Review (1)

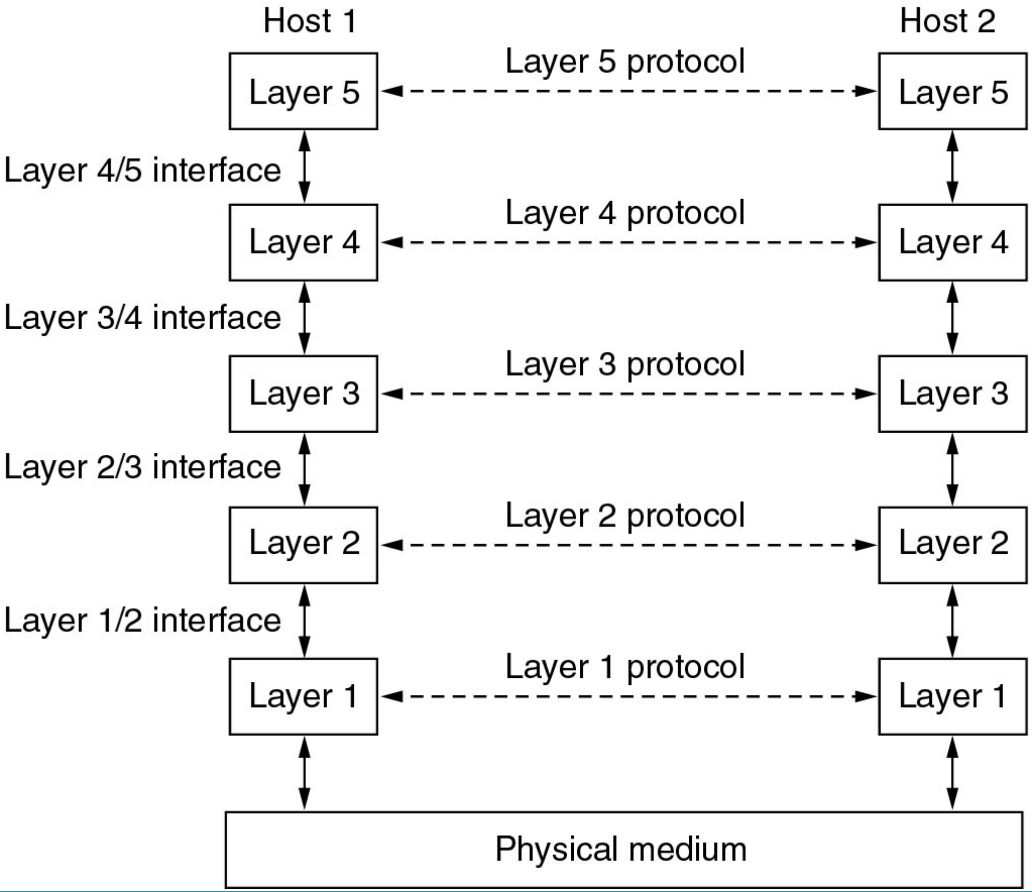
COMP90007 Internet Technologies

Lecturer: Ling Luo

Semester 2, 2020

Network Protocol Hierarchies

- Layers, protocols and interfaces



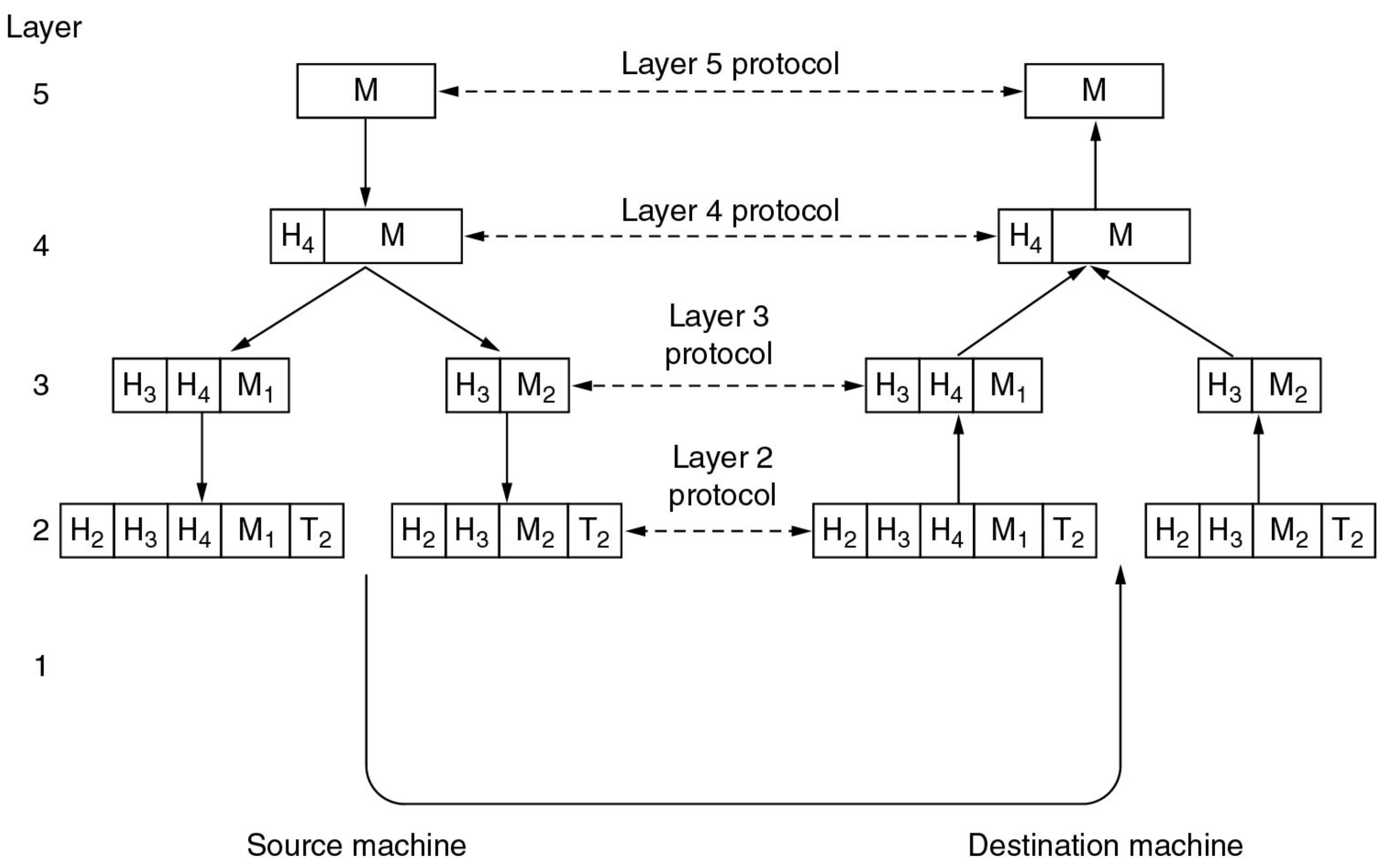
Consider the network as a stack of **layers**

