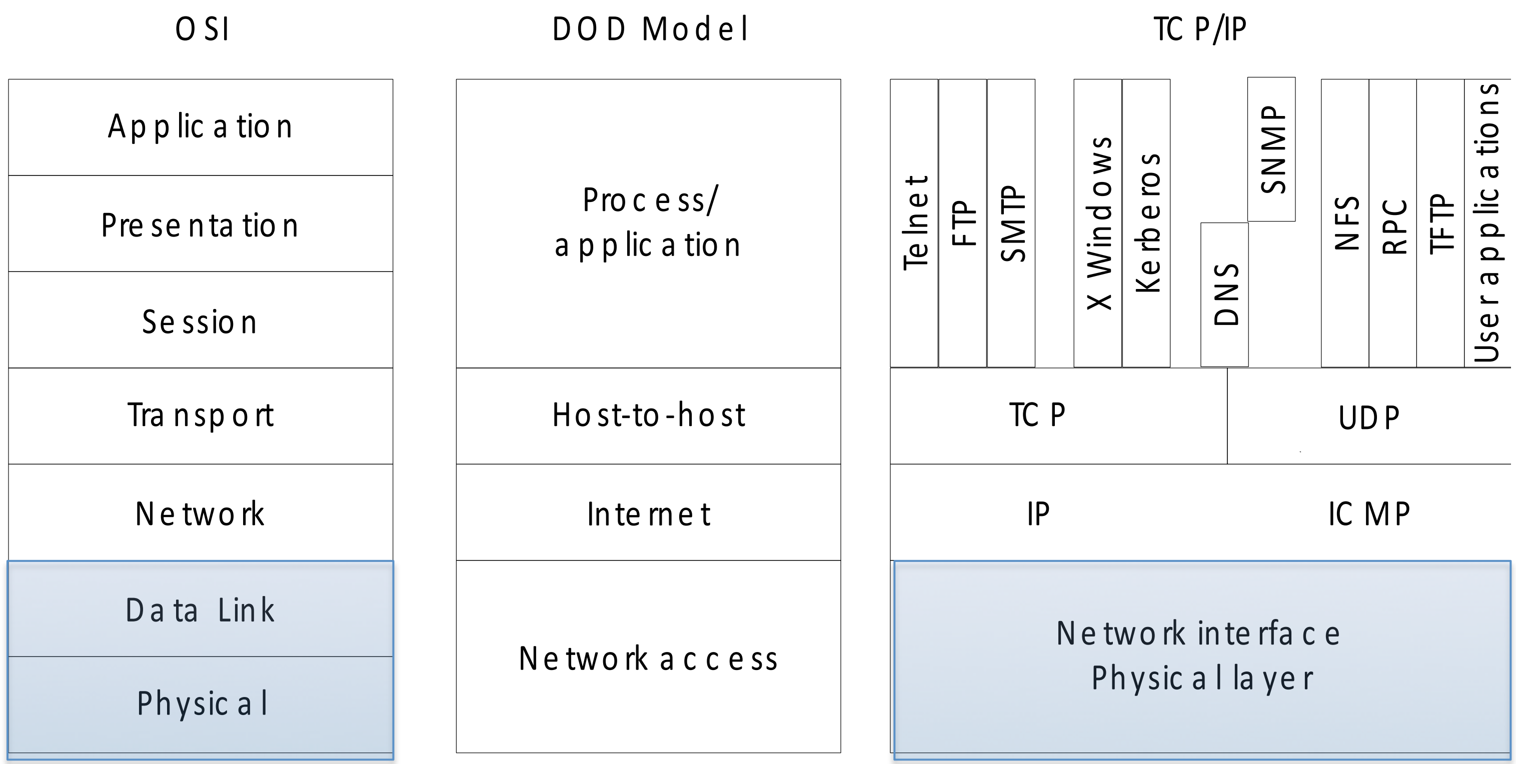
Computer Network

Getting Connected

How TCP/IP Corresponds to OSI



Problems

- In Chapter 1 we saw networks consists of links interconnecting nodes.
  - How to connect two nodes together?
- Concept of “cloud”
  - How to connect a host to a cloud?

Chapter Outline

- Perspectives on Connecting nodes
- Encoding **Physical Layer**
- Framing **Data Link Layer**
- Error Detection **Data Link Layer**
- Reliable Transmission **Data Link Layer** **Stop & Wait Protocol ACK once**
- Ethernet and Multiple Access Networks **Data Link Layer**

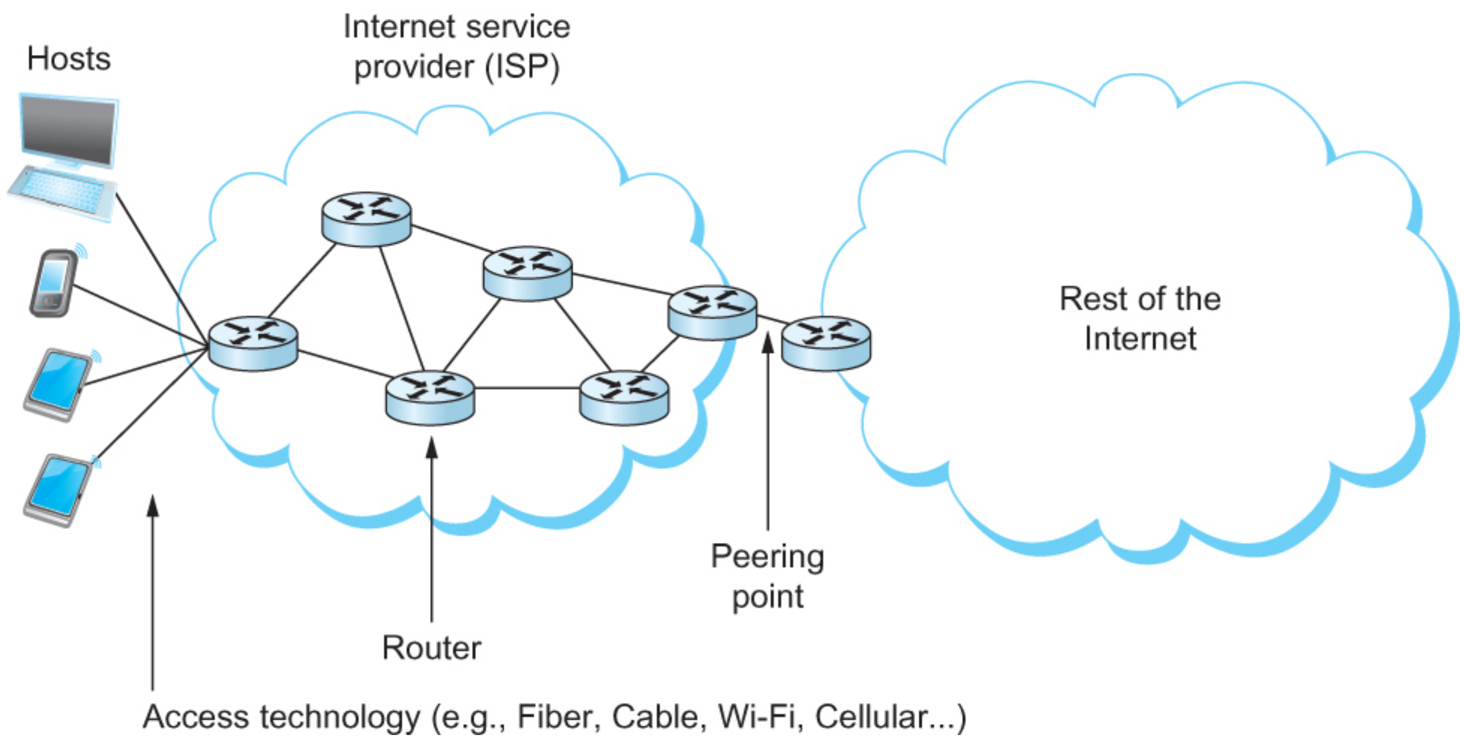
Chapter Goal

- Exploring different communication medium over which we can send data
- Understanding the issue of encoding bits onto transmission medium so that they can be understood by the receiving end
- Discussing the matter of delineating the sequence of bits transmitted over the link into complete messages that can be delivered to the end node (framing problem)
- Discussing different technique to detect transmission errors and take the appropriate action

Chapter Goal (contd.)

