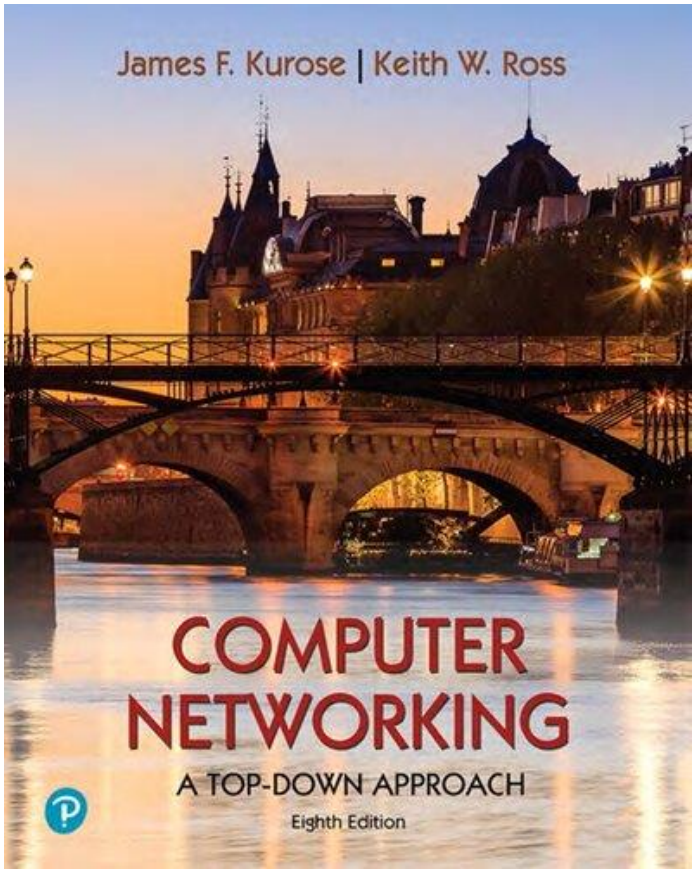
I3304
Network administration and security

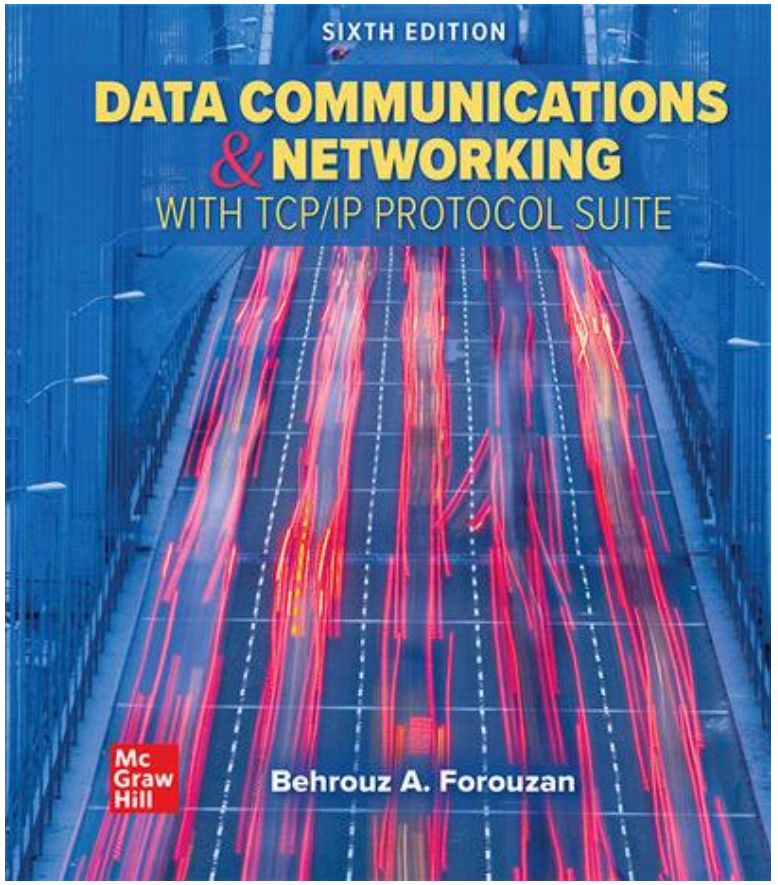
Ahmad Fadlallah

Before to Start

- I3304: 50 Hours course
- Instructor Information
  - Instructor: Ahmad Fadlallah
  - Office Hours: department schedule or by appointment
  - email: ahmad.fadlallah@ul.edu.lb
- Course Information
  - Lectures (Labs included):
    - Wednesday 08:00 –9:40
    - Thursday 16:30-18:00
  - Exercises: integrated in the course

Reference Textbooks

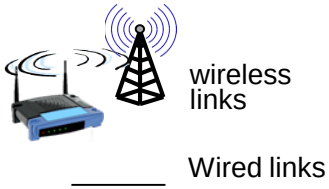


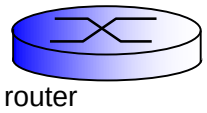


Outline

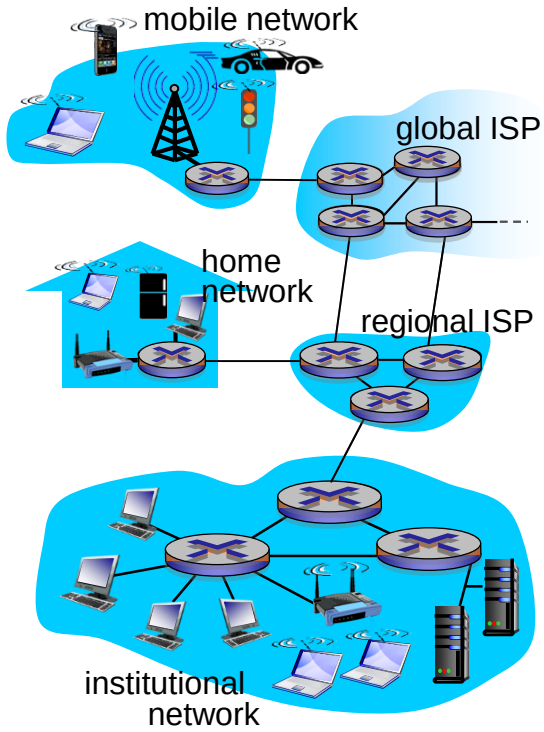
- Introduction
  - Introduction to the course
  - Recall Network Basics (I2208)
- Network Layer
  - IP packet structure (Recall)
  - Static Routing
  - Dynamic Routing Algorithm
  - Dynamic Routing Protocols
  - NAT (Network Address Translation)
- Transport Layer
  - Function of the transport layer
  - UDP Protocol
  - TCP Protocol
    - Connection management
    - Flow control
    - Congestion control
- Application Layer
  - HTTP protocol
  - FTP protocol
  - Mail protocols
  - DNS
- Introduction to Security
  - Security services
  - Cryptography
  - Digital Signature
  - Principle of network security protocols

What's the Internet: "nuts and bolts" view





- Billions of connected computing devices:
  - hosts = end systems
  - running network apps
- Communication links
  - fiber, copper, radio, satellite
  - transmission rate: bandwidth
- Packet switches: forward packets (chunks of data)
  - Routers and switches



“Fun” Internet-connected devices

IP picture frame
http://www.ceiva.com/

Web-enabled toaster +
weather forecaster

Tweet-a-watt:
monitor energy use

Internet
refrigerator

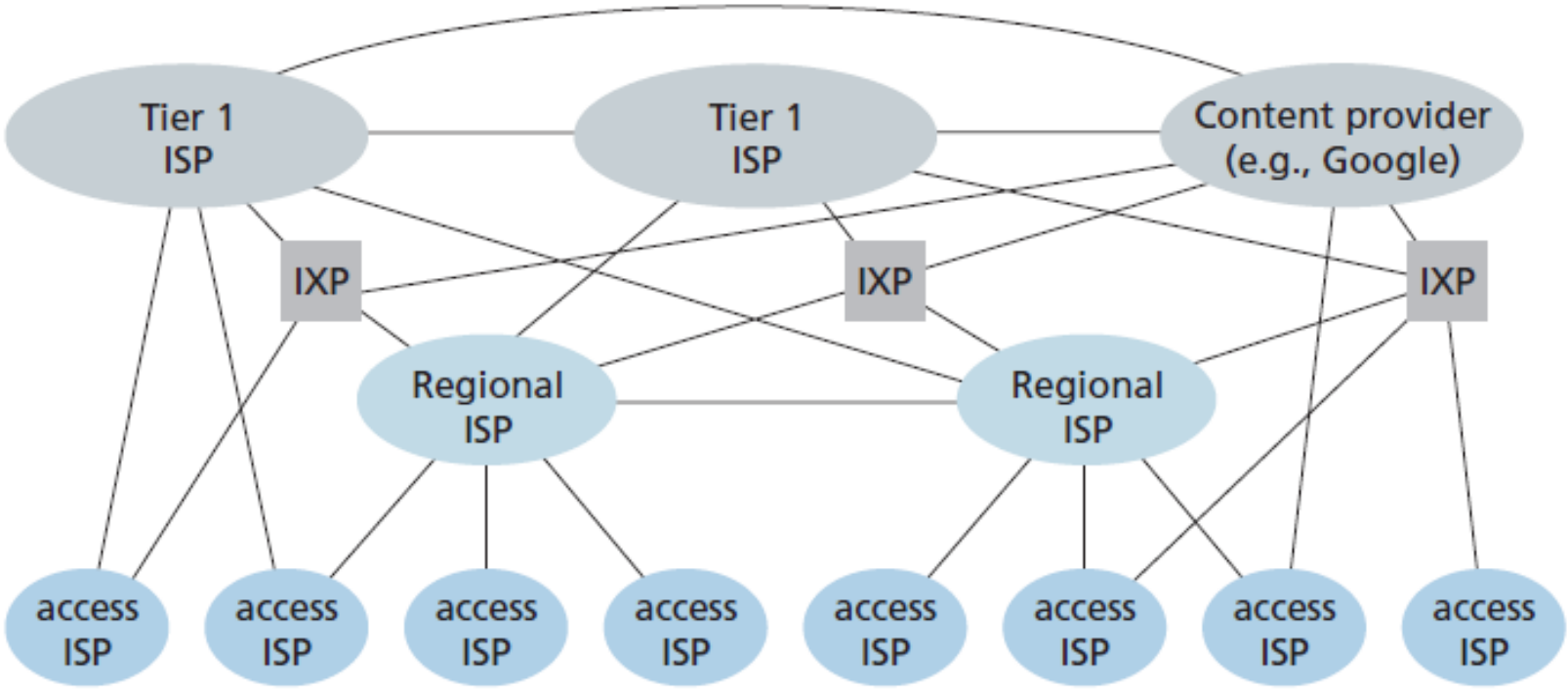
Slingbox: watch,
control cable TV remotely

sensorized,
bed
mattress

Internet phones

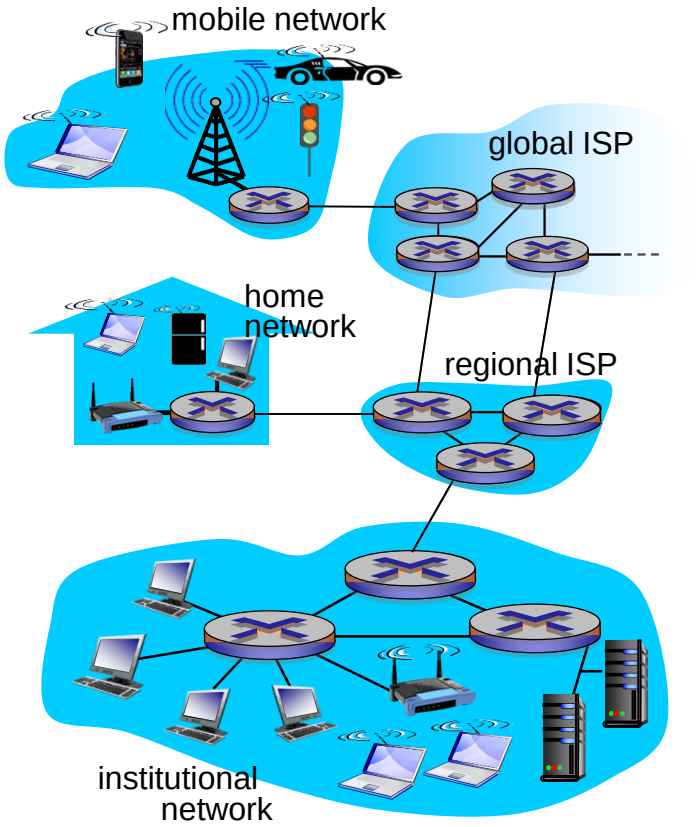
What's the Internet: "nuts and bolts" view