Each layer offers **services** to layers above it through **interface**

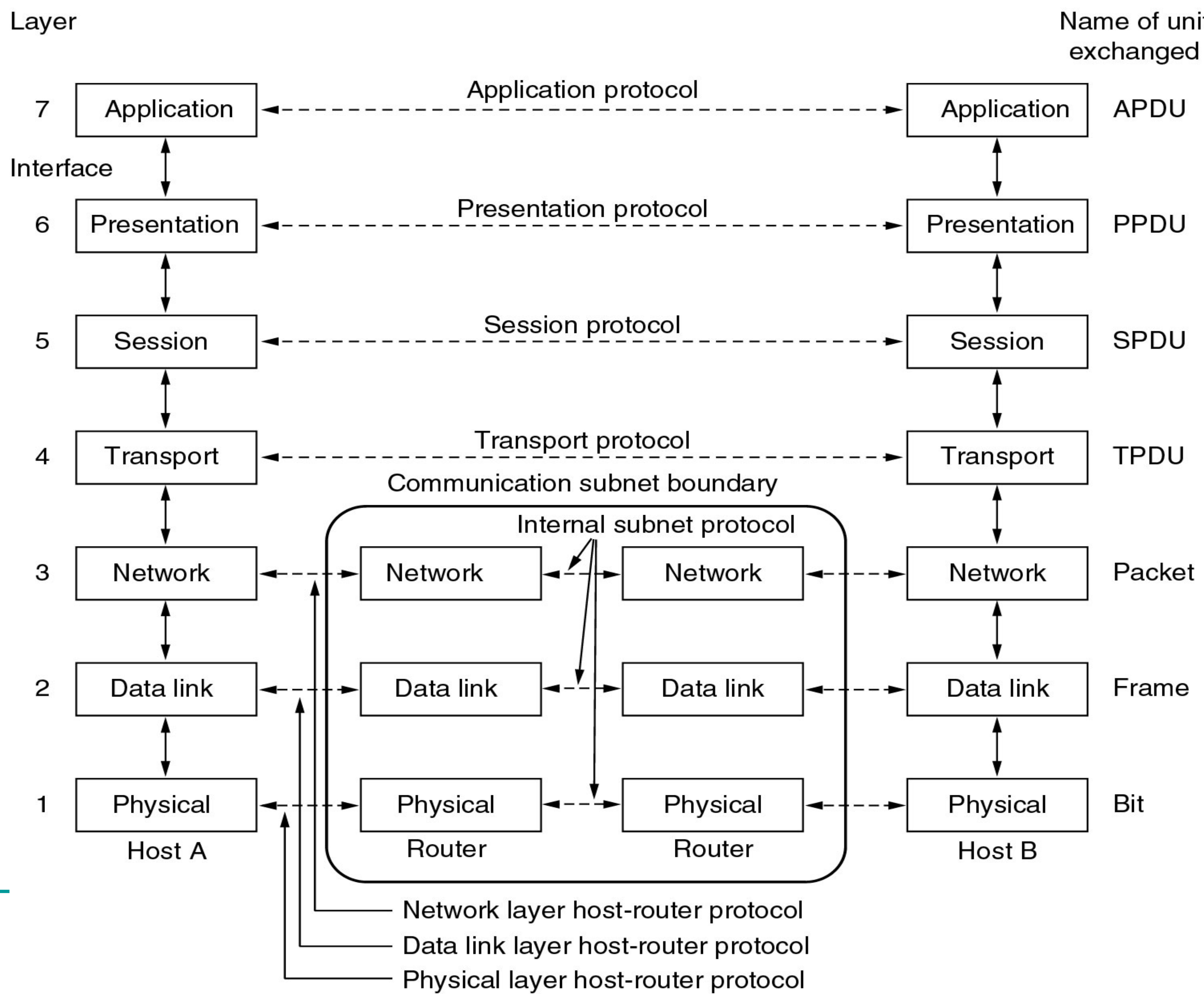
Protocol is an agreement between the communicating parties on how communication is to proceed

Network Protocol Hierarchies (2)

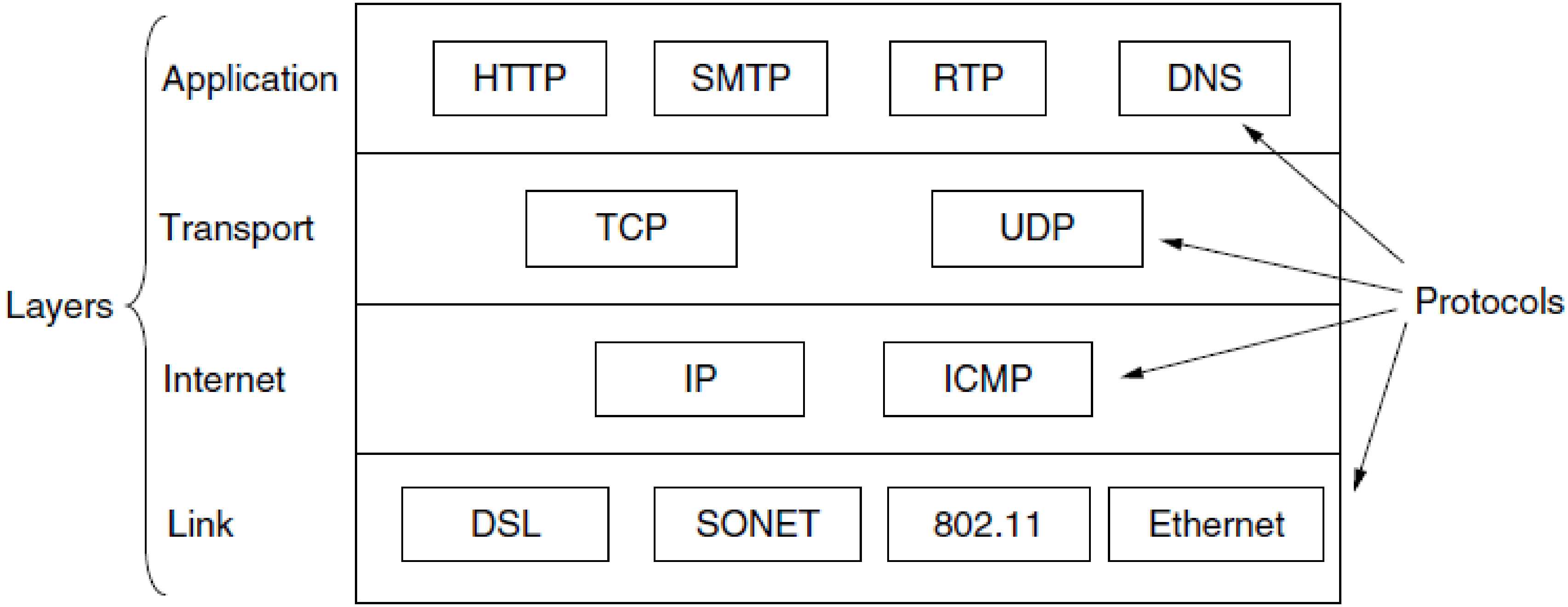
- Information flow supporting virtual communication in layer 5



OSI Reference Model



TCP/IP: Protocols



Hybrid Model

- The hybrid reference model used in this semester

5	Application layer
4	Transport layer
3	Network layer
2	Data link layer
1	Physical layer

Physical Layer

- The physical layer is concerned with the electrical, timing and mechanical interfaces of the network
  - **Mechanical**: material, cable length …
  - **Electrical**: voltage levels, signal strength …
  - **Timing**: data rate, latency

Compare Transmission Media (1)

Wired: twisted pairs, coaxial cable, fibre optics …
Wireless: radio, microwave, infrared, satellite …