- Discussing the issue of making the links reliable in spite of transmission problems (reliable delivery) – Error Detection
- Introducing Media Access Control Protocols
  - PPP (point-to-point protocol)
  - Carrier Sense Multiple Access with Collision Detection (CSMA/CD)
    - Ethernet uses CSMA/CD

Perspectives on Connecting



An end-user's view of the Internet

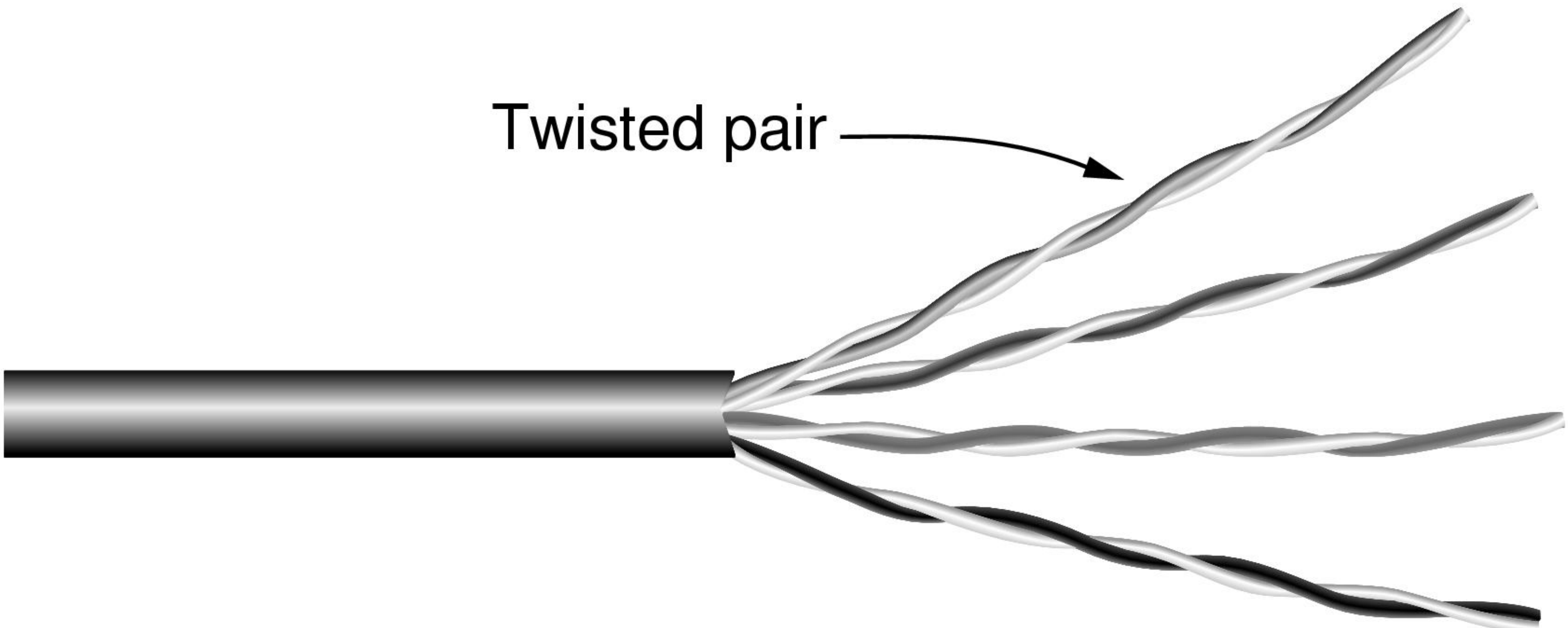
OSI Reference Model

OSI Layer	Function
Application	User interface, communication apps
Presentation	Character sets, encryption, compression
Session	Maintain connection, login, upper layer errors
Transport	Other (guaranteed delivery)
Network	Network ID, routing
Data Link	Access control, data flow, framing, device ID, error detection
Physical	Electrical & physical interface, topology, encoding

Physical Connection (Link)

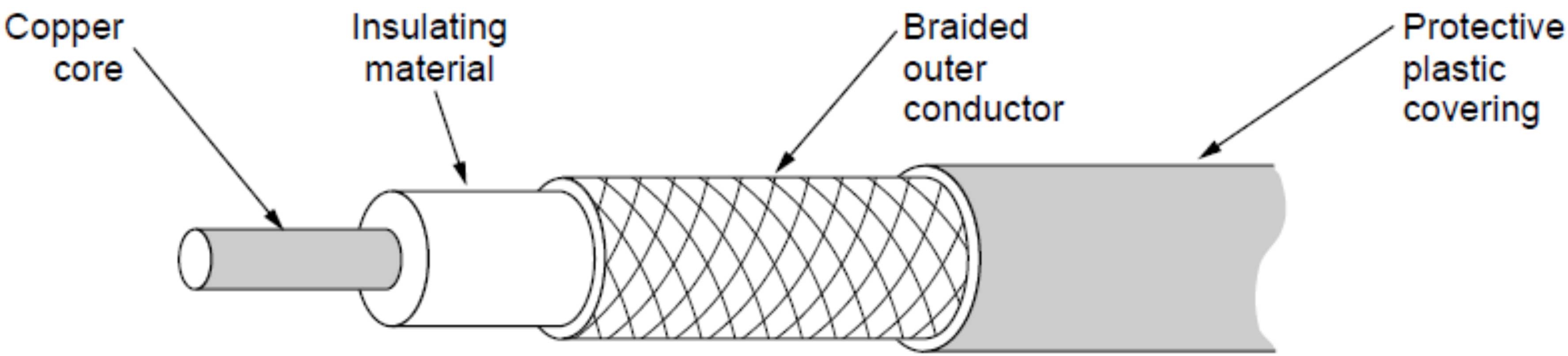
- Typically copper wire in some form
  - Twisted-pair (DSL Point-to-Point)
  - Coaxial cable (Ethernet Multi Access)
- Optical fiber
  - Commercial fiber-to-the home services
  - Many long-distance links in the Internet’s backbone
- Air/free space (for wireless links)

Twisted Pairs



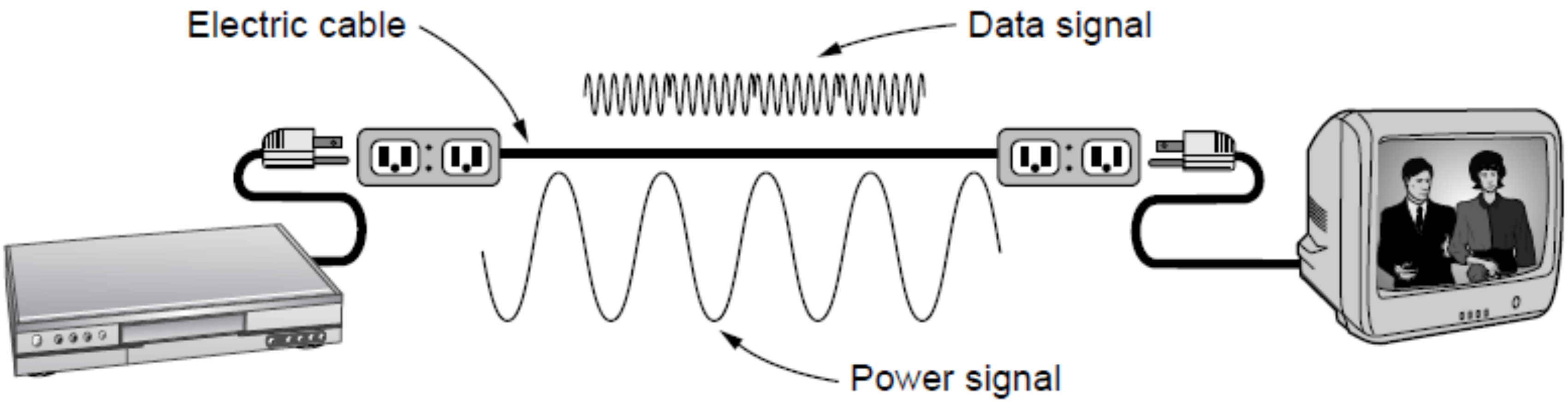
Category 5 UTP cable with four twisted pairs

Coaxial Cable



A coaxial cable

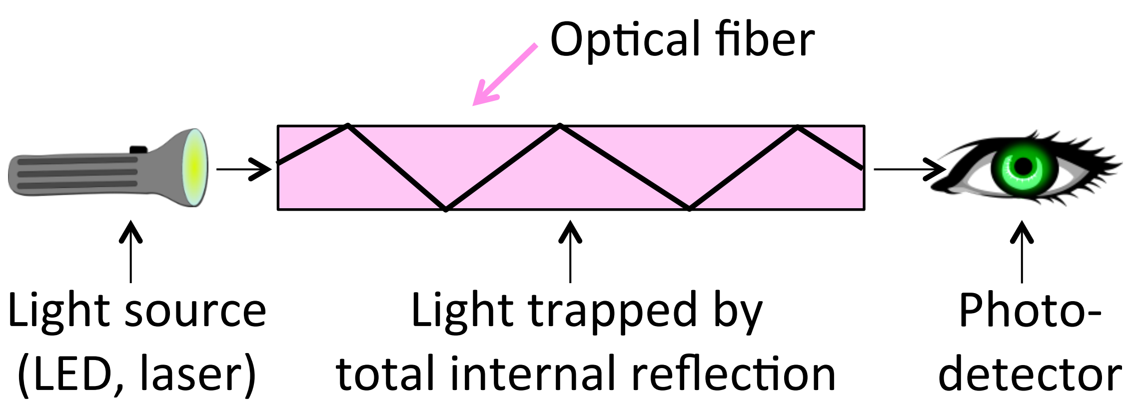
Power Lines



A network that uses household electrical wiring.

