RLMCA201 COMPUTER NETWORKS

REJI R

ASSISTANT PROFESSOR

SAINTGITS

Vision & Mission

Vision

- **Emerge as a centre of excellence in the area of Computer Applications.**

Mission

- **To mould the students with sound theoretical and practical knowledge in computing applications.**
- **To produce industrious and ethically upright professionals.**
- **To develop innovative thinking and research culture among students.**

Course Objective & Outcome

To introduce students to modern computer networks

To lay foundation for Internet technologies and related topics .

Expected outcome

Students will gain proficiency in various network protocols and models.

Syllabus & Calendar

- MCA_Lateral_First_Semester_Syllabus_Final.pdf
- ktu calendar.pdf

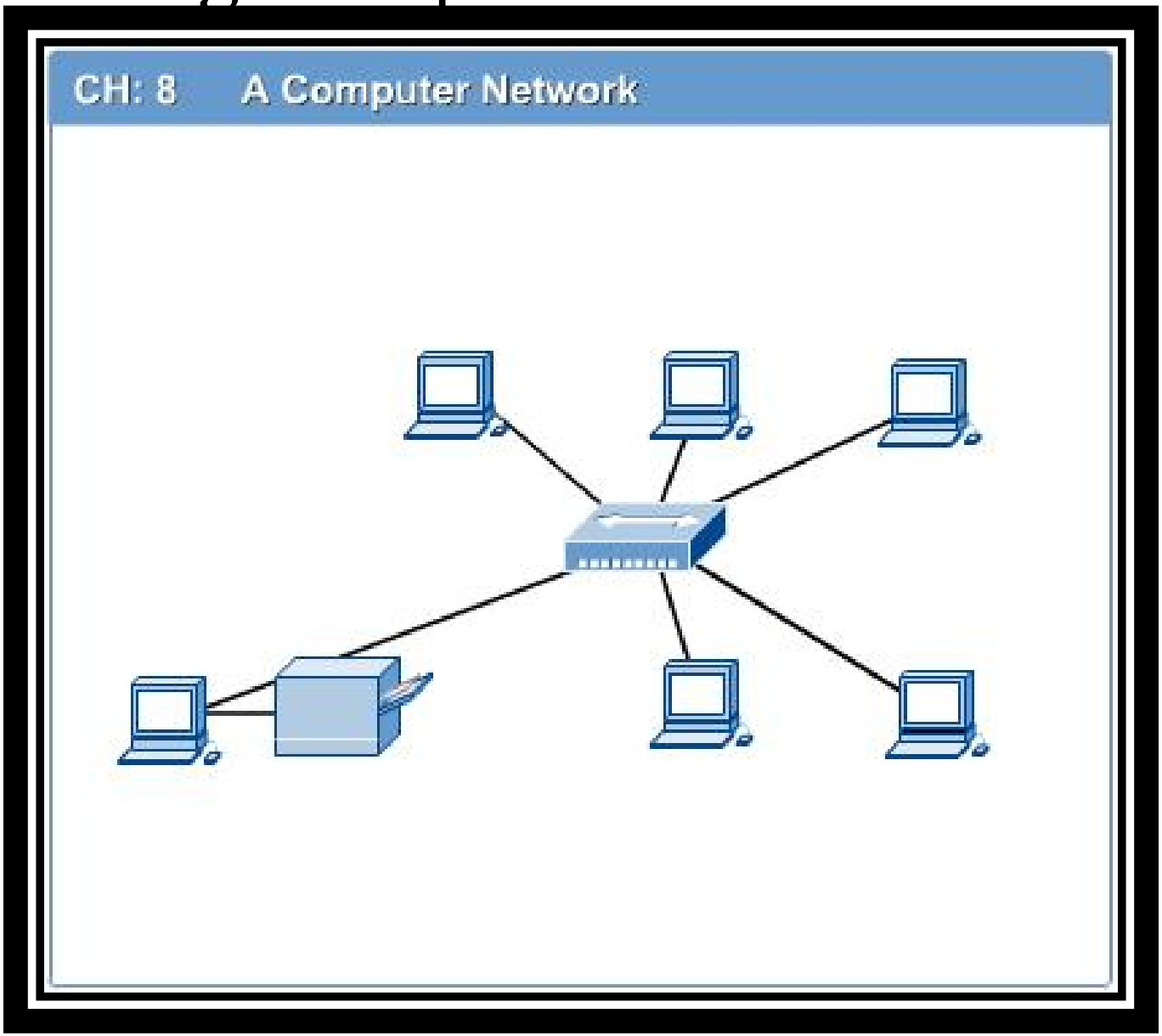
Module I

- Basic communications model - Protocol layers and service models – Basic definitions - OSI model - Internet protocols, the role of standards organizations, History of Internet, Security in the Internet, concept of Quality of Service (QoS).

Computer Networks

- A large number of separate but interconnected computers are called **computer networks.**
- Two computers are said to be interconnected if they are able to exchange information.

Fig: computer network



Computer network connects two or more autonomous computers.

The computers can be geographically located anywhere.

Networks come in many sizes, shapes and forms.

Computer network and distributed system.

The key distinction is that in a distributed system, a collection of independent computers appears to its users as a single coherent system.

Usually, it has a single model or paradigm that it presents to the users. Often a layer of software on top of the operating system, called **middleware, is** responsible for implementing this model.

A well-known example of a distributed system is the **World Wide Web. It runs on top of the Internet and presents a** model in which everything looks like a document (Web page).

- In a nut shell we can say that a distributed system is a software system built on top of a network.

Uses of Computer Networks

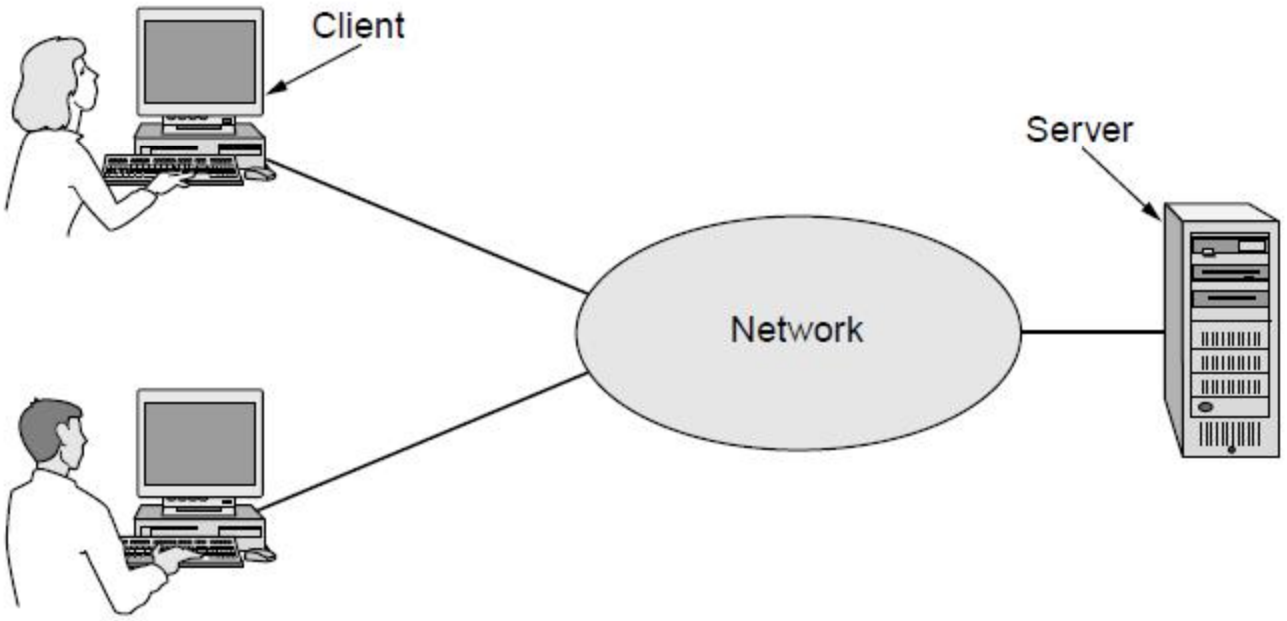
- Business Applications
- Home Applications
- Mobile Users
- Social Issues

Tag	Full name	Example
B2C	Business-to-consumer	Ordering books online
B2B	Business-to-business	Car manufacturer ordering tires from supplier
G2C	Government-to-consumer	Government distributing tax forms electronically
C2C	Consumer-to-consumer	Auctioning second-hand products online
P2P	Peer-to-peer	Music sharing

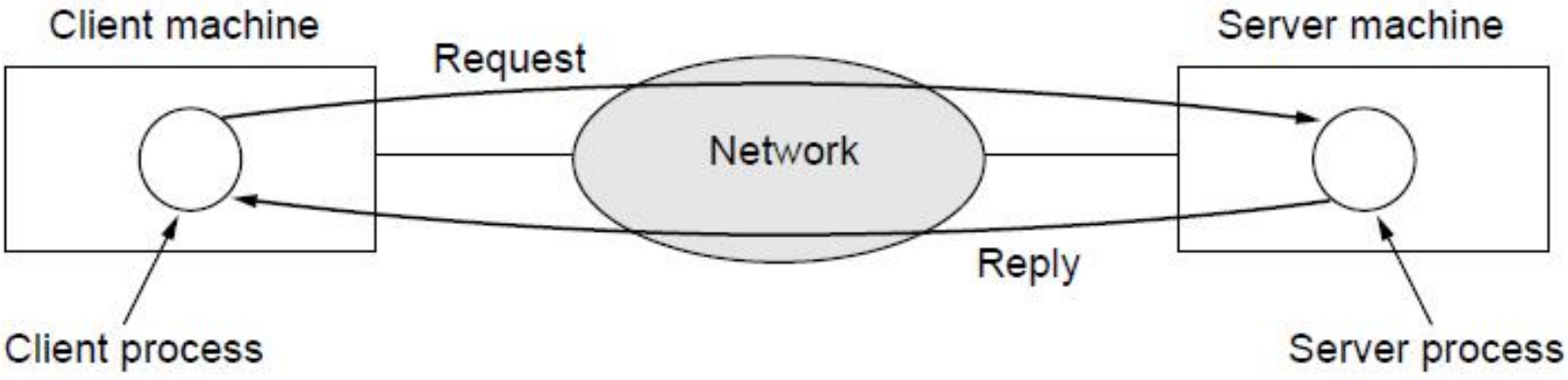
Terminologies

- Client
- Server
- Unicast
- Multicast
- Broadcast
- simplex
- Half duplex
- Full duplex

A network with two clients and one server



The client-server model involves requests and replies



Social Issues

- Network neutrality
- Digital Millennium Copyright Act
- Profiling users
- Phishing

Applications of Networks

- **Resource Sharing**
  - Hardware (computing resources, disks, printers)
  - Software (application software)
- **Information Sharing**
  - Easy accessibility from anywhere (files, databases)
  - Search Capability (WWW)
- **Communication**
  - Email
  - Message broadcast
- **Remote computing**
- **Distributed processing (GRID Computing)**

Types

- Personal area networks
- Local area networks
- Metropolitan area networks
- Wide are networks
- The internet

Classification of interconnected processors by scale.

Interprocessor distance	Processors located in same	Example
1 m	Square meter	Personal area network
10 m	Room	Local area network
100 m	Building	
1 km	Campus	
10 km	City	Metropolitan area network
100 km	Country	Wide area network
1000 km	Continent	
10,000 km	Planet	The Internet

- Basic Communications Model

- Communication model is used to exchange data between two parties

- **Source**

  Data to be transmitted is generated by this device, example: telephones, personal computers etc.

- **Transmitter**

  The data generated by the source system are not directly transmitted in the form they are generated. The transmitter transforms and encodes the information in such a form to produce electromagnetic waves or signals.

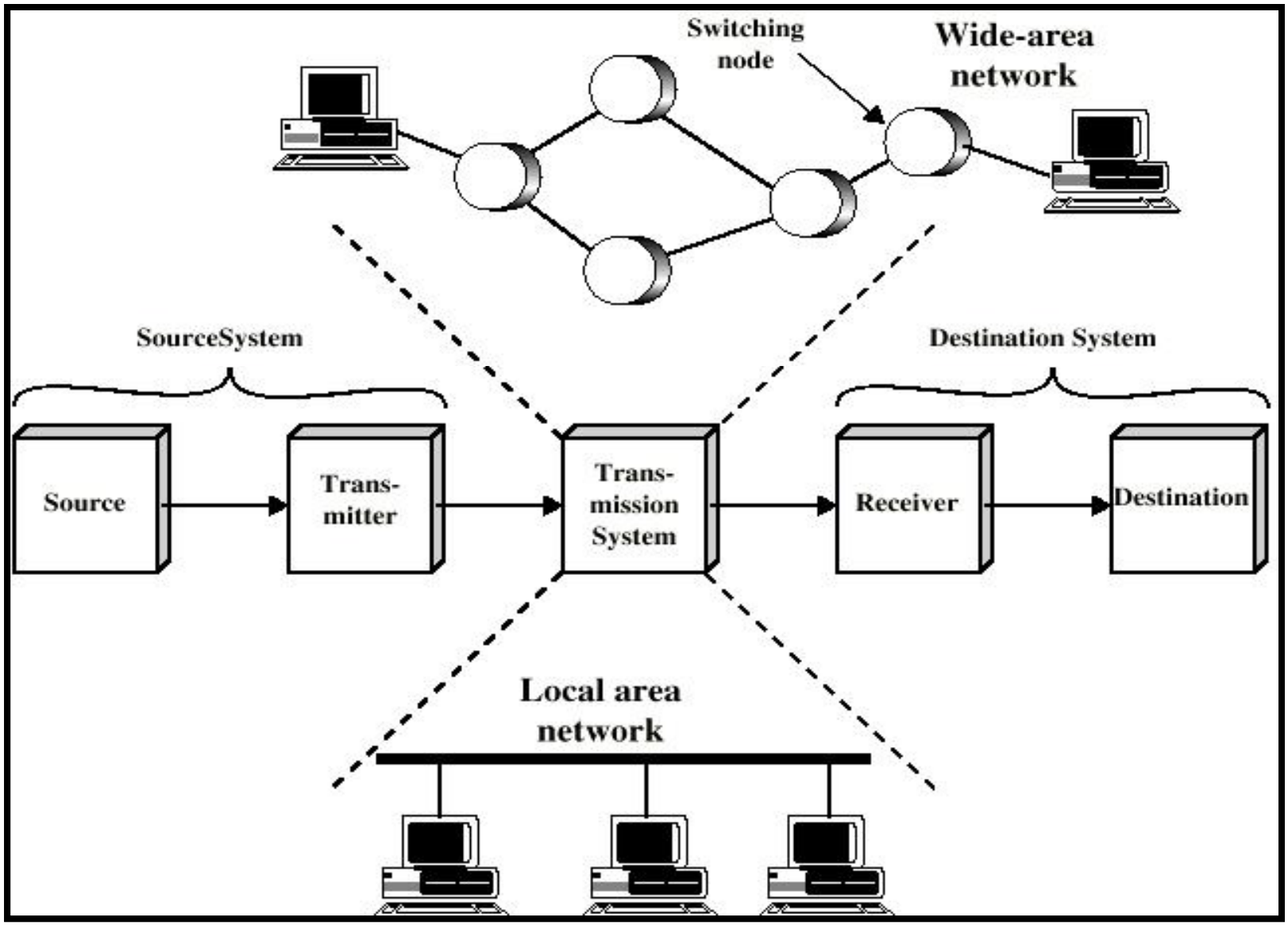
- **Transmission System**
- A transmission system can be a single transmission line or a complex network connecting source and destination.
- **Receiver**
- Receiver accepts the signal from the transmission system and converts it to a form which is easily managed by the destination device.
- **Destination**
- Destination receives the incoming data from the receiver.

