

COMPUTER NETWORKS


Unit-I Part-1





Course Objectives

1. To equip the students with an overview of
 - ▣ *The concepts and fundamentals of computer networks.*
2. Familiarize the students with
 - ▣ *The standard models for communication between machines in a network. (i.e. TCP/IP stack or OSI reference stack)*
 - ▣ *The protocols of the various layers. (i.e. FTP at Application layer, and so on.)*



Unit-I Part-1 (Introduction)

- ❑ Network hardware
- ❑ Network software
- ❑ OSI Reference model
- ❑ TCP/IP Reference model
- ❑ Example Networks: ARPANET, Internet

Introduction



□ Computer Network

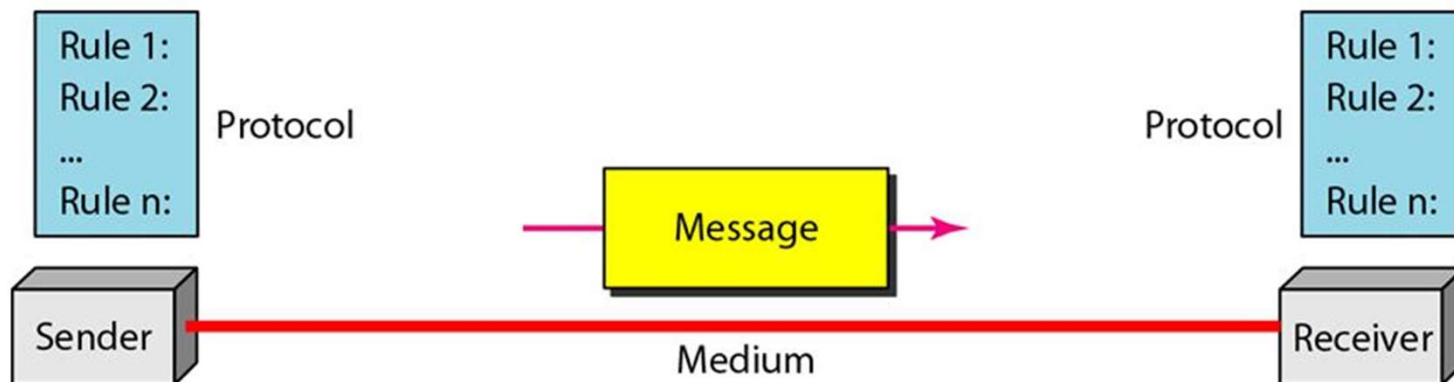
- A large number of separate but interconnected computers serving computational needs of an Organization.
- Internet being the most well-known example of a network of networks.

□ Distributed system

- a collection of independent computers appears to its users as a single coherent system
- A well-known example of a distributed system is the World Wide Web.

What is a Message

- Message: A written, or recorded communication sent to a recipient who cannot be contacted directly.
- In Computer Networks, a message will always have two parts
 - ▣ Header (The Address and Control information)
 - ▣ Payload (The Data)



Uses of Computer Networks



- ▣ Business Applications
 - Web applications, Email, VoIP and E-commerce
- ▣ Home Applications
 - Instant messaging, Twitter, Facebook, IPTV, IOT
- ▣ Mobile Applications
 - Short Message Service(SMS), Location Sharing, m-commerce, NFC, Wearable computing



▣ Social Issues

- New-found freedom brings with it many unsolved social, political, and ethical issues.
- Providing Net neutrality, Privacy and Security are challenging.

Network Hardware



- All Computer Networks can be classified based on
 - ▣ Transmission technology used and
 - ▣ Scale of the network.

- Types of transmission technology
 - ▣ point-to-point links and
 - ▣ broadcast links.

Classification based on Transmission Technology

- Point-to-point links
 - ▣ connect individual pairs of machines.
 - ▣ Information from source node to destination node is sent in short messages, generally called packets.
- Broadcast links or network
 - ▣ communication channel is shared by all the machines on the network
 - ▣ packets sent by any machine are received by all other nodes.

Classification based on Network Scale



- An alternative criterion for classifying networks is by scale.
- Distance is important as a classification metric because different technologies are used at different scales.
- Examples
 - Local Area Networks
 - Metropolitan Area Networks
 - Wide Area Networks
 - Wireless Networks
 - Home Networks
 - Internetworks

Classification based on Network 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