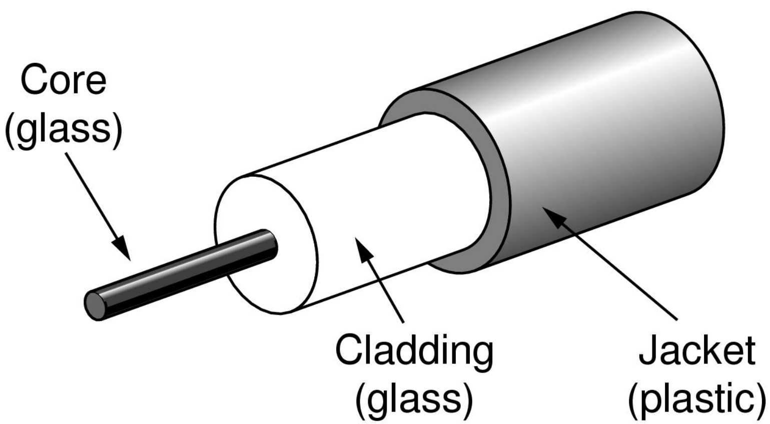
Fiber

- Long, thin, pure strands of glass
  - Enormous bandwidth (high speed) over long distances



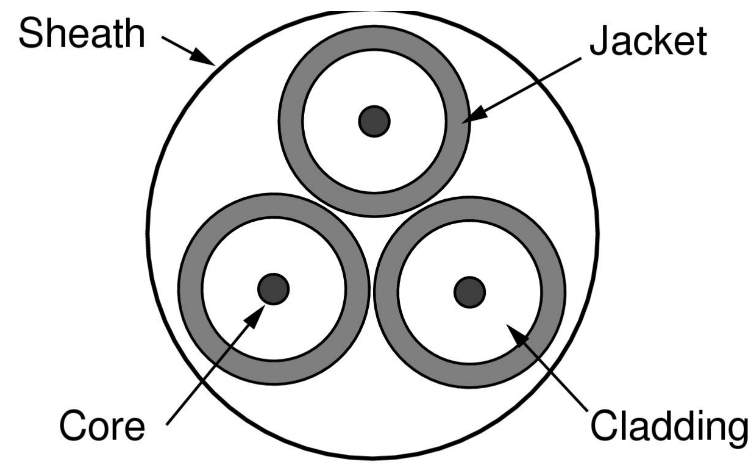
Fiber Cables

- Two varieties: <u>multi-mode</u> (shorter links, cheaper) and <u>single-mode</u> (up to ~100 km)



(a)

One fiber

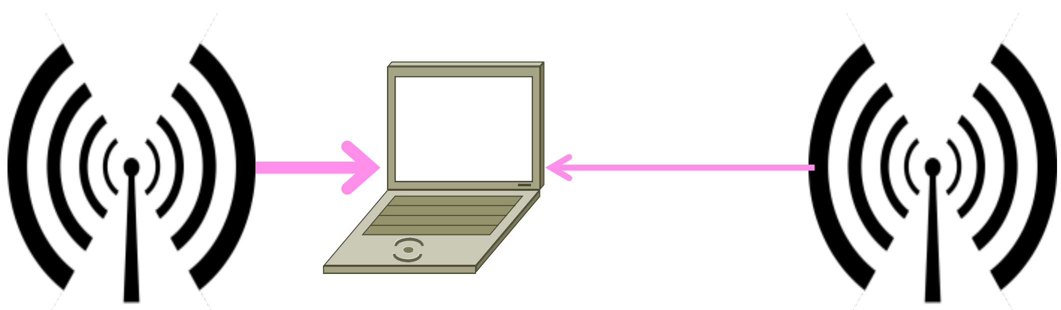


(b)

Fiber bundle in a cable

Wireless

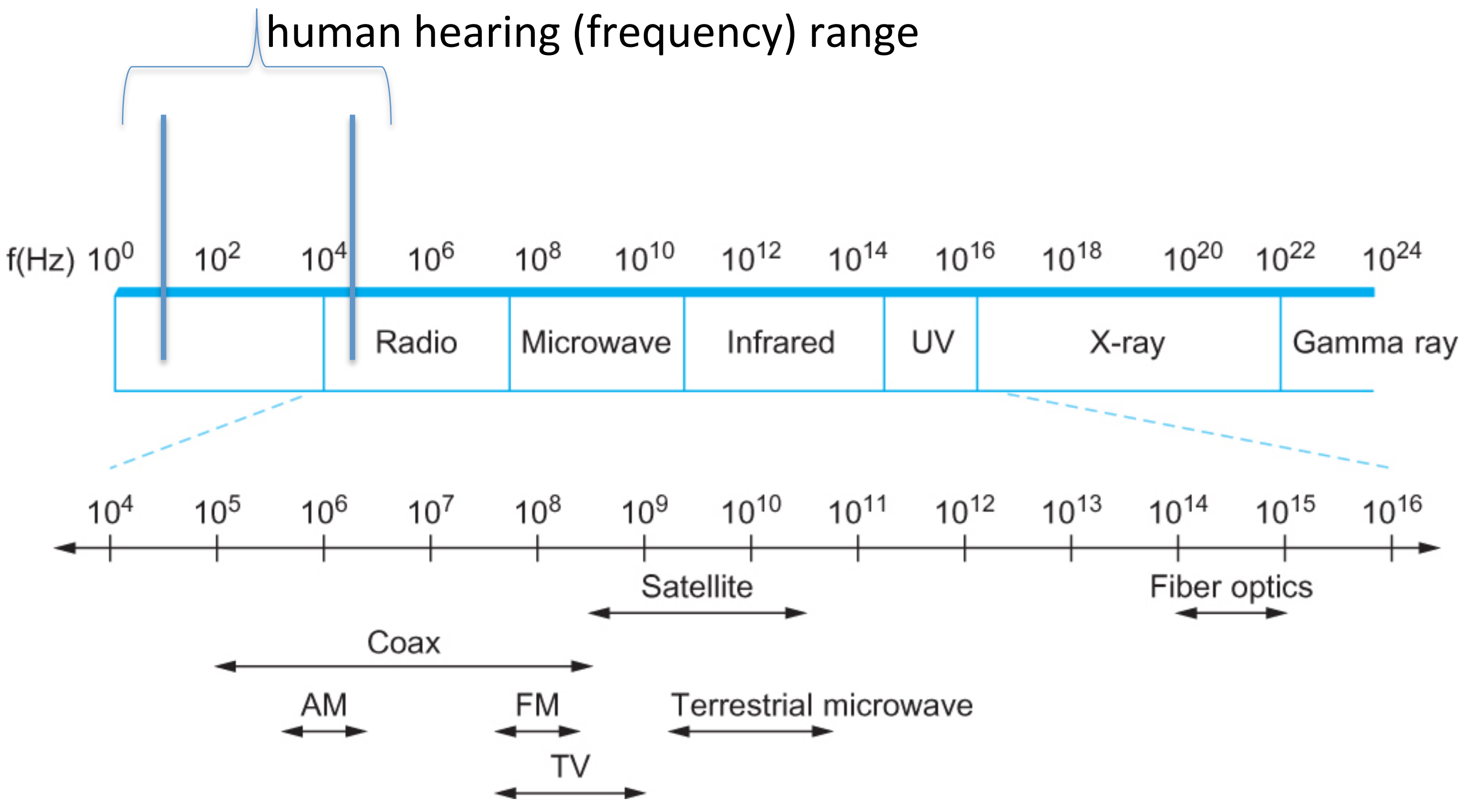
- Sender radiates signal over a region
  - In many directions, unlike a wire, to potentially many receivers
  - Nearby signals (same freq.) <u>interfere</u> at a receiver; need to coordinate use



Physical Connection (Link)

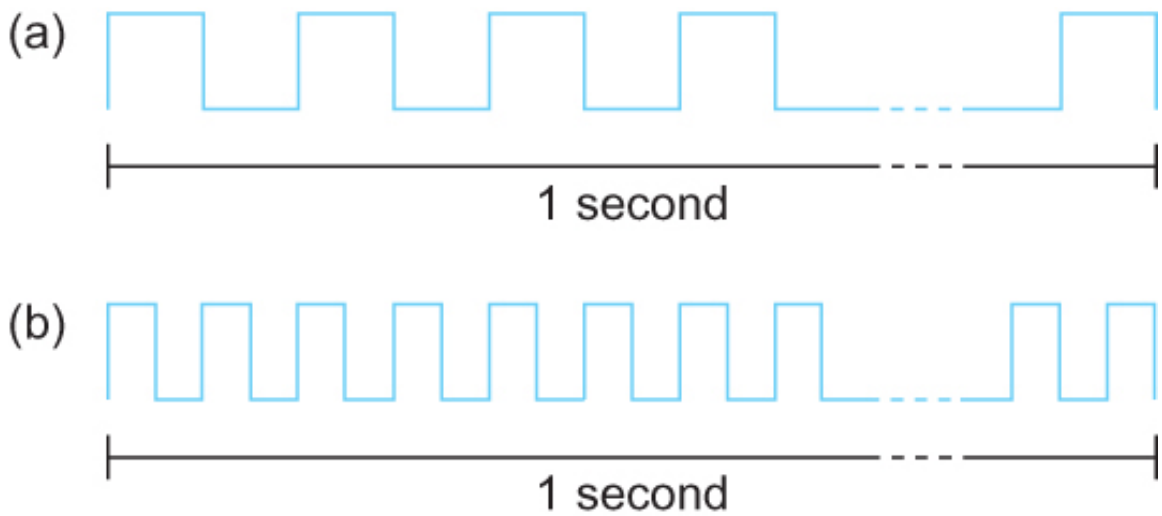
- Frequency
  - Measured in Hertz, with which the electromagnetic waves oscillate
  - Distance between the adjacent pair of maxima or minima of a wave measured in meters is called wavelength
- Wavelength = C_m / Frequency
  - Where C_m is the speed of light in medium
  - For a 300Hz wave through copper with $C_c = 2/3 \times 3 \times 10^8$ (m/s)
  - Wavelength = 667×10^3 meters

Physical Connection (Link)



Electromagnetic spectrum

Bandwidth



Bits transmitted at a particular bandwidth can be regarded as having some width:

(a) bits transmitted at 1Mbps (each bit 1 μs wide);

(b) bits transmitted at 2Mbps (each bit 0.5 μs wide).

