Encoding, Framing, Error Detection

Reference:

Peterson and Davie, "Computer Networks: A Systems Approach", 4th Edition, Morgan Kaufmann, 2007

Network Links

- Different physical media are used to propagate signals, full duplex links are usually used in switched networks
- Twisted pair
  - e.g. telephone wire
- Coaxial cable
  - E.g. TV cable
- Optical fiber
  - for long distance, high speed communication
- Wireless link
  - Terrestrial radio channels (wireless LAN, wide area celluar access)
  - Satellite radio channels

Features of Cables/Fibers

cable	Bandwidth (Mbps)	distance
category 5 twisted pair	10-100	100 m
thin coax	10-100	200 m
thick coax	10-100	500 m
multimode fiber	100	2 km
single-mode fiber	1-10Gbps and more	40 km

Leased Links

- DS and OC links
  - DS: Digital Signal hierarchy
    - DS0: 64kbps telephone signal
    - DS1, DS3 – See table in next slide
  - OC: Optical Carrier hierarchy
    - Based on SONET (synchronous optical network), TDM
    - STS: synchronous transport signal (name in electrical domain); OC: optical carrier (name in optical domain)
    - OC1, OC3, OC-12… See table in next slide
  - Provide dedicated bandwidth
  - Connect any arbitrary pair of nodes
  - Expensive

Leased links from the Phone Company

STS: Synchronous Transport Signal

Connection	Bandwidth
DS1 (T1)	1.544 Mbps
DS3 (T3)	44.736 Mbps
STS1 (OC1)	51.84 Mbps
STS3 (OC3)	155.52 Mbps
STS12 (OC12)	622.08 Mbps
STS24 (OC24)	1.24416 Gbps
STS48 (OC48)	2.48832 Gbps
STS192 (OC192)	9.95328 Gbps
STS768 (OC768)	39.81312 Gbps

OC: Optical Carrier

Last Mile Links

- To connect home to Internet
- Last hop (or first hop) of the network to reach home/office users
- Inexpensive
- Cannot connect arbitrary pair of nodes

- access networks (Refer Lecture notes 1 for more details)
  - xDSL (Digital Subscriber Line)
    - High speed transmission over Twisted pair copper (Telephone network)
  - ADSL (Asymmetric DSL)

  - Cable MODEM
    - Uses cable TV channel for data transmission
  - Optical access networks, passive optical networks (PONs)
    - Ethernet PON (EPON), GPON (Gigabit PON)

Bandwidth (Hz) vs. Channel Capacity (bps)

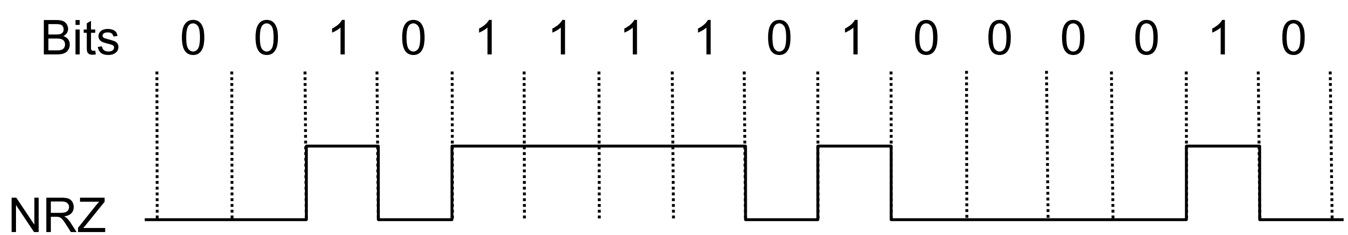
- Shannon's capacity theorem
- B = 3300-300 = 3000 Hz (phone link, voice signal)
  - $C = B \log_2(1+S/N)$
  - C: channel capacity, B: bandwidth
  - S/N: Signal-to-Noise ratio (measured in dB)
- Typical decibel ratio for S/N is 30 dB
  - $dB = 10 \log_{10}(S/N)$
  - $30 \text{ dB} \Rightarrow S/N = 1000$
- $C = 3000 \times \log_2(1001) \approx 30$ Kbps

Encoding

- This topic is left as self study.
- It is not examinable.
- You can skip slides 8-14

What is Encoding?

- Signals propagate over a physical medium
  - modulate electromagnetic waves
  - e.g., vary voltage
- Encode binary data onto signals
  - e.g., 0 as low signal and 1 as high signal
  - known as Non-Return to zero (NRZ)



Problem: Consecutive 1s or 0s

- Low signal (0) may be interpreted as no signal
- Baseline wander problem
  - Usually the receiver keeps the average value of the signal to distinguish low and high signals
  - Long sequence of 1s or 0s can change the average
- Unable to recover clock

Why Transitions are necessary?