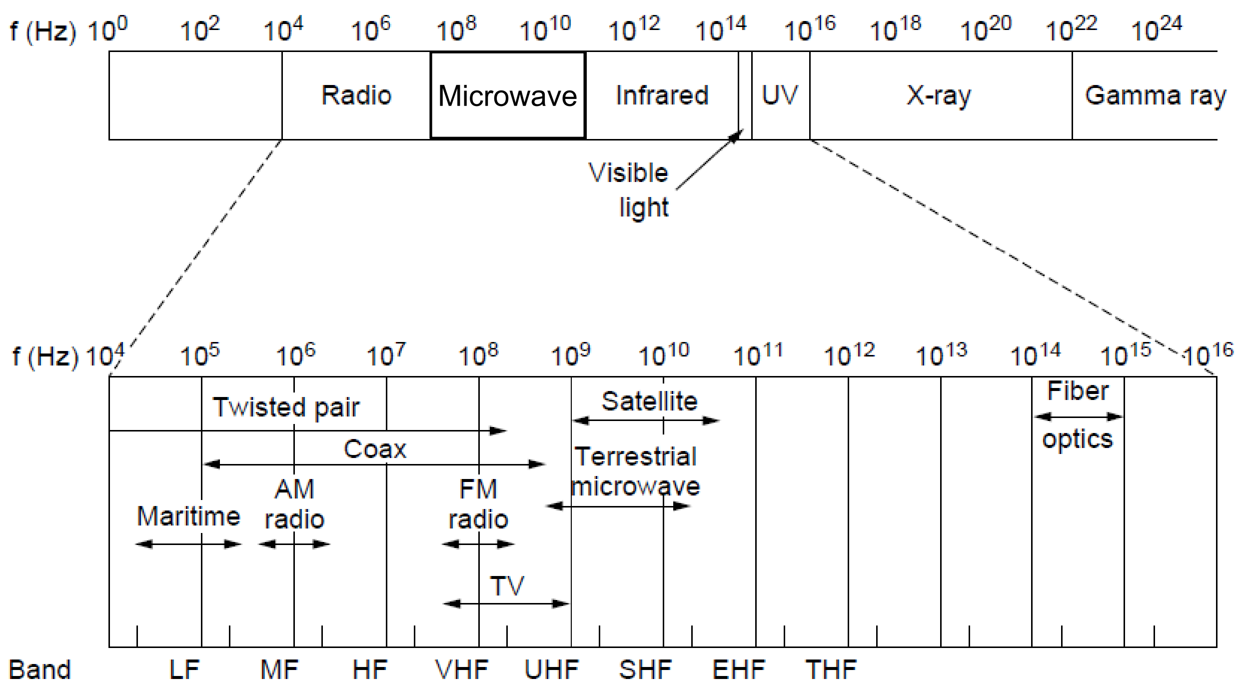
Compare the properties of wires and fibre:

Property	**Wires**	**Fibre**
Distance	Short (100s of m)	Long (tens of km)
Bandwidth	Moderate	Very High
Security	Easy to tap	Hard to tap
Cost	Inexpensive	More Expensive
Convenience	Easy to use	Harder to use

Compare Transmission Media (2)

Wireless Electromagnetic Spectrum

- Radio: wide-area broadcast
- Microwave: LANs and 3G/4G
- Infrared/Light: line-of-sight



Data Communication using Signals (1)

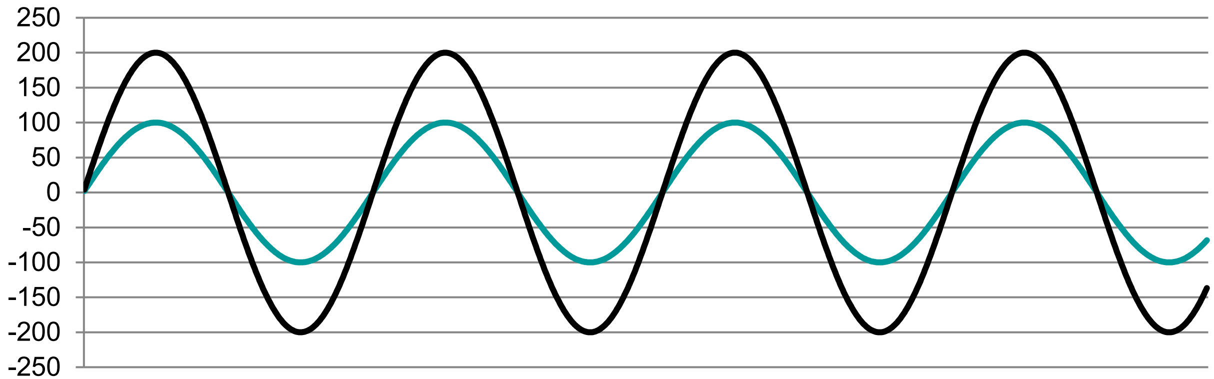
- Information is transmitted by varying a physical property e.g. voltage, current

- For a sinewave :

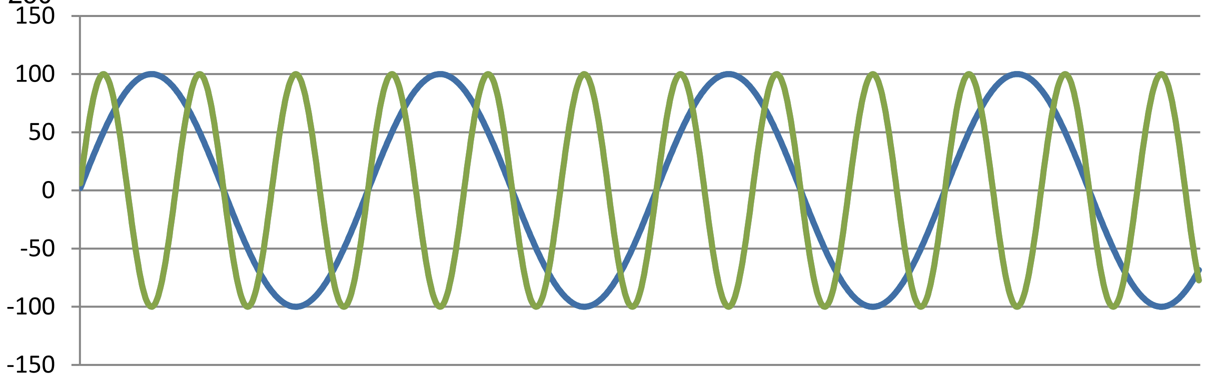
  function: $c * \sin(a * t + b)$

  c: amplitude, a/(2π):frequency and b:phase can change the behaviour of the function.

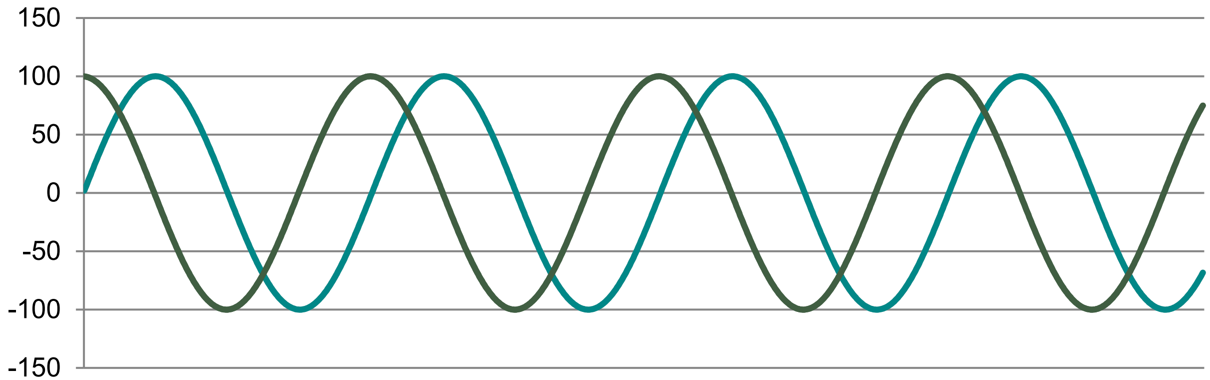
Data Communication using Signals (2)



Change in Amplitude



Change in Frequency



Change in Phase

Maximum Data Rate of a Channel

- Nyquist's theorem relates the data rate to the bandwidth (B) and number of signal levels (V) (channel **without noise**):

$$\boxed{\text{Max. data rate} = 2B \log_2 V \text{ bits/sec}}$$

- Shannon's theorem relates the data rate to the bandwidth (B) and signal strength (S) relative to the **noise** (N):

$$\boxed{\text{Max. data rate} = B \log_2(1 + S/N) \text{ bits/sec}}$$

Message Latency

- **Transmission delay**
  - T-delay = Message in bits / Rate of transmission
    = M/R seconds
- **Propagation delay**
  - P-delay= length of the channel/ speed of signals
    = Length / Speed of signal (2/3 of speed of light for wire)
- **Latency** = L = T-delay + P-delay

Data Link Layer

- Functions of the data link layer:
  1. Provide a well-defined service interface to network layer
  2. Handling transmission errors
  3. Data flow regulation
- Primary process:
  - Take **packets** from network layer, and encapsulate them into **frames** (containing a header, a payload, a trailer)