Bandwidth

Service	Bandwidth (typical)
Dial-up	28–56 kbps
ISDN	64–128 kbps
DSL	128 kbps–100 Mbps
CATV (cable TV)	1–40 Mbps
FTTH (fibre to the home)	50 Mbps–1 Gbps

Common services available to connect your home

Latency

- One way to measure latency is round-trip time (RTT)
  - Measures the time it takes for the message to go from one end of the network to another and back
- Latency is influenced by three limiting/delaying factors:
  - Propagation delay (nothing including a bit on a wire can travel faster than the speed of light)
  - Transmit delay(inversely proportional to the medium BW)
  - Queuing delay

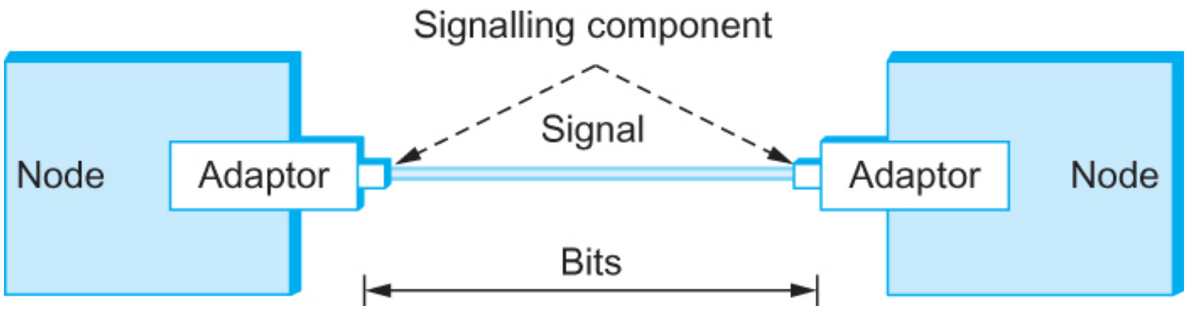
Encoding vs Modulation

- Defining two more terms:
  - Placing binary data on a signal is called encoding.
  - Modulation involves modifying the signals in terms of their frequency, amplitude, and phase.

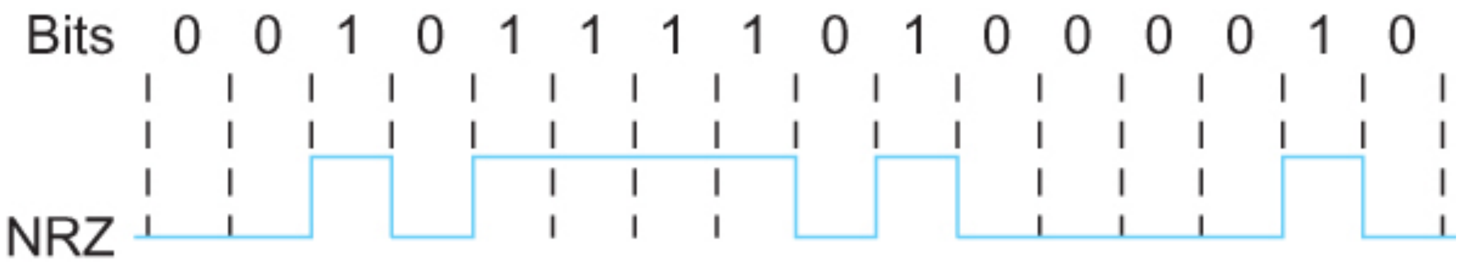
> In electronics and telecommunications, **modulation** is the process of varying one or more properties of a periodic waveform, called the carrier signal, with a **modulating** signal that typically contains information to be transmitted.
>
> Modulation - Wikipedia, the free encyclopedia
> en.wikipedia.org/wiki/**Modulation** Wikipedia

http://en.wikipedia.org/wiki/Modulation

Encoding and Transmitting the Signal



Signals travel between signaling components; bits flow between adaptors



NRZ encoding of a bit stream

Encoding

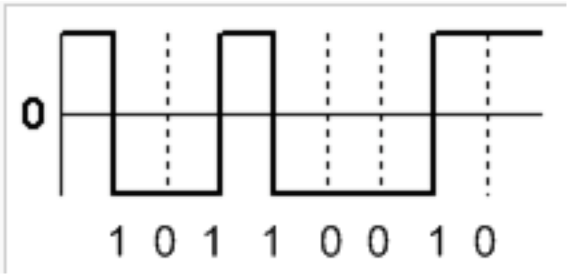
- First problem with NRZ
  - Baseline wander
    - The receiver keeps an average of the signals it has seen so far
    - Uses the average to distinguish between low and high signal
    - When a signal is significantly lower than the average, it is 0, else it is 1
    - Too many consecutive 0's and 1's cause this average to change, making it difficult to detect

Encoding

- Second problem with NRZ
  - Clock recovery
    - Every clock cycle, the sender transmits a bit and the receiver recovers a bit
    - The sender and receiver have to be precisely synchronized
    - Frequent transition from high to low or vice versa are necessary to enable clock recovery
      - Whenever the signal changes the receiver knows it is at a clock cycle boundary and it can resynchronize itself.
    - Both the sending and decoding process is driven by a clock

Encoding

- NRZI
  - Non Return to Zero Inverted
  - Sender makes a transition from the current signal to encode 1 and stay at the current signal to encode 0
    - Transition represent the 1 bit
    - No transition represent the 0 bit



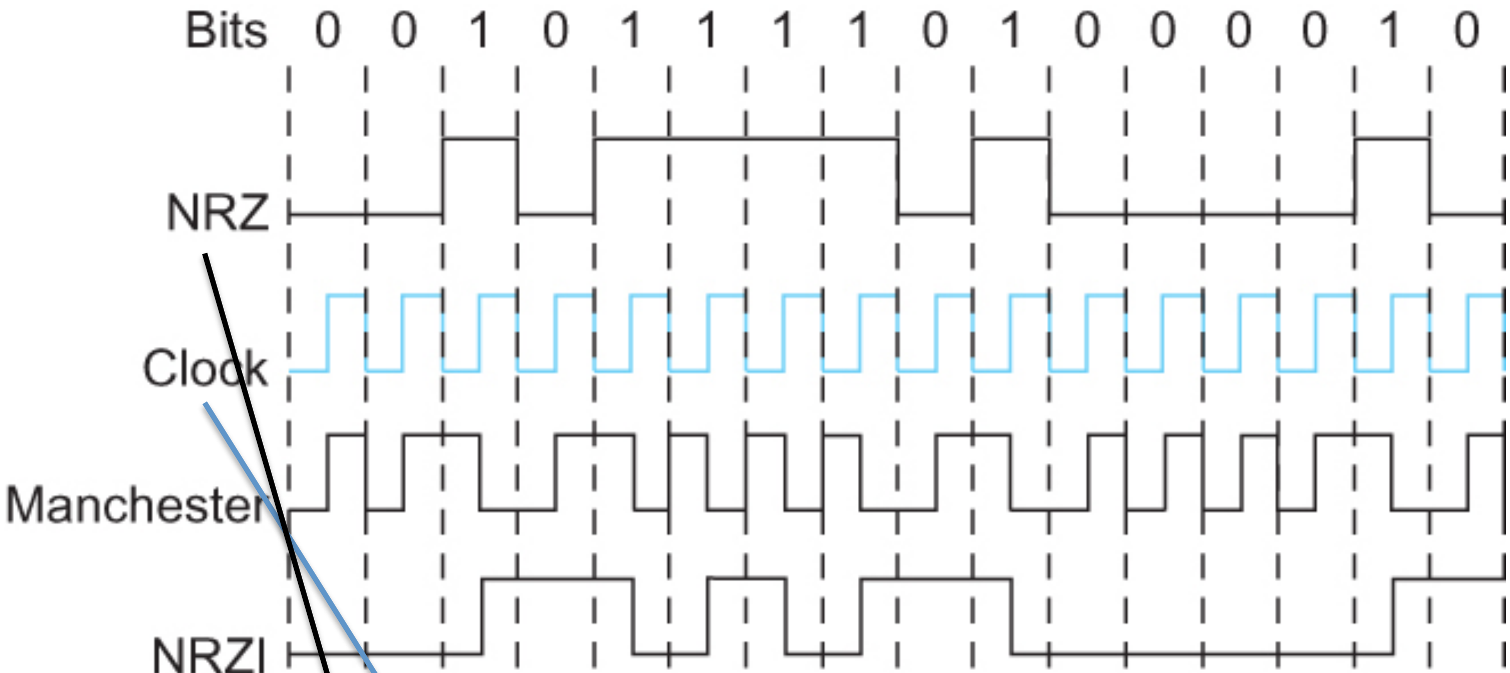
  - Solves the consecutive 1’s (or 0’s) to some extend