- Internet: "network of networks"
  - Interconnected ISPs



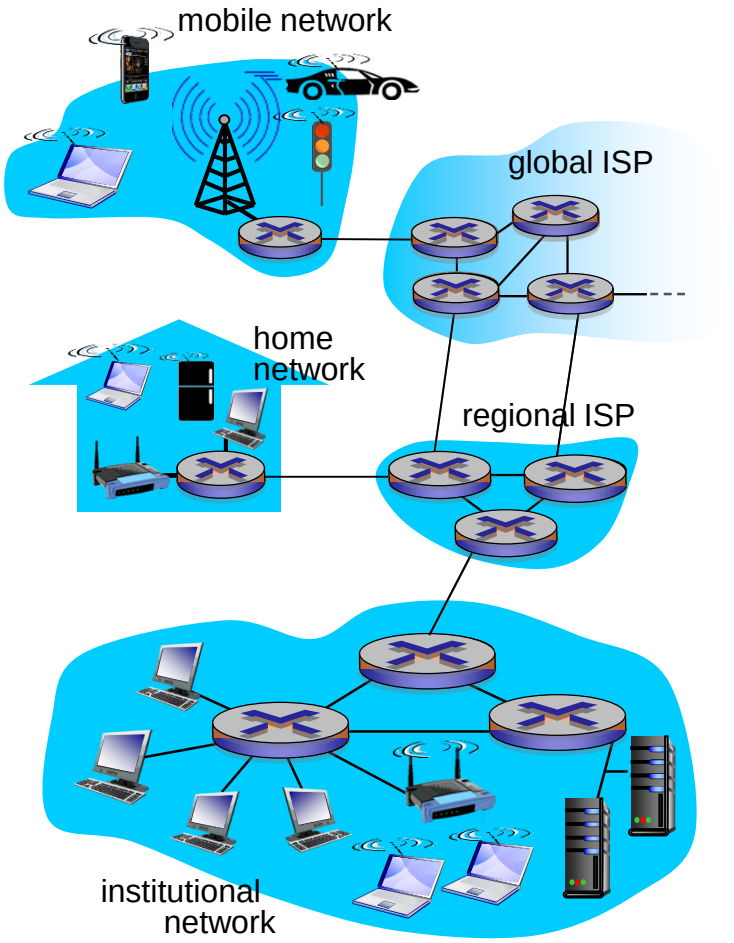
What's the Internet: "nuts and bolts" view

- Protocols control sending, receiving of messages
  - e.g., TCP, IP, HTTP, Skype, 802.11
- Internet standards
  - RFC: Request for comments
  - IETF: Internet Engineering Task Force



What's the Internet: a service view

- Infrastructure that provides services to applications:
  - Web, VoIP, email, games, e-commerce, social nets, …
- Provides programming interface to apps
  - hooks that allow sending and receiving app programs to "connect" to Internet
  - Provides service options, analogous to postal service



What's a protocol?

Human protocols

- "what's the time?"
- "I have a question"
- introductions

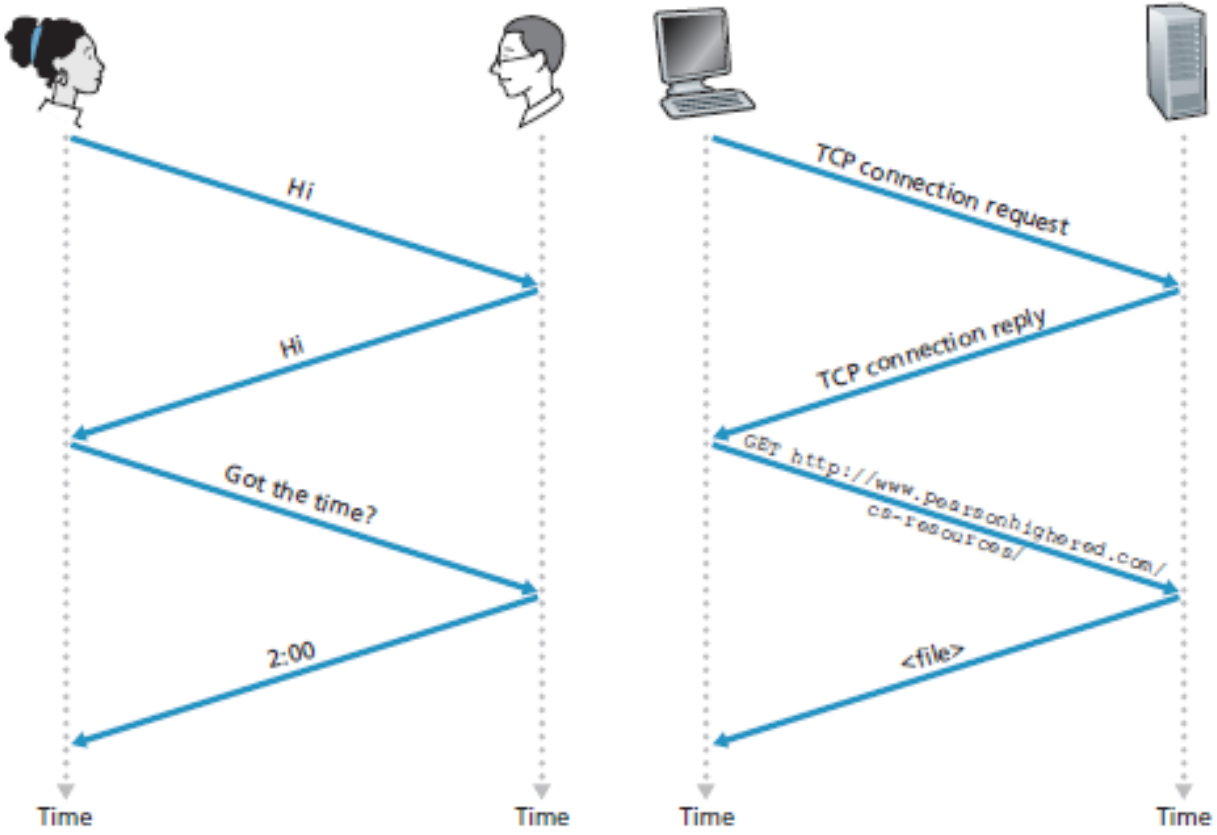
Network protocols

- Machines rather than humans
- All communication activity in Internet governed by protocols

… specific messages sent
… specific actions taken when messages received, or other events

protocols define format, order of messages sent and received among network entities, and actions taken on message transmission, receipt

What's a protocol?



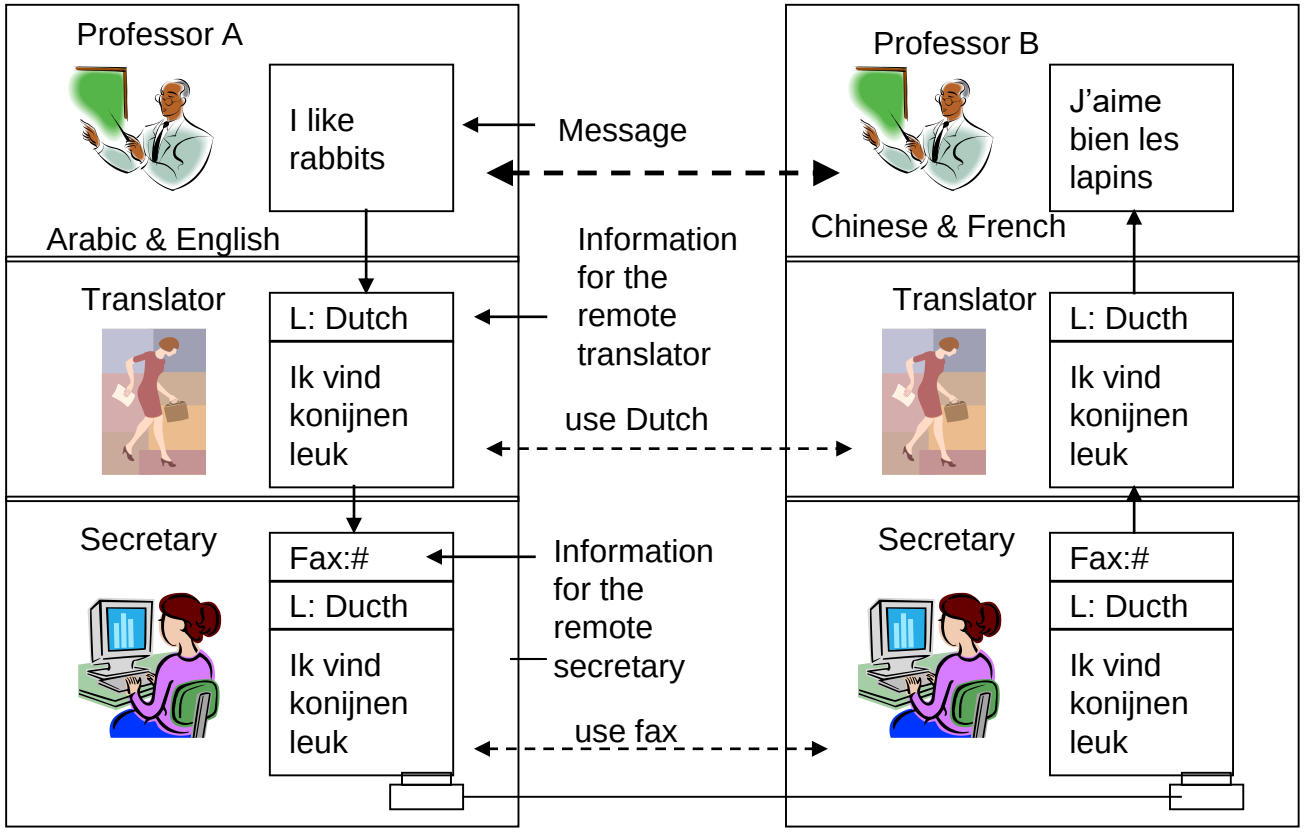
Q: other human protocols?

Why layering?