- **Data Communication**
- The exchange of data between two devices through a transmission medium is Data Communication. The data is exchanged in the form of 0's and 1's. The transmission medium used is wired/wireless. For data communication to occur, the communication device must be part of a communication system.

- Data Communication has two types Local and Remote which are discussed below :
- **Local :**
- Local communication takes place when the communicating devices are in the same geographical area, same building, face-to-face between individuals etc.
- **Remote :**
- Remote communication takes place over a distance

- **Components of Data Communication**
- **Message :** It is the information to be delivered.
- **Sender :** Sender is the person who is sending the message.
- **Receiver :** Receiver is the person to whom the message is to be delivered.
- **Medium :** It is the medium through which message is to be sent for example modem.
- **Protocol :** These are some set of rules which govern data communication.
-

Simplified Network Model



- **Protocol layers and service models**

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

Protocols

- Set of rules that Govern Data Communication

- Used for communications between entities in a system.
- Entities
  - User Applications
  - e-mail facilities
  - Terminals
- Systems
  - Computer
  - Terminal
  - Remote sensor

Protocol Architecture

- Task of communication broken up into modules.
- For example file transfer could use three modules
  - File transfer Application
  - Communication service module
  - Network access module
- Key elements of a protocol are syntax, semantics and it's timing.

- Layers can offer two different types of services to the layers above them.
  - Connection oriented
  - Connection less

Connection Oriented

- Connection oriented service is modeled after the telephone system.
- To talk to some one you pick up the phone, dial the number, talk and then hang up.

In connection oriented service

1. Establish a connection
2. Use the connection
3. Release the connection.

Connection less

- Is modeled after the postal system.
- Each message(letter) carries the full designation address and each one is routed to the system independent of all others.

- Message sequence
- Byte streams

Connection-Oriented Versus Connectionless Service

	Service	Example
Connection-oriented	Reliable message stream	Sequence of pages
	Reliable byte stream	Movie download
	Unreliable connection	Voice over IP
Connection-less	Unreliable datagram	Electronic junk mail
	Acknowledged datagram	Text messaging
	Request-reply	Database query

Six different types of service.

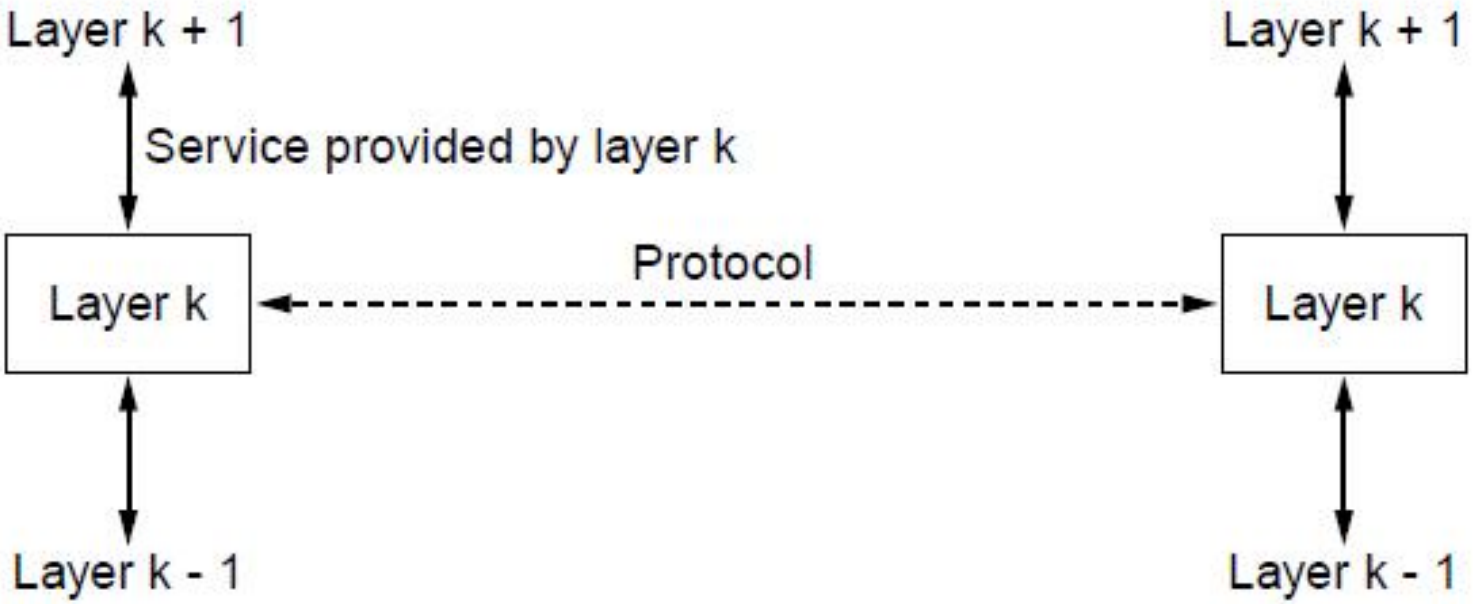
Service Primitives (operations)

Six service primitives that provide a simple connection-oriented service

Primitives are different for connection oriented and

Primitive	Meaning
LISTEN	Block waiting for an incoming connection
CONNECT	Establish a connection with a waiting peer
ACCEPT	Accept an incoming connection from a peer
RECEIVE	Block waiting for an incoming message
SEND	Send a message to the peer
DISCONNECT	Terminate a connection

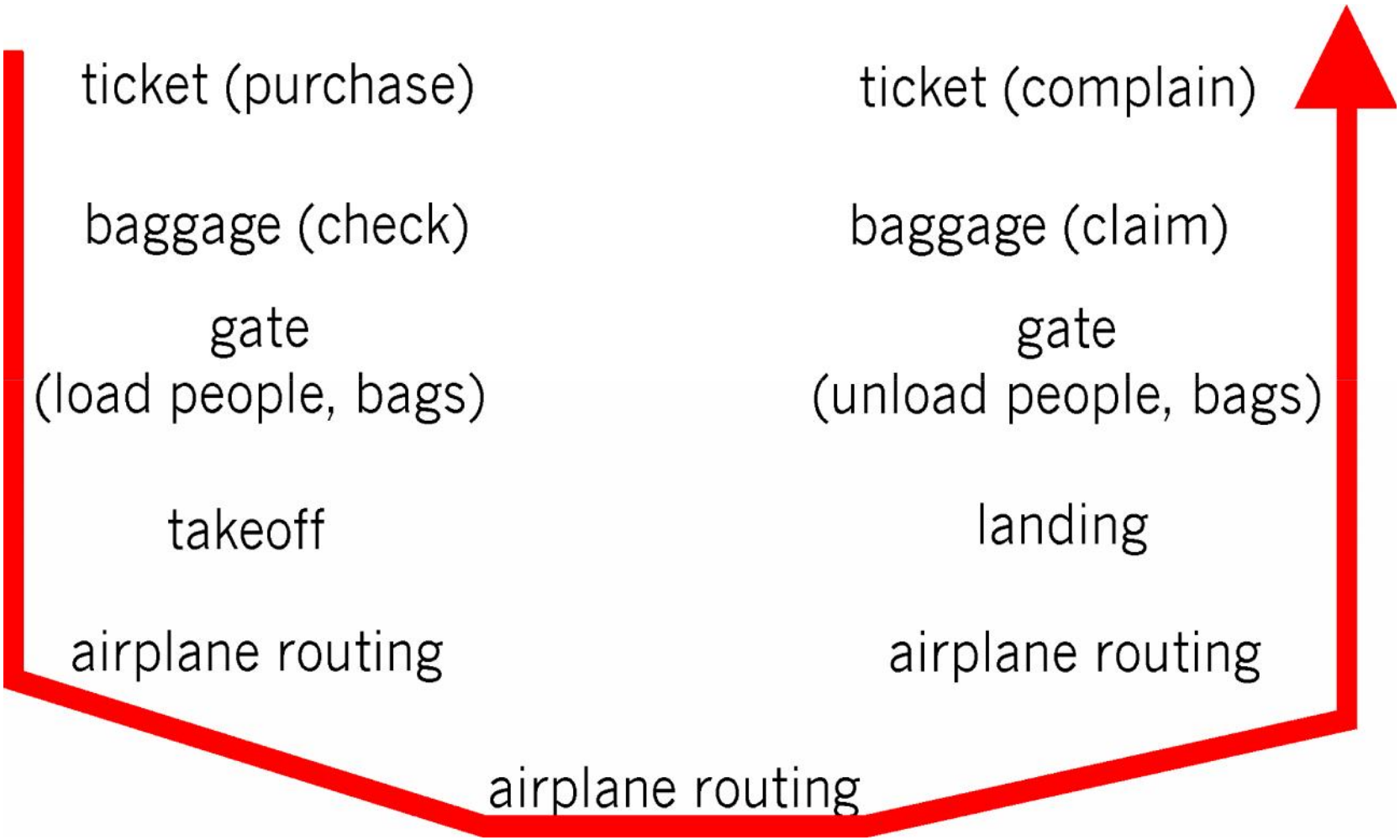
The Relationship of Services to Protocols

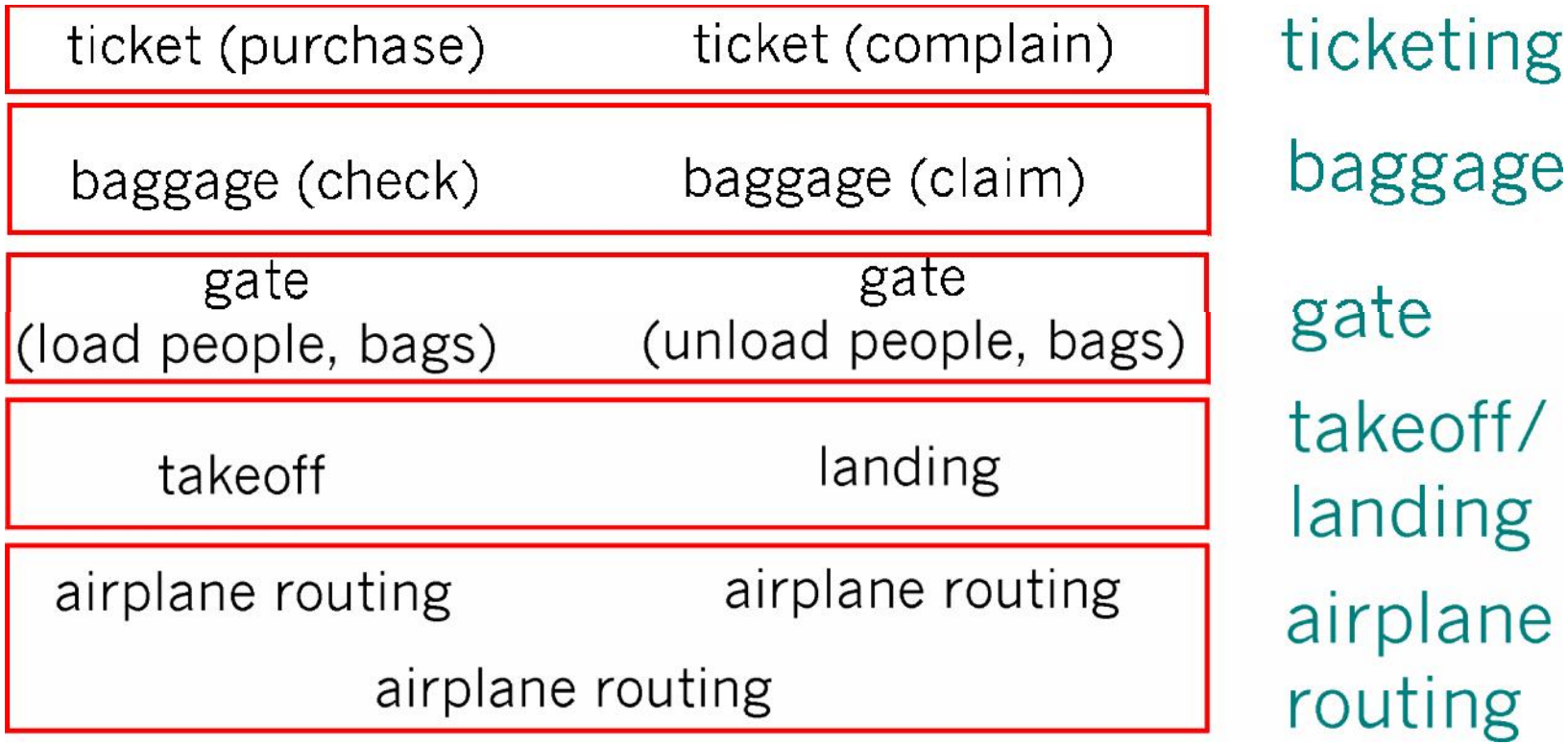


The relationship between a service and a protocol.

- **Service** is a set of primitives that a layer provides to the layer above it.
- A **service** relates to an interface between two layers, with the lower layer being the service provider and the upper layer being the service user.
- Entities use **protocols** to implement their service definitions.

Layered Architecture example





Horizontal "layering" of airline functionality

Advantage

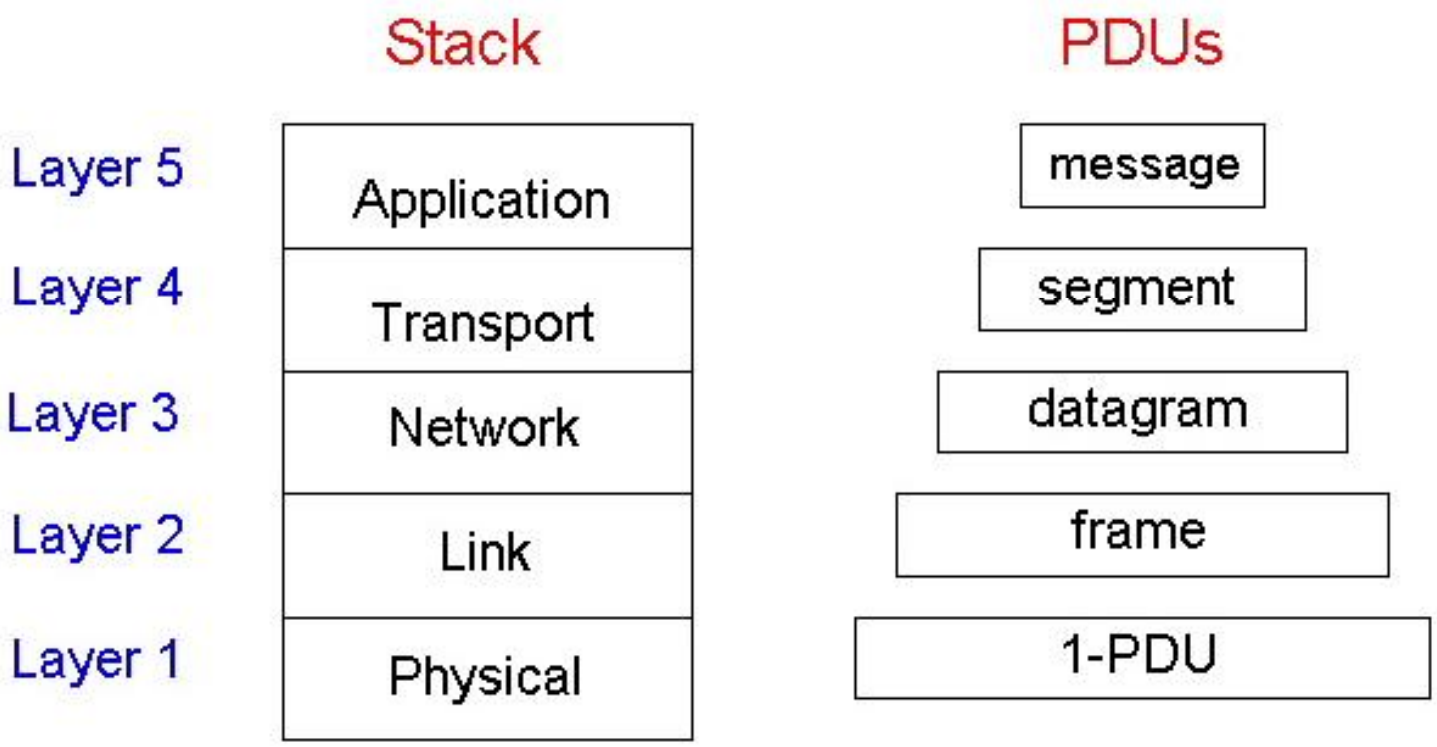
Layering provides a structured way to discuss system components.