- Receiver can recover clock and synchronize with the detected transition
- Absence of transitions may imply that some error has occurred, thus aiding error detection
- An encoding scheme must ensure that sufficient number of transitions take place and at the same time keeping the signal/modulation rate (baud rate) close to the data rate (bit rate)
- Signal rate: the rate at which signal elements are transmitted

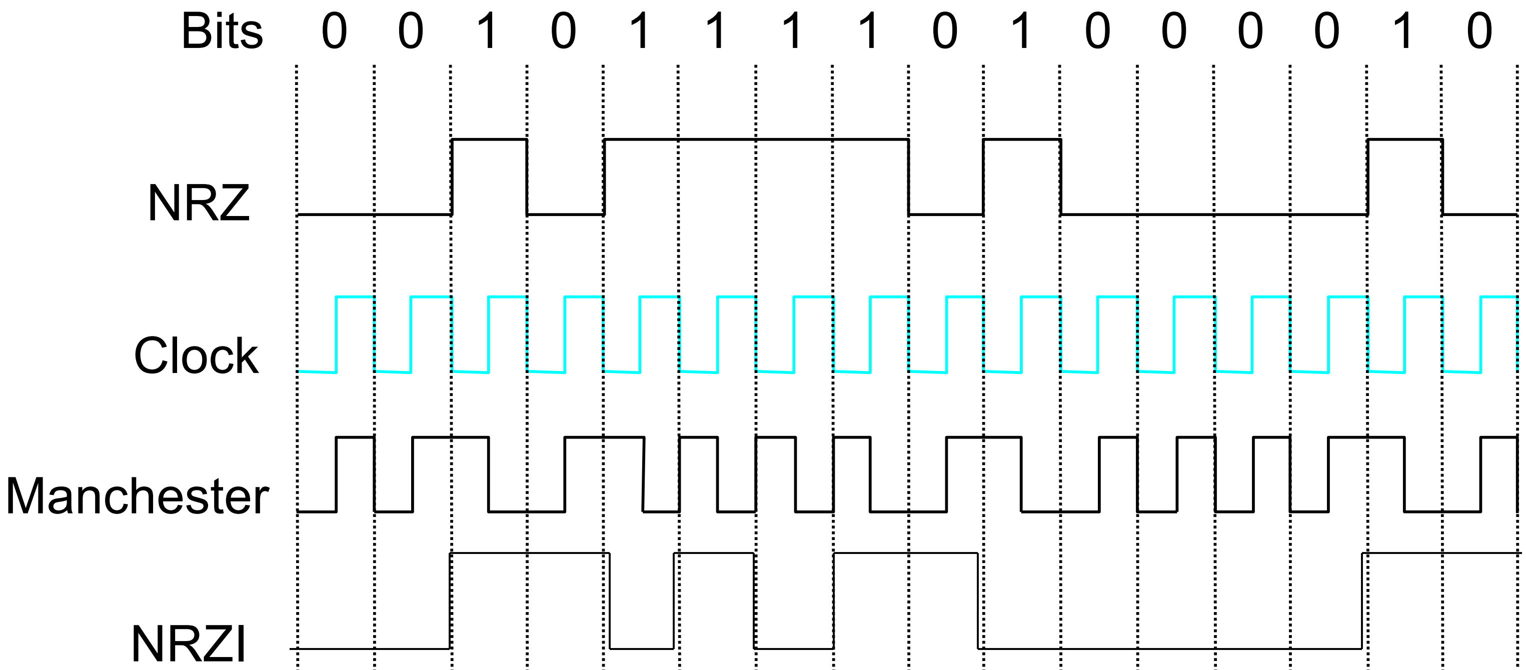
Alternative Encoding Techniques

- Non-return to Zero Inverted (on 1's) (NRZI)
  - make a transition from current signal to encode a one; stay at current signal to encode a zero
  - solves the problem of consecutive ones
  - Used in digital magnetic recording and signal transmission from terminals to computers
- Manchester
  - Low-to-high transition to encode a 0 and high-to-low transition to encode a 1
  - Used in LANs (e.g. Ethernet)
  - only 50% efficient (data rate/signal rate)

Encoding Techniques (cont)