Dealing with complex systems:

- Explicit structure allows *identification*, relationship of complex system's pieces
- Modularization eases maintenance, updating of system
  - Change of implementation of layer's service transparent to rest of system

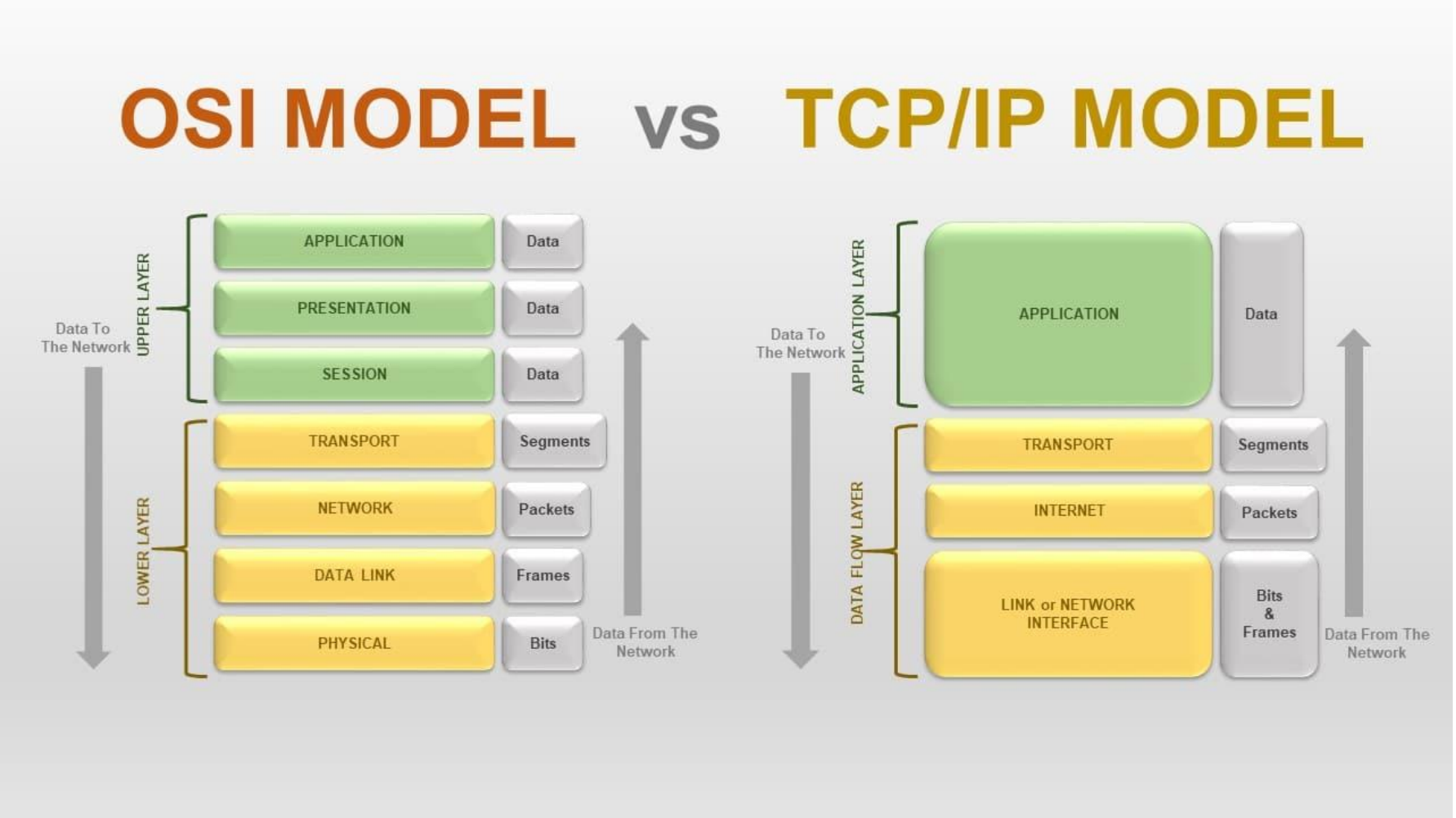
Analogy


Professor A
I like rabbits
Message
Professor B
J'aime bien les lapins
Arabic & English
Chinese & French
Information for the remote translator
Translator
L: Dutch
Ik vind konijnen leuk
use Dutch
Translator
L: Ducth
Ik vind konijnen leuk
Secretary
Fax:#
L: Ducth
Ik vind konijnen leuk
Information for the remote secretary
use fax
Secretary
Fax:#
L: Ducth
Ik vind konijnen leuk

Reference Models

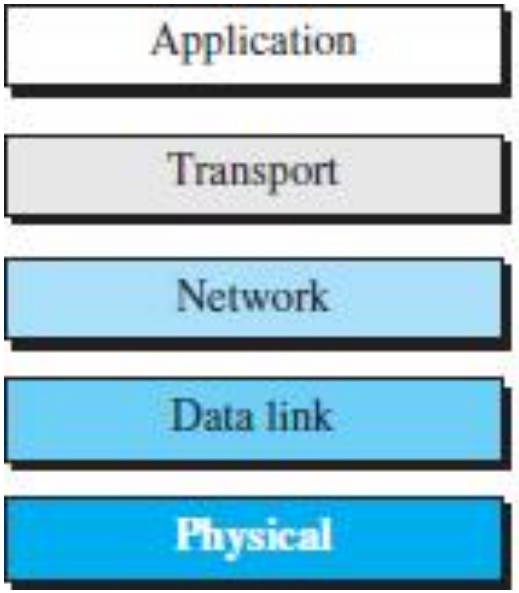
- There are two competing models for how the software is layered: the OSI and the TCP models.
- OSI (Open Systems Interconnection)
  - Developed by ISO (International Standards Organization)
  - 7 layers
- TCP (Transfer Control Protocol)
  - Used in the ARPANET and in the Internet.
  - Common mechanism that is surpassing the OSI Model.
  - 5 layers

Reference Models



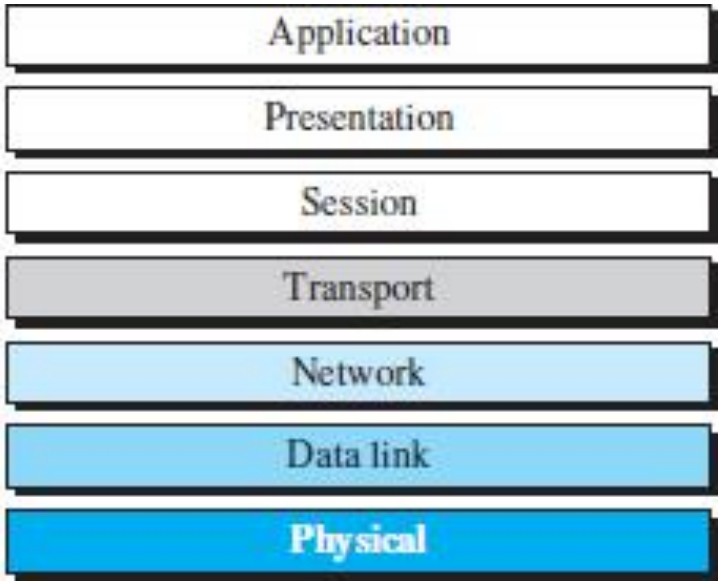
Internet Protocol Stack

- **Application**: supporting network applications
  - FTP, SMTP, HTTP
- **Transport**: process-process data transfer
  - TCP, UDP
- **Network**: routing of datagrams from source to destination
  - IP, routing protocols
- **Link**: data transfer between neighboring network elements
  - Ethernet, 802.111 (WiFi), PPP
- **Physical**: bits “on the wire”

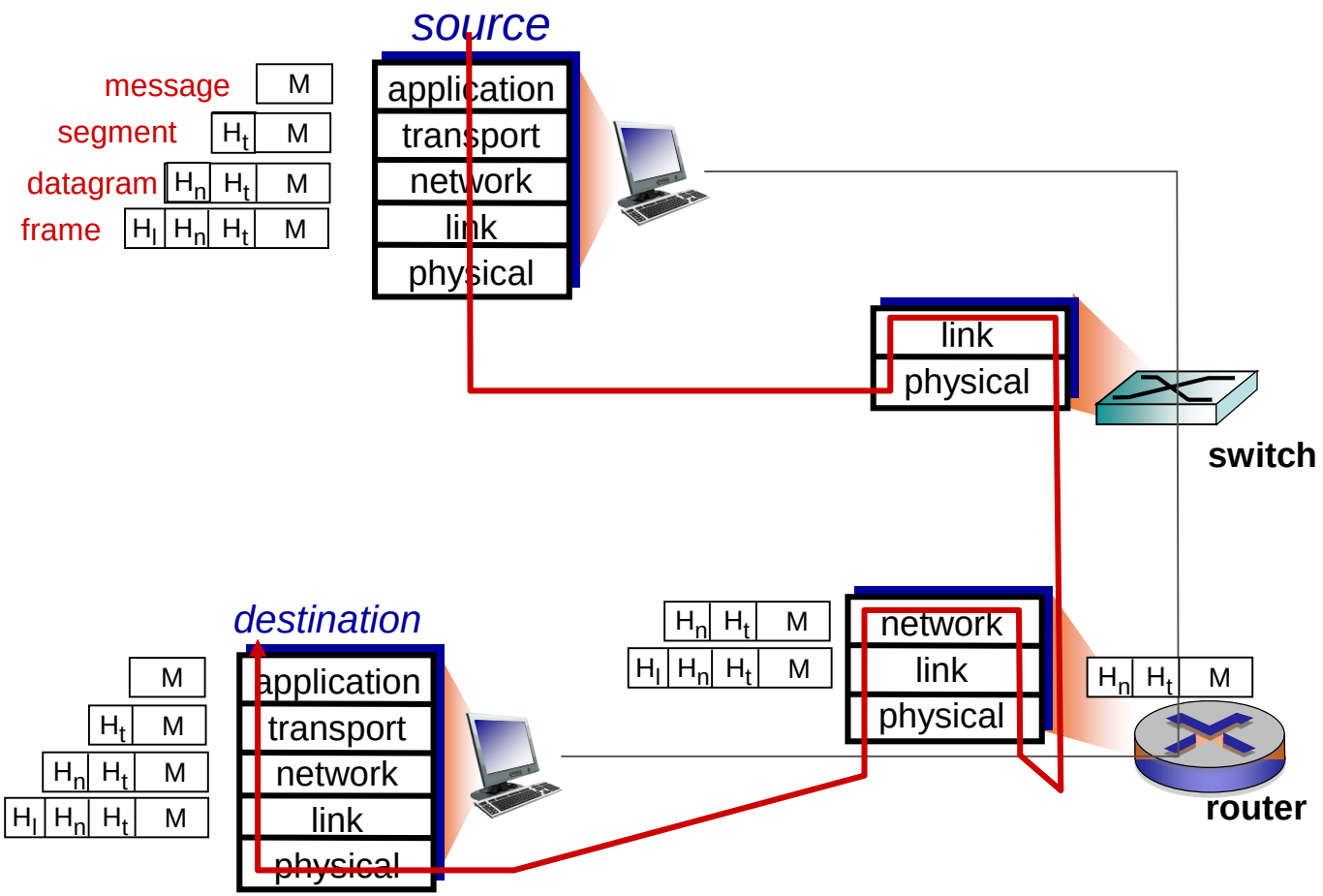


ISO/OSI reference model

- **Presentation**: allow applications to interpret meaning of data, e.g., encryption, compression, machine-specific conventions
- **Session**: *synchronization*, check-pointing, recovery of data exchange
- Internet stack "missing" these layers!
  - these services, if needed, must be implemented in application
  - needed?