Encoding

- Manchester encoding
  - Merging the clock with signal by transmitting Ex-OR of the NRZ encoded data and the clock
    - Manchester = NRZ (XOR) Clock
  - Clock is an internal signal that alternates from low to high, a low/high pair is considered as one clock cycle

x	y	x XOR y
0	0	0
0	1	1
1	0	1
1	1	0

Encoding



x	y	x XOR y
0	0	0
0	1	1
1	0	1
1	1	0

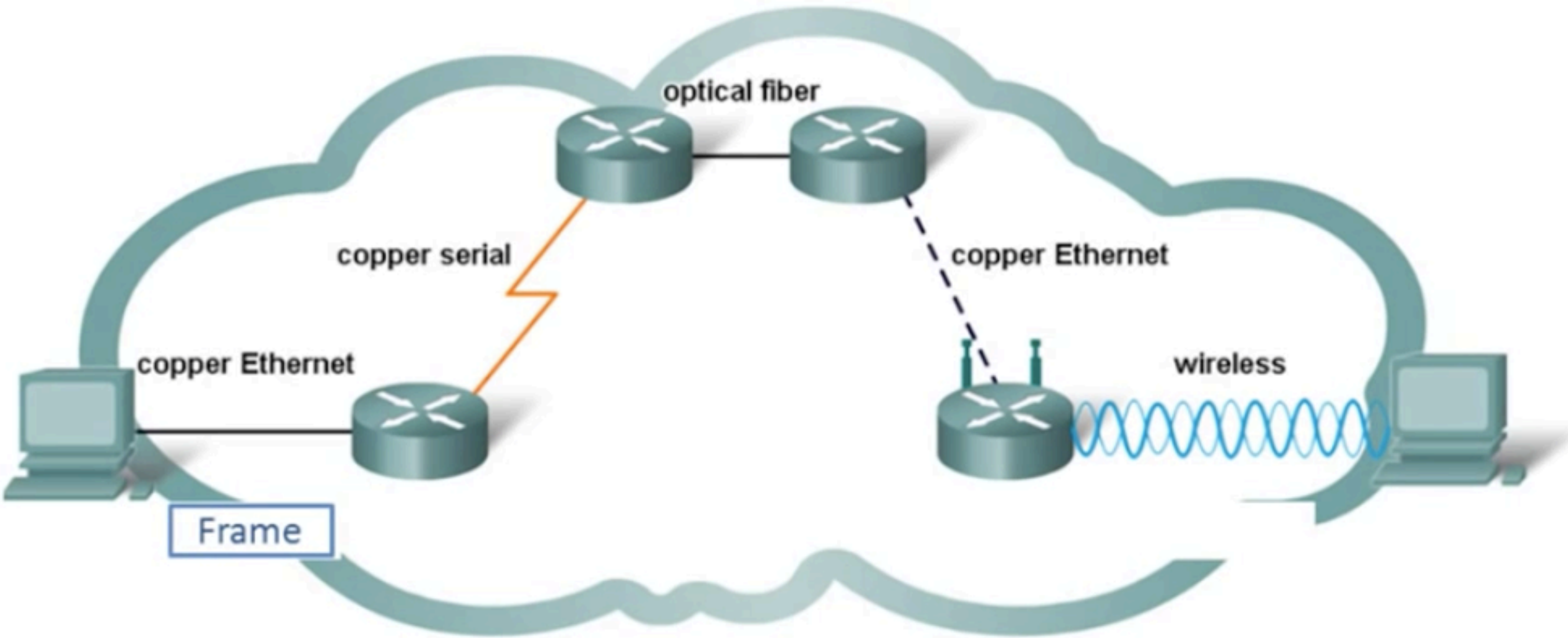
the sender make a transition from the current signal
to encode a 1 and stay at the current signal to encode a 0.

OSI Reference Model

OSI Layer	Function
Application	User interface, communication apps
Presentation	Character sets, encryption, compression
Session	Maintain connection, login, upper layer errors
Transport	Other (guaranteed delivery)
Network	Network ID, routing
Data Link	Access control, data flow, framing, device ID, error detection
Physical	Electrical & physical interface, topology, encoding

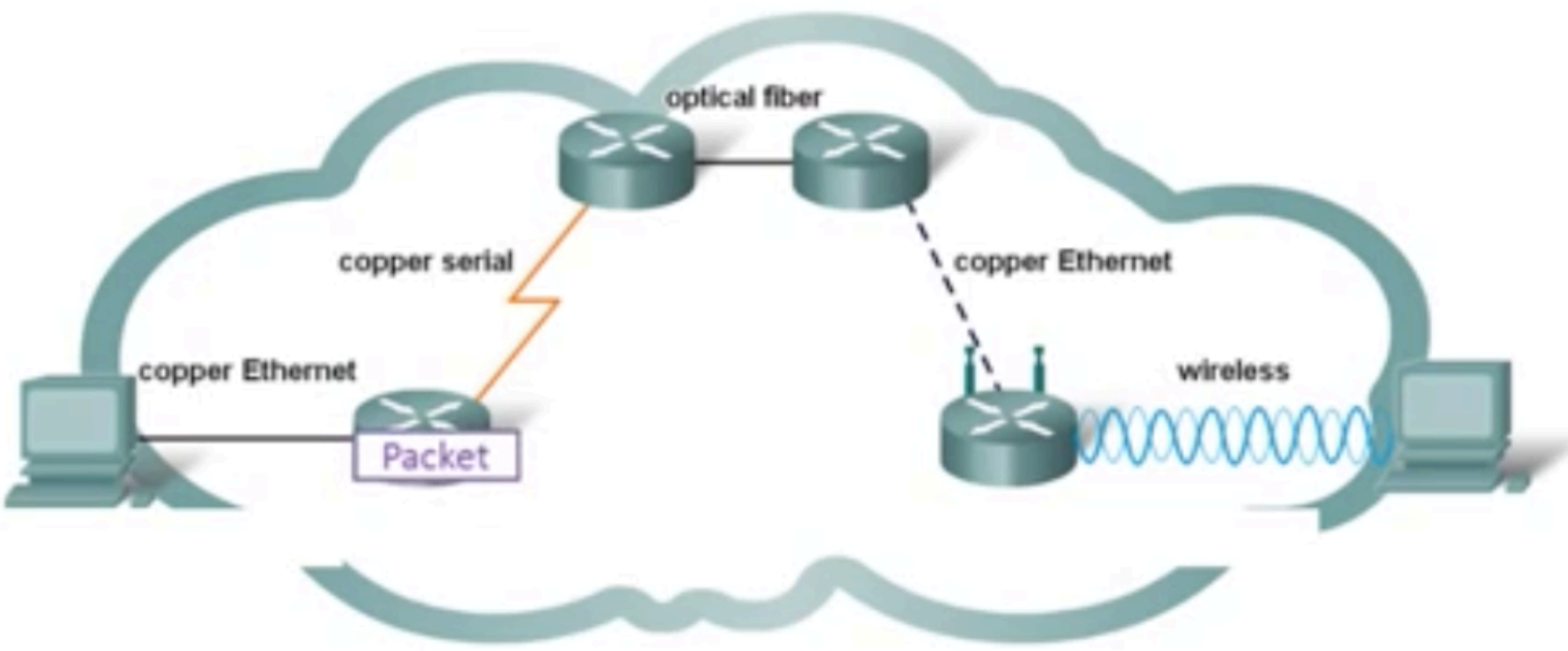
Data Link Layer

- Is responsible for controlling the transfer of frames across the media
- Sits underneath the Network layer providing a transparency to the IP packets regardless of the delivery pathway and access technologies used



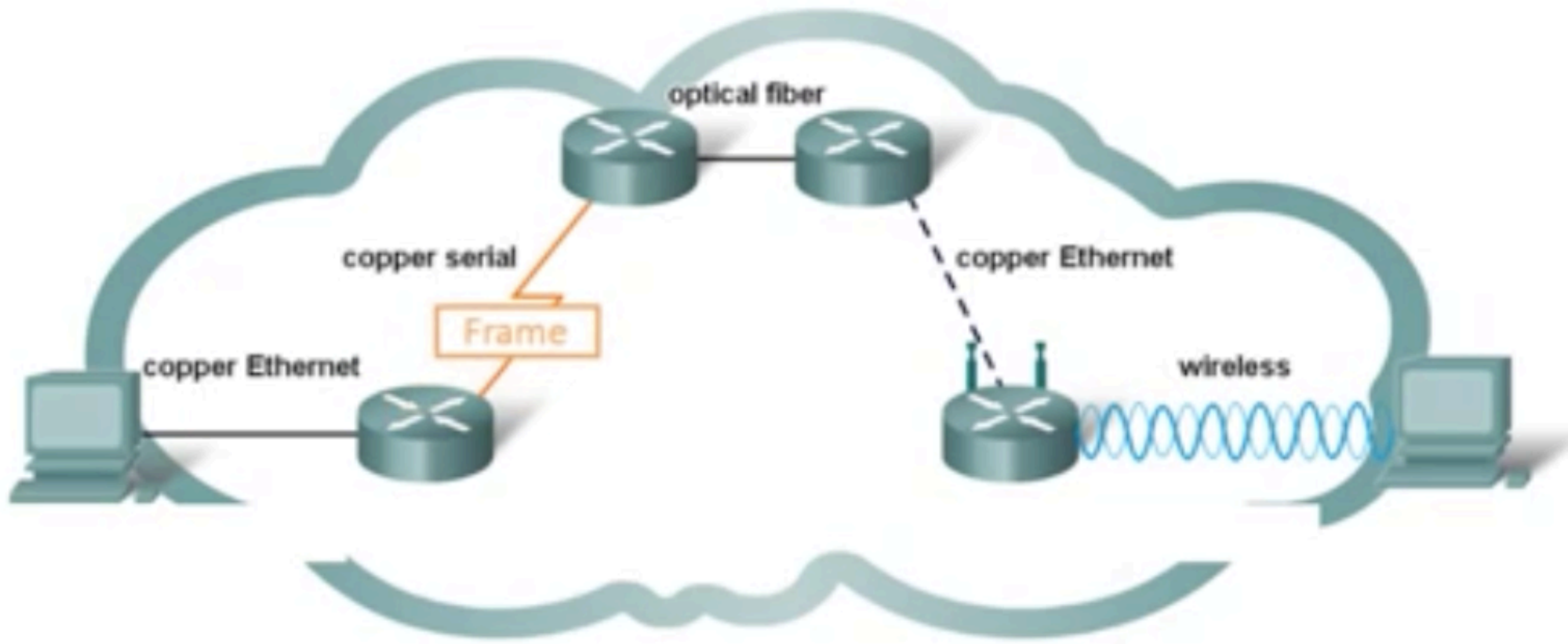
Data Link Layer

- The PDU (protocol Data Unit) for the Data Link Layer is called a frame
- At each node along the path
  - The Frame is decapsulated into a packet
  - The frame is also checked for errors