Framing

- Methods:
  - Character (Byte) count
  - Flag bytes with byte stuffing
  - Start and end flags with bit stuffing
- Most data link protocols use a combination of character count and one other method

Error Control

- Adding check bits to ensure that a garbled message by the physical layer is not considered as the original message by the receiver
- Error Control deals with
  - **<u>Detecting</u>** the error
    - Parity
    - Checksum
    - Cyclical Redundancy Check (CRC)
  - **<u>Correcting</u>** the error
    - Hamming Code

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 Hamming distance is 5
    - 0000011111
    - 1111100000
    - 1111111111
- 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)

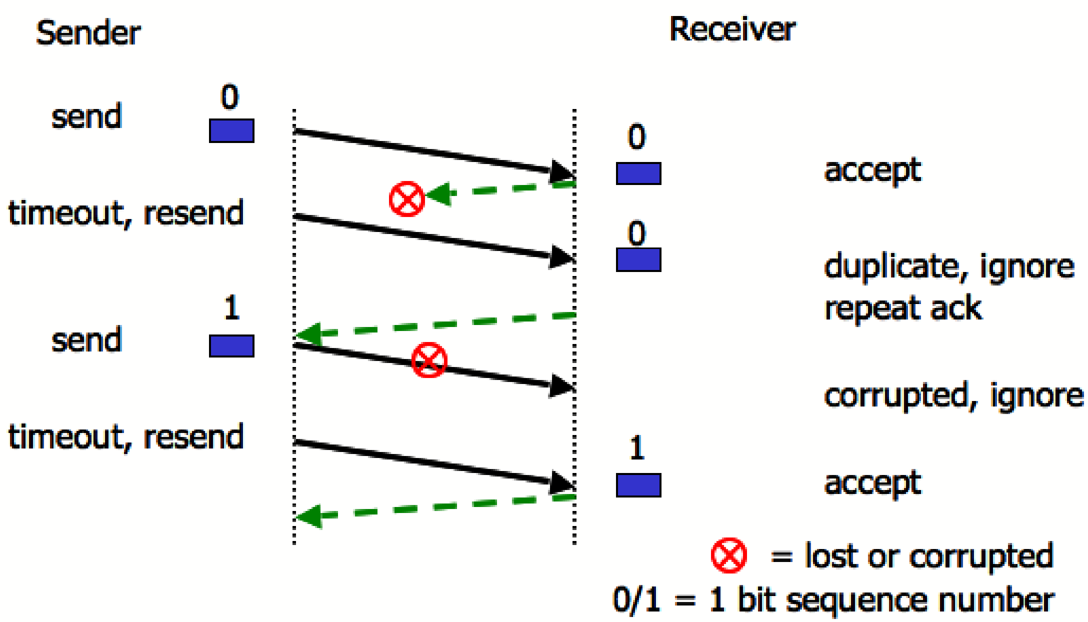
Flow Control

- The **fast senders** vs **slow receivers** problem requires a solution
- Principles to control when sender can send next frame

  Feedback based flow control: ack
  - Stop and wait
  - Sliding window: go-back-N, selective repeat

Stop and Wait Protocol

- ARQ (Automatic Repeat reQuest)
  - Ack and Timeout



Link Utilisation in Stop and Wait Protocols

Link Utilisation (U) measures efficiency in communication.

T_f = Transmission delay, time needed to transmit a frame of length L;

T_p= Propagation delay;

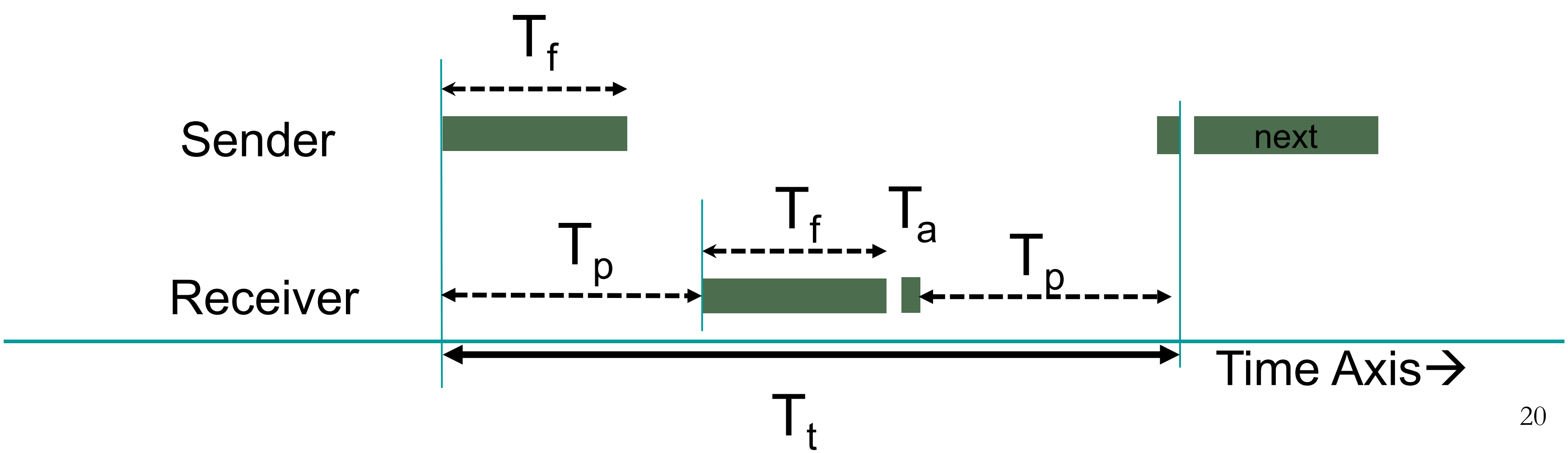
T_a= Time for transmitting an Ack, and we can assume T_a = 0.