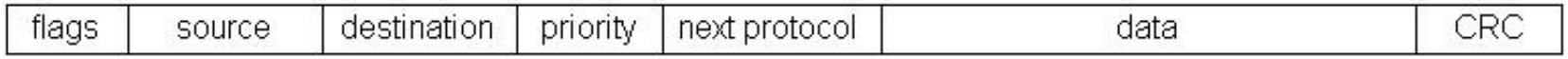


Encapsulation

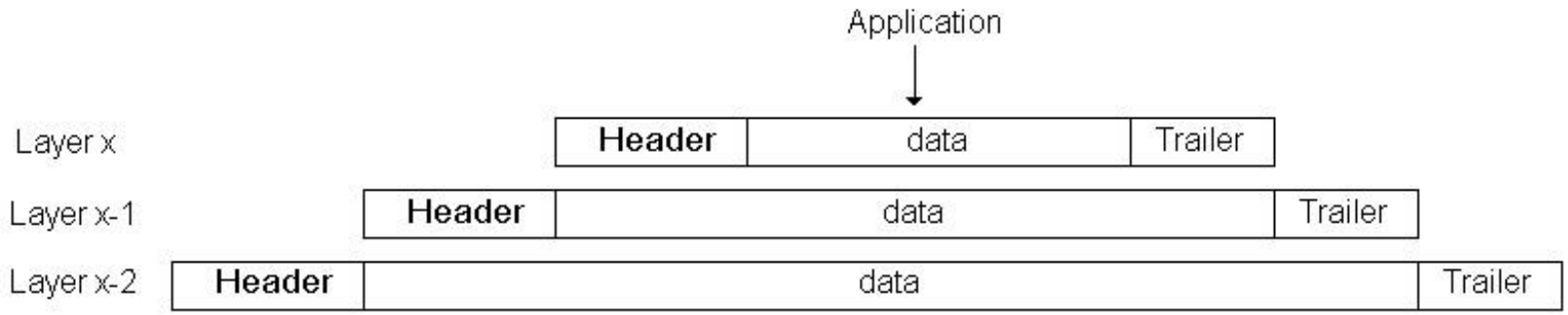


Reference Models

- Headers, Data, and Trailers



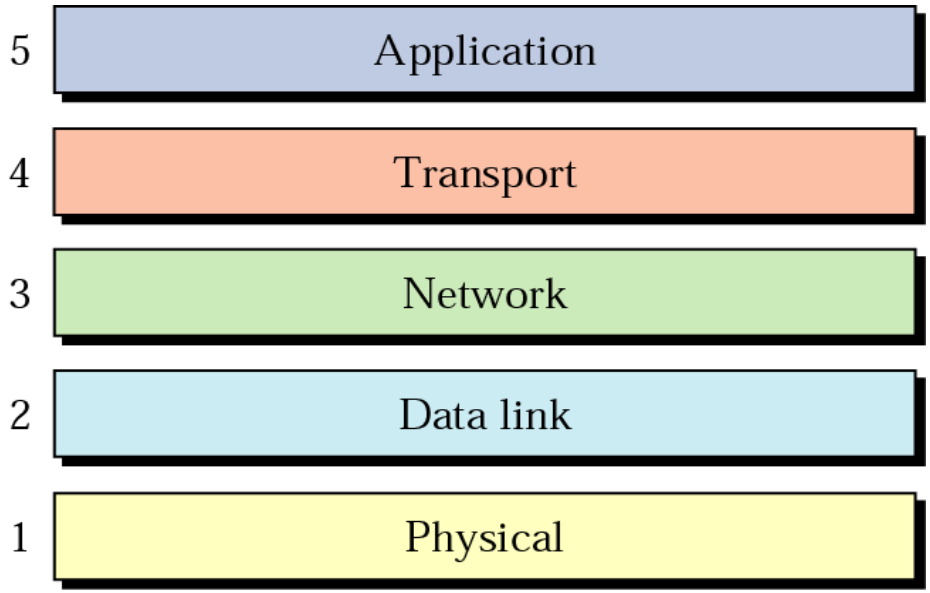
- Encapsulation



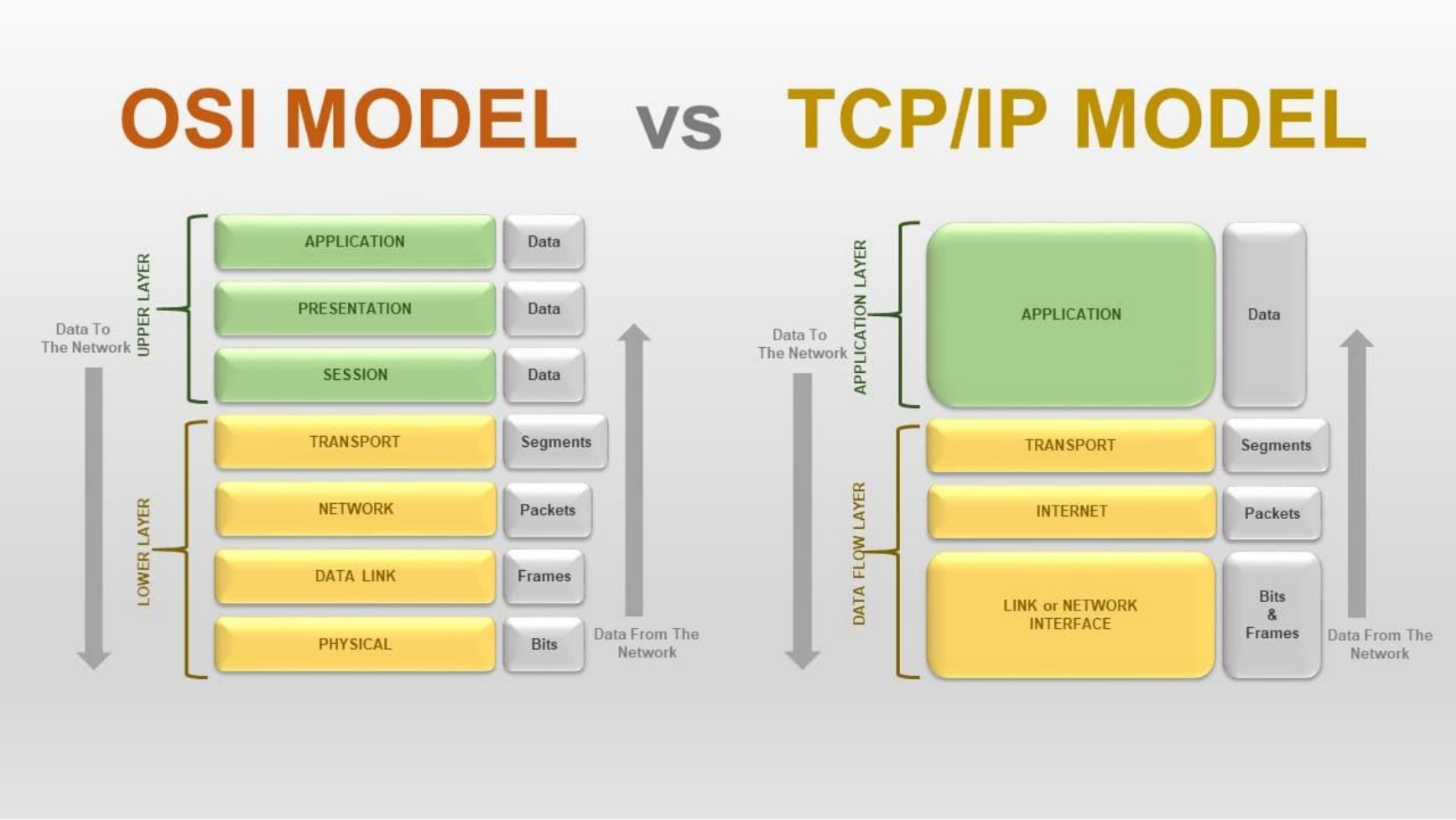
TCP/IP MODEL

Internet Layers

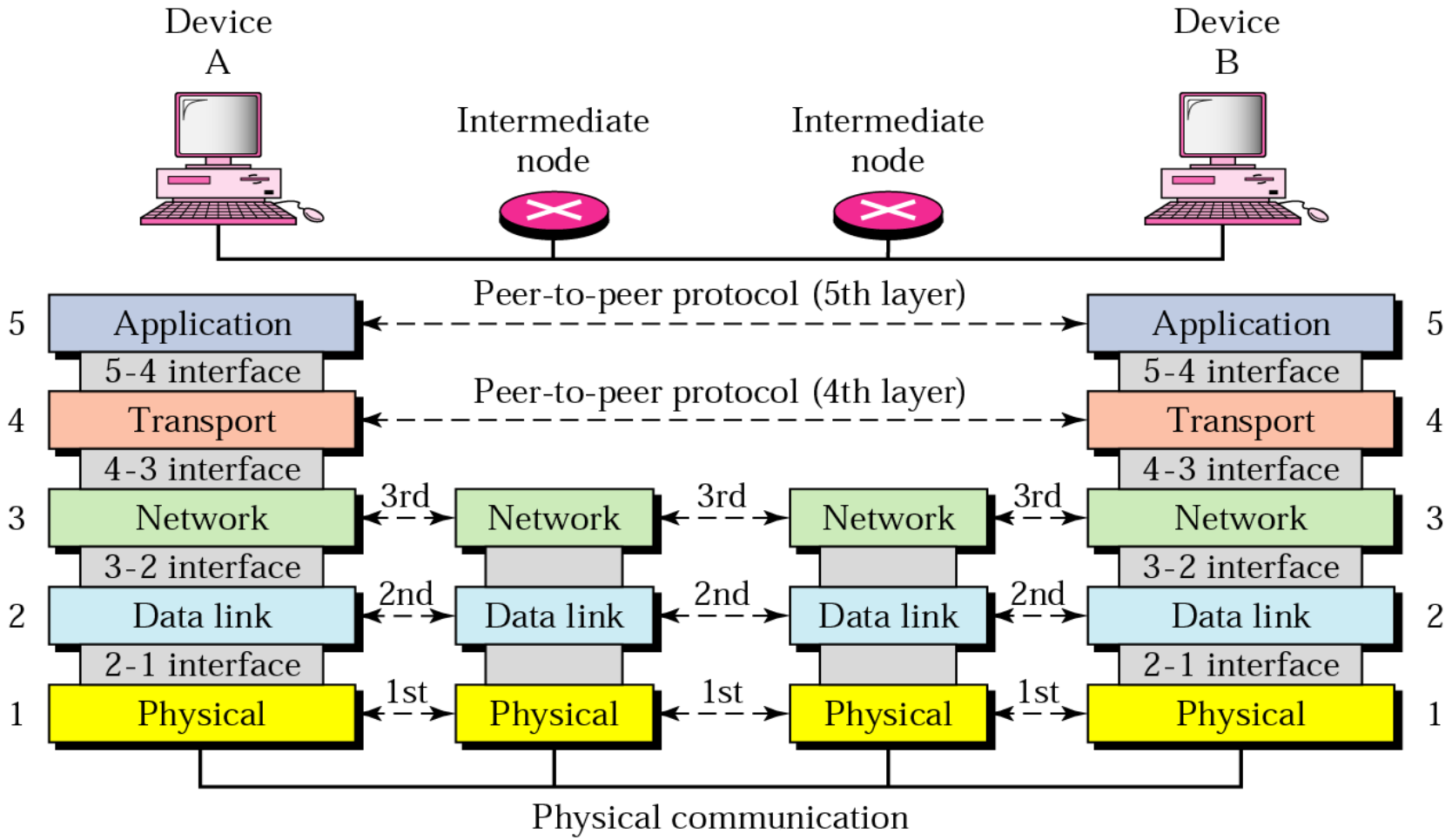
- Internet Model
  - Dominant model in data communications and networking
  - 5 ordered layers; often referred to as TCP/IP protocol suite