- 4B/5B
  - every 4 bits of data encoded in a 5-bit code
  - 5-bit codes selected to have no more than one leading 0 and no more than two trailing 0s
  - thus, never get more than three consecutive 0s
  - 1000 mapped to 10010, 11111 signifies that line is idle (special symbol); mapping is predefined
  - resulting 5-bit codes are transmitted using NRZI
  - achieves 80% efficiency
  - Used for long distance communication (eg. FDDI)
  - FDDI: Fiber Distributed Data Interface used in MANs

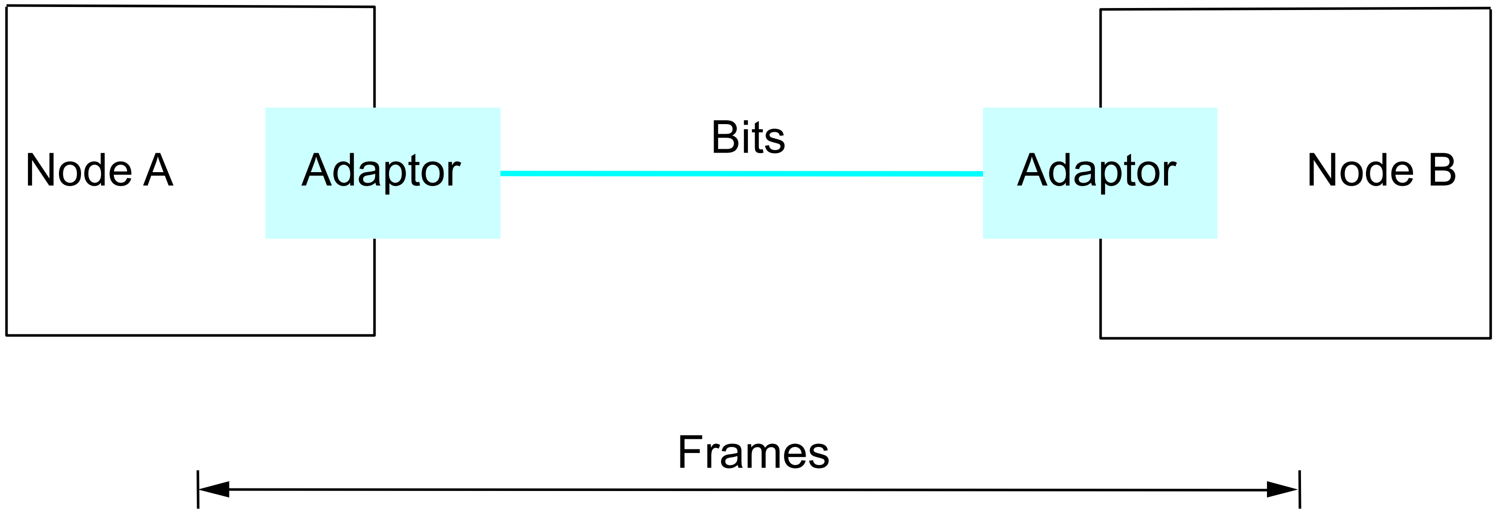
Encoding Techniques (cont.)



Framing

What is Framing?

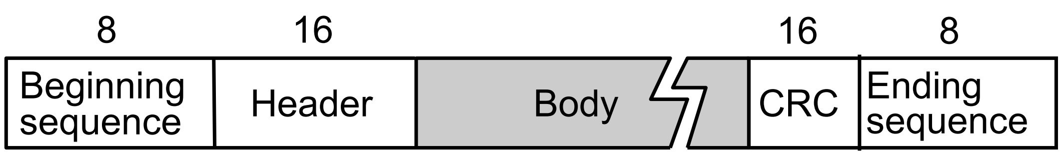
- Break sequence of bits into a frame
  - How do we recognize that this group of bits form a frame
- Typically implemented by network adaptor
- Data link layer function (Layer 2)



Framing Approaches

- How is a frame recognized?
- Sentinel-based

  delineate frame with special pattern: 01111110 (flag)
  - e.g., HDLC (high-level data link control protocol), PPP (point-to-point protocol)



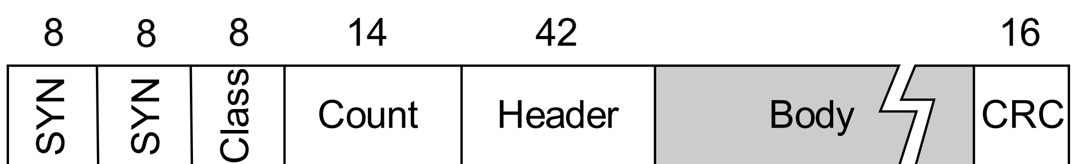
  - HDLC is an important, widely-used ISO-OSI standard data link protocol
    - Basis for other data link control protocols such as LLC (logical link control), frame relay, and ATM
  - problem: special pattern appears in the payload
  - solution: *bit stuffing* (HDLC)
    - sender: insert 0 after five consecutive 1s
    - receiver: remove 0 that follows five consecutive 1s