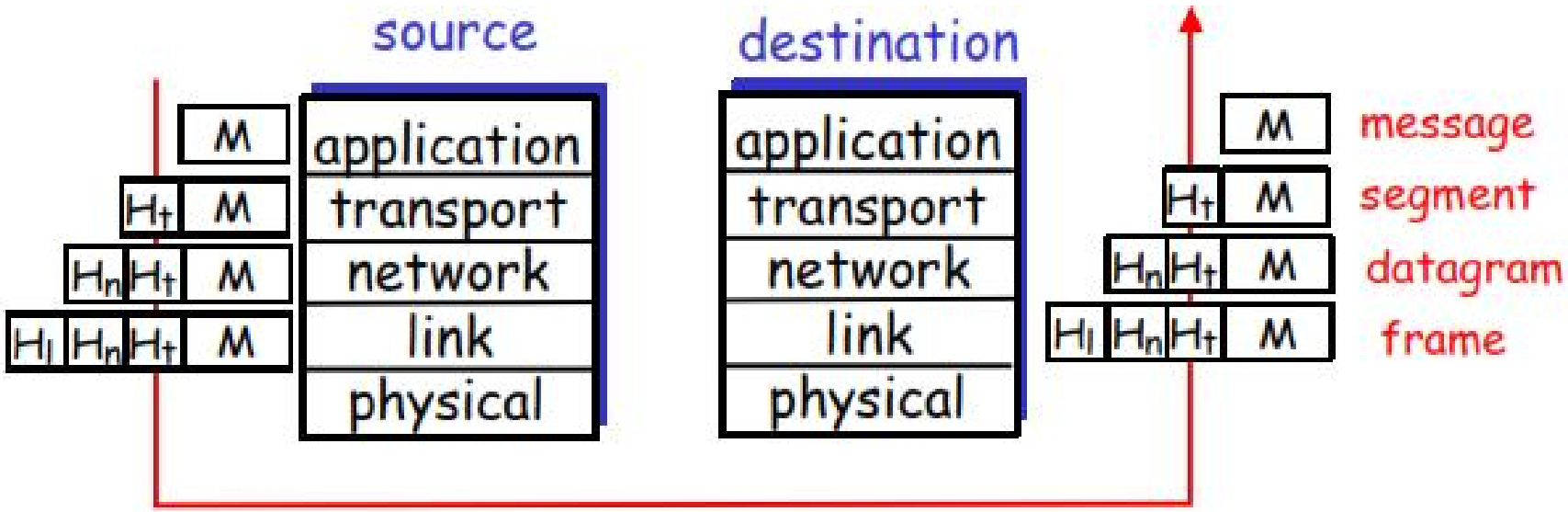
Modularity makes it easier to update system components.

Draw backs of layering

- One potential drawback of layering is that one layer may duplicate lower-layer functionality.
- For example, many protocol stacks provide error recovery on both a per-link basis and an end-to-end basis.
- A second potential draw- back is that functionality at one layer may need information (for example, a time- stamp value) that is present only in another layer; this violates the goal of separation of layers.

Internet protocol stack




source
destination
application
transport
network
link
physical
application
transport
network
link
physical
M
H_t M
H_n H_t M
H_l H_n H_t M
M
message
H_t M
segment
H_n H_t M
datagram
H_l H_n H_t M
frame

Application layer

- The application layer is where network applications and their application-layer protocols reside.
- The Internet's application layer includes many protocols, such as the HTTP protocol (which provides for Web document request and transfer).
- SMTP (which provides for the transfer of e-mail messages).
- FTP (which provides for the transfer of files between two end systems).
- We'll see that certain network functions, such as the translation of human-friendly names for Internet end systems like www.ietf.org to a 32-bit network address, are also done with the help of a specific application-layer protocol, namely, the domain name system (DNS). (**Data is called as Message)**

Transport Layer

- The Internet's transport layer transports application-layer messages between application endpoints.
- In the Internet there are two transport protocols, TCP and UDP
- TCP: Connection oriented

  Features: Guaranteed delivery

  Flow of control

  Congestion control.

- UDP: Connection less
- No Reliability, no flow control, and no congestion control.
- Transport-layer packet is called as a segment.

Network layer

- The Internet's network layer is responsible for moving network-layer packets known as datagrams from one host to another.
- The Internet's network layer includes the celebrated IP Protocol, which defines the fields in the datagram as well as how the end systems and routers act on these fields.
- There is only one IP protocol, and all Internet components that have a network layer must run the IP protocol.
- Network layer also have Routing protocols

Link layer

- The Internet's network layer routes a datagram through a series of routers between the source and destination.
- To move a packet from one node (host or router) to the next node in the route, the network layer relies on the services of the link layer.
- Examples of link- layer protocols include Ethernet,WiFi, and the cable access network's DOCSIS protocol.
- Link layer packets are called as frames.

Physical layer

- While the job of the link layer is to move entire frames from one network element to an adjacent network element, the job of the physical layer is to move the individual bits within the frame from one node to the next.
- The protocols in this layer are again link dependent and For example, Ethernet has many physical-layer protocols: one for twisted-pair copper wire, another for coaxial cable, another for fiber, and so on. In each case, a bit is moved across the link in a different way.

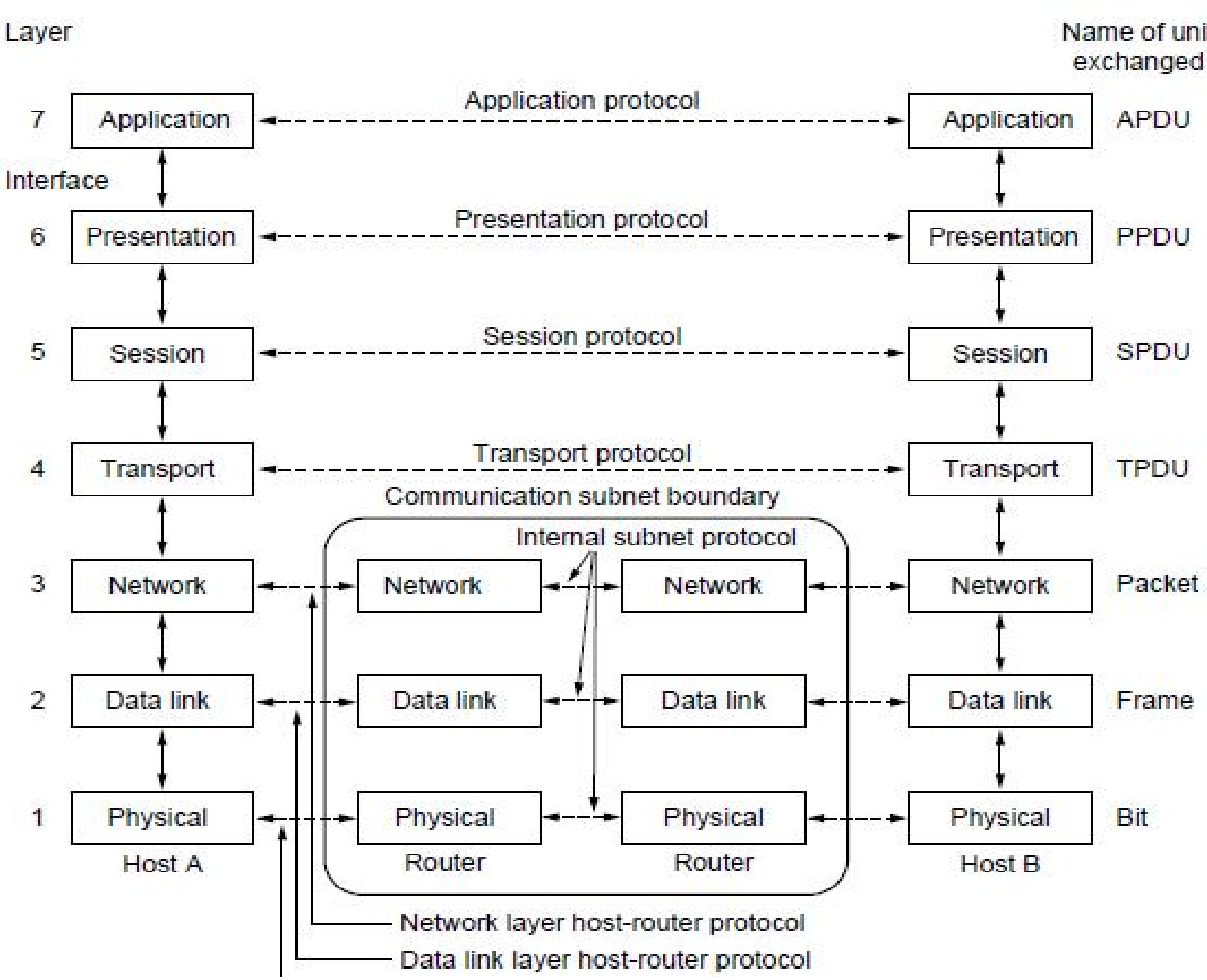
Reference Models

- **OSI reference model**
- TCP/IP reference model
- Model used
- Comparison of OSI and TCP/IP
- Critique of OSI model and protocols
- Critique of TCP/IP model

The OSI Reference Model

Principles for the seven layers

- Layers created for different abstractions
- Each layer performs well-defined function
- Function of layer chosen with definition of international standard protocols in mind
- Minimize information flow across interfaces between boundaries
- Number of layers optimum


Layer
Name of unit exchanged
7
Application
Application protocol
Application
APDU
Interface
6
Presentation
Presentation protocol
Presentation
PPDU
5
Session
Session protocol
Session
SPDU
4
Transport
Transport protocol
Transport
TPDU
Communication subnet boundary
Internal subnet protocol
3
Network
Network
Network
Network
Packet
2
Data link
Data link
Data link
Data link
Frame
1
Physical
Physical
Physical
Physical
Bit
Host A
Router
Router
Host B
Network layer host-router protocol
Data link layer host-router protocol

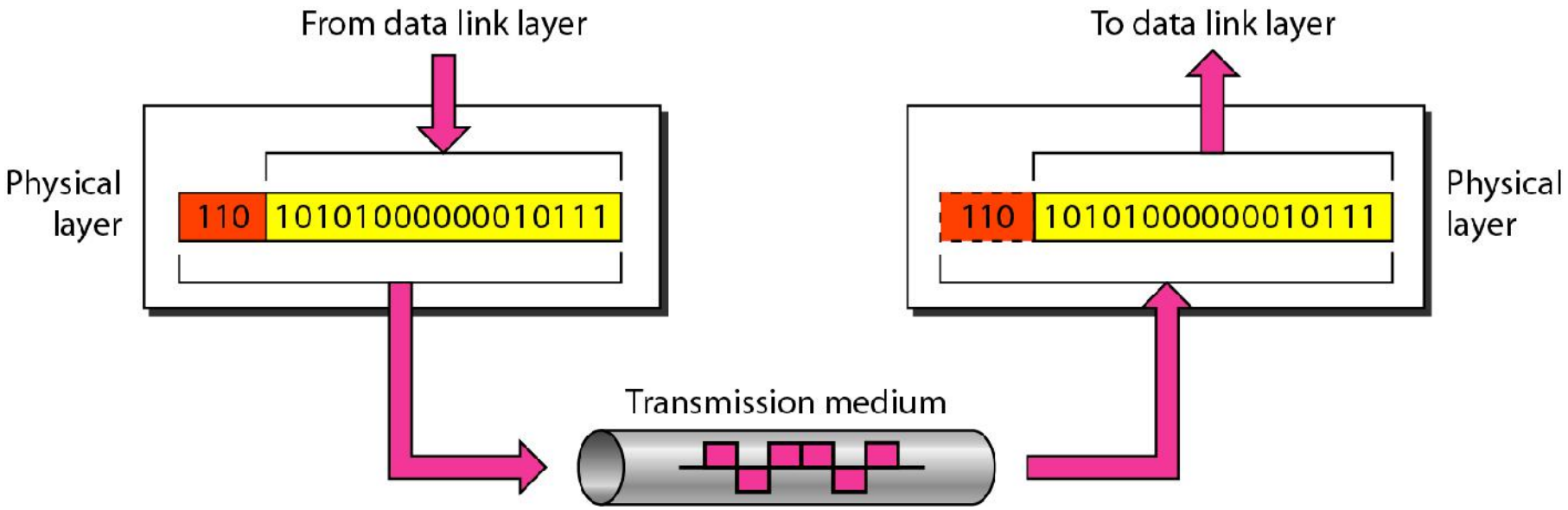
OSI Reference Model Layers

- Physical layer
- Data link layer
- Network layer
- Transport layer
- Session layer
- Presentation layer
- Application layer

Physical (Layer 1)

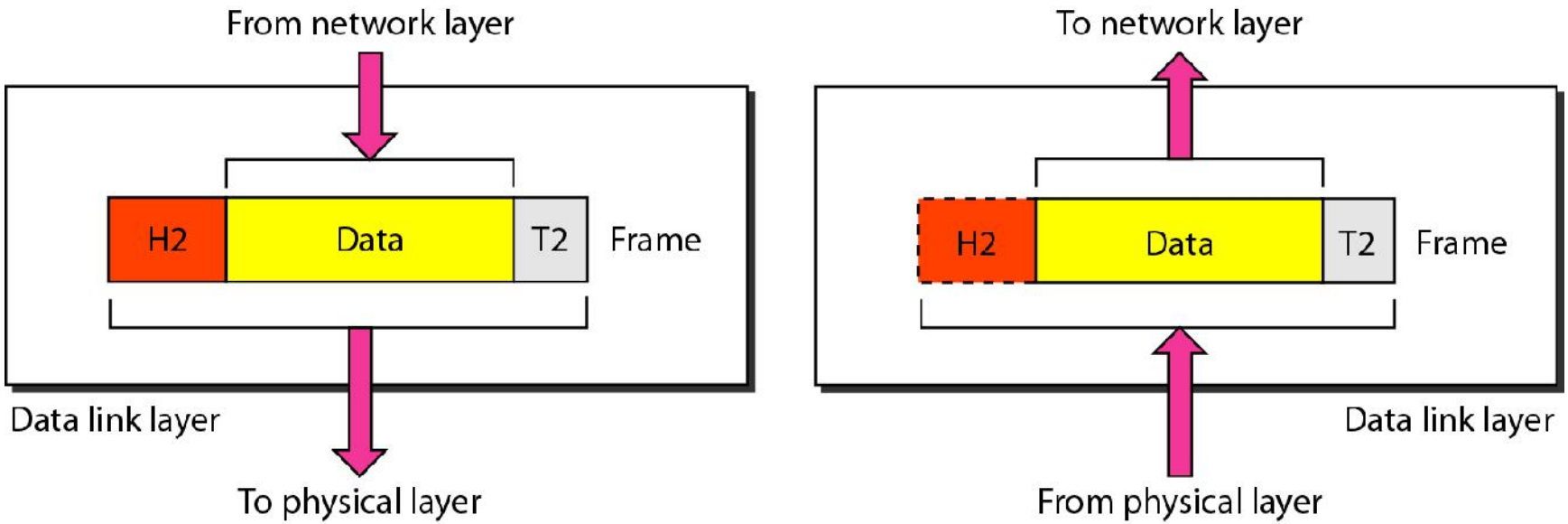
- Controls the transmission of the actual data onto the network cable.
- It defines the electrical signals, line states and encoding of data and the connector type used.
- Eg: 10 BaseT