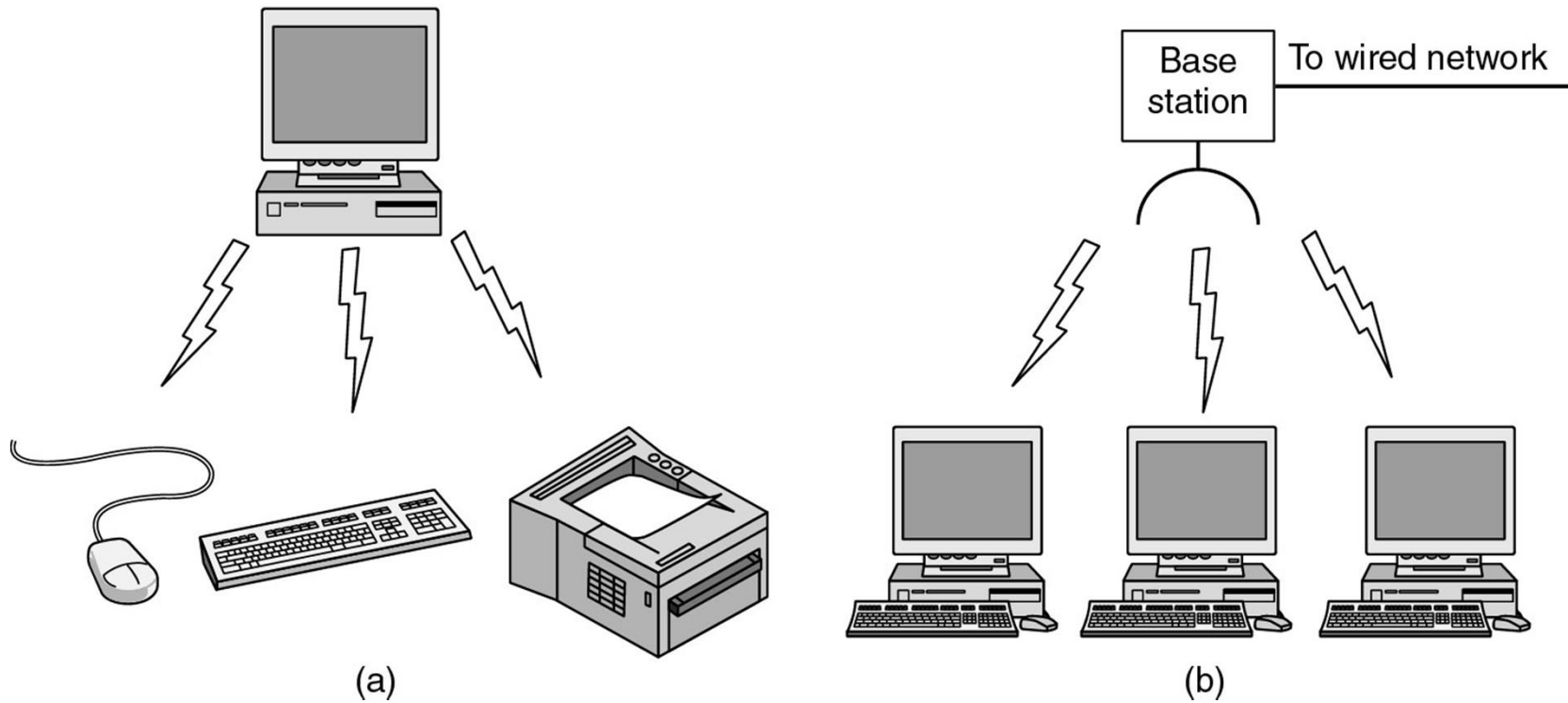
Classification of interconnected processors by scale.

Personal Area Networks



- PANs (Personal Area Networks) let devices communicate over the range of a person.
- A common example is a wireless network that connects a computer with its peripherals.
- Bluetooth is a network design for a short-range wireless network to connect components without wires.

Wireless Networks



(a) Bluetooth configuration

(b) Wireless LAN

Local Area Networks



- A LAN (Local Area Network) is a privately owned network that operates within and nearby a single building like a home, office or factory.
- LANs are widely used to share resources (e.g., printers) and exchange information among computers.
- Types of LANs
 - ▣ Wired and Wireless

Wireless and wired LANs

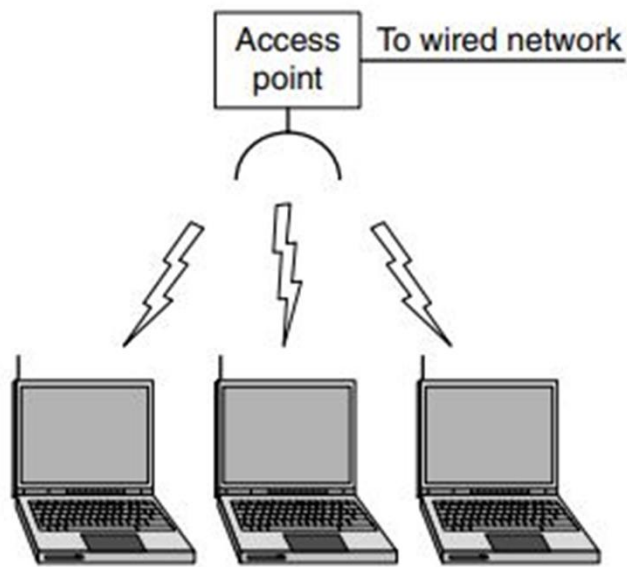
□ Wired LANs

- ▣ The wired LANs standard is called IEEE 802.3, popularly known as Ethernet.
- ▣ Each computer speaks the Ethernet protocol and connects to a box called a **switch** with a point-to-point link