T_t= T_f + 2T_p

U = (Time of transmitting a frame)/(Total time for the transfer) = **T_f / T_t**

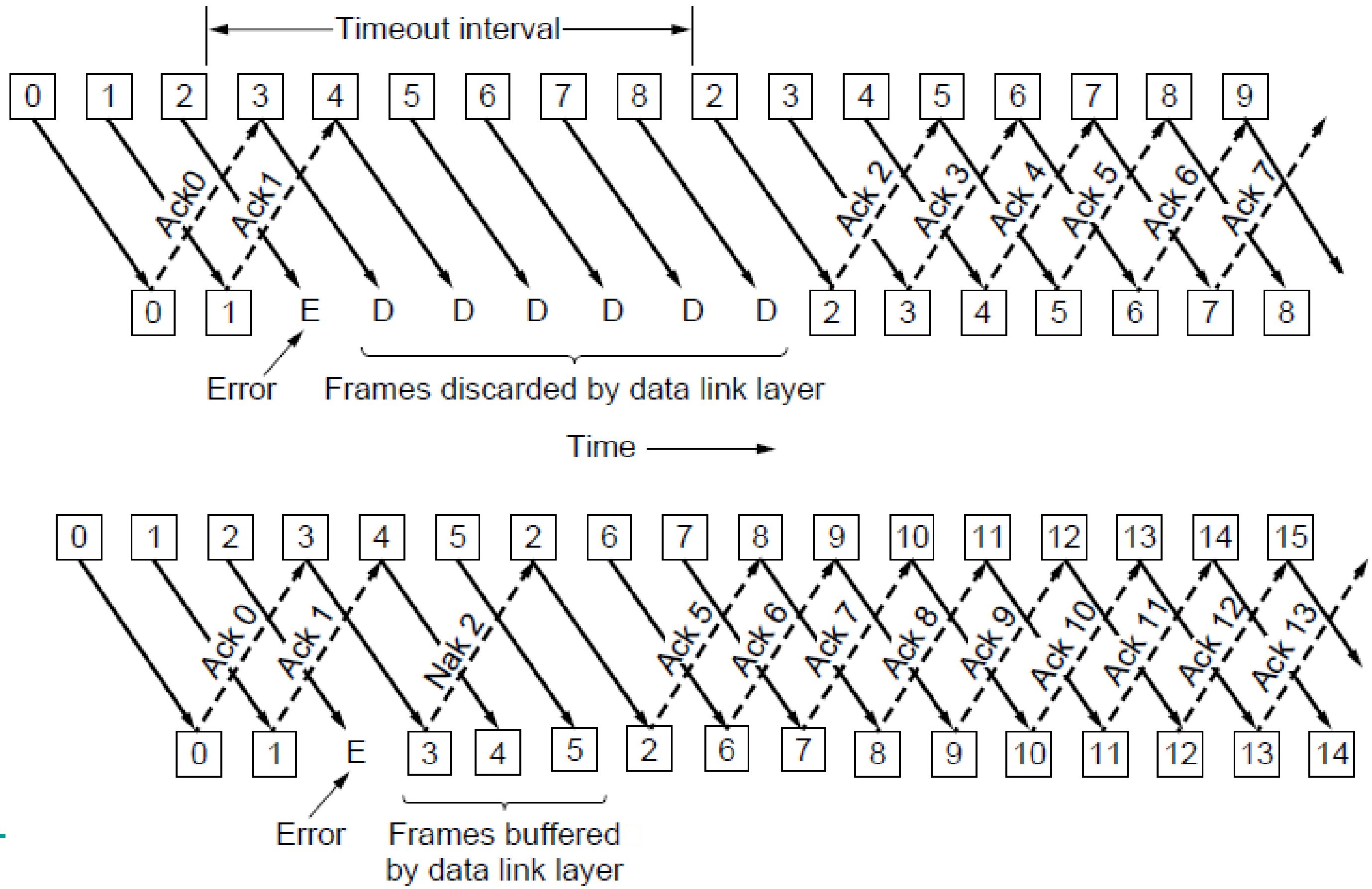
Given bit rate B and T_f = L/B, we have

$$\mathbf{U} = T_f / (T_f + 2T_p) = (L/B) / (L/B + 2T_p) = \mathbf{L/ (L+ 2T_p B)}.$$



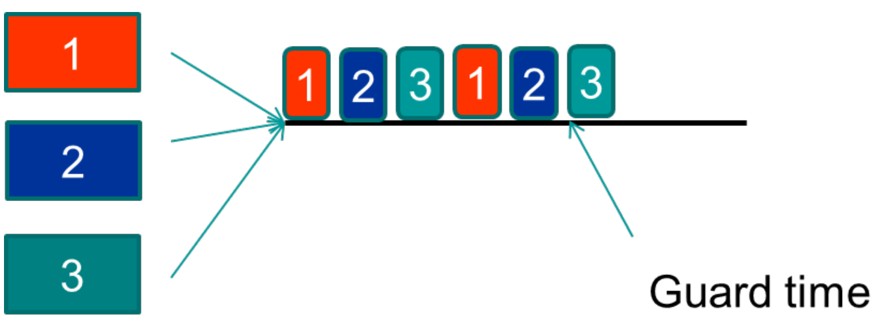
Go-Back-N vs. Selective Repeat

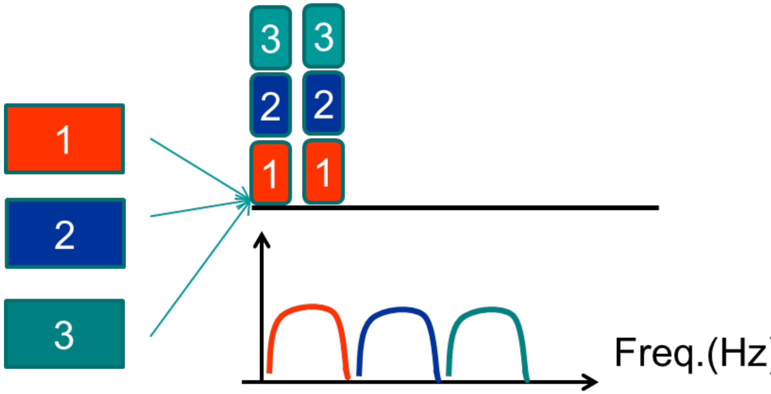
- Trade-off between efficient use of bandwidth and data link layer buffer space



Medium Access Control

- MAC sub-layer is used to assist in resolving transmission conflicts
- Static channel allocation
  - Time division multiplexing
  - Frequency division multiplexing



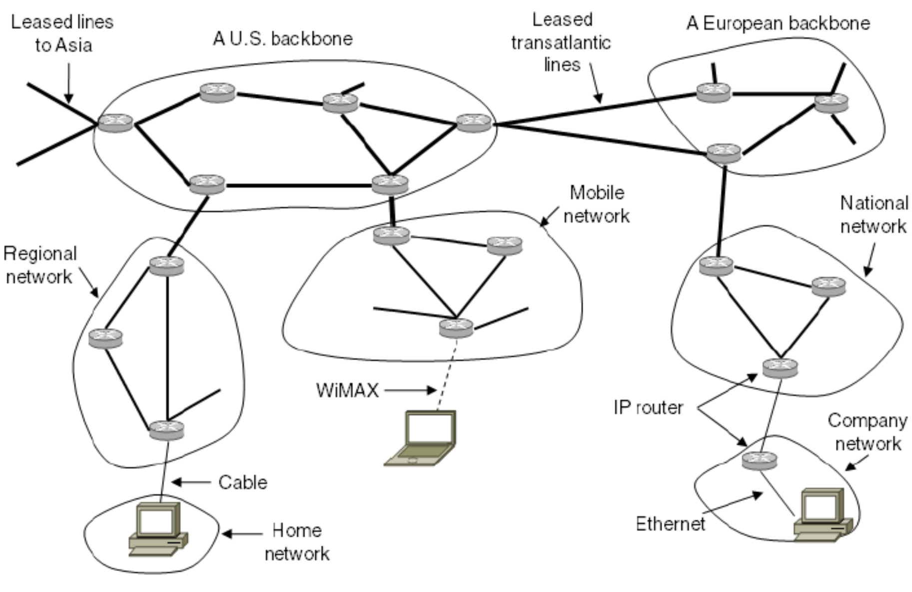


Medium Access Control

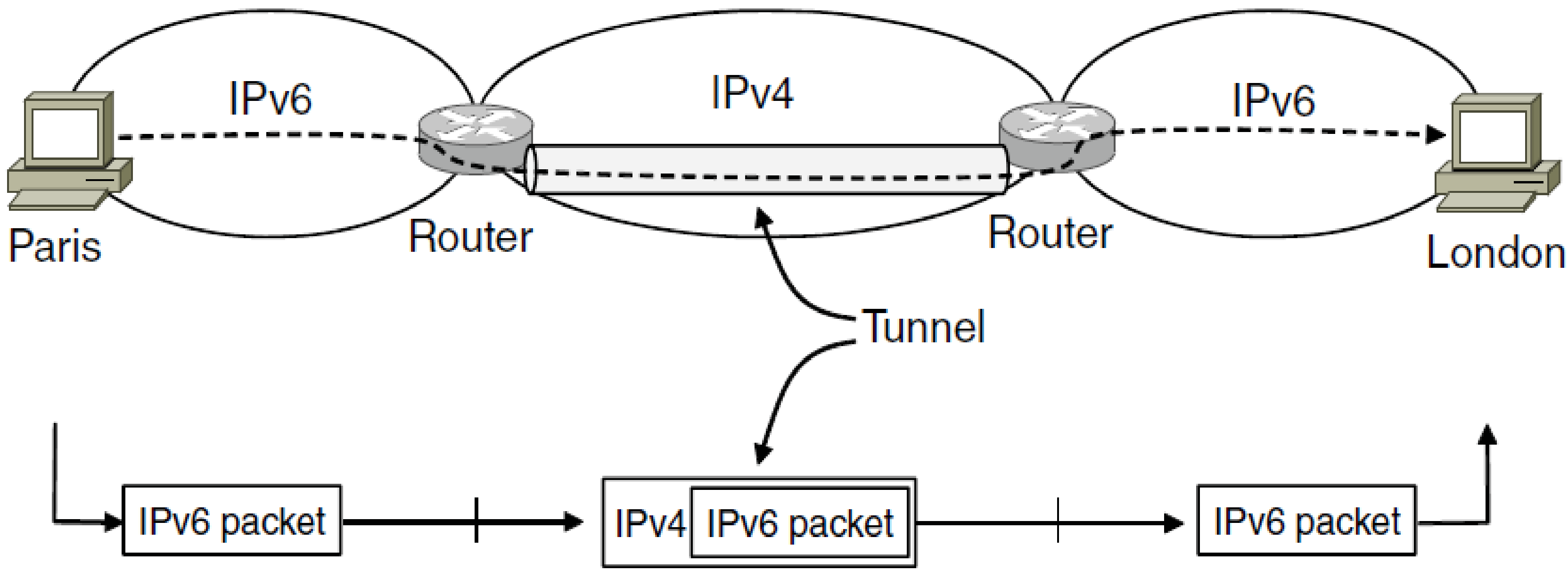
- Contention
  - ALOHA, Slotted ALOHA
  - Carrier Sense Multiple Access: 1-persistent, non-persistent, p-persistent, with collision detection
- Collision Free: bit map, binary countdown
- Limited Contention: adaptive tree walk
- Wireless LANs: MACA/MACAW