Physical layer



Data Link (Layer 2)

- At this layer, data packets are encoded and decoded into bits. It furnishes transmission protocol knowledge and management and handles errors in the physical layer, flow control and frame synchronization.
- Error detection and correction
- Lower sub layer: MAC
- Upper sub layer : LLC

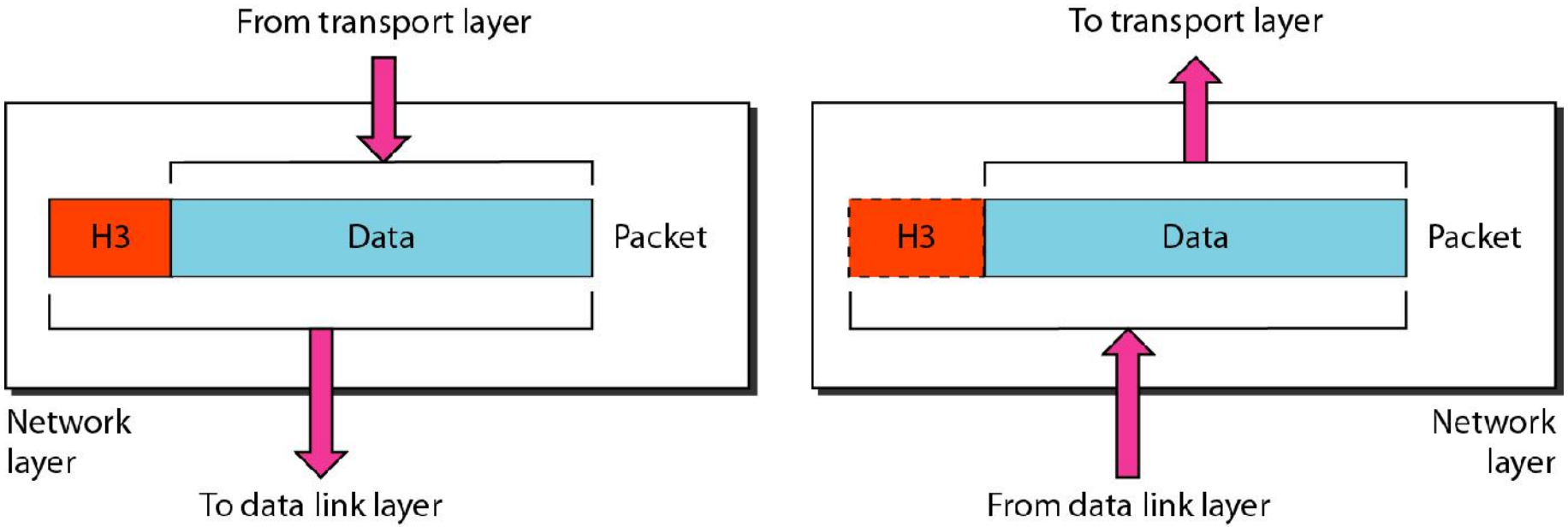

From network layer
H2
Data
T2
Frame
Data link layer
To physical layer
To network layer
H2
Data
T2
Frame
Data link layer
From physical layer

Network (Layer 3)

- This layer provides Switching and routing technologies and creating logical paths, known as virtual circuits, for transmitting data from node to node

- Addressing and routing
- Logical address(IP)
- Physical address(MAC)

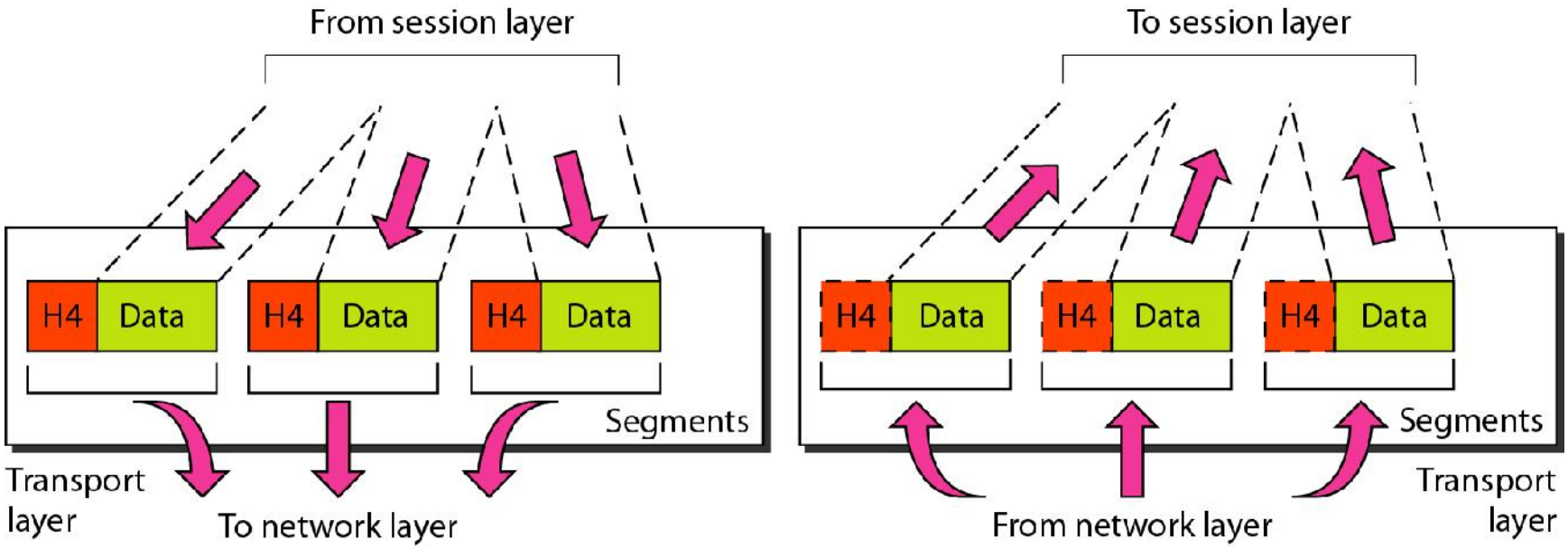
Network layer



Transport (Layer 4)

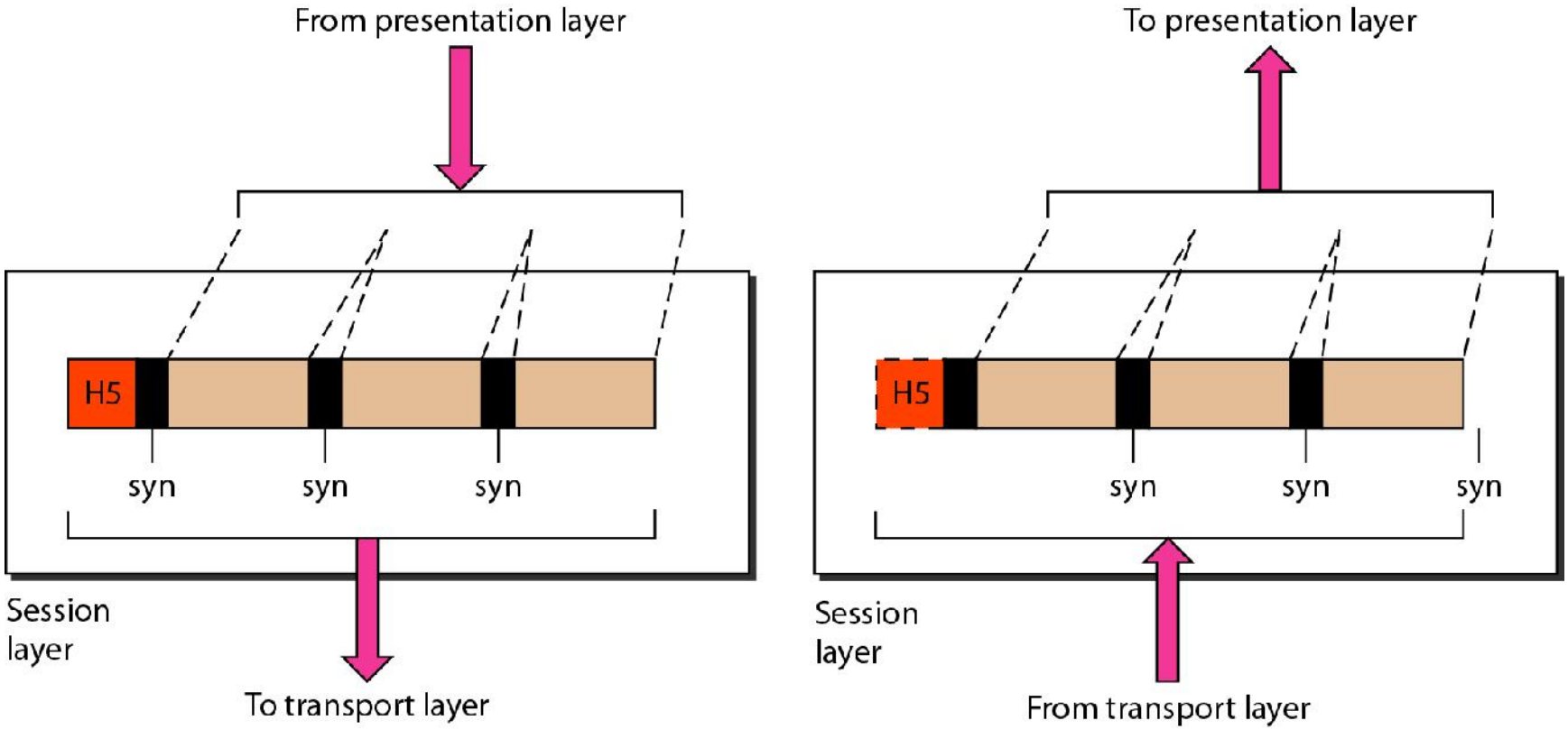
- This layer is responsible for flow control and ensuring messages are delivered error free.
- On the sending side , messages are packed for efficient transmission at the transport layer and assigned a tracking number so they can be reassembled in proper order.

- The transport layer of the OSI model offers end to end communication between end devices through the network.


From session layer
To session layer
H4
Data
H4
Data
H4
Data
H4
Data
H4
Data
H4
Data
Segments
Segments
Transport layer
To network layer
From network layer
Transport layer

Session (Layer 5)

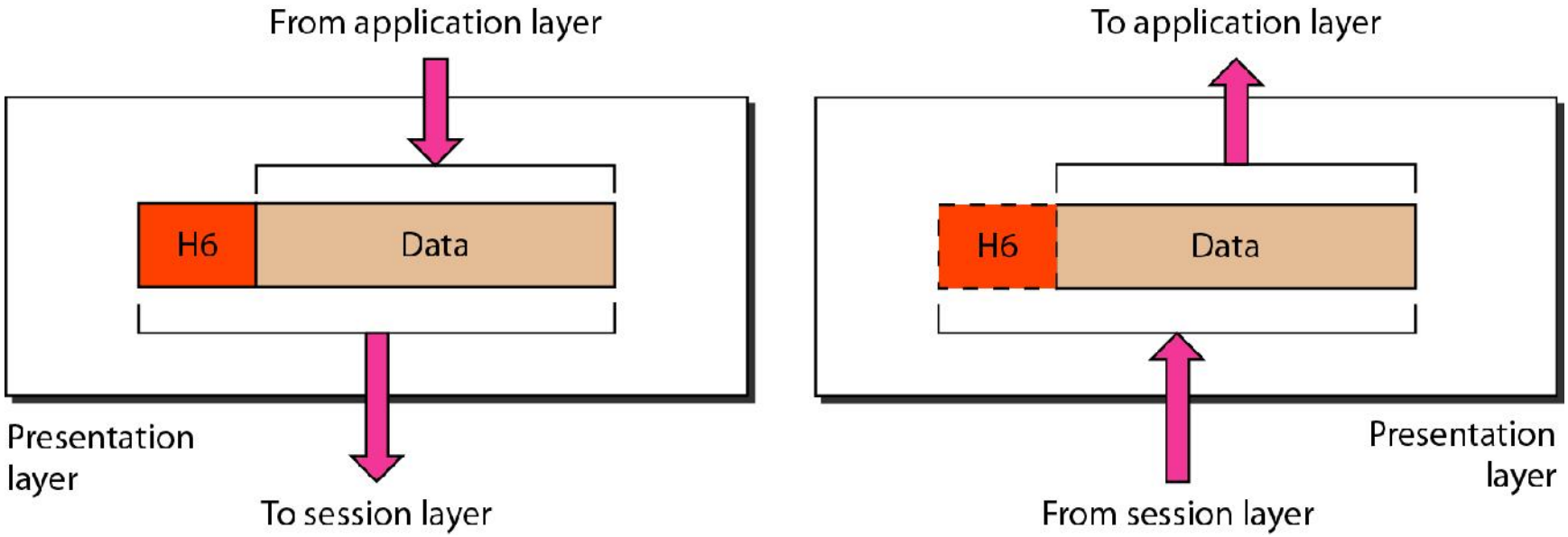
- This layer is responsible for establishing, maintaining and terminating a connection called a session.
- A session is an exchange of message between computers.
- Managing sessions include synchronization of user tasks and dialog control.


From presentation layer
H5
syn
syn
syn
Session
layer
To transport layer
To presentation layer
H5
syn
syn
syn
Session
layer
From transport layer

Presentation (Layer 6)

- This layer is responsible for data translation(formatting), compression and encryption.
- Eg: EBCIDIC characters are converted into ASCII.
- Data is compressed for transmission and uncompressed on receipt.
- Encryption techniques are implemented at presentation layer.