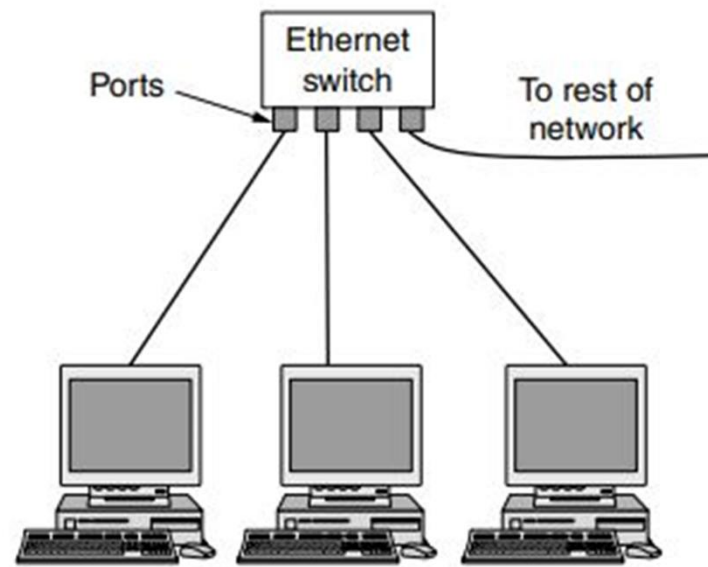
□ Wireless LANs

- ▣ It use an **AP** (Access Point), wireless router, or base station to relays packets between the wireless computers and the Internet.
- ▣ The wireless LANs standard is called IEEE 802.11, popularly known as Wi-Fi.

Wireless and wired LANs

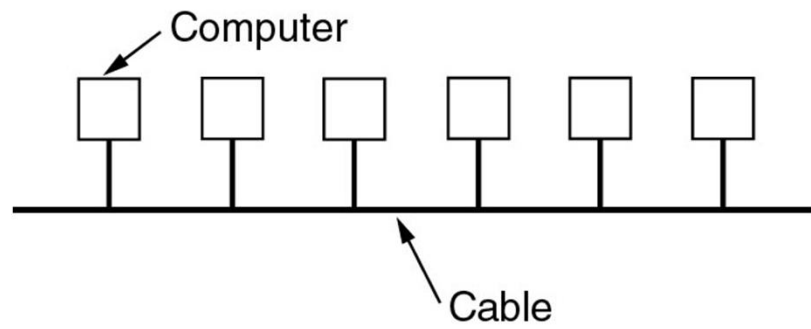


(a) 802.11

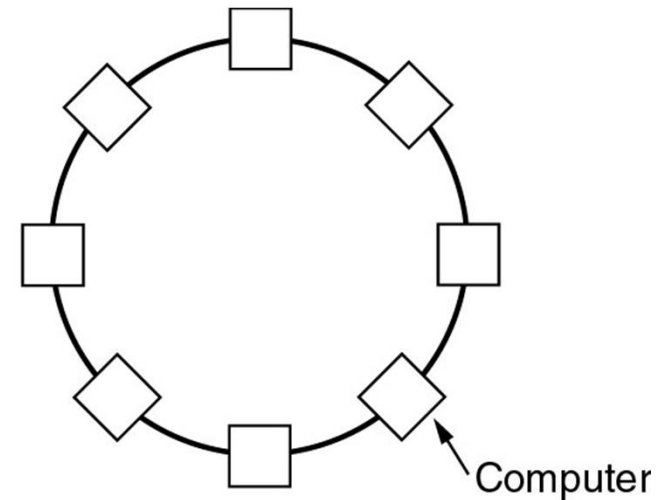


(b) Switched Ethernet

Local Area Networks



(a)



(b)

