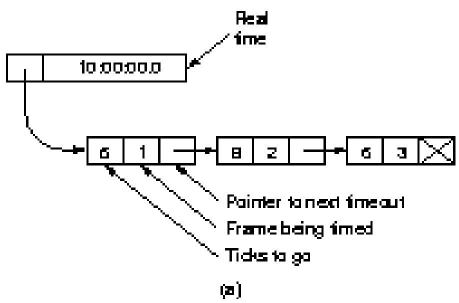


Fig 3-17

Selective Repeat

- Sliding Window + Retransmit just the bad frame when Nak received
- Out-of-order buffering required at destination
- Loses time (and hence throughput) if bursty loss of frames
- Acks not cumulative.
- Non-sequential arrival of packets
  $\Rightarrow$ ensure no overlap with old window when receiver advances window
  $\Rightarrow$ Maximum Window = (Sequence Number Space)/2

Selective Repeat: Example

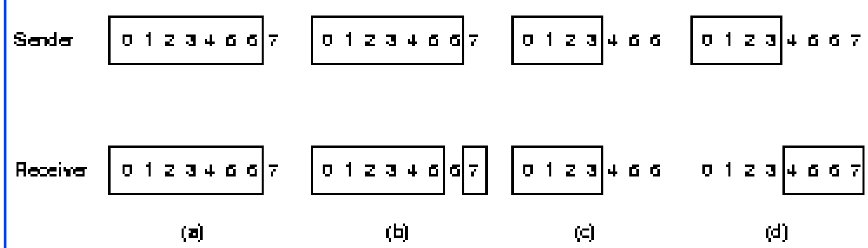


Fig 3-19

Selective Repeat (Cont)

- Enhancement to piggybacking
  - Auxiliary Ack timer
  - Set timer when packet to be acked is received
  - If no reverse data, generate Ack when timer goes off
- Send negative ack (Nak) when out-of-order frame received
  - Source retransmits Nak'ed frame
  - Naks not cumulative
  - Do not send duplicate Nak

Example Data link Protocols

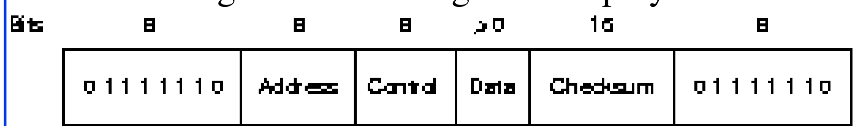
- HDLC
- SLIP
- PPP
- ATM

HDLC Family

- Synchronous Data Link Control (SDLC): IBM
- High-Level Data Link Control (HDLC): ISO
- Link Access Procedure-Balanced (LAPB): X.25
- Link Access Procedure for the D channel (LAPD): ISDN
- Link Access Procedure for modems (LAPM): V.42
- Link Access Procedure for half-duplex links (LAPX): Teletex
- Point-to-Point Protocol (PPP): Internet
- Logical Link Control (LLC): IEEE
- Advanced Data Communications Control Procedures (ADCCP): ANSI
- V.120 and Frame relay also use HDLC

HDLC

- High-level Data Link Control
- Bit-oriented, bit-stuffing for transparency
- Control field for seq numbers, acks etc
- Data field arbitrarily long (practical limits: checksum efficiency)
- CRC using CRC-CCITT generator polynomial



HDLC Frame Types

- Information, Supervisory, Unnumbered frames
- Sliding window with 3-bit sequence number, piggybacked acks
- Connection Management through supervisory frames

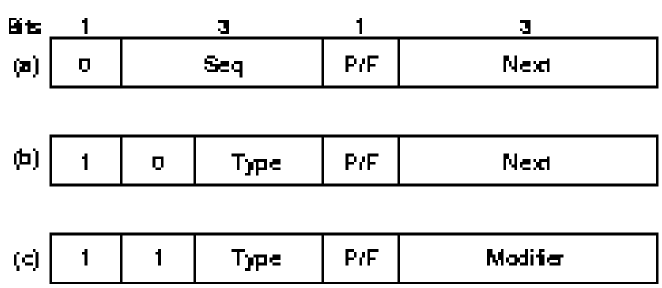


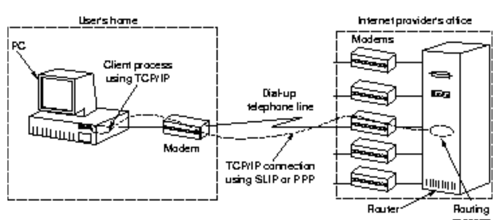
Fig 3-25

HDLC Frames

- Information Frames: User data
  - Piggybacked Acks: Next frame expected
  - Poll/Final = Command/Response
- Supervisory Frames: Flow and error control
  - Go back N and Selective Reject
  - Final ⇒ No more data to send
- Unnumbered Frames: Control
  - Mode setting commands and responses
  - Information transfer commands and responses
  - Recovery commands and responses
  - Miscellaneous commands and responses

Data Link Layer in the Internet

- Point-to-Point link scenarios
- Router-router leased line (PPP)
- dial-up host-router connection (SLIP, future PPP)
- SLIP: Not an approved Internet Standard
  ⇒ incompatibilities
- PPP: Official Internet Standard.