Data Link Layer

- Packet is then encapsulated into a new frame compatible with the new link that the packet wants to travel on next
- Repackaging of the packet into a new frame is done if necessary at each link until it reaches the destination



Data Link Layer

- Data Link layer sits underneath the Network layer
- Bridges the gap between the physical network below and a logical network above
- Factors to be considered before implementing a layer 2 protocol
  - The geographic scope (network size)
  - The physical layer implementation
  - The number of hosts involved

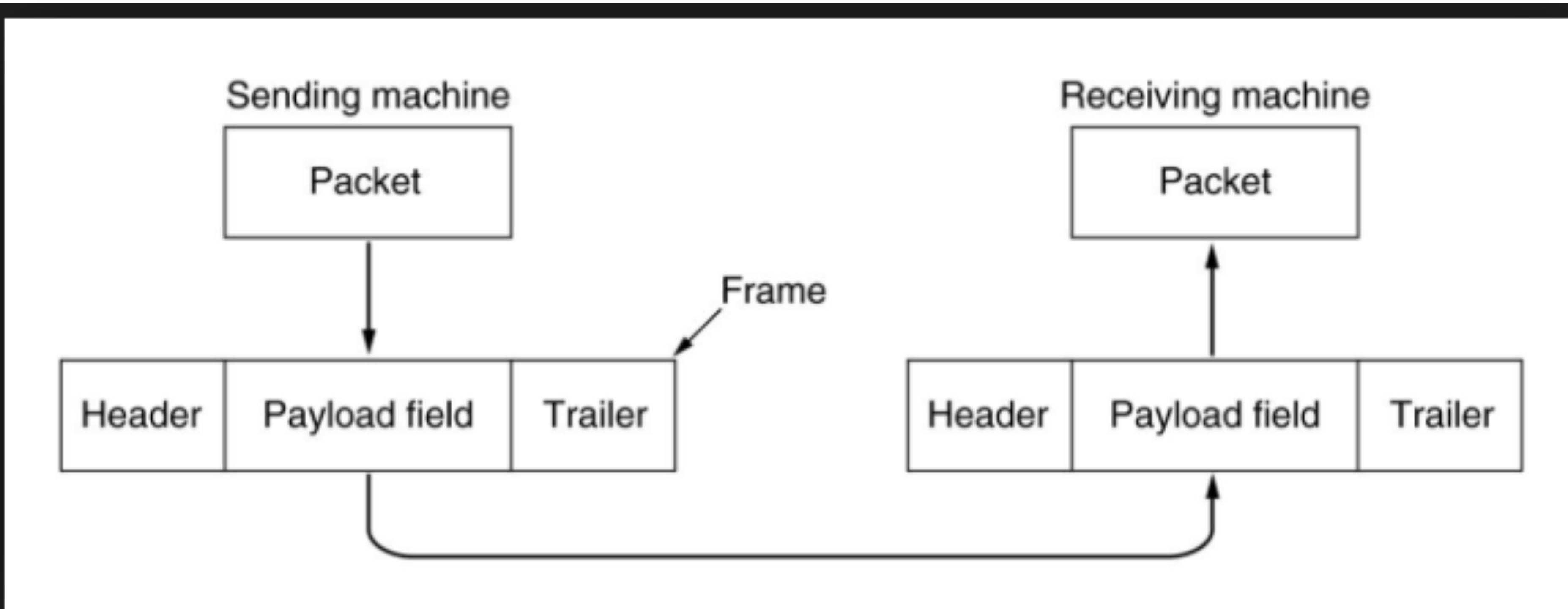
Framing

Frame (networking)

From Wikipedia, the free encyclopedia

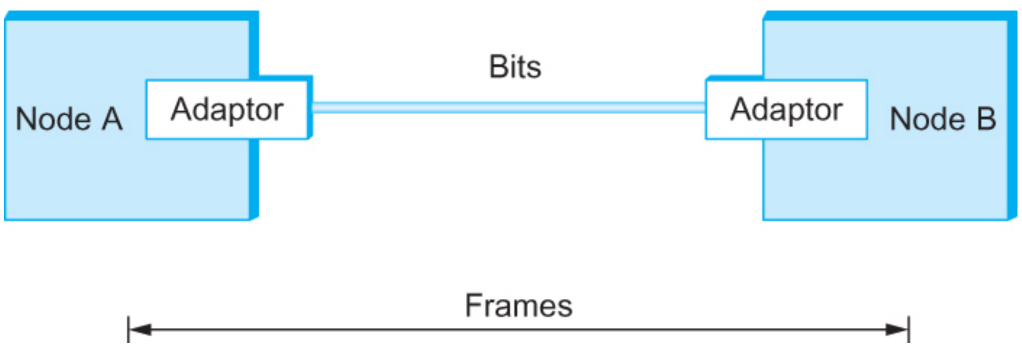
A **frame** is a digital data transmission unit in computer networking and telecommunication. A frame typically includes frame synchronization features consisting of a sequence of bits or symbols that indicate to the receiver the beginning and end of the payload data within the stream of symbols or bits it receives. If a receiver is connected to the system in the middle of a frame transmission, it ignores the data until it detects a new frame synchronization sequence.

In computer networking, a frame is a data packet in Layer 2 of the OSI model.[1] A frame is "the unit of transmission in a link layer protocol, and consists of a link layer header followed by a packet."[2] Examples are Ethernet frames, Point-to-Point Protocol (PPP) frames, and V.42 modem frames.



Framing

- *Frames* are exchanged between nodes.
- It is the network adaptor that enables the nodes to exchange frames.



Bits flow between adaptors, frames between hosts

Framing

- Two Categories (approaches) of Framing Protocols

1. Byte-oriented approach
   - Looking for a specific byte (character) or byte count to determine where the frames starts or ends

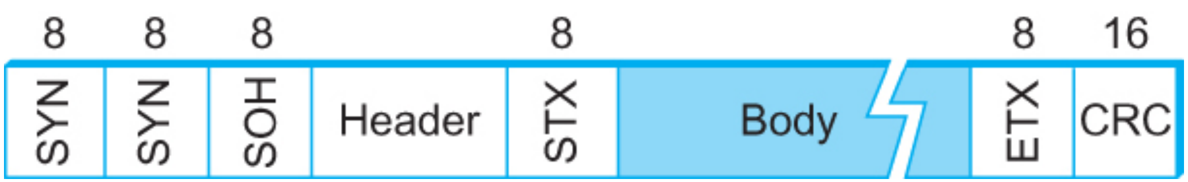
2. Bit-oriented approach
   - Looking for a series (or combination) of bits to synchronize

Framing

- Byte-oriented Protocols
  - Views each frame as a collection (group) of bytes (characters)
  - Two approaches
    - Flag-based
      - BISYNC (Binary Synchronous Communication Protocol)
        - » Developed by IBM (late 1960)
      - Point-to-Point Protocol (PPP)
    - Byte-counting
      - DDCMP (Digital Data Communication Protocol)
        - » Developed by Digital Equipment Corporation (1974)

Framing

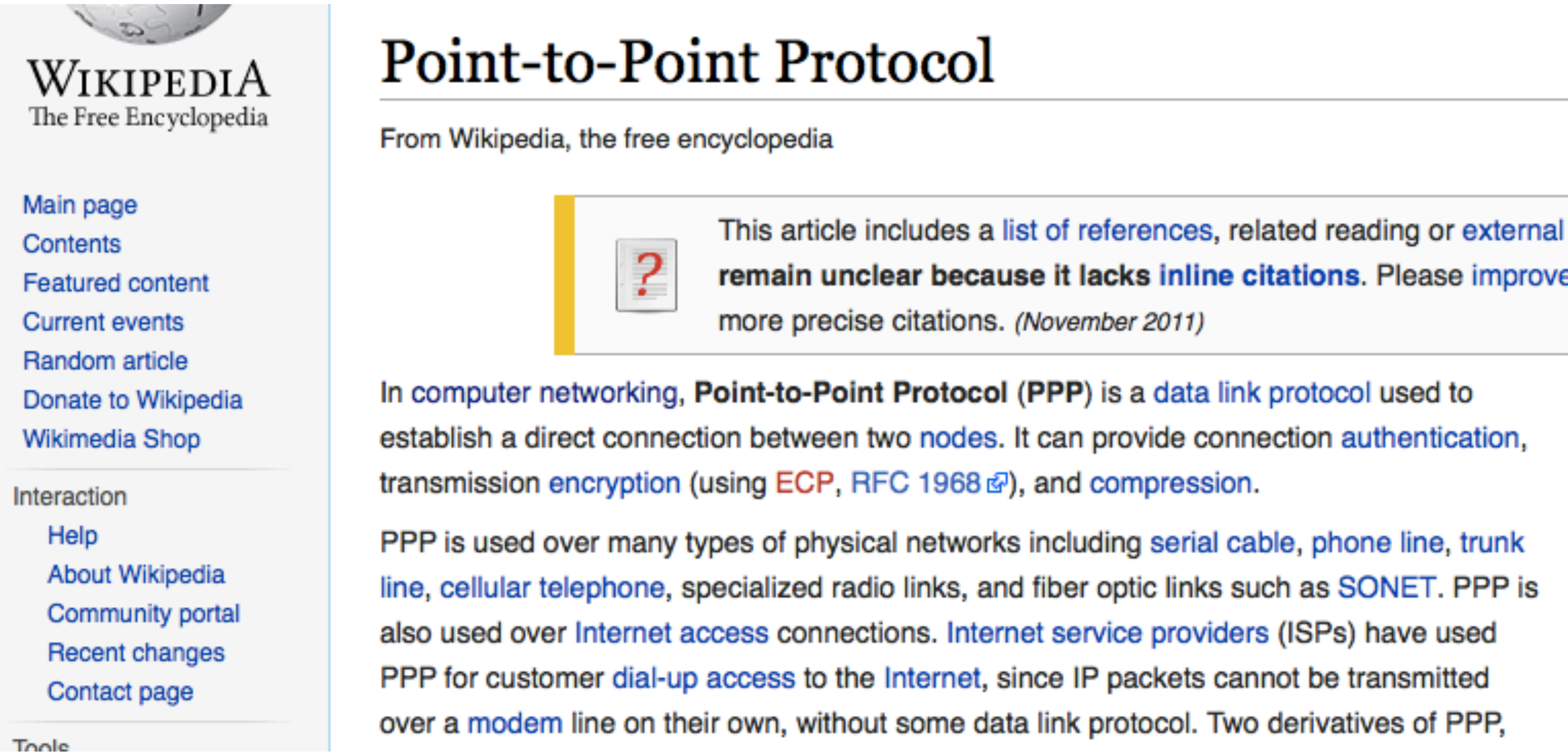
- BISYNC
  - Frames transmitted beginning with leftmost field
  - Beginning of a frame is denoted by sending a special SYN (synchronize) character (twice-> Binary)
  - Data portion of the frame is contained between special flag character STX (start of text) and ETX (end of text)
  - SOH : Start of Header
  - DLE : Data Link Escape
  - CRC: Cyclic Redundancy Check