Two broadcast networks

(a) Bus

(b) Ring

Static and Dynamic broadcast network designs

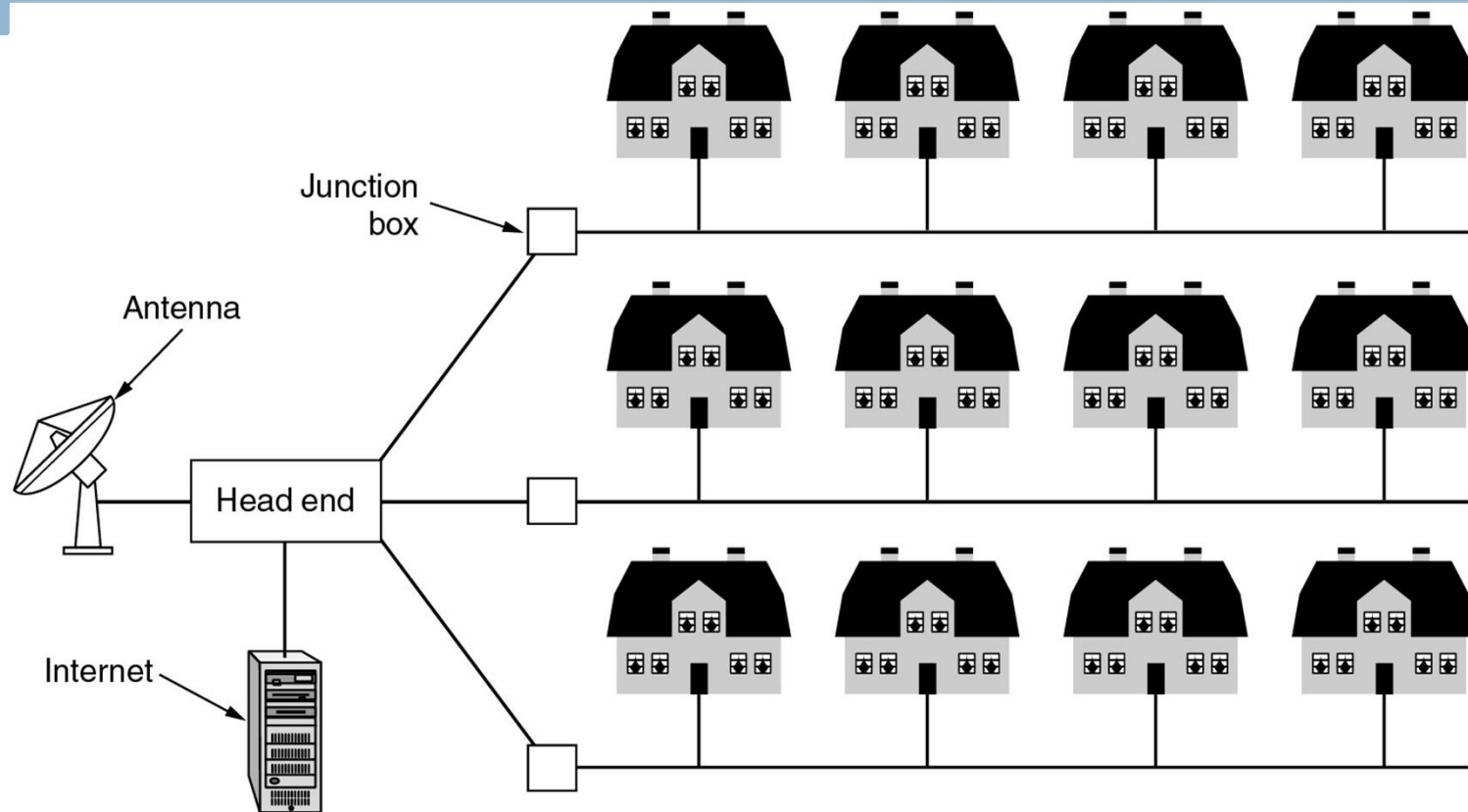
- Both wireless and wired broadcast networks can be divided into static and dynamic designs.
- Static designs
 - A typical static allocation would be to divide time into discrete intervals and use a round-robin algorithm, allowing each machine to broadcast only when its time slot comes up.
 - Static allocation wastes channel capacity.
- Dynamic designs
 - Dynamic allocation methods for a common channel are either centralized or decentralized.
 - In the centralized channel allocation method, there is a single entity, for example, the base station in cellular networks, which determines who goes next.
 - In the decentralized channel allocation method, there is no central entity; each machine must decide for itself whether to transmit.

Metropolitan Area Networks



- A MAN (Metropolitan Area Network) covers a city.
- The best-known examples of MANs are the cable television networks available in many cities.
- The latest MAN, which has been standardized as IEEE 802.16 and is popularly known as WiMAX.