Byte Stuffing in PPP

- Widely used as a data link control to connect a PC to ISP using dialup modem and a telephone line
- Can also be used as a data link control to connect two routers
- Can operate over ADSL, SONET links etc.
- As in HDLC, a frame is delineated with the special pattern: 01111110 (7E hex) (referred to as flag)
- An integer number of bytes are carried. Byte stuffing is used.
- Byte 7D (hex) is used as escape character
- Sender
  - Replace flag (7E) or escape byte (7D) by two bytes. The first byte is the escape byte (7D) and the second byte is the one obtained by exclusive-or-ing the original byte and 20 (hex). i.e. 7D is replaced by 7D 5D, 7E is replaced by 7D 5E
- Receiver
  - When 7D is received, remove it, and exclusive-or the next byte with 20 (hex)
- Example
  - Original data: 57 8A 7E 0F 7D 17
  - Data sent after byte stuffing and framing: 7E 57 8A 7D 5E 0F 7D 5D 17 7E

Approaches (contd.)

- Counter-based (Eg: DDCMP, Ethernet)
  - include payload length in header (count field)
  - eDDCMP (Digital Data Communication Message Protocol)



  - Count: no of bytes in “Body”; receiver uses count value to decide the bytes to be received/accumulated to form a frame
  - problem: count field corrupted
    - Count value may decrease or increase
  - solution: catch when CRC fails, wait for SYN
  - The above frame error can cause back-to-back frames to be incorrectly received (Example scenario?)

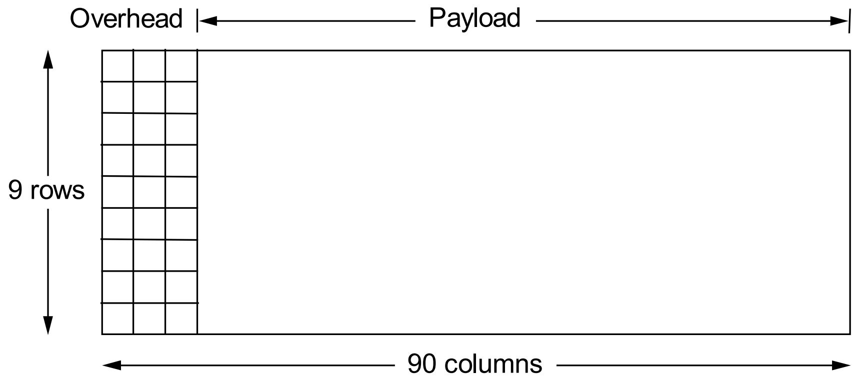
Approaches (contd.)

Clock-based

- e.g., SONET: Synchronous Optical Network; SDH: Synchronous Digital Hierarchy; they are similar
- each frame is 125μs long
- Looks for special bit pattern (2 Byte) for every 125μs. all bits received during this 125μs constitute one frame
- STS-1: 810 bytes (6480 bits) per 125μs = 51.84 Mbps
  - STS: synchronous transport signal (name in electrical domain); OC: optical carrier (name in optical domain)
  - STS-n: synchronous transport signal level n
  - STS-1 frame has 3 bytes overhead per row
  - 2 bytes of overhead is a special pattern to indicate the start of a frame
  - No bit stuffing used, looks for special bit pattern for every 810 bytes
- STS-*n carries n STS-1 frames*
- STS-3, 3×810=2430 bytes in 125μs implies rate = 3×51.84=155.52Mbps
- Multiplexing is by byte interleaving
- OC-n (optical carrier level n): STS-n in optical domain
- Refer table for SONET/SDH rates

SONET STS-1 Frame

STS-1 Frame



SONET/SDH Line Rates

SONET		Optical Carrier	Line rate (Mbps)
STS-1		OC-1	51.84
STS-3		OC-3	155.52
STS-12		OC-12	622.08
STS-48		OC-48	2488.32
STS-192		OC-192	9953.28

Higher line rates have been evolving: OC-768, OC-1920, …

Error Detection

Error detection on a link

- Consider a link connecting a sender and receiver
- Sender sends a data frame with n bits
- Bits may be corrupted during propagation on the link
- Receiver needs a mechanism to verify if all the bits are received correctly without any error
  - Error detection mechanism takes data bits as input and outputs "yes" or "no"

Cyclic Redundancy Check (CRC)