BISYNC Frame Format

Framing

- Point-to-point Protocol (PPP)



WIKIPEDIA
The Free Encyclopedia

Main page
Contents
Featured content
Current events
Random article
Donate to Wikipedia
Wikimedia Shop

Interaction
Help
About Wikipedia
Community portal
Recent changes
Contact page

Tools

Point-to-Point Protocol

From Wikipedia, the free encyclopedia

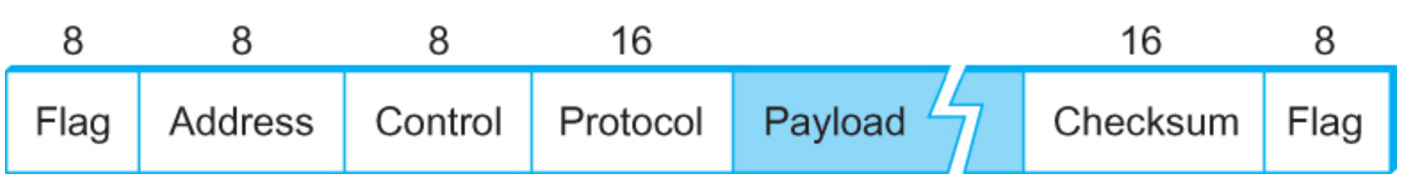
This article includes a list of references, related reading or external **remain unclear because it lacks inline citations**. Please improve more precise citations. *(November 2011)*

In computer networking, **Point-to-Point Protocol** (**PPP**) is a data link protocol used to establish a direct connection between two nodes. It can provide connection authentication, transmission encryption (using ECP, RFC 1968), and compression.

PPP is used over many types of physical networks including serial cable, phone line, trunk line, cellular telephone, specialized radio links, and fiber optic links such as SONET. PPP is also used over Internet access connections. Internet service providers (ISPs) have used PPP for customer dial-up access to the Internet, since IP packets cannot be transmitted over a modem line on their own, without some data link protocol. Two derivatives of PPP,

Framing

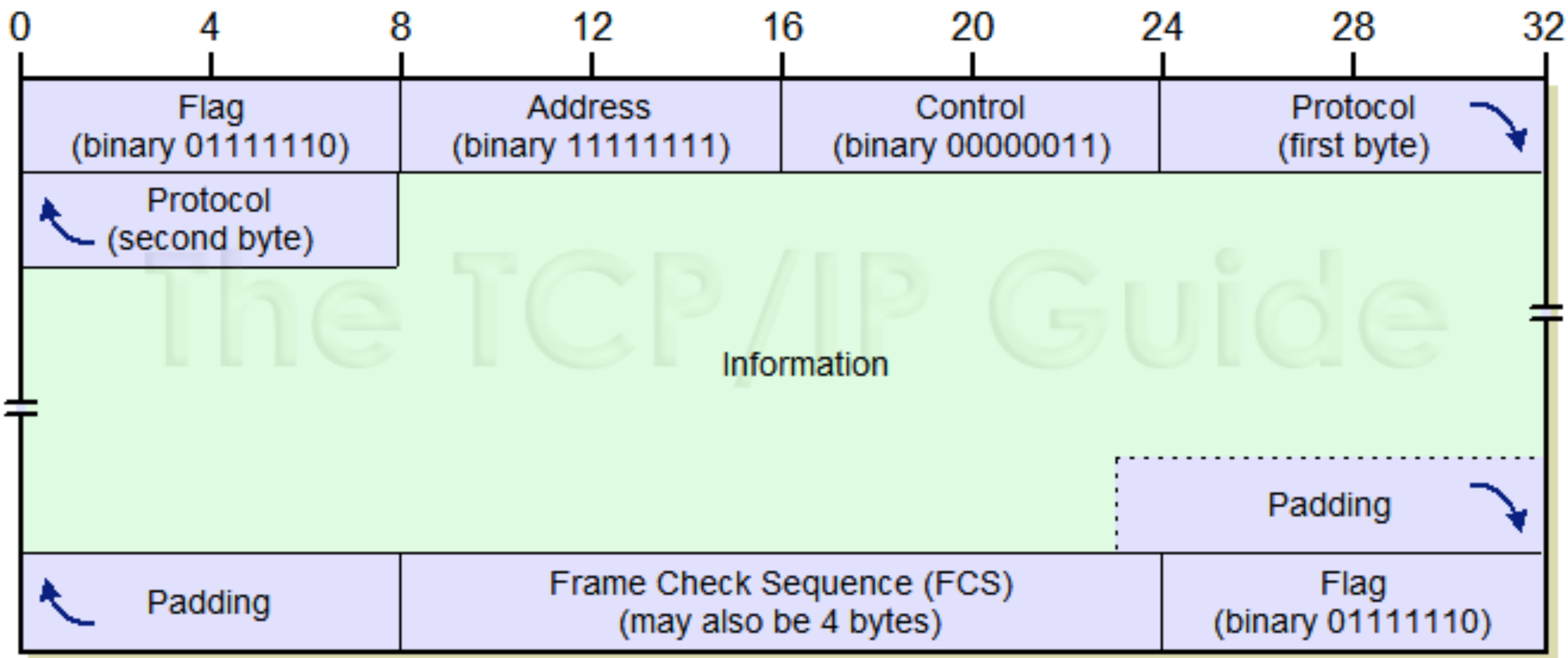
- PPP also uses flag-based approach
  - Special start/end of frame character denoted as Flag
    - 0 1 1 1 1 1 1 0
  - Broadcast address, control Byte : default numbers (11111111) and (00000011) respectively
  - Protocol of the encapsulated datagram for demux : IP / IPX
  - Payload : negotiated (default is 1500 bytes)
  - Checksum : for error detection



PPP Frame Format

Framing

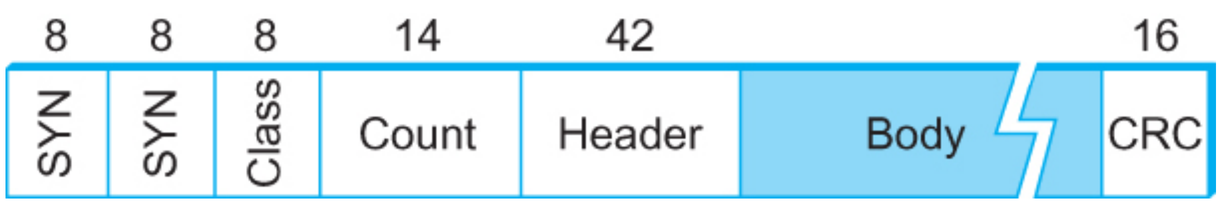
- PPP also uses flag-based approach



PPP Frame Format

Framing

- Byte-counting approach
  - Used in DDCMP (Digital Data Communication Protocol)
  - *count* : how many bytes are contained in the frame
  - If *count* is corrupted
    - Framing error



DDCMP Frame Format

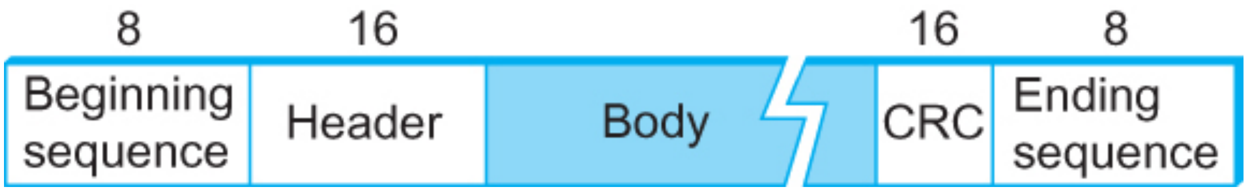
Framing

- Bit-oriented Protocol
  - They were developed to overcome the limitations of character oriented protocols
  - It does not rely on a specific code or character flag for interpretation of line control.
    - To allow independence of codes (code transparency).
  - Transparency is achieved by means of *bit stuffing.*