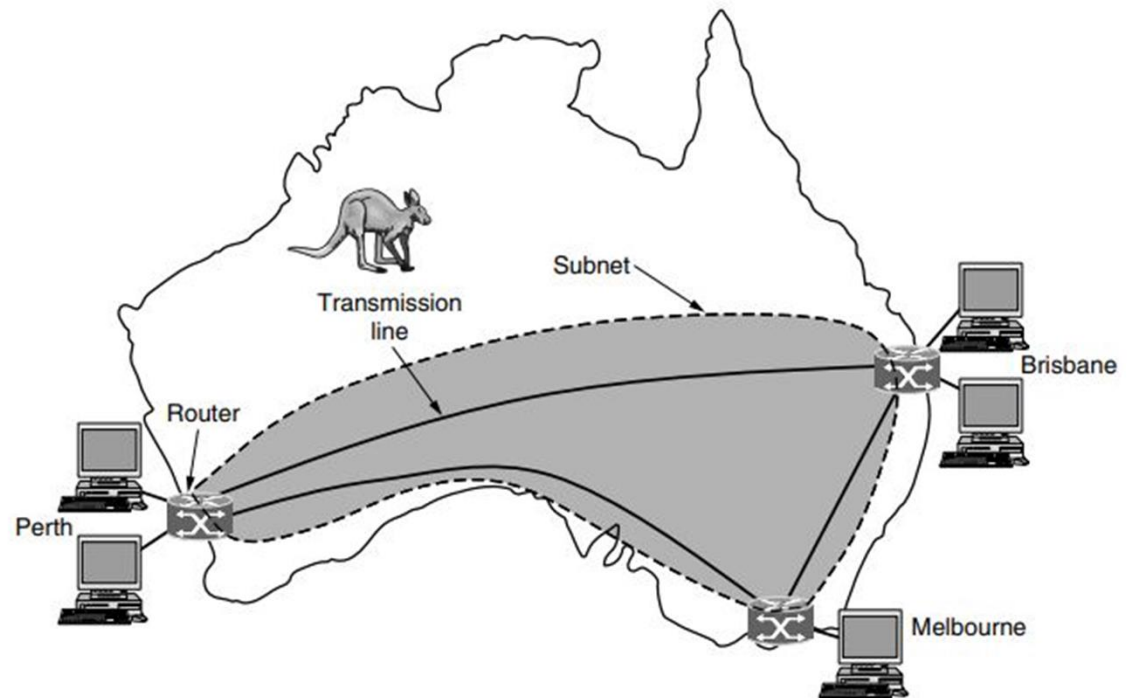
Metropolitan Area Networks



A metropolitan area network based on cable TV.

Wide Area Networks

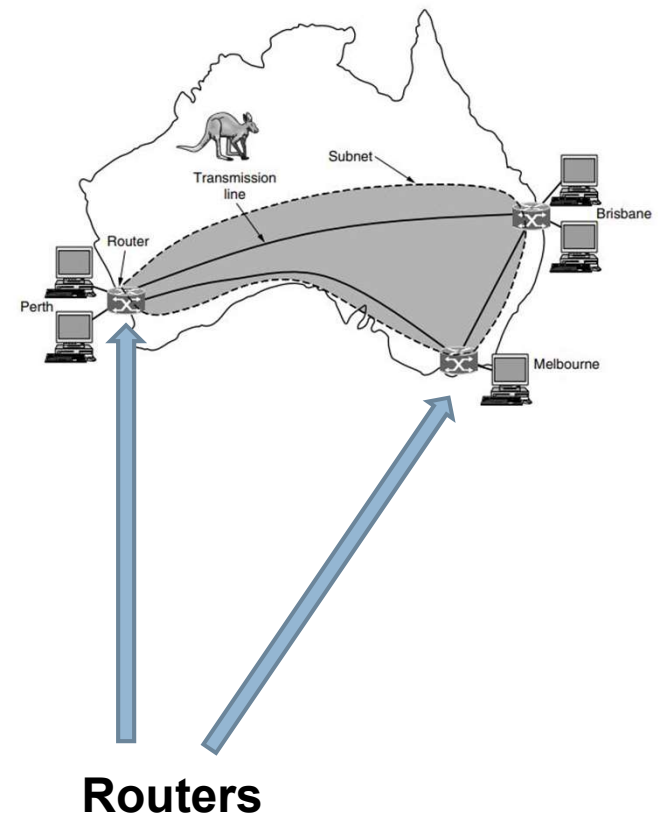
- A WAN (Wide Area Network) spans a large geographical area, often a country or continent. Examples include satellite and cellular networks



Example of a WAN that connects three branch offices in Australia.