Network Layer

- Internet is a collection of many networks that is interconnected by the IP protocol
- Provides a **best-effort** service to **route datagrams** from source host to destination host



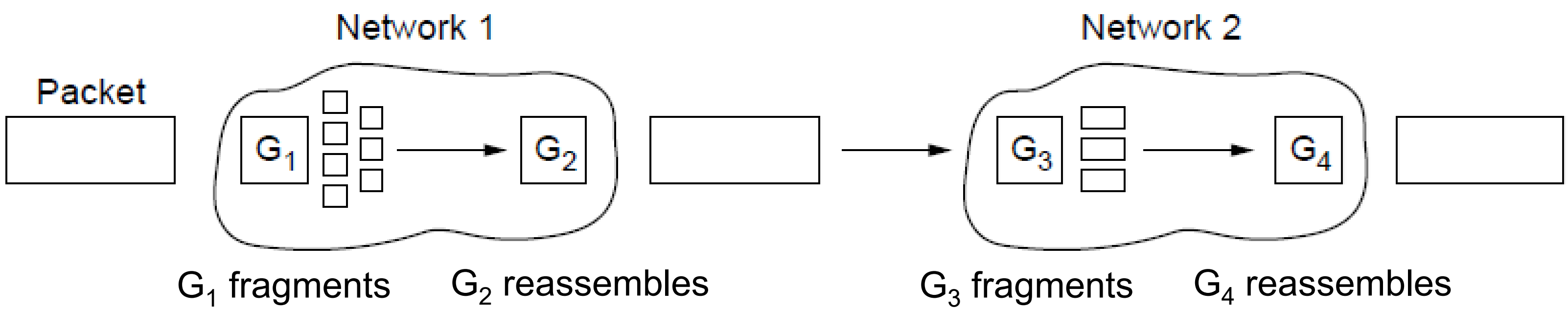
Connecting Different Networks (1)



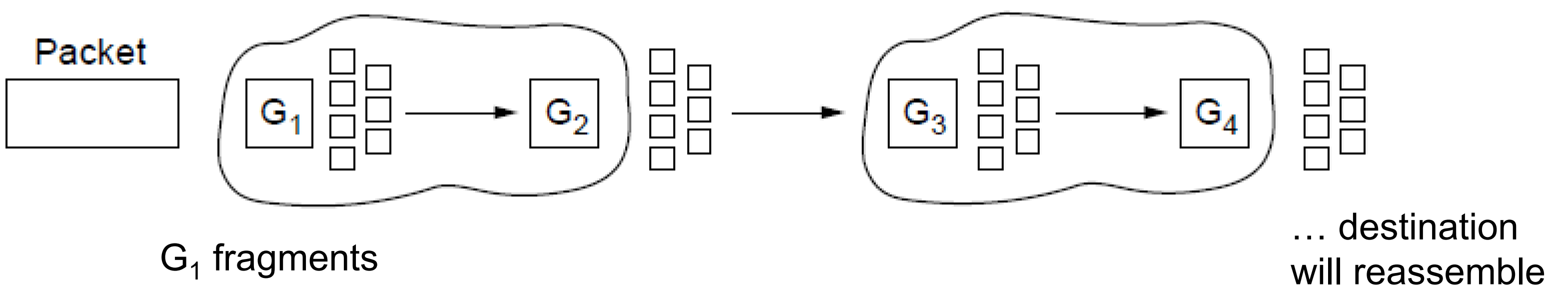
Tunneling IPv6 Packets through IPv4

Connecting Different Networks (2)

- Large packets need to be routed through a network whose maximum packet size is too small.
- **Solution: Fragmentation and Reassembly**.



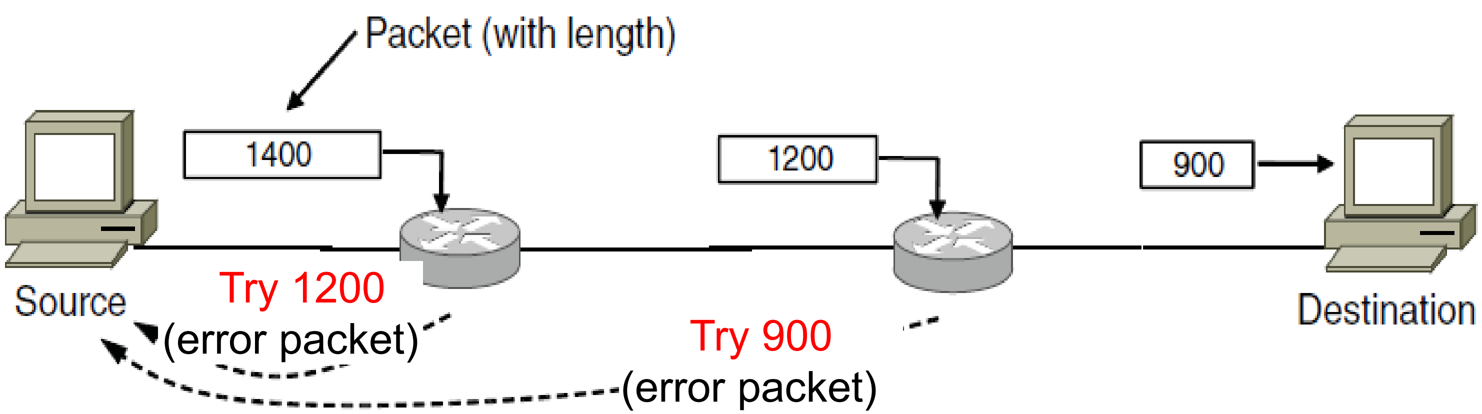
a) Transparent – packets fragmented / reassembled in each network.



b) Non-transparent – fragments are reassembled at destination.
Each packet requires packet number, byte offset, end of packet flag.