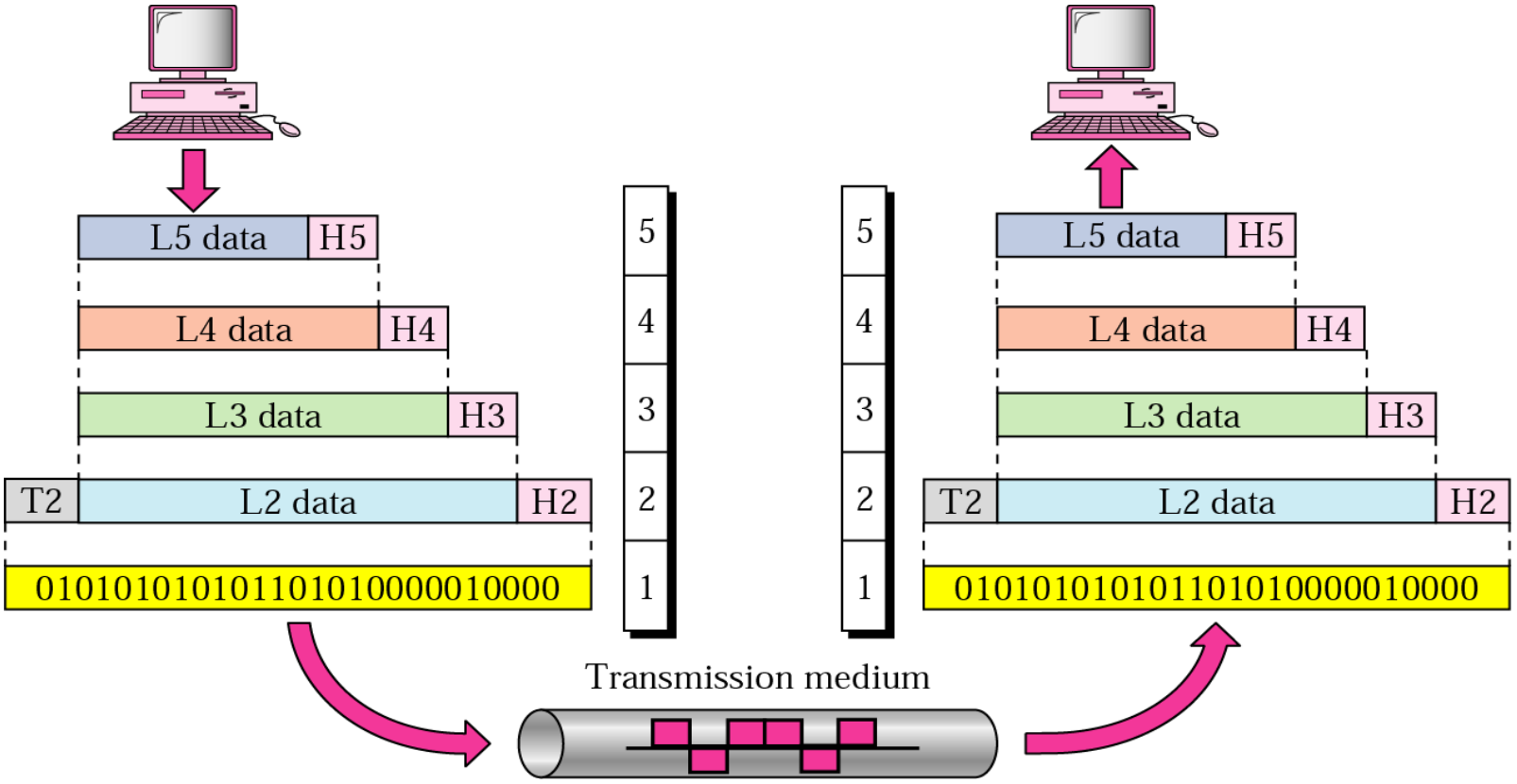
Internet Layers



Peer-to-Peer Processes

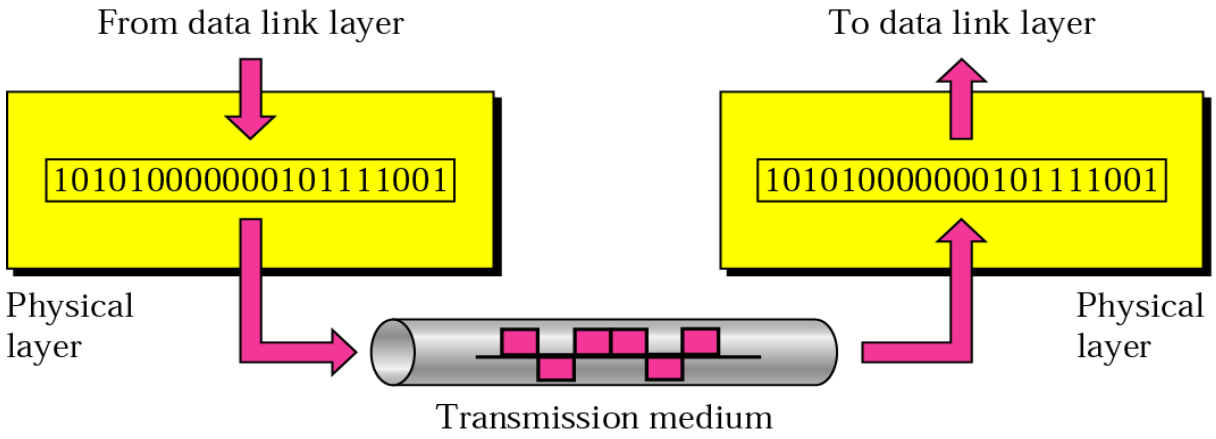


An exchange using the Internet model



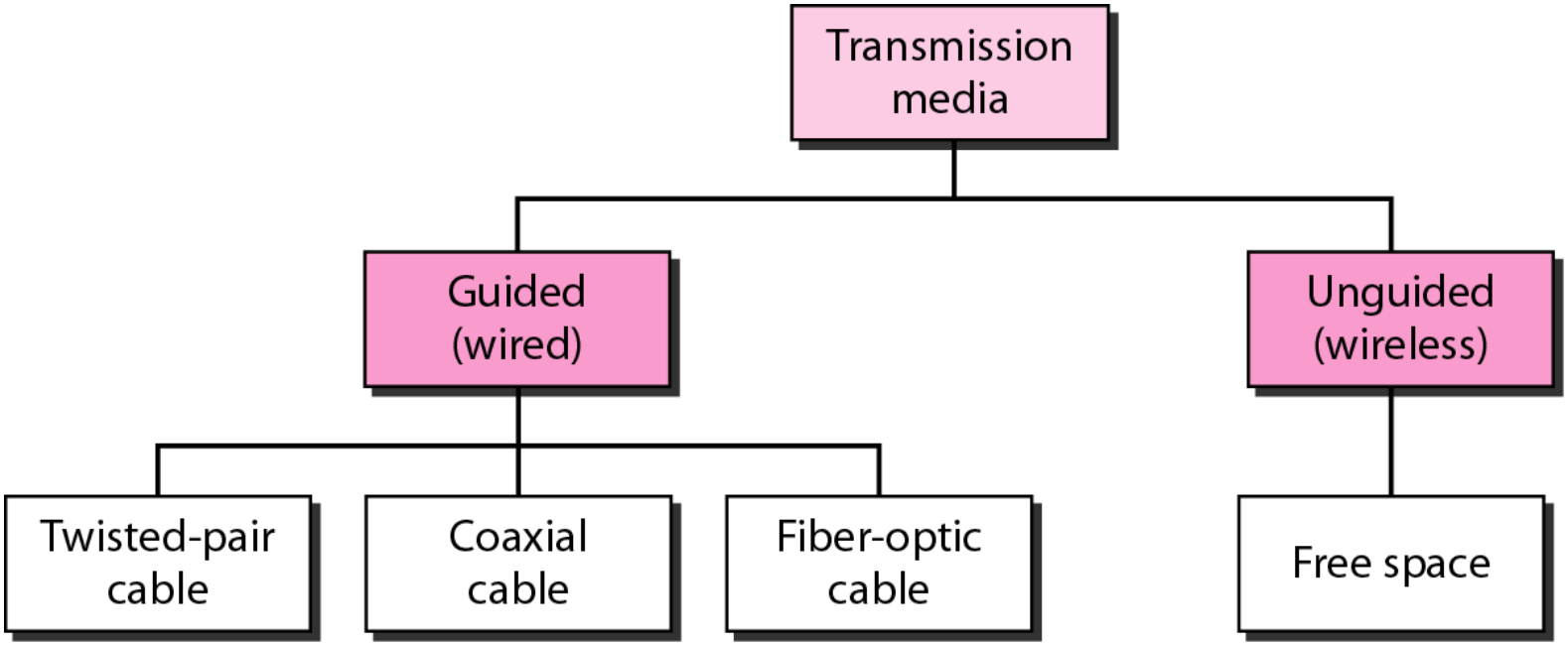
Physical Layer

- Physical characteristics of interfaces and media
  - Representation of bits without interpretation
  - **Data rate**: number of bits per second
  - Synchronization of bits



The physical layer is responsible for transmitting individual bits from one node to the next.