Wide Area Networks

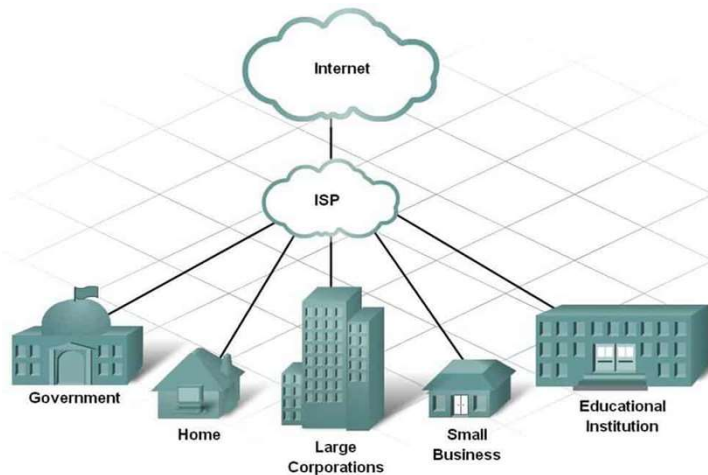
- Each of these offices contains computers, called **Hosts**.
- The network that connects the hosts from different offices is then called the **Subnet**.
- In most WANs, the subnet consists of two distinct components:
 - ▣ transmission lines and
 - ▣ switching elements
- **Transmission lines** move bits between machines.
 - ▣ They can be made of copper wire, optical fiber, or even radio links.
- Switching elements are specialized computers that connect two or more transmission lines, now most commonly known as **Router**.



Types of WANS: VPN and ISP

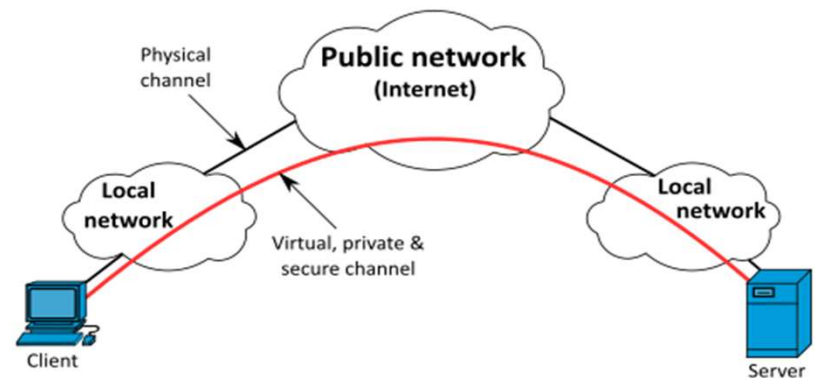
Internet Service Provider (ISP)

- It is an organization that provides services for accessing, using, or participating in the Internet.
- It owns the network infrastructure and provides service to customers who pay for the



Virtual Private Network (VPN)

- It is used to provide private access to corporate applications and resources to remote users and offices.
- For security, the private network connection may be established using a tunneling protocol.



Internetworks



- A collection of interconnected networks is called an internetwork or internet.
- This is in contrast to the worldwide Internet (which is one specific internet), which we will always capitalize.
- The Internet uses ISP networks to connect enterprise networks, home networks, and many other networks.