Connecting Different Networks (3)

- Path MTU Discovery: alternative to Fragmentation
- Advantage: the source knows what length packet to send
- If the routes and path MTU change, new error packets will be triggered and the source will adapt to the new path

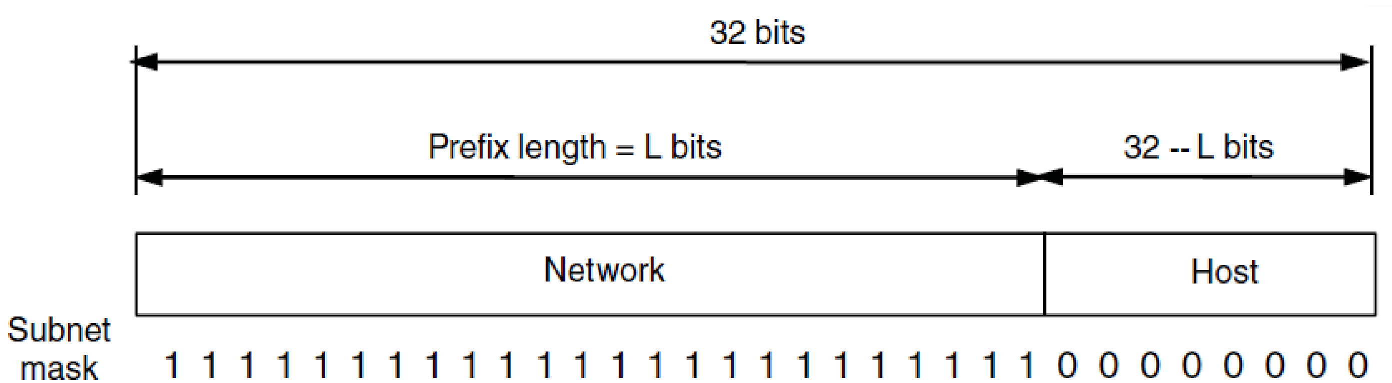


IP Addresses

- network portion + host portion
- **Prefix:** determined by the network portion, all hosts on a single network has the same network portion.

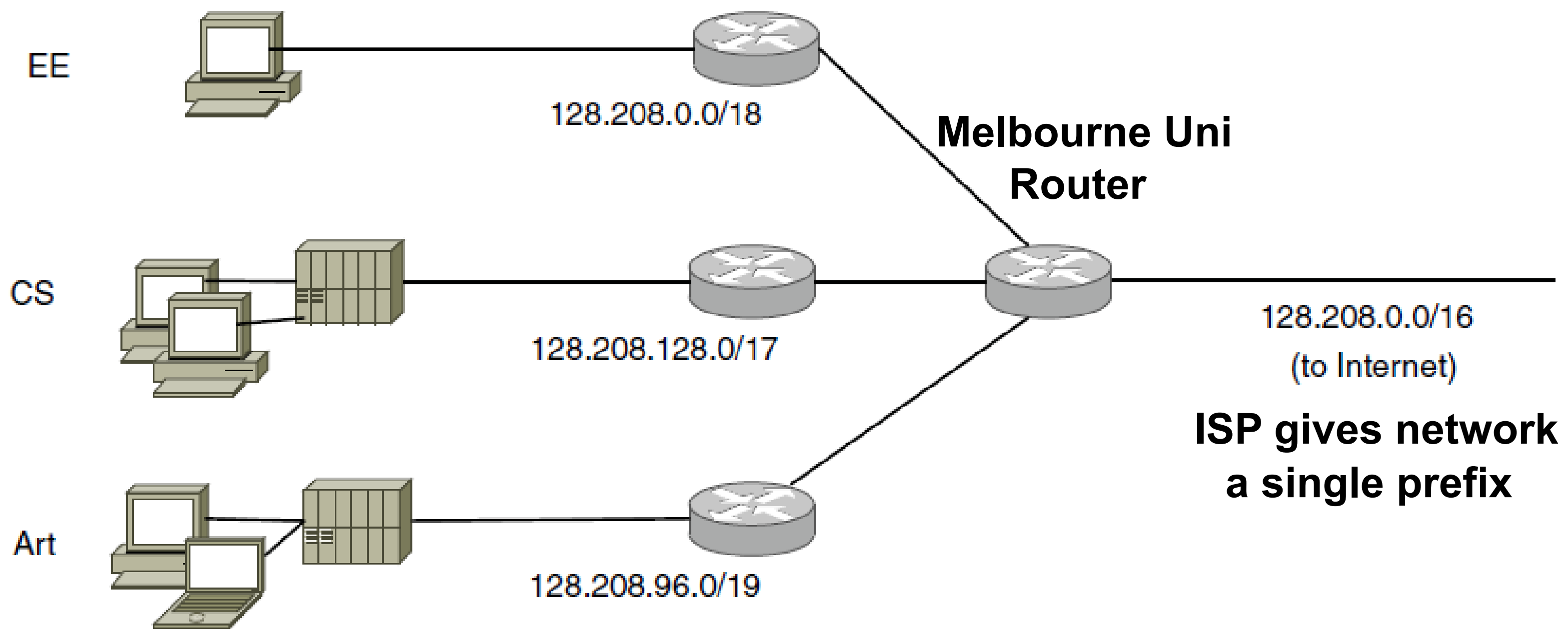
  prefix is written as: lowest address/bit-length

  18.2.31.0/24, 18.2.0.0/16
- **Subnet mask**: all 1s in the network portion
- **Extract** prefix: ANDed the IP address with the subnet mask



Subnets

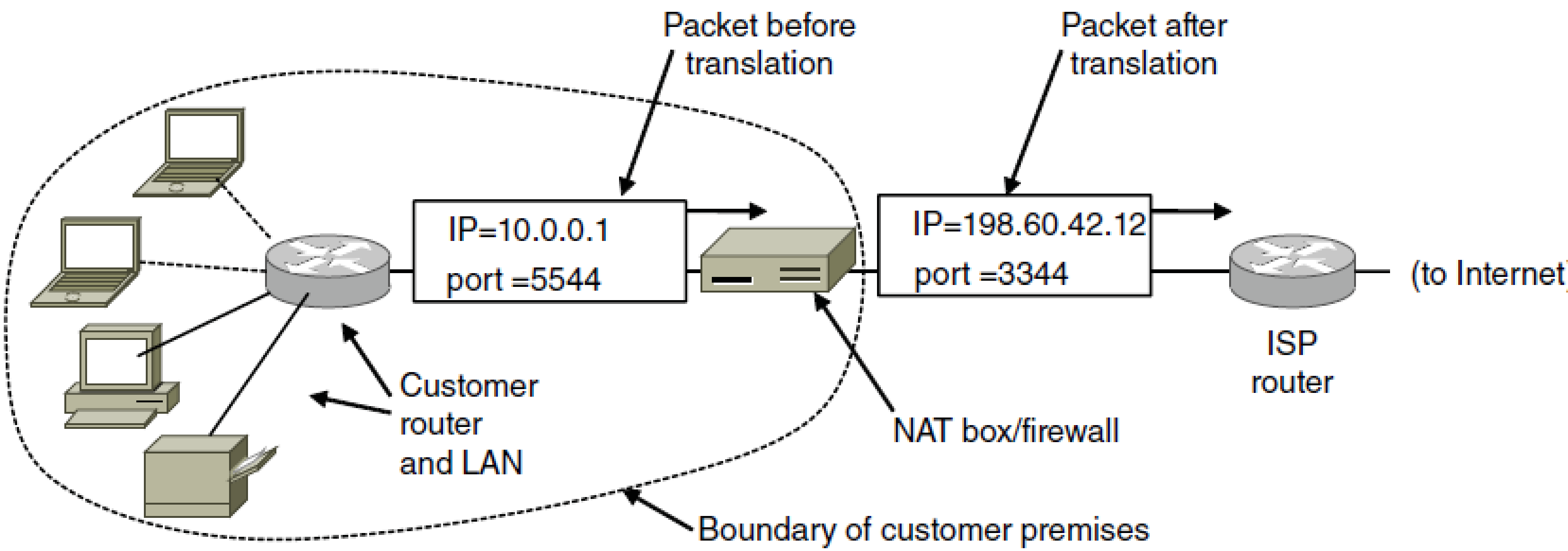
- Subnetting allows networks to be split into several parts for internal uses whilst acting like a single network for external use
- Looks like a single prefix outside the network