SLIP: Serial Line IP

- For dial-up lines. Reference: RFC 1055 and 1144.
- Raw IP packets + Character flags + Character stuffing
- Later versions: header compression

SLIP Problems

- No error detection or correction
- Supports only IP
  - Each side must know other's IP address in advance
    ⇒ dynamic IP address assignment not possible
    ⇒ Issue because of shortage of IP addresses
- No authentication ⇒ you do not know whom you are dialing up to

PPP

- Point to Point Protocols
- Reference: RFCs 1661, 1662 1663
- Frame method to unambiguously delineate frames and for error control
- Link Control Protocol(LCP): link management
- Network Control Protocol (NCP): Supports multiple network layers

The Ohio State University Raj Jain

49

PPP Frames

Bytes	1	1	1	1 or 2	Variable	2 or 4	1
	Flag 01111110	Address 11111111	Control 00000011	Protocol	Payload	Checksum	Flag 01111110

- Resembles HDLC, but character-oriented
- (The HDLC flag 01111110 is considered as a character and stuffed)
- PPP can run over dial-up lines, SONET lines, or bit-oriented HDLC (inter-router) lines

The Ohio State University Raj Jain

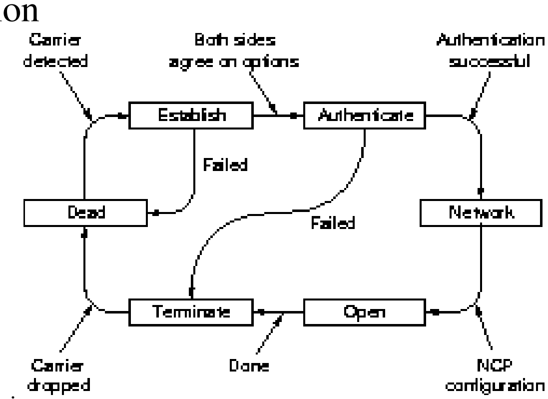
50

PPP Procedures

- Connection setup:
  - Home PC Modem calls Internet Provider's router: sets up physical link
  - PC sends series of LCP packets as PPP payload
    - Select PPP (data link) parameters
    - Authenticate
  - PC sends series of NCP packets as PPP payload
    - Select network parameters
    - E.g., Get dynamic IP address

PPP Procedures (Cont)

- Connection Teardown:
  - NCP first followed by LCP and physical connection



ATM Cell Transmission

- Lines assumed reliable
- Lightweight data links:
  minimum error checking, no flow control
- Data link functionality
  = Transmission convergence (TC) sublayer

HEC

- Header Error Control
- Corrects 1-bit errors
- No checksum for payload
- ATM designed for fiber: highly reliable, 99.64% errors are 1-bit errors
- Reliable data link
  $\Rightarrow$ EX-OR a sequence of cells and
  reconstruct up to 1 lost/garbled cell at destination

ATM on Synchronous medium

- Transmit cells according to predefined timing pattern
- Generate idle cell if no data cell available
- Operation and Management (OAM) cells: Used by ATM switches to exchange control information
- Mappings from ATM to other systems (T1, T3, FDDI exist)

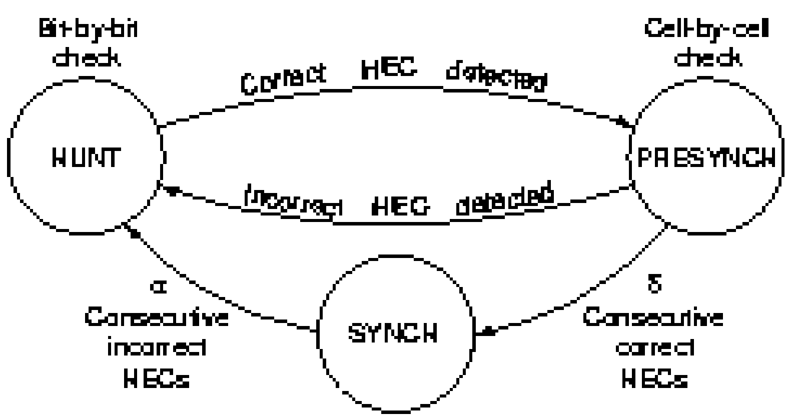
ATM Cell Reception

- Problem: Finding Cell boundaries in the some bit streams
- No flags like HDLC
- Trick: receiver layer looks for HEC
- E.g., Use 40 bit shift register

ATM Reception (Cont)

- HEC = last 8 bits computed over first 32 bits
- Accuracy limited since HEC small
- Improve accuracy with finite state machine
- HUNT, PRESYNCH and SYNCH states
- Verify guess about HEC
- Check 424 bits ahead to see if HEC test passes again
- Repeat check δ times
- If not synchronized, discard cell and resynchronize

Cell Delineation



Summary

- Function: Convert raw bit stream to frame stream
- Framing methods
- Error and Flow Control: Sliding Window
- HDLC, SLIP, PPP, ATM Data Link

Homework

- Read sections complete chapter 3 except 3.5
- Exercises: 2, 9, 19, 25