- Add k bits of redundant data to an n-bit message
  - want $k << n$
  - e.g., $k = 32$ and $n = 12{,}000$ (1500 bytes), Ethernet
- K-bit binary number is calculated as a remainder obtained as a result of division involving message bits and a divisor (known to sender and receiver)
  - Division has equivalent procedure in polynomial theory
- Represent n-bit message as n-1 degree polynomial
  - e.g., n=8, degree=7, maximum 8 terms
  - MSG=10011010 as $M(x) = x^7 + x^4 + x^3 + x^1$
- Let k be the degree of some divisor polynomial (generator polynomial)
  - e.g., k=3, maximum four terms.
  - $C(x) = x^3 + x^2 + 1$ (known to sender and receiver)

An Analogy for CRC – Simplified Example

- Sender and receiver agree on using a divisor (eg: 5)
- Msg: 27; remainder 2 when msg is divided by the divisor
- Sender sends <27,2> to receiver through a link (channel)
- Receiver receives <x,y>; calculates reminder r from x/5 and checks if r is equal to y
  - Case 1: <27,2> implies no error, error detection successful
  - Case 2: <26,2> implies error; error is detected
  - Case 3: <37,2> implies no error, but there is an error; so error undetected; why? The error value 10 is divisible by the divisor 5
- Note: Checking if remainder(x/5) is equal to y is the same as checking if remainder ([x-y]/5) is 0. (receiver can use division this way)
- The analogy is to illustrate the idea behind CRC (but not same)
  - CRC is more capable (stronger error detection), more complex
  - CRC uses polynomial equivalent of msg, divisor, divisions to use proven theory for strong error detection

CRC (contd.)

- **Sender:** Transmit polynomial $P(x)$ that is evenly divisible by $C(x)$ (divisor or generator polynomial, degree k) for a given message $M(x)$
  - shift left k bits, i.e., $M(x)x^k = T(x) =$ *message bits followed by k 0's*
  - subtract remainder $R(x)$ of $[T(x) / C(x)]$ from $T(x)$ to get $P(x)$
    - *P(x) is M(x) appended by R(x) (Note: R(x) is a k bit remainder*
  - Receiver polynomial $P(x) + E(x)$
    - E(x) is an error polynomial which corrupts 0 or more bits during signal propagation
  - $E(x) = 0$ implies no errors
  - Modulo-2 arithmetic, i.e., binary addition with no carry is used
    - 1+1=0; 1-1=0;1+0=1;0-1=1 (resembles XOR operation)

- **Receiver: Divide ($P(x)$ + $E(x)$) by $C(x)$; remainder zero only if:**
  - $E(x)$ was zero (no error), or
  - $E(x)$ is exactly divisible by $C(x)$ (error goes undetected in this case)

- Receiver divides whatever it has received (including the k remainder bits) by the divisor polynomial. If the remainder is not zero, the error is detected. If the remainder is zero, either there is no error or the error is undetected.

CRC Calculation – An Example

```
          1 1 0 1 0 1 1 1
        ___________________
1 1 0 1 | 1 0 1 0 0 1 1 0 0 0 0
          1 1 0 1
          -------
            1 1 1 0
            1 1 0 1
            -------
                1 1 1 1
                1 1 0 1
                -------
                    1 0 0 0
                    1 1 0 1
                    -------
                      1 0 1 0
                      1 1 0 1
                      -------
                        1 1 1 0
                        1 1 0 1
                        -------
                          0 1 1
```

k = 3, n = 8

M = 1 0 1 0 0 1 1 0

C = 1 1 0 1 (degree k=3)

T = M appended by k 0's = 1 0 1 0 0 1 1 0 0 0 0

R = 0 1 1 (k bit remainder)

P = T-R=1 0 1 0 0 1 1 0 0 1 1

P = T-R= the same as T appended by R

Note: with modulo-2 arithmetic T-R is the same as T+R

Selecting $C(x)$

- All single-bit errors can be detected as long as x^k and x^0 terms have non-zero coefficients.
- Any odd number of errors can be detected as long as $C(x)$ contains the factor $(x + 1)$
- Any 'burst' error (i.e., sequence of consecutive error bits) for which the length of the burst is less than or equal to k bits can be detected
- Most burst errors of larger than k bits can also be detected
- CRC-8, CRC-10, CRC-12, CRC-16, CRC-32
  - CRC-N: a polynomial with degree N. i.e. Divisor C has N+1 bits; remainder R has N bits
  - These CRC- polynomials are generally given in books
  - Ethernet uses CRC-32 (32 bit long; poly with degree 32, $x^{32}+\ldots+1$)