Network is divides into subnets internally

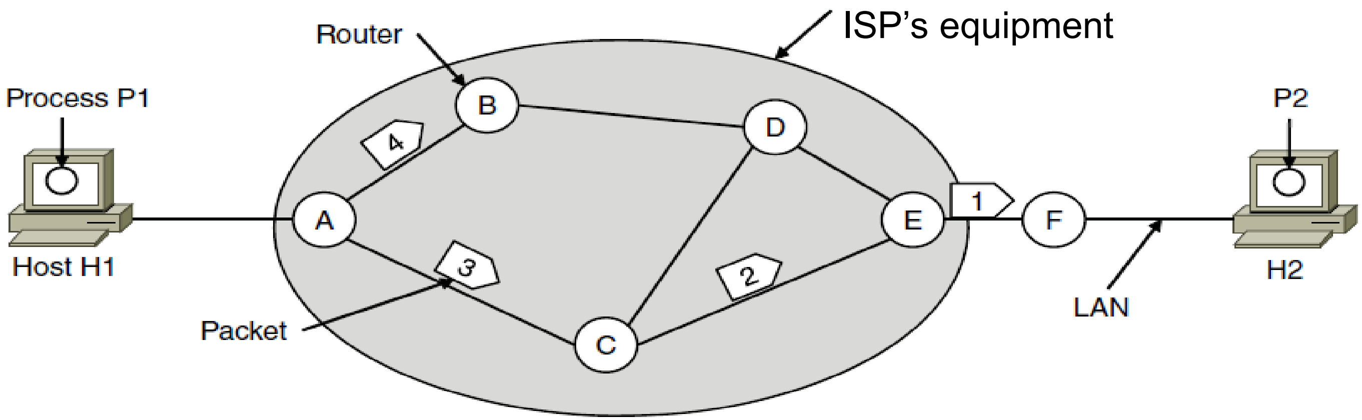
Network Address Translation (NAT)

- NAT box maps one external IP address to many internal IP addresses
  - Uses TCP/UDP port to distinguish connections
  - Violates layering; popular tool in conserving global address space



Routing within a Datagram Subnet

- **Connectionless - post office model**: packets are routed individually based on destination addresses in them
- Packets can take different paths
- E.g., P1 sends a long message to P2



A's table (initially)

Dest.	Line
A	⊠
B	B
C	C
D	B
E	C
F	C

A's table (later)

A	⊠
B	B
C	C
D	B
E	B
F	B

C's Table

A	A
B	A
C	⊠
D	E
E	E
F	E

E's Table

A	C
B	D
C	C
D	D
E	⊠
F	F

Routing table (can be fixed or change over time)

Routing algorithm – manages the routing table

Virtual-Circuit vs. Datagram Subnets

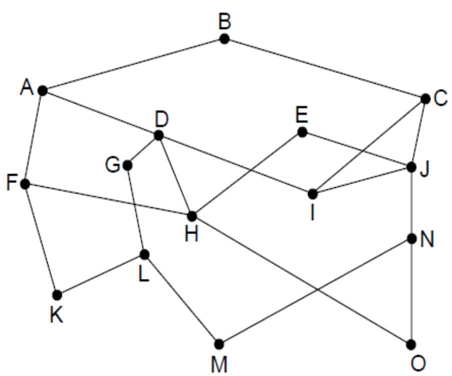
Issue	Datagram network	Virtual-circuit network
Circuit setup	Not needed	Required
Addressing	Each packet contains the full source and destination address	Each packet contains a short VC number
State information	Routers do not hold state information about connections	Each VC requires router table space per connection
Routing	Each packet is routed independently	Route chosen when VC is set up; all packets follow it
Effect of router failures	None, except for packets lost during the crash	All VCs that passed through the failed router are terminated
Quality of service	Difficult	Easy if enough resources can be allocated in advance for each VC
Congestion control	Difficult	Easy if enough resources can be allocated in advance for each VC

Routing Algorithms

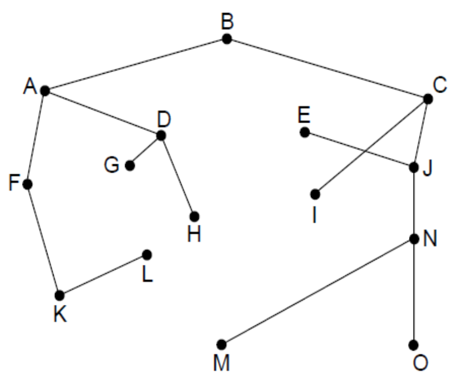
- Non-adaptive
  - Shortest path routing
  - Flooding
- Adaptive
  - Distance vector routing
  - Link state routing
- Hierarchical routing
- Broadcasting routing
- Multicasting routing

Shortest Path Routing

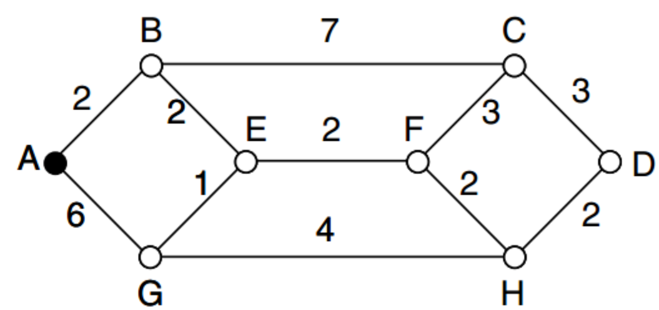
- To choose a path between 2 routers, the algorithm finds the shortest path between them on the graph
- Metrics: number of hops, distance, delay etc.



Network

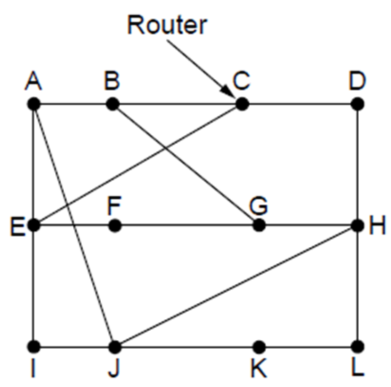


Sink tree of best paths to router B



Distance Vector Routing

- Each router maintains a table which includes the best known distance to each destination and which line to use to get there.
- Global information shared locally.



Network

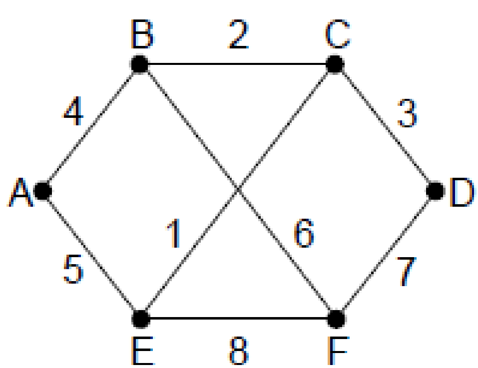
To	A	I	H	K	New estimated delay from J	Line
A	0	24	20	21	8	A
B	12	36	31	28	20	A
C	25	18	19	36	28	I
D	40	27	8	24	20	H
E	14	7	30	22	17	I
F	23	20	19	40	30	I
G	18	31	6	31	18	H
H	17	20	0	19	12	H
I	21	0	14	22	10	I
J	9	11	7	10	0	–
K	24	22	22	0	6	K
L	29	33	9	9	15	K
	JA delay is 8	JI delay is 10	JH delay is 12	JK delay is 6		

Vectors received at J from neighbors A, I, H and K

New vector for J

Link State Routing

- An alternative to distance vector: **too long to converge** after the network topology changed
- Widely used in the Internet
- More computation but simpler dynamics
- Local information shared globally using flooding



Network

Link State Packets

A		B		C		D		E		F	
Seq.		Seq.		Seq.		Seq.		Seq.		Seq.	
Age		Age		Age		Age		Age		Age	
B	4	A	4	B	2	C	3	A	5	B	6
E	5	C	2	D	3	F	7	C	1	D	7
		F	6	E	1			F	8	E	8

LSP for each node

Broadcast Routing

- Broadcast routing allows hosts to send messages to all other hosts.
  - Single distinct packet to each destination
  - Multi-destination routing
  - Flooding
  - Reverse path forwarding