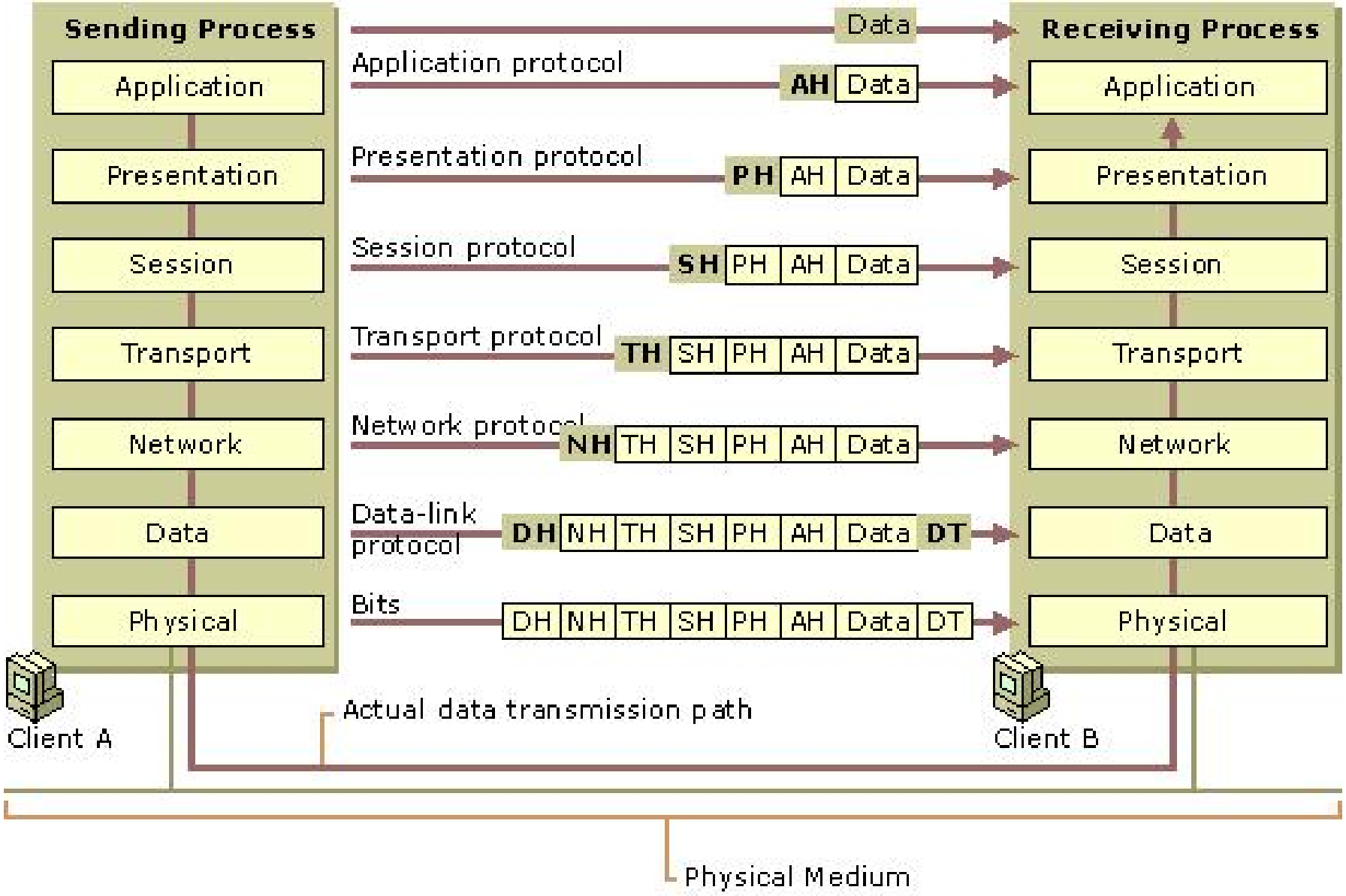
- Three fundamental functions:
- Data presentation
- Data compression
- Data encryption

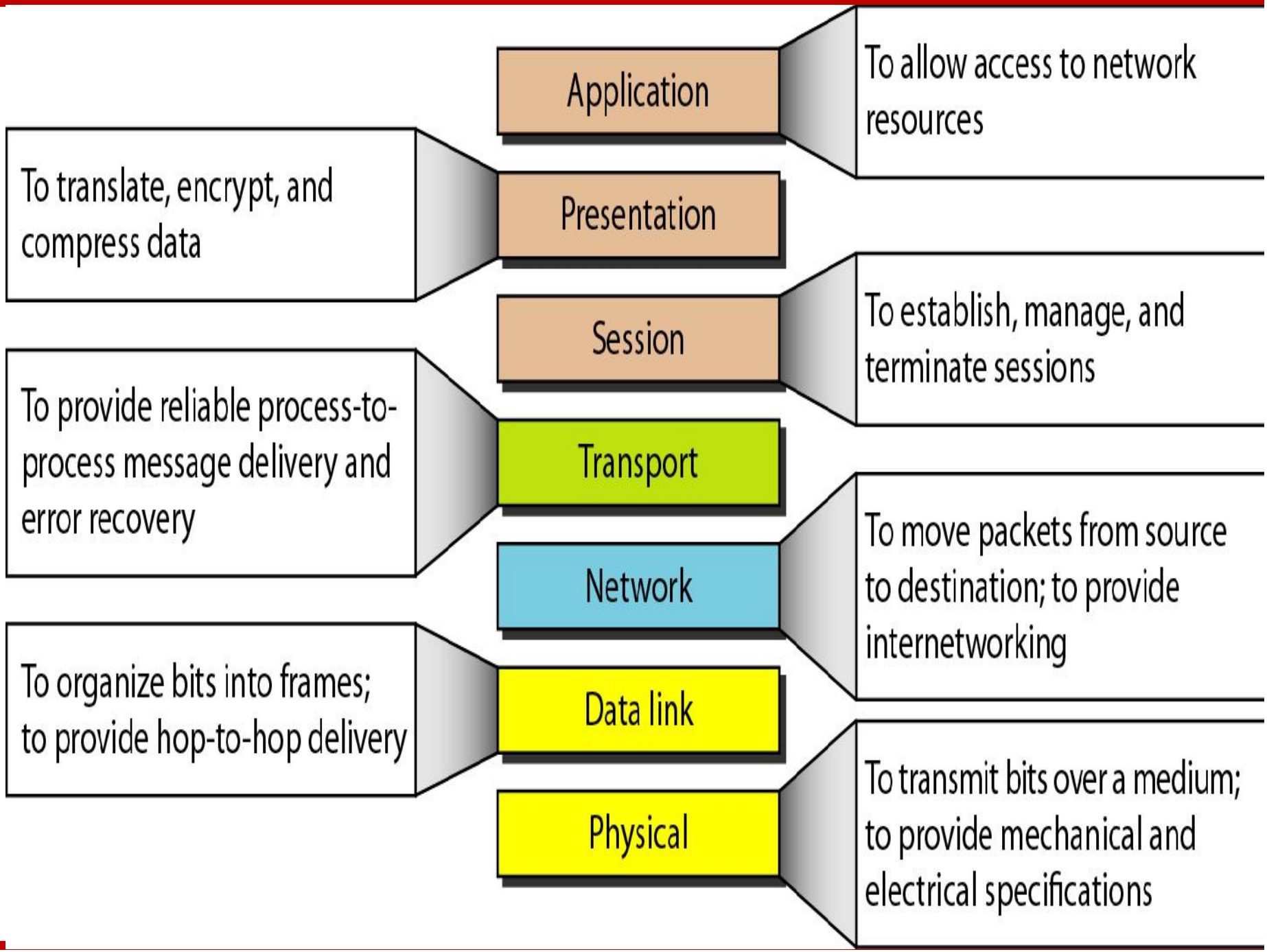

From application layer
H6
Data
Presentation layer
To session layer
To application layer
H6
Data
Presentation layer
From session layer

Application (Layer 7)

- Highest layer of OSI Model
- Provide applications with access to network services
- Provides services to the user of OSI environment.
- Login, password checking, file transfer etc are some of the functions of the application layer.
- It provides the operating system with direct access to network services.

Data Flow in the OSI Model

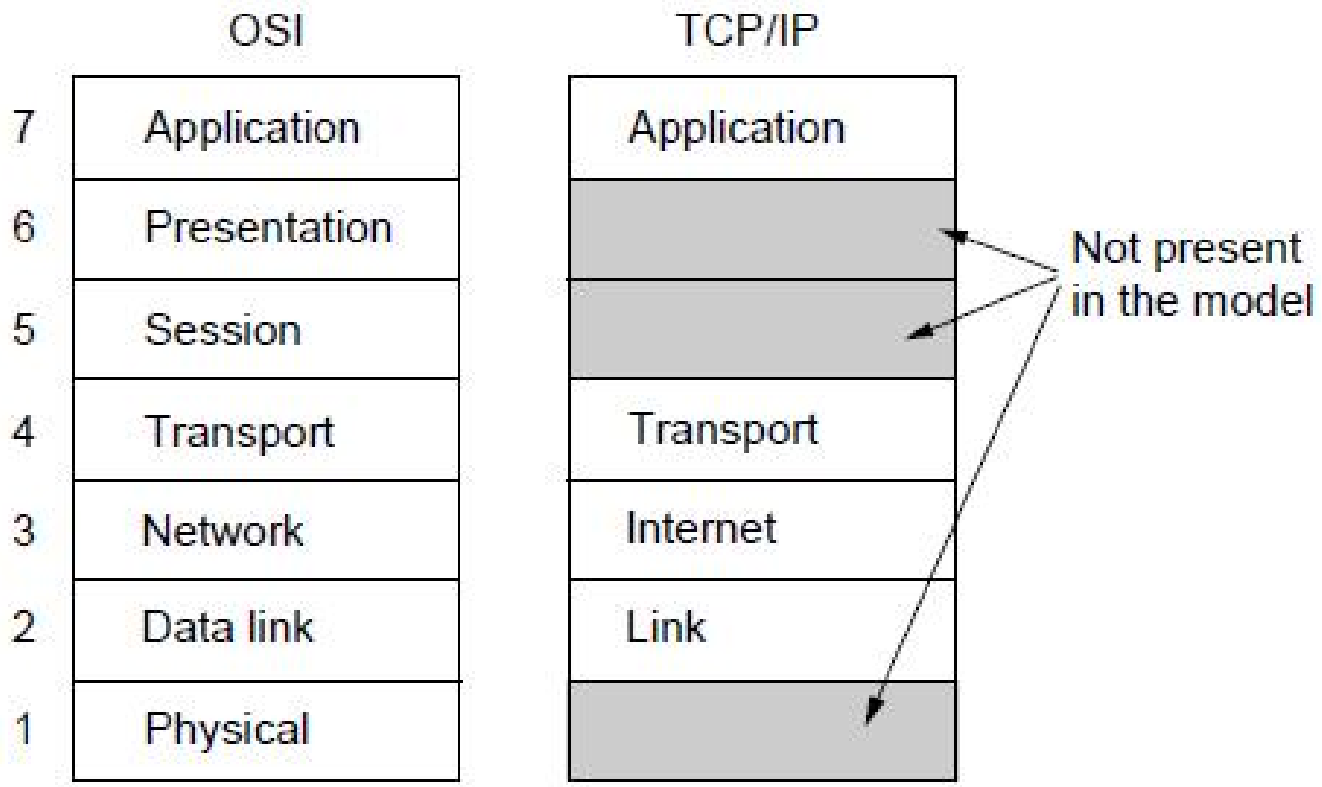



Application
To allow access to network resources
To translate, encrypt, and compress data
Presentation
Session
To establish, manage, and terminate sessions
To provide reliable process-to-process message delivery and error recovery
Transport
Network
To move packets from source to destination; to provide internetworking
To organize bits into frames; to provide hop-to-hop delivery
Data link
Physical
To transmit bits over a medium; to provide mechanical and electrical specifications

The TCP/IP Reference Model Layers

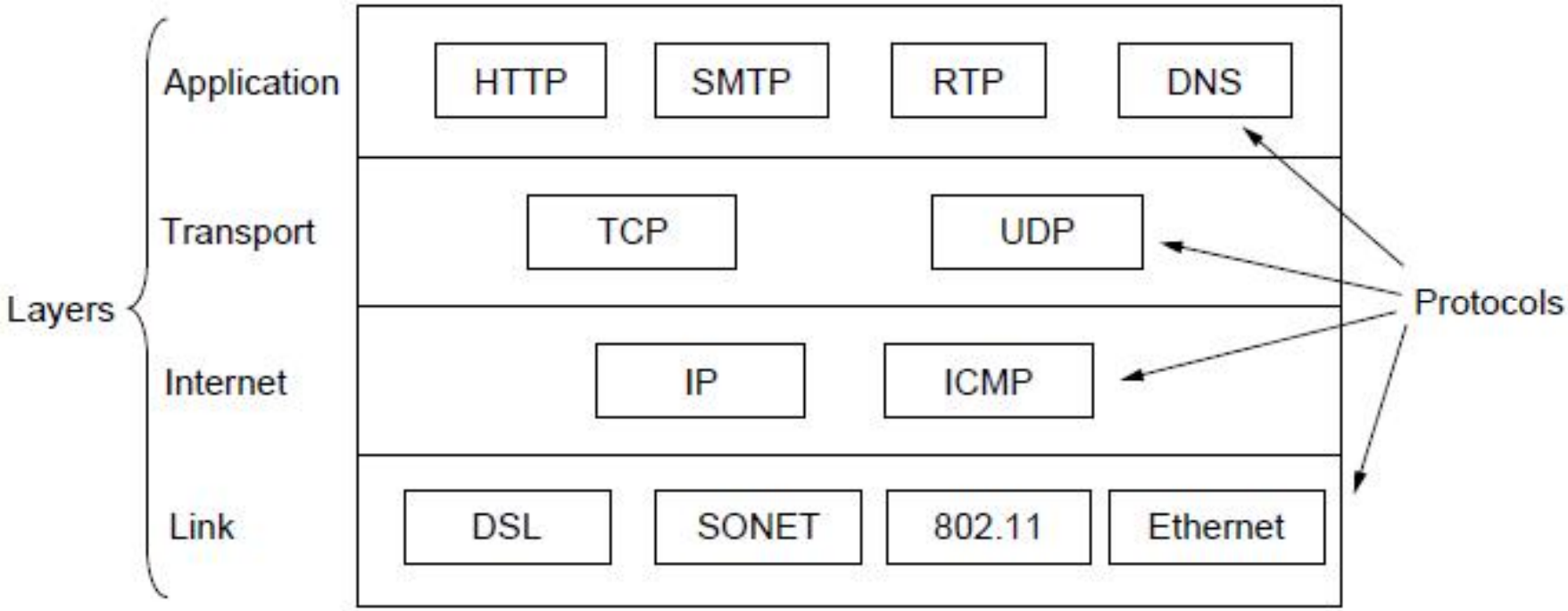
- Link layer
- Internet layer
- Transport layer
- Application layer

The TCP/IP Reference Model (1)



The TCP/IP reference model

The TCP/IP Reference Model (2)



The TCP/IP reference model with some protocols we will study

- RTP: real time transport protocol
- DNS : domain name Systems
- I CMP: The Internet Control Message Protocol
- **DSL** (Digital Subscriber Line)
- Synchronous Optical Networking (**SONET**)