Internetworks

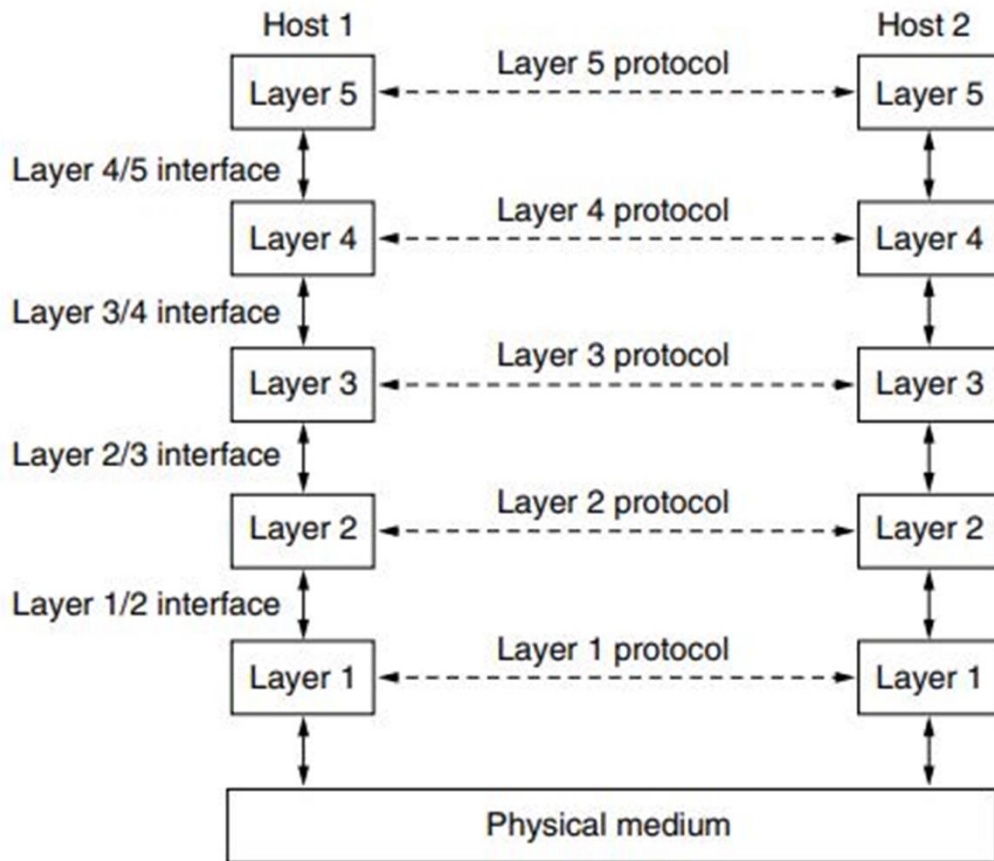


- Internetworks are created
 - ▣ if different organizations have paid to construct different parts of the network and each maintains its part.
 - ▣ if the underlying technology is different in different parts (e.g., broadcast versus point-to-point and wired versus wireless).
- A machine that makes a connection between two or more networks and provides the necessary translation, both in terms of hardware and software, is called a gateway.

Network Software

- The **Protocol Hierarchies** form the keystones of the network software.
- To reduce their design complexity
 - Most networks are organized as a stack of layers.
 - Each layer is built upon the one below it.
 - The number of layers, the name of each layer, the contents of each layer, and the function of each layer differ from network to network.
 - The purpose of each layer is to offer certain services to the higher layers while shielding those layers from the details of how the offered services are actually implemented.
 - In a sense, each layer is a kind of virtual machine, offering certain services to the layer above it.

Network Architecture.



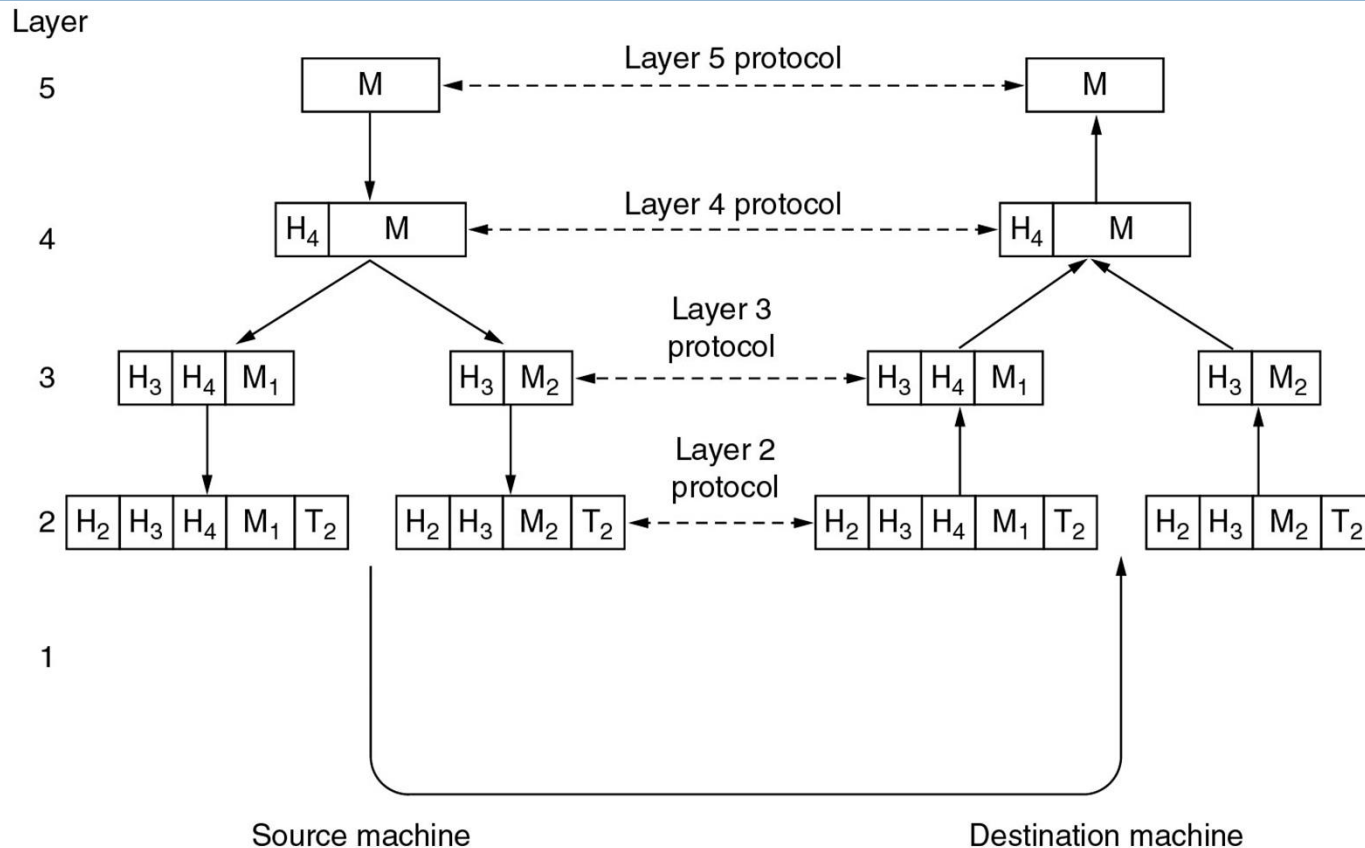
- The **physical medium** through which actual communication occurs.
- The **virtual communication** is shown by dotted lines and physical communication by solid lines.
- Between each pair of adjacent layers is an **interface**.
- A set of layers and protocols is called a **Network Architecture**.