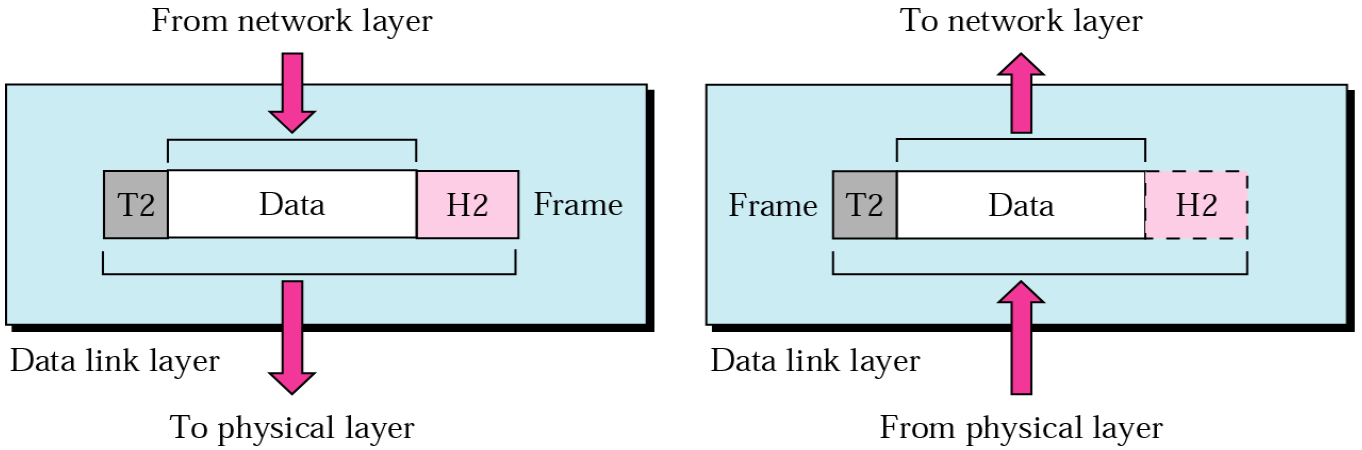
Transmission Media



Data link Layer

Data Link Layer Responsibilities

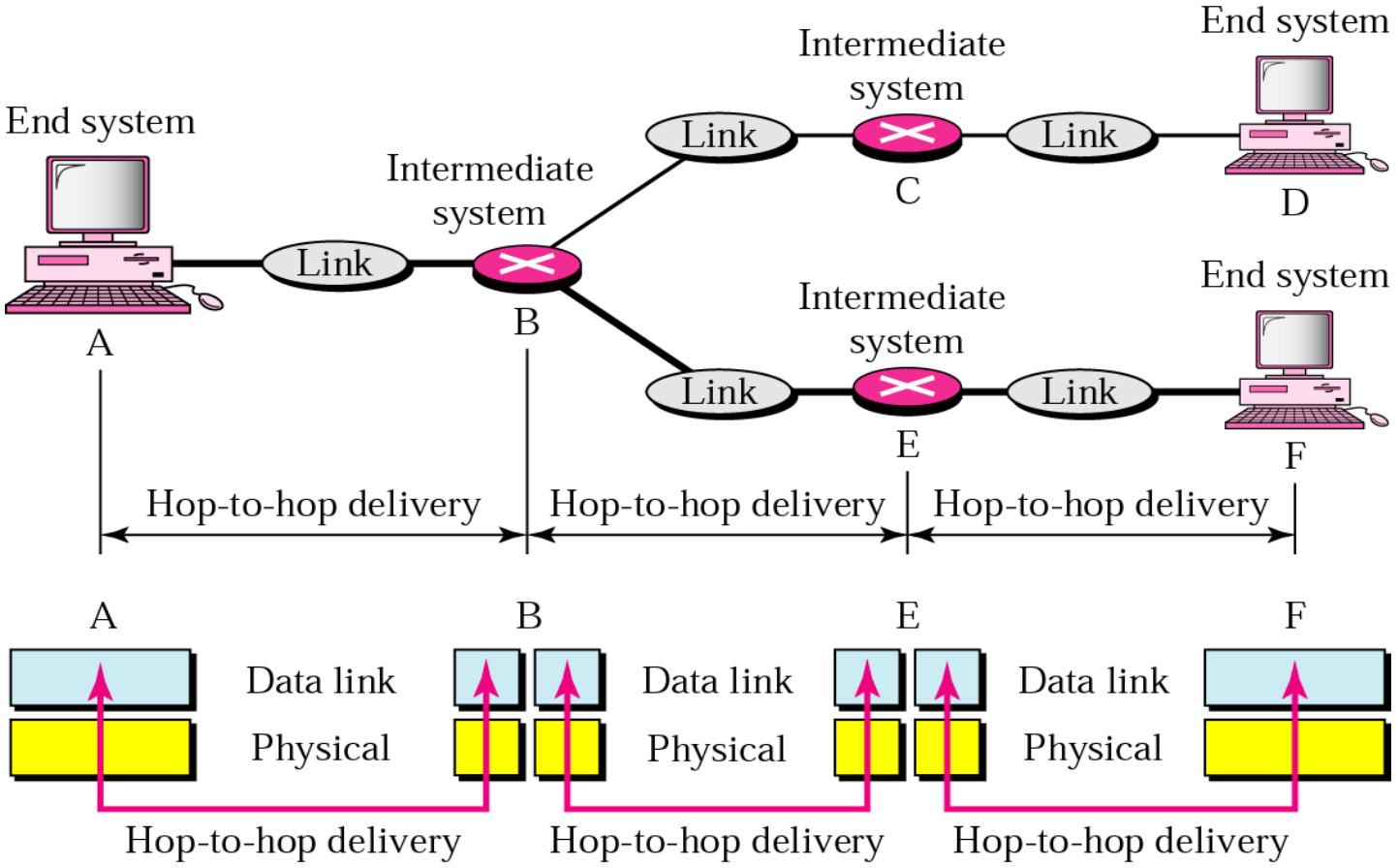
- Defines frames into manageable **data units**
  - Physical addressing
  - Flow control
  - Error control
  - Access control



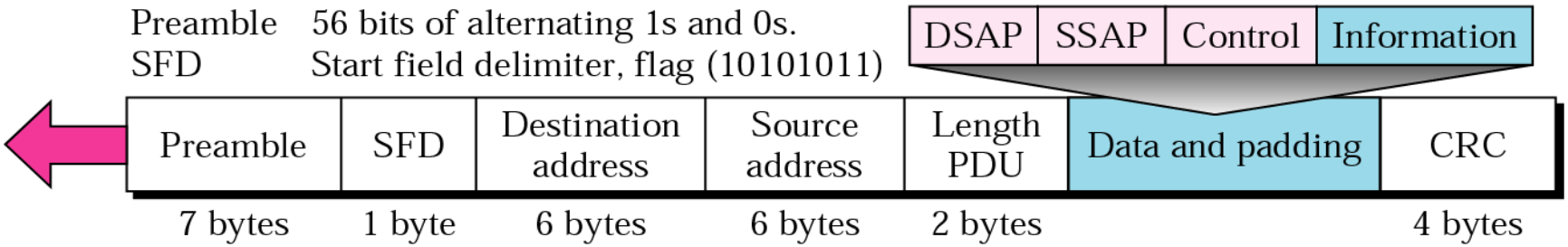
Note:

The data link layer is responsible for transmitting frames from one node to the next.

Node-to-node delivery



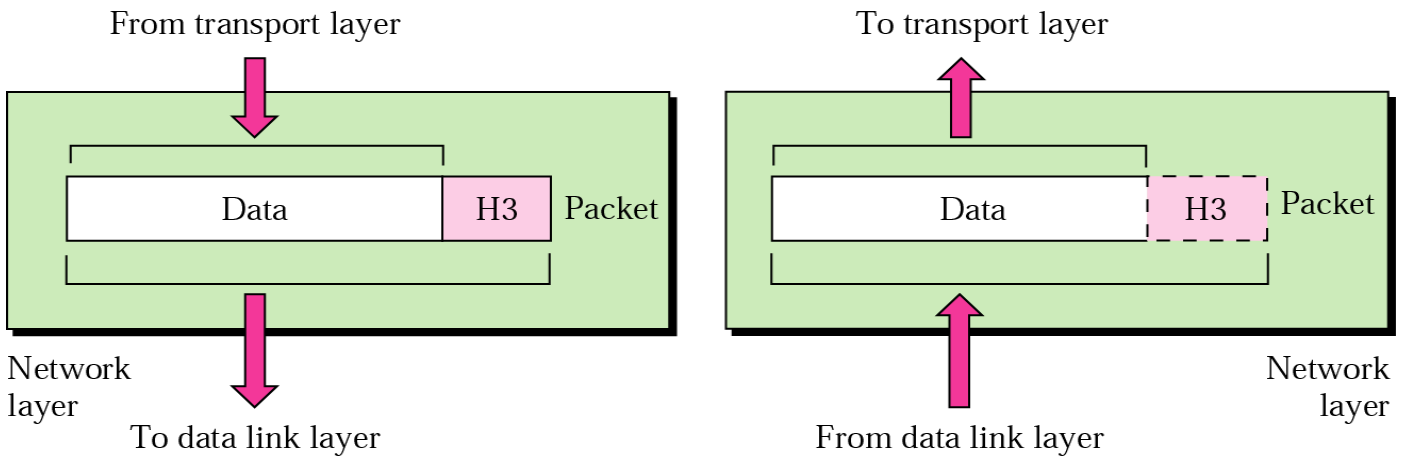
802.3 MAC frame



- Preamble – *7 bytes* of alternating 0s and 1s to alert the receiver and allow it to synchronize
- Start Frame Delimiter (SFD) – *1 byte* – 10101011 signals the beginning of a frame, last chance for synchronization – last 2 bits are 11
- Destination address (DA) – *6 bytes* – contains the physical address of the destination station or stations
- Source address (SA) – *6 bytes* – contains the physical address of the sender
- Length/type – if less than 1518 then it defines the length of the data field – if more than 1536 then it defines the type of the PDU packet that is encapsulated
- Data – data encapsulated from upper-layer protocols : *46 ~ 1500 bytes*
- CRC – CRC-32

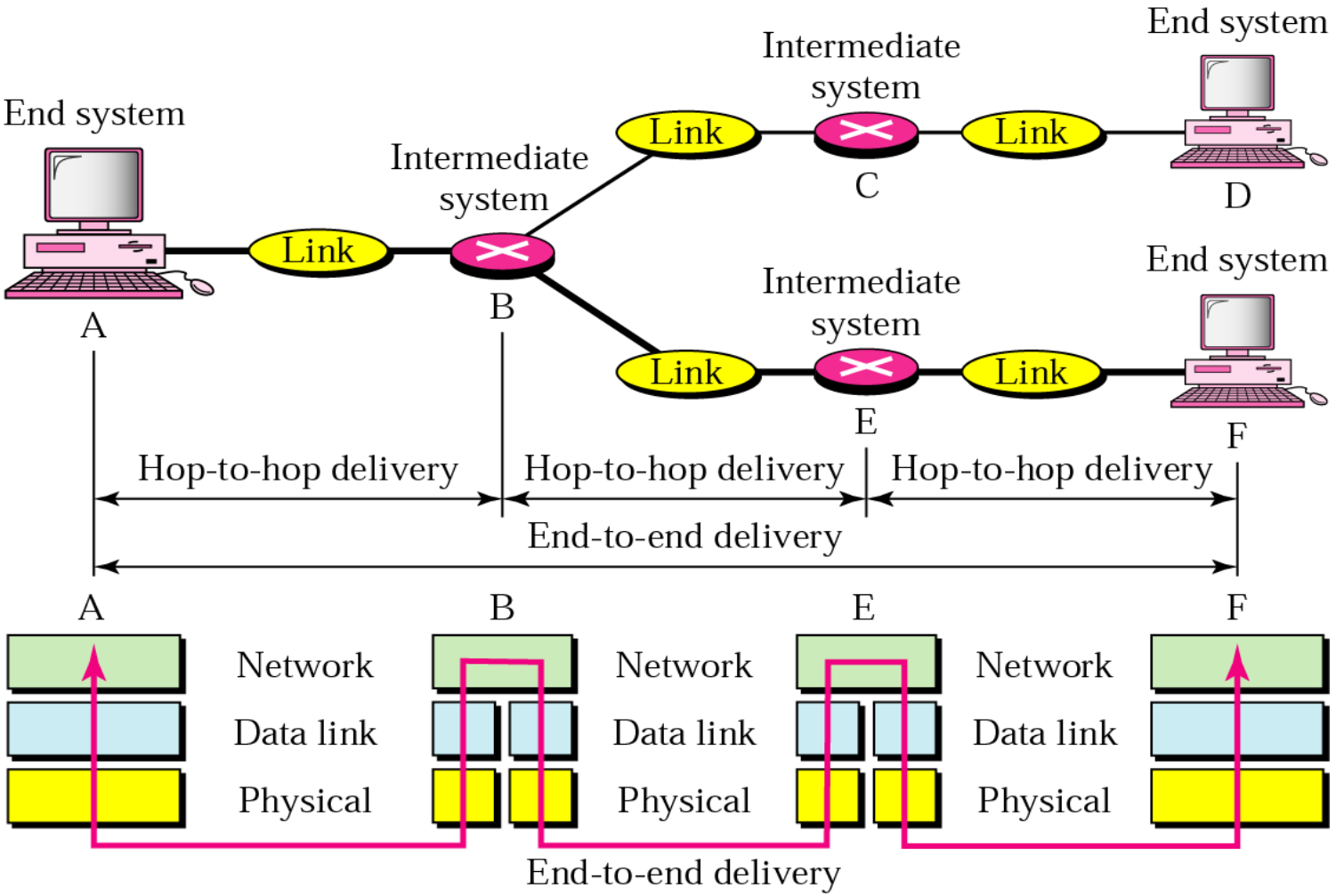
Network layer

- Network Layer Responsibilities
  - Source-to-destination delivery, possibly across multiple networks
  - Logical addressing
  - Routing