Comparison of the OSI and TCP/IP Reference Models

Concepts central to OSI model

- Services
- Interfaces
- Protocols

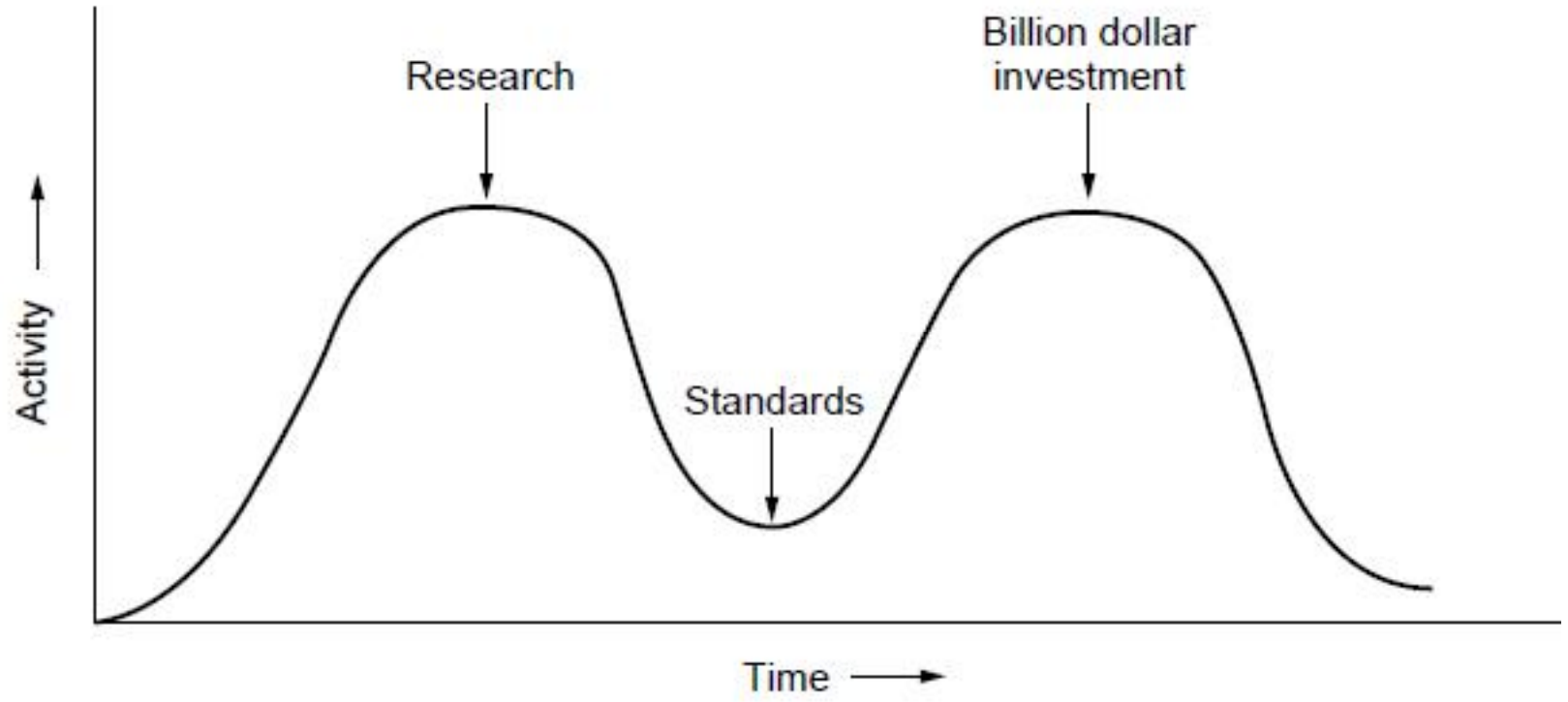
Critique of the OSI Model and Protocols

- Bad timing.
- Bad technology.
- Bad implementations.
- Bad politics.

Critique of TCP/IP

- Service, interface an protocols not distinguished
- Not a general model
- Host to network layer not really a layer
- No mention of physical layer
- Minor protocols deeply fixed, hard to replace.

OSI Model Bad Timing



The apocalypse of the two elephants.

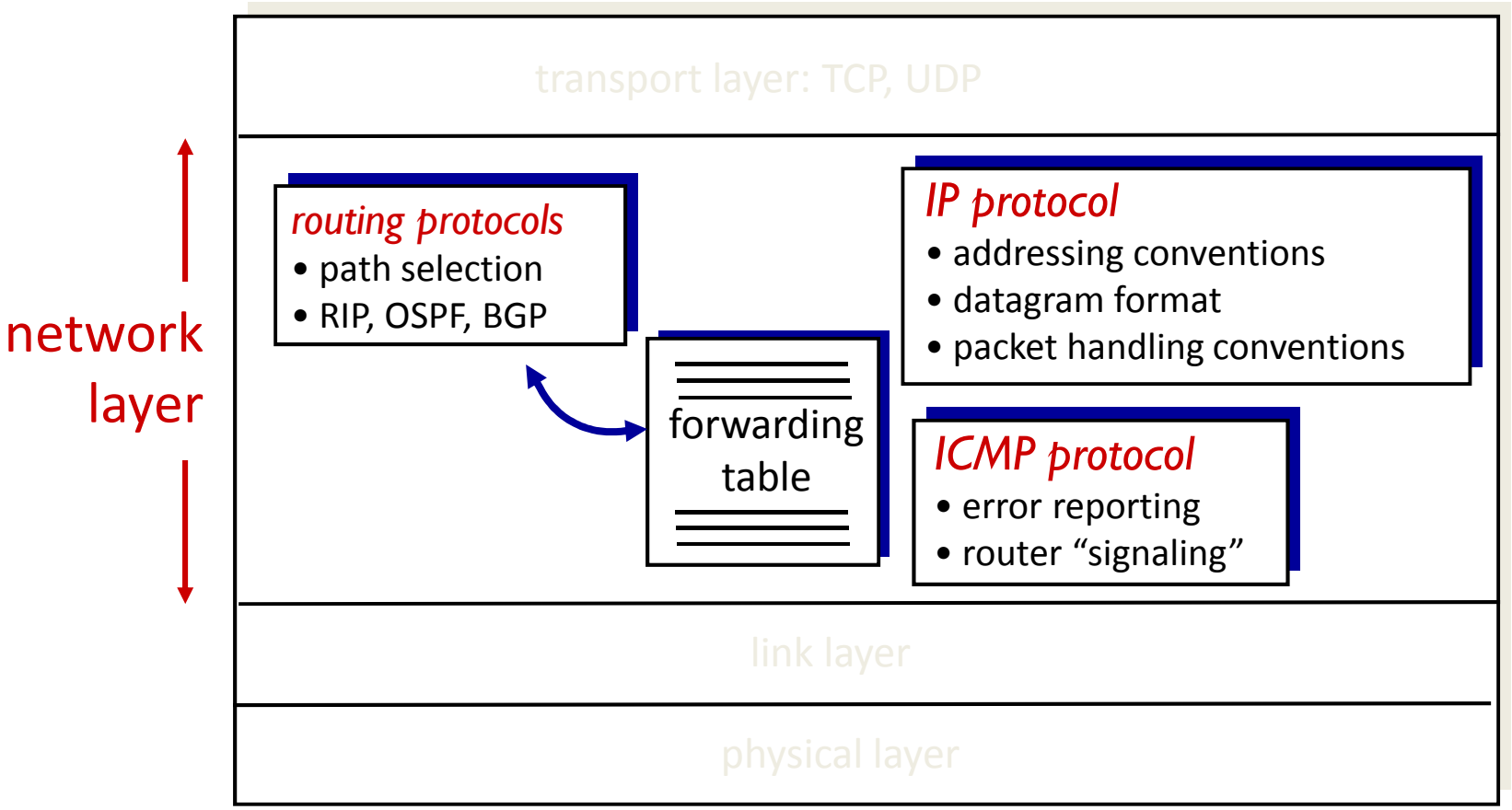
Internet protocols

- IP (Internet Protocol)
  - most widely used internetworking protocol
  - foundation of all internet-based applications
- • Only protocol at Layer 3

- • Defines
- – Internet addressing
- – Internet packet format
- – Internet routing

The Internet network layer

host, router network layer functions:

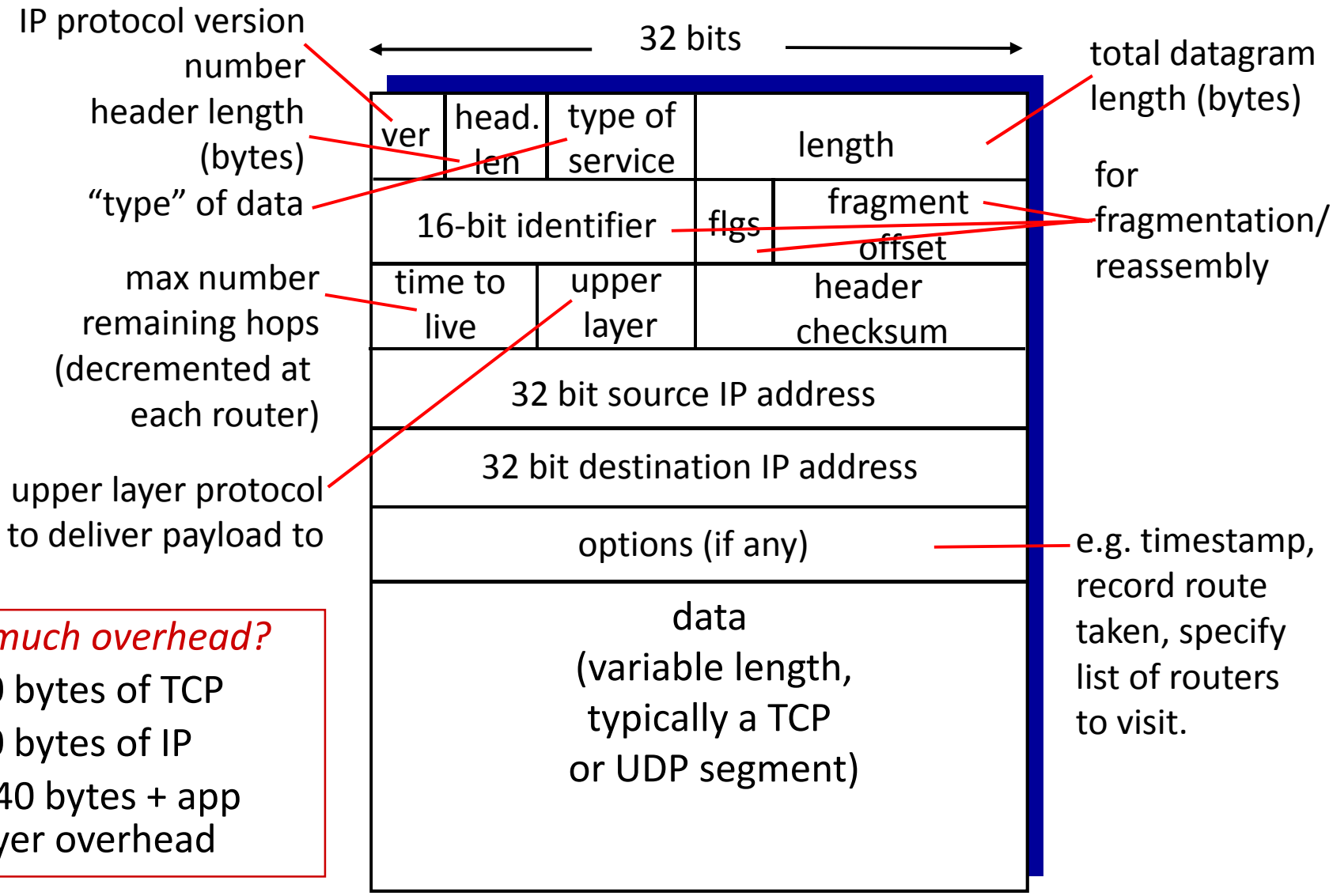


Internet Packets

- Contains sender and destination addresses
- Size depends on data being carried
- Called *IP datagram*
- Two Parts Of An IP Datagram

- **Header**
  - Contains source and destination address
  - Fixed-size fields
- **Data Area** (Payload)
  - Variable size up to 64K
  - No minimum size

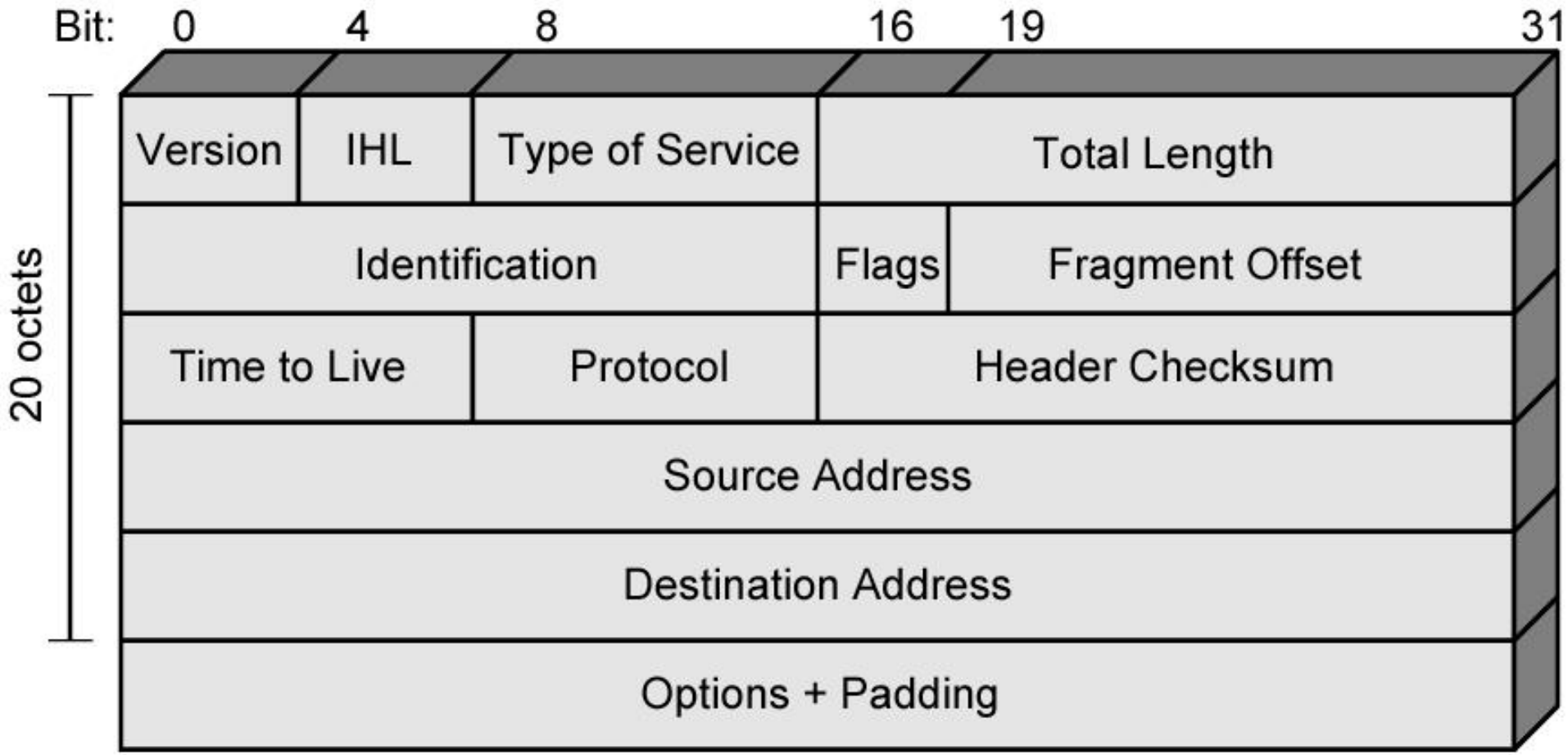
IP datagram format



how much overhead?