Framing

- Bit-oriented Protocol
  - HDLC : High Level Data Link Control
    - Beginning and Ending Sequences

      0 1 1 1 1 1 1 0



HDLC Frame Format

Framing

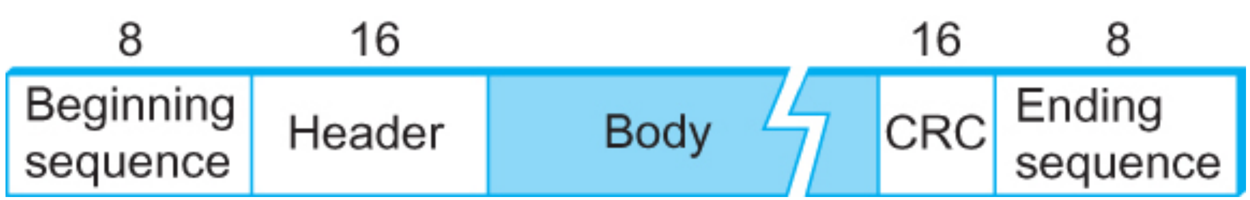
Original sequence 00111111011111111111000111110100

Stuffing

Transmitted sequence (after stuffing) 001111101011111011111010001111100100

Destuffing

Recovered sequence (after destuffing) 00111111011111111111000111110100



HDLC Frame Format

Framing

- HDLC Protocol
  - After any time five consecutive 1's transmitted from the body of the message (i.e. excluding when the sender is trying to send the distinguished 01111110 sequence):
    - The sender inserts 0 before transmitting the next bit

Framing

- HDLC Protocol
  - After detecting 5 consecutive 1's
    - If next bit 0 (0111110)
      - Stuffed, so discard that bit
    - If next bit 1 look at the next bit
      - If 0, then end of the frame marker (01111110)
      - If 1, then error has been introduced in the bitstream
        - » Discard the whole frame (01111111)
        - » The receiver needs to wait for the next 01111110 before it can start receiving again

OSI Reference Model

OSI Layer	Function
Application	User interface, communication apps
Presentation	Character sets, encryption, compression
Session	Maintain connection, login, upper layer errors
Transport	Other (guaranteed delivery)
Network	Network ID, routing
Data Link	Access control, data flow, framing, device ID, error detection
Physical	Electrical & physical interface, topology, encoding

Error Detection

- Bit errors are introduced into frames
  - Because of
    - Electrical interference
    - Thermal noises
- Detecting Error
  - Two approaches when the recipient detects an error
    - Retransmitted message
    - Reconstructs the message

Error Detection

- Common technique for detecting transmission error
  - CRC (Cyclic Redundancy Check)
    - Used in HDLC, DDCMP, CSMA/CD, Token Ring
  - Other approaches
    - Two Dimensional Parity (BISYNC)
    - Checksum (IP)

Error Detection

- Basic Idea of Error Detection
  - To add redundant information to a frame that can be used to determine if errors have been introduced.
  - Imagine (Extreme Case)
    - Transmitting two complete copies of data
      - Identical → No error
      - Differ → Error
      - Poor Scheme ??? Why?
        - » For n bit message, we use n bit redundant information
        - » Error can still go undetected. How?
    - In general, we can provide strong error detection technique
      - k redundant bits, n bits message, k << n
      - In Ethernet, a frame carrying up to 12,000 bits of data requires only 32-bit CRC

Error Detection

- Extra bits are redundant
  - They add no new information to the message
  - Derived from the original message using some algorithm
  - Both the sender and receiver know the algorithm

Sender

m	**r**

Receiver

m	**r**

The sender applies the
algorithm to the message
to generate the redundant bits

Receiver computes r using m
applying the same algorithm.
If they match, no error

Error-Detection Algorithms

- At data link layer
  - Two-dimensional Parity
  - Cyclic Redundancy Check (CRC)
- At higher layers (TCP/IP)
  - Checksum

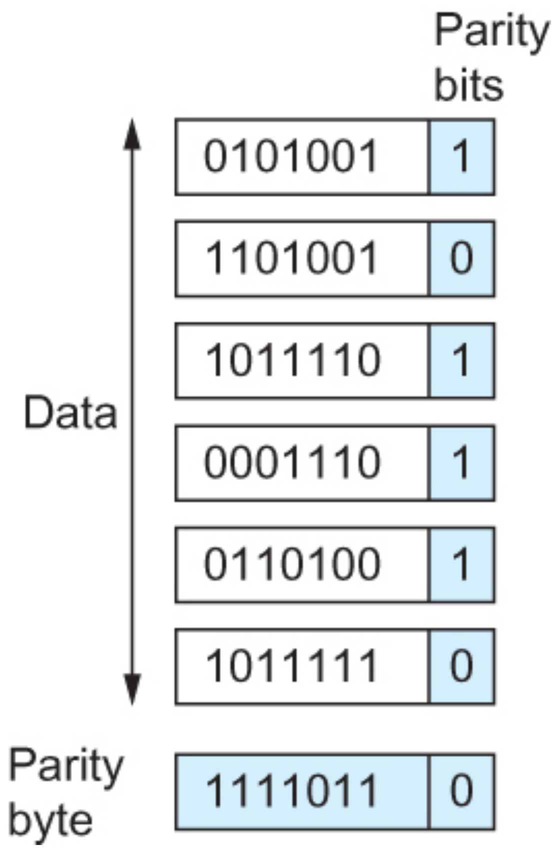
Two-dimensional parity

- Two-dimensional parity It is based on "simple" (one-dimensional) parity, which usually involves adding one extra bit to a 7-bit code to balance the number of 1s in the byte.
- One-dimensional parity:
  - Odd parity sets the eighth bit to 1 if needed to give an odd number of 1s in the byte, and
  - Even parity sets the eighth bit to 1 if needed to give an even number of 1s in the byte

Two-dimensional parity

- Two-dimensional parity does a similar calculation for each bit position across each of the bytes contained in the frame.
- This results in an <u>extra parity byte for the entire frame</u>, in addition to a parity bit for each byte
- Two-dimensional parity catches all 1-, 2-, and 3-bit errors and most 4-bit errors

Two-dimensional parity



Two Dimensional Parity even parity

Cyclic Redundancy Check (CRC)

- Given any bit string (say, 110001), we can associate it to a polynomial with a single variable *x*:

  $1.x^5+1.x^4+0.x^3+0.x^2+0.x^1+1.x^0 = x^5+x^4+1$ and the degree of the polynomial is 5.

  An *n*-bit frame has a maximum degree of *n*-1.

- Let M(x) be a message polynomial and C(x) be a divisor polynomial (also called generator pol.).
  – C(x) has a degree of k (k <= n)
  – M(x)/C(x) leave a remainder of 0

Cyclic Redundancy Check (CRC)

- The receiver computes M(x)/C(x) and if the remainder is nonzero, then an error has occurred.
- The only thing the sender and the receiver should know is C(x).

Cyclic Redundancy Check (CRC)

- Six generator (divisor) polynomials that have become international standards are:
  - CRC-8 = x^8+x^2+x+1
  - CRC-10 = $x^{10}+x^9+x^5+x^4+x+1$
  - 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 = $x^{32}+x^{26}+x^{23}+x^{22}+x^{16}+x^{12}+x^{11}+x^{10}+x^8+x^7+x^5+x^4+x^2+x+1$

Cyclic Redundancy Check (CRC)

CRC-16-CCITT	X.25, V.41, HDLC *FCS*, XMODEM, Bluetooth, PACTOR, SD, DigRF, many others; known as *CRC-CCITT*
CRC-16-CDMA2000	mobile networks[16]
CRC-16-DECT	cordless telephones[25]
CRC-16-T10-DIF	SCSI DIF
CRC-16-DNP	DNP, IEC 870, M-Bus
CRC-16-IBM	Bisync, Modbus, USB, ANSI X3.28, SIA DC-07, many others; also known as *CRC-16* and *CRC-16-ANSI*
Fletcher	Used in Adler-32 A & B Checksums
CRC-17-CAN	CAN FD[27]
CRC-21-CAN	CAN FD[27]
CRC-24	FlexRay[19]
CRC-24-Radix-64	OpenPGP, RTCM104v3
CRC-30	CDMA
Adler-32	Zlib
CRC-32	HDLC, ANSI X3.66, ITU-T V.42, Ethernet, Serial ATA, MPEG-2, PKZIP, Gzip, Bzip2, PNG,[28] many others

Cyclic Redundancy Check (CRC)

- Properties of Divisor/Generator Polynomial
  - In general, it is possible to prove that the following types of errors can be detected by a C(x) with the stated properties
    - All single-bit errors, as long as the x^k and x^0 terms have nonzero coefficients.(CRC-8 = x^8+x^2+x+1)
    - 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) 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 *k* bits.
      - Most burst errors of larger than *k* bits can also be detected.

Internet Checksum Algorithm

- Not used at the link level
- Add up all the words that are transmitted and then transmit the result of that sum
  - The result is called the checksum
- The receiver performs the same calculation on the received data and compares the result with the received checksum
- If any transmitted data, including the checksum itself, is corrupted, then the results will not match, so the receiver knows that an error occurred