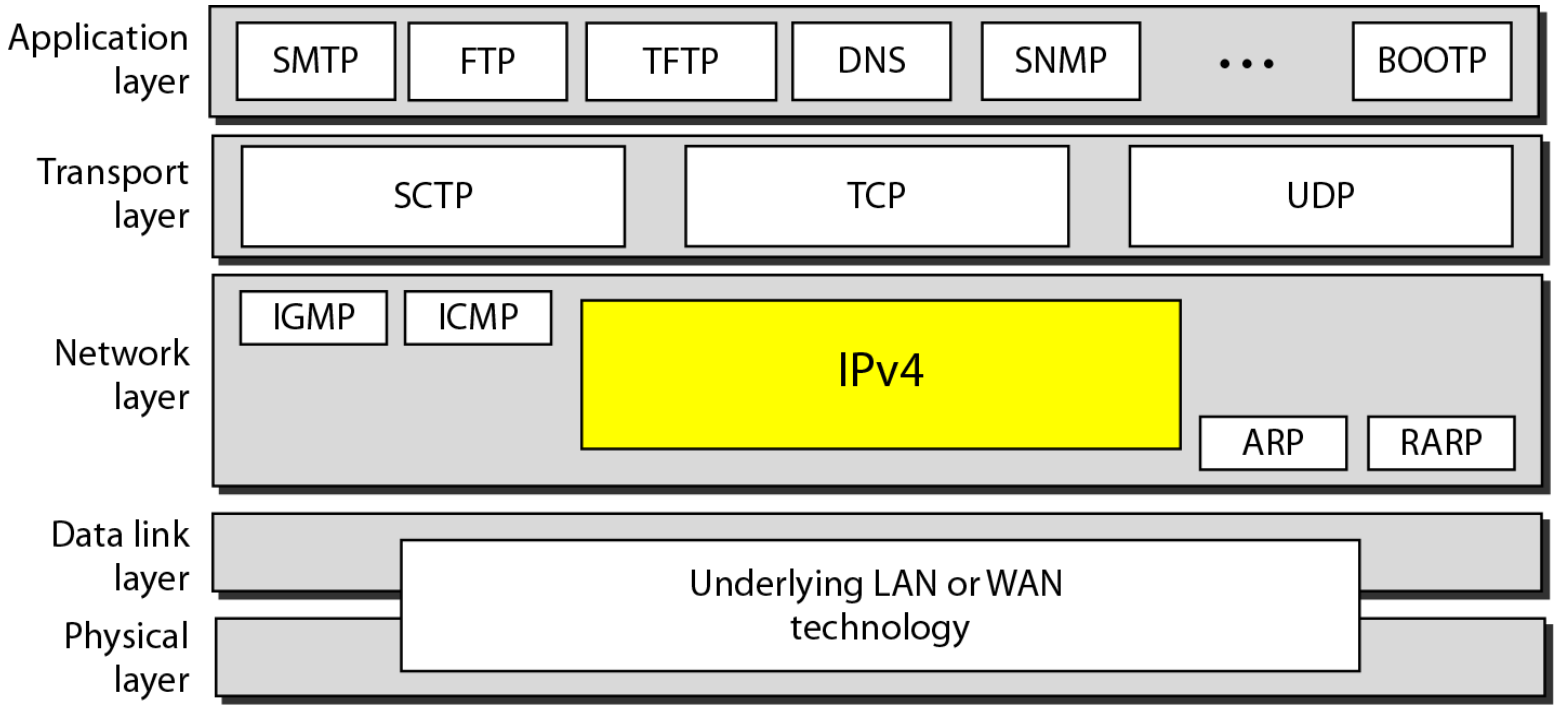


The network layer is responsible for the delivery of packets from the original source to the final destination.

Source-to-Destination delivery



IPv4



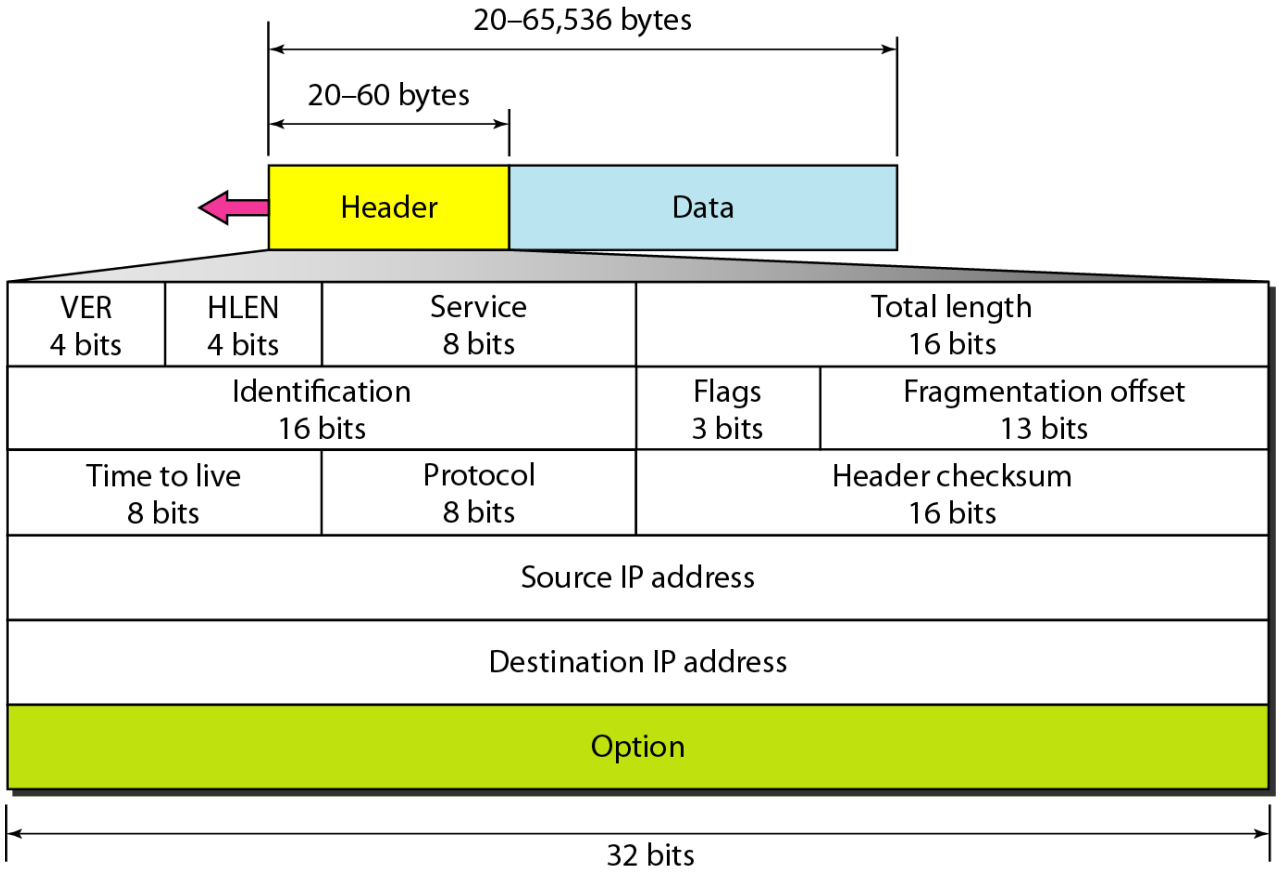
Position of IPv4 in TCP/IP protocol suite

IPv4

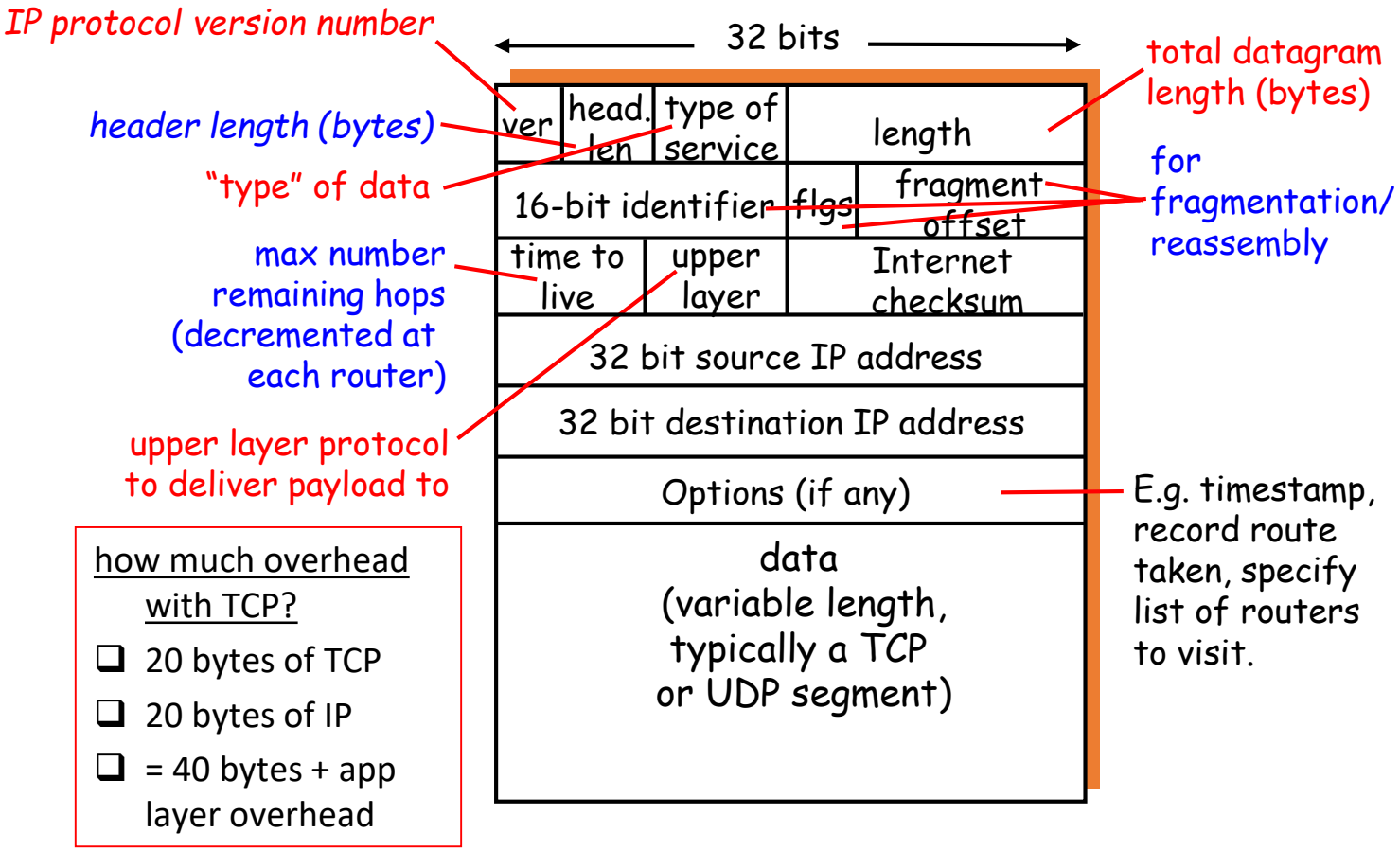
- Best-effort delivery
  - IPv4 is an unreliable and connectionless datagram protocol
  - A best-effort delivery service.
  - best-effort ➔ IPv4 provides no error control or flow control (except for error detection on the header).
- Connectionless protocol
  - Each datagram is handled independently
  - Datagrams sent by the source to the same destination could
    - Arrive out of order
    - be lost or corrupted during transmission.
  - IPv4 relies on a high-level protocol to take of all these problem.

IPv4 Datagrams

- Packets in the IPv4 layer are called Datagrams.



IP datagram format

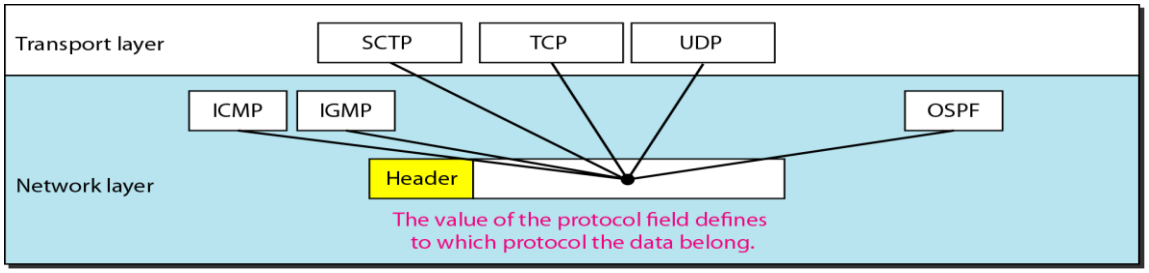


IPv4 Datagram (cont'd)

- A datagram is a variable-length packet consisting of a header and data.
- Header
  - ⊙ Length : 20 – 60 bytes
  - ⊙Contains information essential to routing and delivery.
- Version (VER) : It defines the Version of IPv4. it is 4.
- Header Length (HLEN) : Defining the total length of the datagram header in 4-byte words.