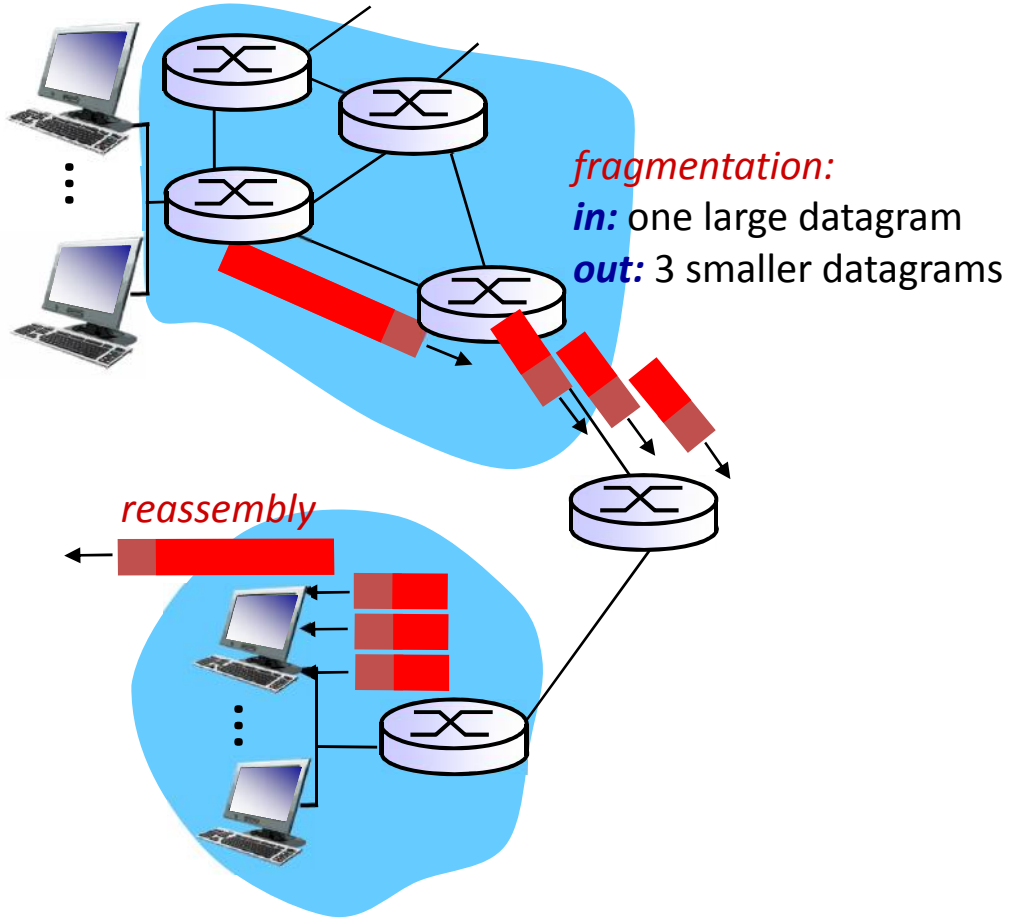
- 20 bytes of TCP
- 20 bytes of IP
- = 40 bytes + app layer overhead

IPv4 Header


Bit:
0
4
8
16
19
31
20 octets
Version
IHL
Type of Service
Total Length
Identification
Flags
Fragment Offset
Time to Live
Protocol
Header Checksum
Source Address
Destination Address
Options + Padding

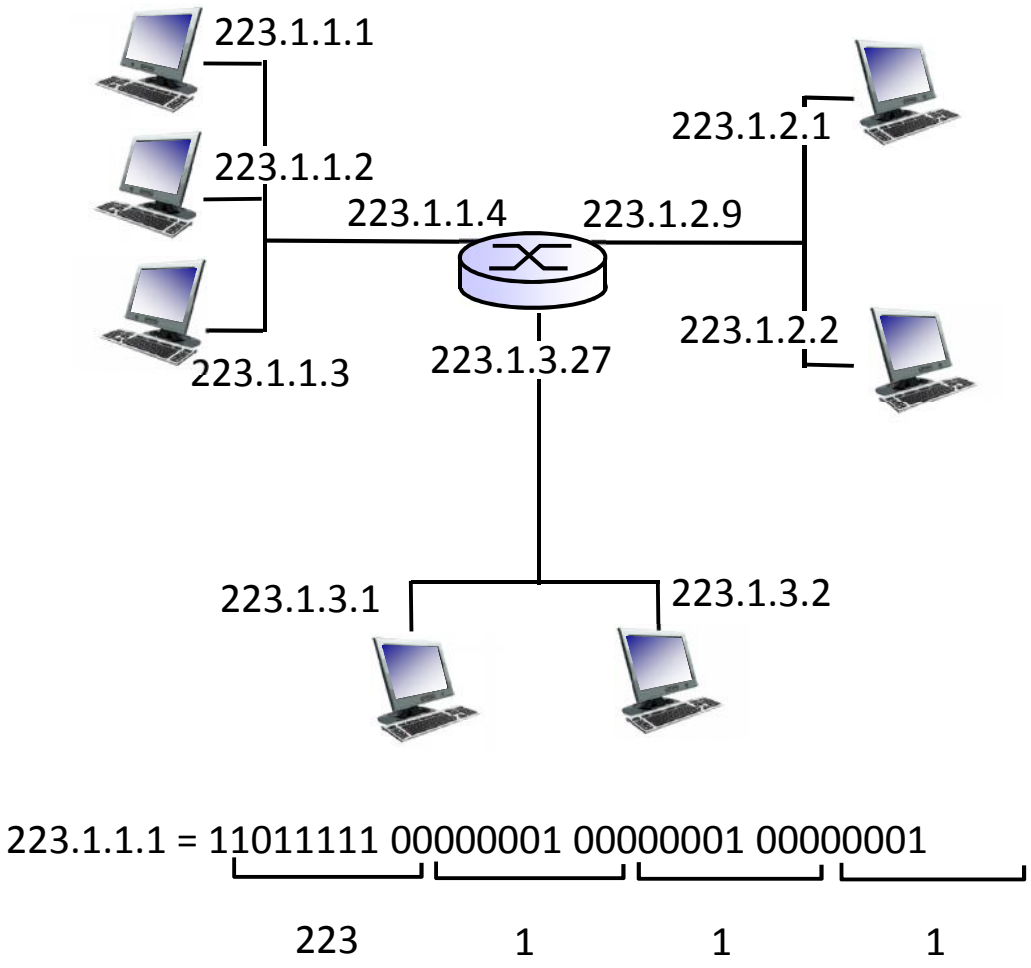
IP fragmentation, reassembly

- large IP datagram divided ("fragmented") within net
  - one datagram becomes several datagrams
  - "reassembled" only at final destination
  - IP header bits used to identify, order related fragments



IP addressing: introduction

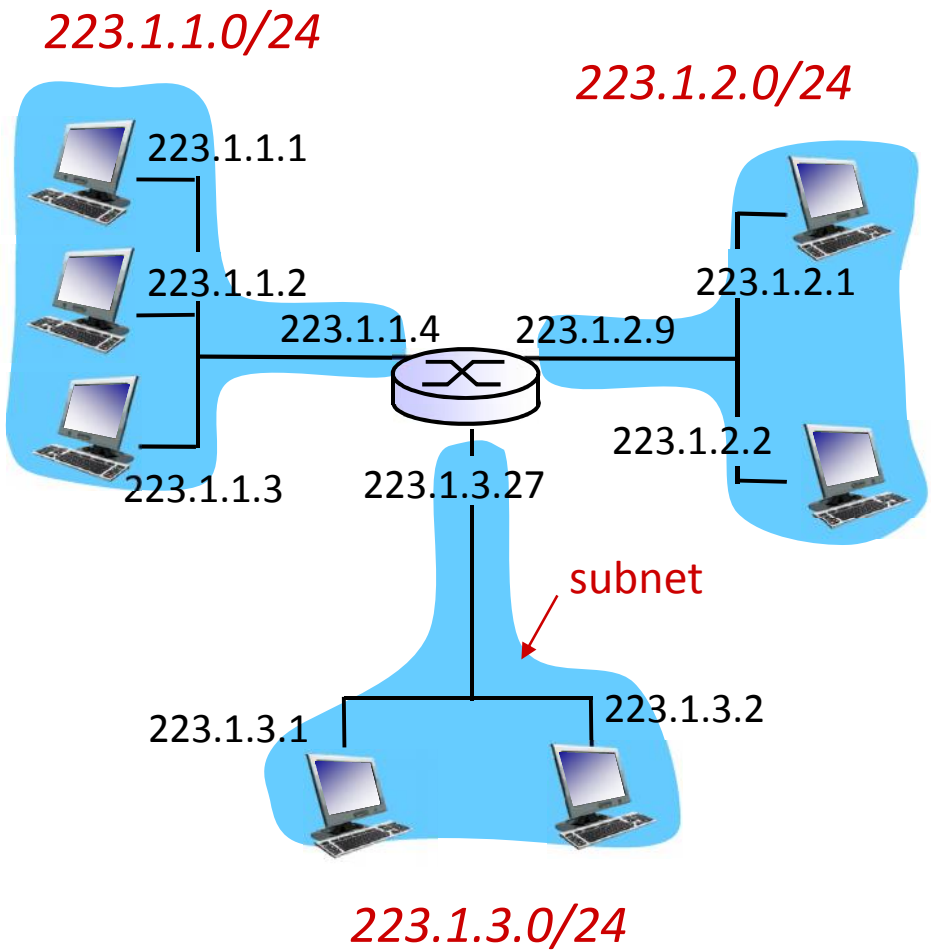
- *IP address:* 32-bit identifier for host, router *interface*
- *interface:* connection between host/router and physical link
  - router's typically have multiple interfaces
  - host typically has one interface
  - IP addresses associated with each interface



Subnets

recipe

- to determine the subnets, detach each interface from its host or router, creating islands of isolated networks



subnet mask: /24

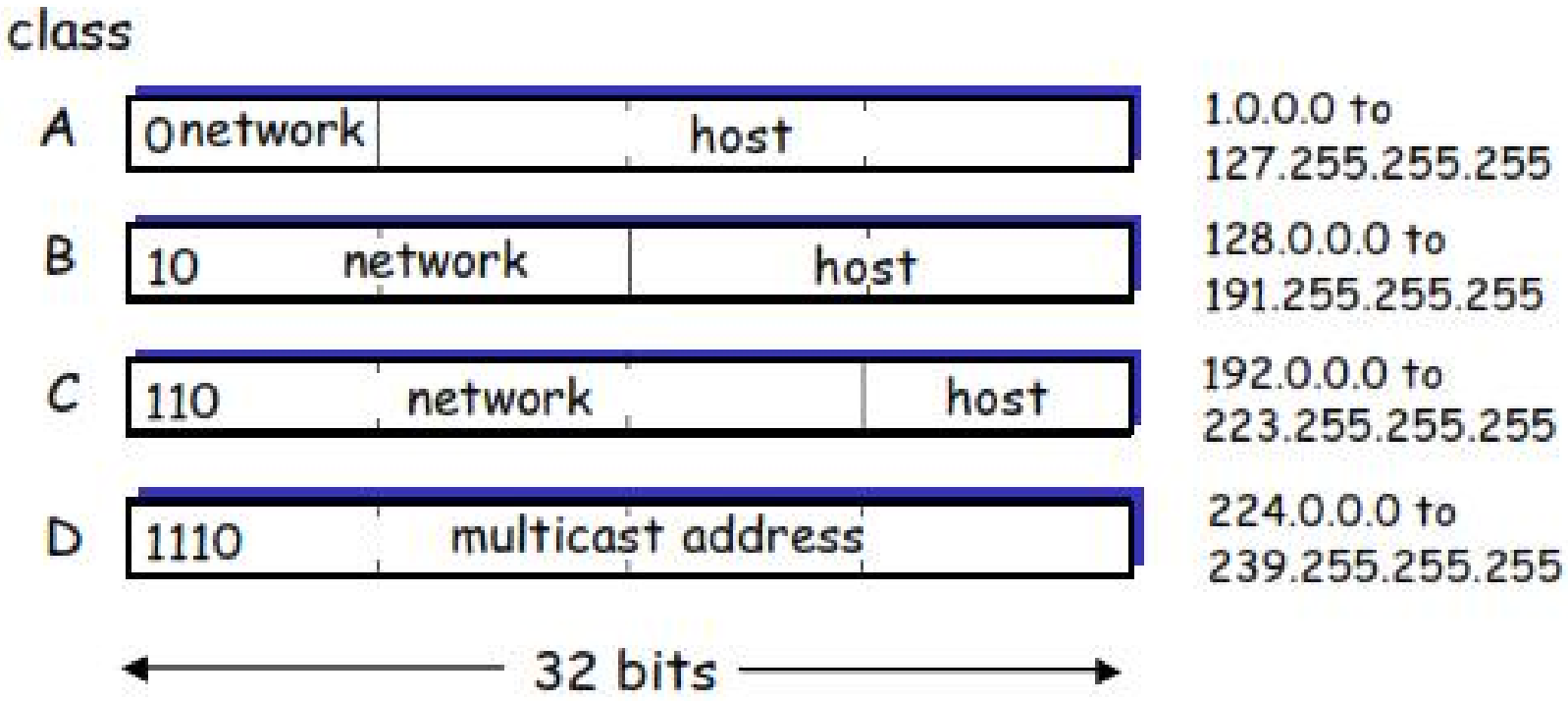
IP ADDRESS

- 32 Bits - divided into two parts
- – Prefix identifies network
- – Suffix identifies host
- Global authority assigns unique prefix to network (IANA)
- Local administrator assigns unique suffix to host

IP Addresses

given notion of "network", let's examine IP addresses:

"class-full" addressing:

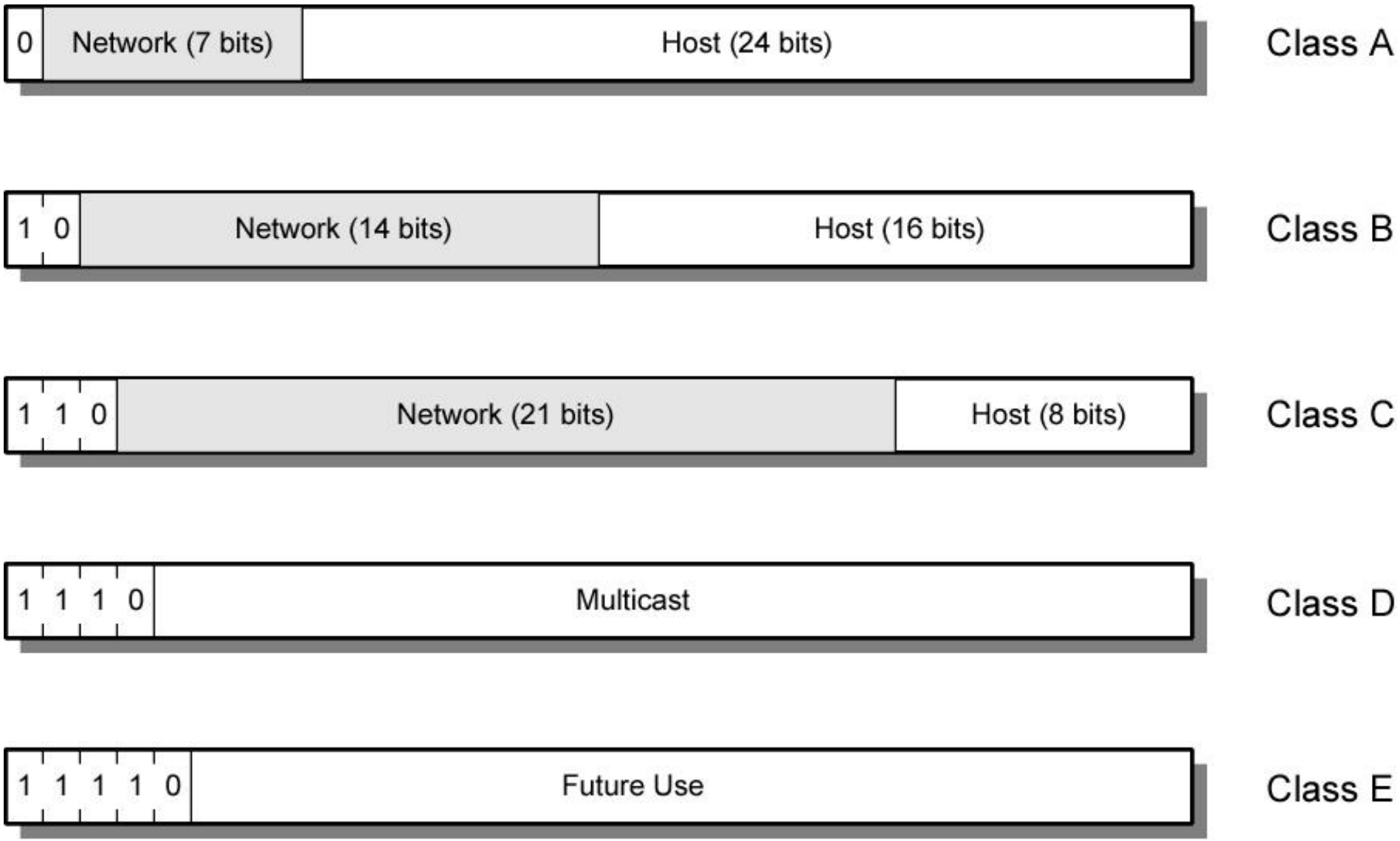


Classes And Network Sizes

Address Class	Prefix Bits	Max Nets	Suffix Bits	Max Hosts Per Net
A	7	128	24	16777216
B	14	16384	16	65536
C	21	2097152	8	256

- Maximum network size determined by class of address
  - Class *A* large
  - Class *B* medium
  - Class *C* small

IPv4 Address Formats



IP Addresses - Class A

- 32 bit global internet address
- Network part and host part
- Class A
  - Start with binary 0
  - All 0 reserved
  - 01111111 (127) reserved for loopback
  - Range 1.x.x.x to 126.x.x.x
  - All allocated

IP Addresses - Class B

- Start 10
- Range 128.x.x.x to 191.x.x.x
- Second Octet also included in network address
- 2^{14} = 16,384 class B addresses
- All allocated

IP Addresses - Class C

- Start 110
- Range 192.x.x.x to 223.x.x.x
- Second and third octet also part of network address
- 2^{21} = 2,097,152 addresses
- Nearly all allocated
  - See IPv6

The Evolution of the Internet

- **Advanced Research Projects Agency (ARPA)** - an organization formed by the United States government in 1958 to investigate and develop new military defense technology.
- **ARPANET** - a network that relied on telephone lines to transmit messages that had been fragmented into small packages of data between computers.
- **Domain Name System (DNS)** - a formal, centralized method for automatically associating IP addresses with host names.
- **NSFNET** - supercomputing centers at five universities across the nation plus a backbone to connect them with each other and, with other organizations.
- **World Wide Web (WWW)** - a collection of multiple Internet servers and a method for organizing data scattered over these servers.

Technical Specifications

- **Internet draft** - a thorough explanation of a proposed standard.
- **Internet Engineering Steering Group (IESG)** - a committee made of IETF technical area directors that oversees IETF decisions.
- **Request for Comments (RFC)** - a numbered document that articulates some aspect of Internet technology.
- **Proposed standard** - reclassified Internet draft.

- **Draft standard** - a proposed standard that has been successfully by at least two independent researchers.

Technical Specifications

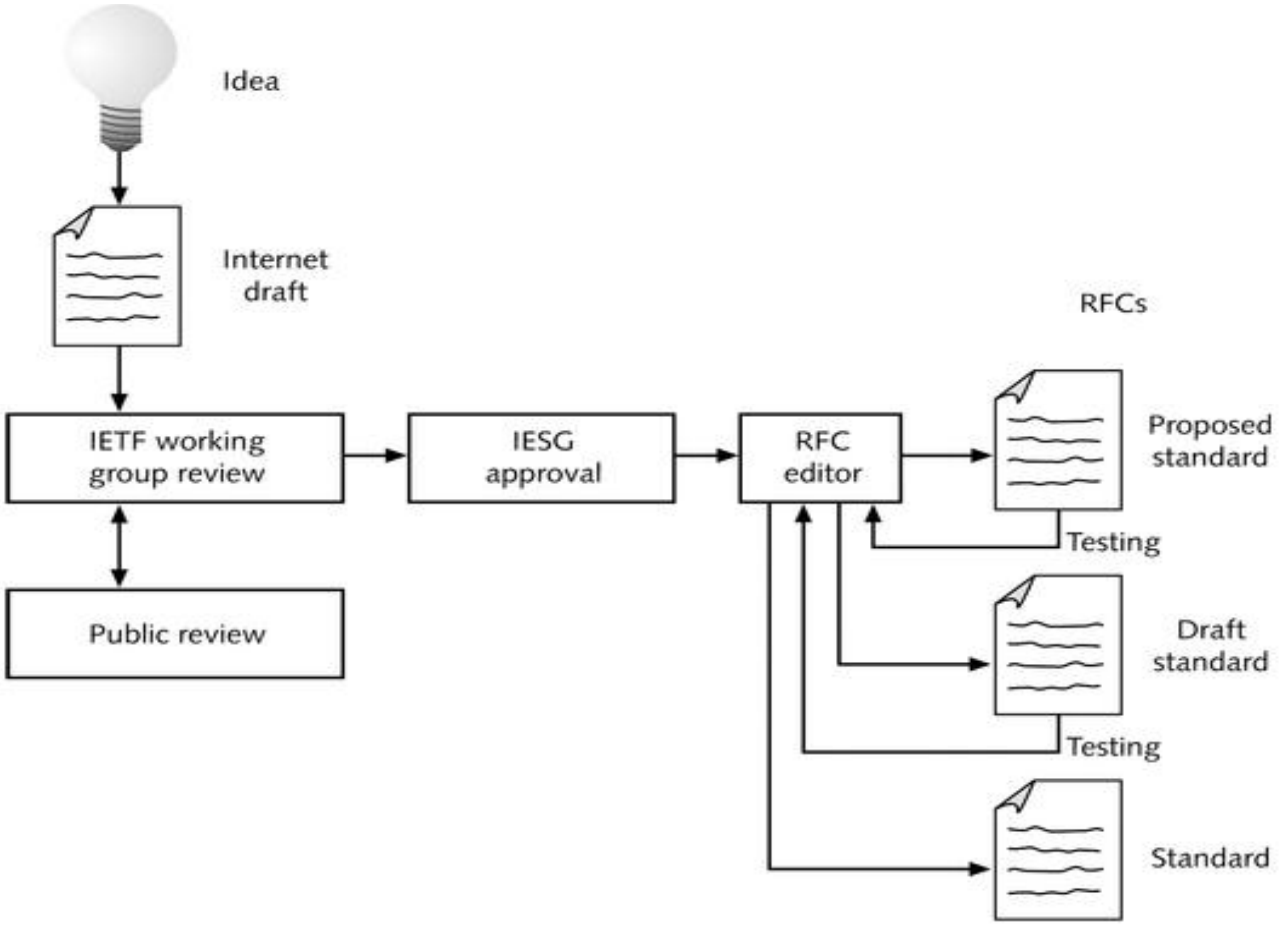


Figure 12-1 Steps in the Internet technical standards process

Technical Specifications

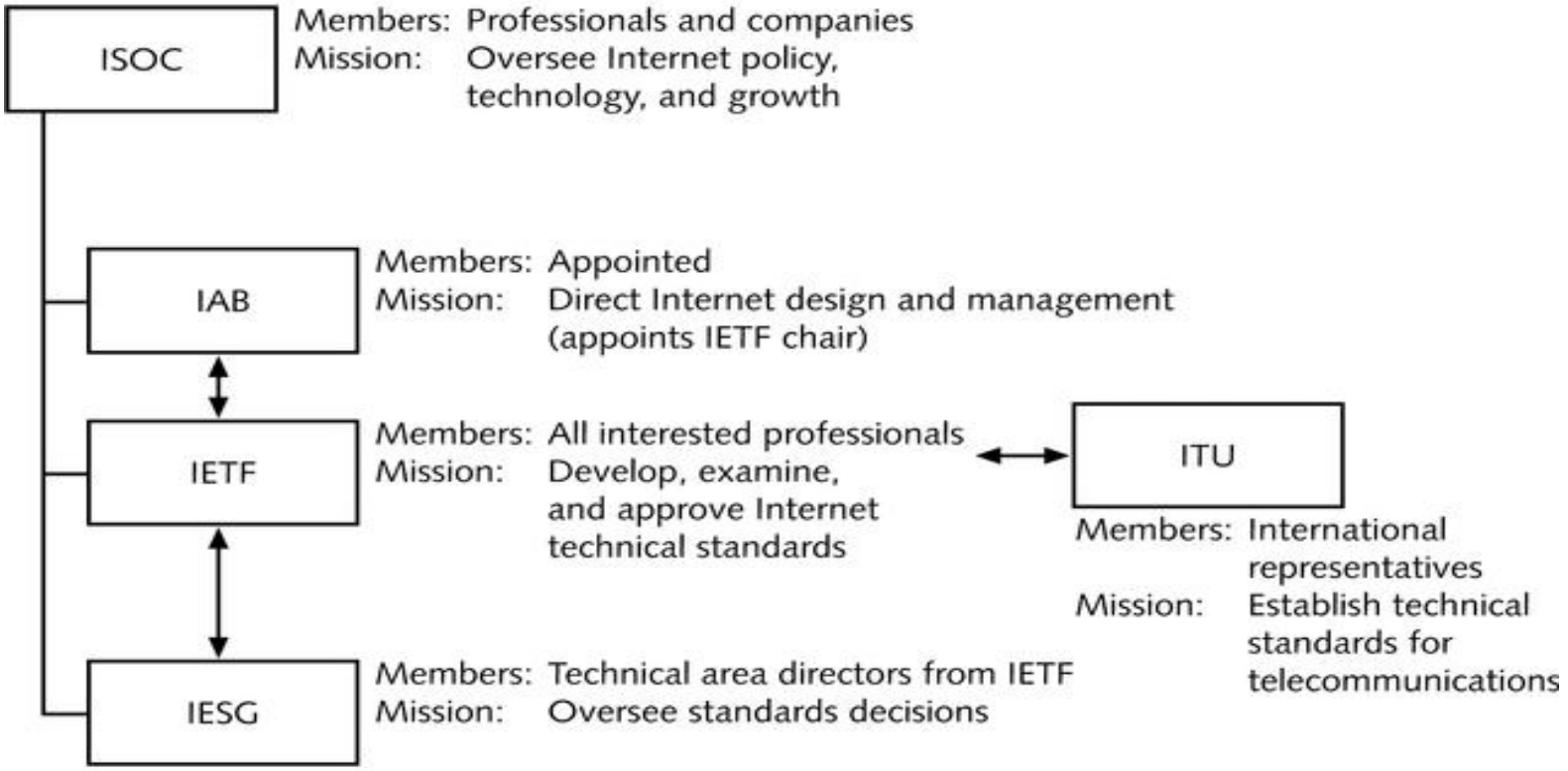


Figure 12-2 Relationships between Internet technical standards authorities

Address Assignments and Naming

- **Internet Assigned Numbers Authority (IANA):**
  - kept records of available and reserved IP addresses.
  - was also responsible for allocating domain names and maintaining the Domain Name System (DNS).

- **Regional Internet Registries (RIRS)** - a not-for-profit agency that manages the distribution of IP addresses to private and public entities.
- **Internet Corporation for Assigned Names and Numbers (ICANN)** - a private nonprofit corporation that is contracted by the government to oversee IP addresses and domain name management, plus accomplish specific Internet management improvements.

Host and Domain Naming

- TCP/IP is a protocol suite that contains several subprotocols.
- Some subprotocols, such as TCP, are connection-oriented.
- Connectionless subprotocols do not guarantee data delivery, but can transmit data faster than connection-oriented subprotocols.

Host and Domain Naming

- Each host belongs to a domain, which also has a name.
- Every host on a TCP/IP network requires a unique IP address to communicate with other hosts.
- Each IP address is a unique 32-bit number, divided into four octets, or 8-bit bytes.

Host Files

```
# IP address          host name                    aliases

122.48.77.239         vivaldi.composers.com        vivaldi
122.48.77.240         brahms.composers.com         brahms
122.48.77.241         grainger.composers.com       grainger
122.48.77.242         dvorak.composers.com         dvorak
122.48.77.243         cpebach.composers.com        cpeb
122.48.77.244         jsbach.composers.com         jsb
```

Figure 12-3 A host file

Domain Name System (DNS)

- A hierarchical way of identifying domain names and their addresses.

- Relies on a database, which is distributed over key computers, known as root servers, across the Internet.

- The last label in a domain name represents a top-level domain (TLD), or the highest level in a DNS hierarchy.
  - For example, in the **www.fcc.gov** domain, the TLD is “gov.”

Domain Name System (DNS)

Table 12-1 Top level domains

Top-Level Domain	Type of Organization
ARPA	Reverse lookup domain (special Internet function)
COM	Commercial
EDU	Educational
GOV	Government
ORG	Noncommercial organization (such as a nonprofit agency)
NET	Network (such as an ISP)
INT	International Treaty organization
MIL	U.S. Military Organization
BIZ	Businesses
INFO	Unrestricted use
AERO	Air-transport industry
COOP	Cooperatives
MUSEUM	Museums
NAME	Individuals
PRO	Professionals, such as doctors, lawyers, and engineers

Name Servers and Space

- **Name space** - the database of Internet IP addresses and their associated names.

- **Resource Record** - a single record that describes one piece of information in the DNS table.

- **Resolvers** - any host on the Internet that need to look up domain name information and associate it with an IP address.

- **Name servers (DNS servers)** - contain databases of names

The Use of Ports

- The logical address on a host where an application makes itself available to incoming data.

- The use of port numbers simplifies TCP/IP communications and ensures that data are transmitted to the correct application.

- Port numbers can have any numeric value from 0 to 65536.

- Port numbers in the range of 0 through 1023 are referred to as **well known port numbers**.

The Use of Ports

Table 12-2 Some common TCP/IP ports

Service	Port Number Assignment	Transport layer protocol used
DHCP	546 (client) and 547 (server)	UDP
DNS	53	TCP or UDP
FTP	20 (for data) 21 (for control)	TCP
HTTP	80	TCP
IMAP	585	TCP
Kerberos	88	TCP
NNTP	119	TCP
POP3	101	TCP
SMTP	25	TCP
SNMP	161	UDP
Telnet	23	TCP

World Wide Web (WWW)

On the client side, access to the Web requires: TCP/IP,

- a unique IP address,
- a connection to the Internet, and
- a browser

On the server side, a Web site requires TCP/IP,

- a connection to DNS servers,
- routers,
- Web server software, and