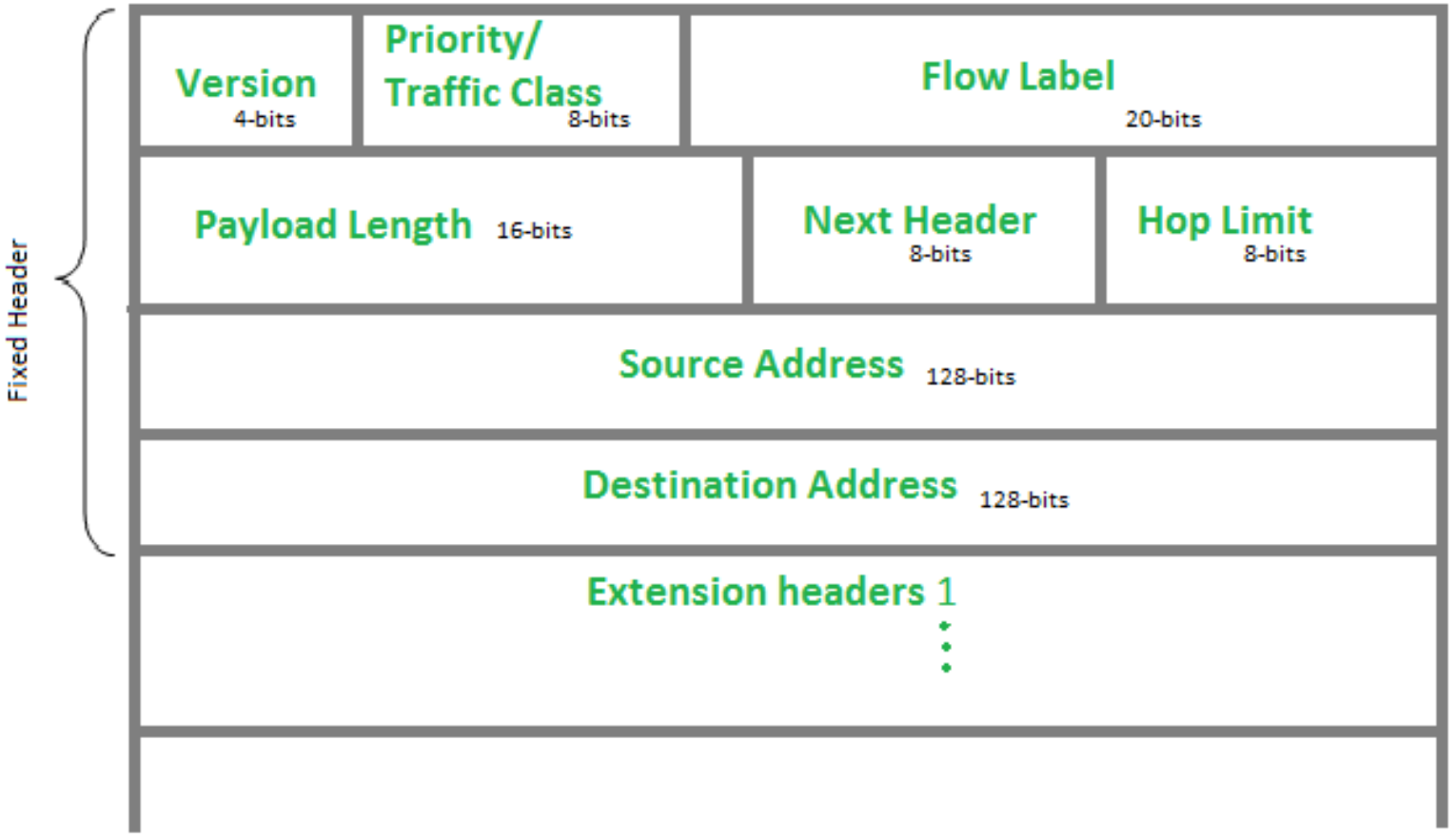
IPv4 Datagram (cont'd)

- Protocol
  - ⊙ Defining the higher level protocol that uses the services of the IP layer
    - TCP, UDP, ICMP, and IGMP
    - Multiplexing data from different higher level protocols



Value	Protocol
1	ICMP
2	IGMP
6	TCP
8	EGP
17	UDP
89	OSPF

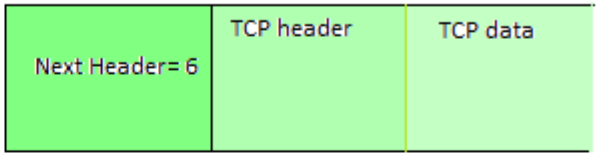
IPv6 Datagram



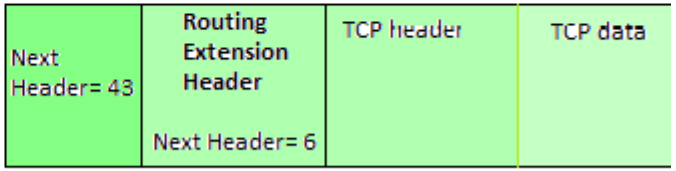
IPv6 Datagram

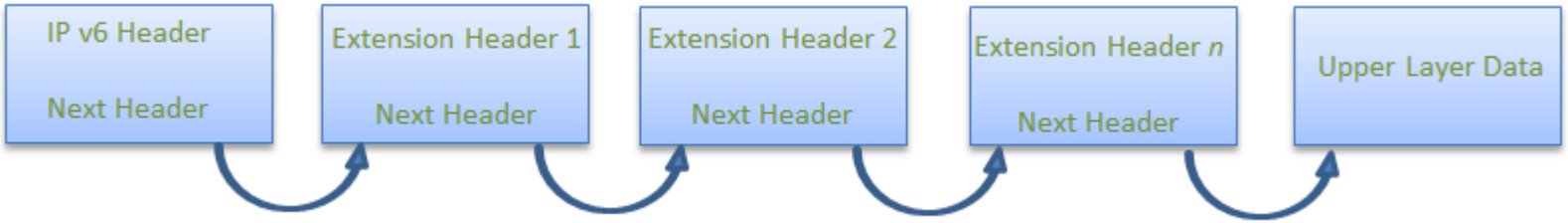
Order	Header Type	Next Header Code
1	Basic IPv6 Header	-
2	Hop-by-Hop Options	0
3	Destination Options (with Routing Options)	60
4	Routing Header	43
5	Fragment Header	44
6	Authentication Header	51
7	Encapsulation Security Payload Header	50
8	Destination Options	60
9	Mobility Header	135
	No next header	59
Upper Layer	TCP	6
Upper Layer	UDP	17
Upper Layer	ICMPv6	58

Example: *TCP is used in IPv6 packet*



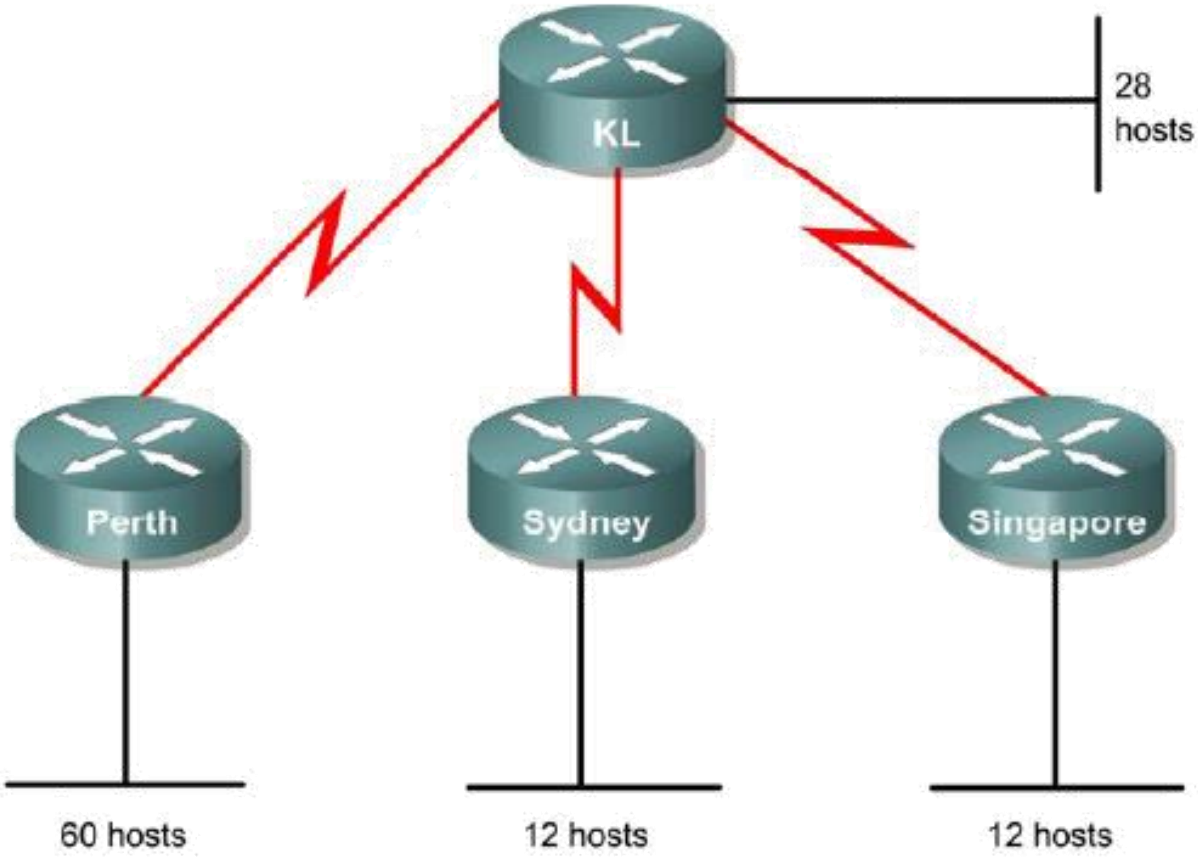
Example2:



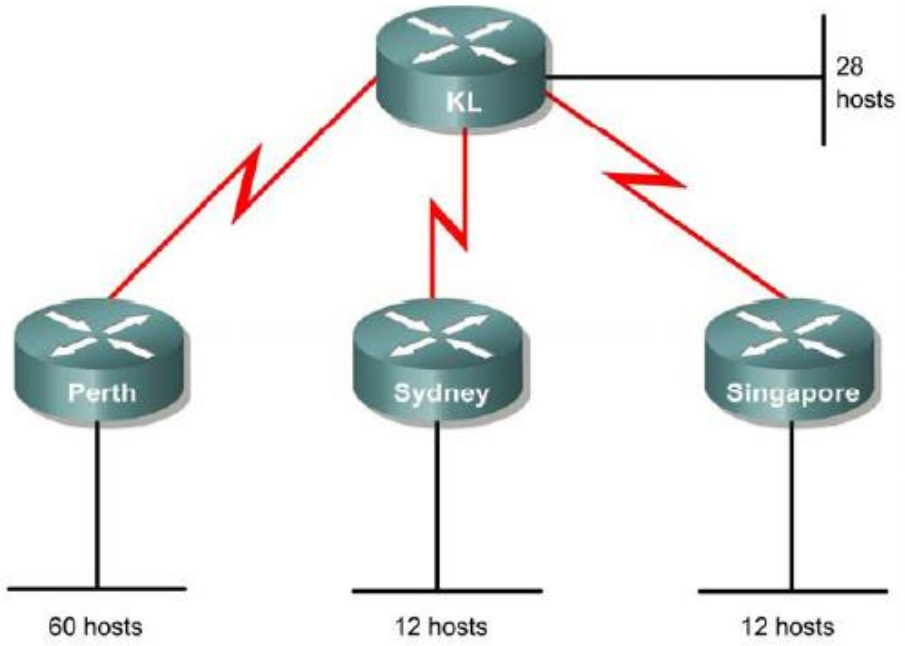


Subnet with VLSM

192.168.10.0/24



Regular Subnet



192.168.10.0/24

7 subnets; The largest subnet needs **60** hosts
If 3 bits for subnet (8 subnets) ➔ 5 bits for host (32 hosts)
If 6 bits for host (64 hosts) ➔ 2 bits for subnet (4 subnets)