Protocol Hierarchies



- The fundamental idea is that a particular piece of software (or hardware) provides a service to its users but keeps the details of its internal state and algorithms hidden from them.
- When a layer on one machine carries on a conversation with same layer on another machine, the rules and conventions used in this conversation are collectively known as the protocol used by the layer.

Protocol Hierarchies



Example information flow in between layer 5 of two different machines. (M for Message, H for Header.)

Design Issues for the Layers



- The key design issues in computer networks at various layers for implementing successful communication across machines are
 - ▣ Reliability
 - ▣ Scalability (evolution of the network)
 - ▣ Resource allocation
 - ▣ Network security

Reliability of Information sent



- It is the design issue of making a network that operates correctly even though it is made up of a collection of components that are themselves unreliable.
- Information transmitted generally gets corrupted due to fluke electrical noise, random wireless signals, hardware flaws, software bugs and so on
- Solution:
 - ▣ Error detection and correction using redundant information added to the data sent.

Reliability of Information path



- It is the issue in finding a working path through a network because most often there are multiple paths between a source and destination.
- There may be some links or routers that are broken.
- Solution:
 - ▣ Routing Protocols: algorithms that are used to select better paths between some source and destination.

Scalability (Evolution of the network)

- Over time, networks grow larger and new designs emerge that need to be connected to the existing network.
- Solution:
 - ▣ Protocol layering: reflecting on the change by customizing the protocols.
- Every layer needs a mechanism for identifying the senders and receivers that are involved in a particular message.
- Solution:
 - ▣ Addressing or naming (i.e. IP addresses and port numbers.)
- Coping with different types of inter-connected networks or internetworking
- Solution:
 - ▣ Fragmentation and re-assembly

Resource allocation

- Networks provide a service to hosts from their underlying resources, such as the capacity of transmission lines.
- To do this well, they need mechanisms that divide their resources so that one host does not interfere with another too much.
- Solution:
 - Multiplexing
- An allocation problem that occurs at every level is how to keep a fast sender from swamping a slow receiver with data.
- Solution:
 - Flow control
- The network is oversubscribed because too many computers want to send too much traffic, and the network cannot deliver it all.
- This overloading of the network is called congestion.
- Solution:
 - Congestion control
 - Regulating QoS parameters

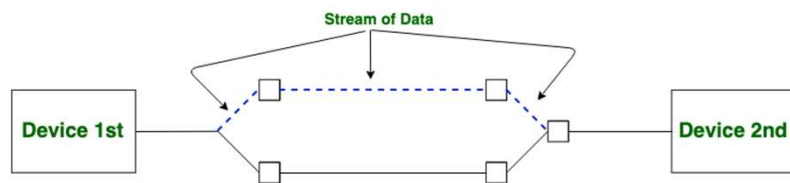
Network security



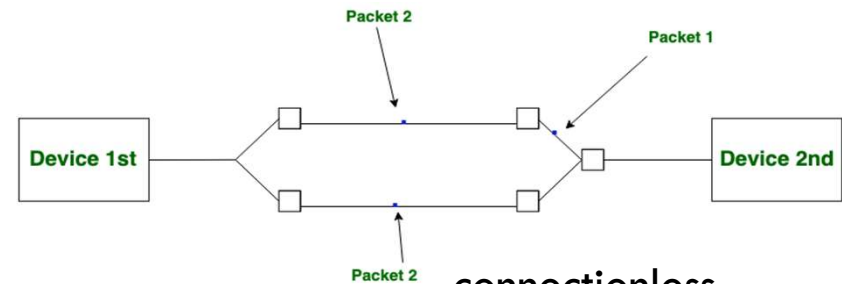
- To secure the network by defending it against different kinds of threats.
- Solution:
 - ▣ Mechanisms that provide **confidentiality** defend against this threat, and they are used in multiple layers.
 - ▣ Mechanisms for **authentication** prevent someone from impersonating someone else.
 - ▣ Mechanisms for **integrity** prevent surreptitious changes to messages, such as altering the content.

Connection-Oriented Vs. Connectionless Services

- Layers can offer two different types of service to the layers above them:
 - ▣ connection-oriented and
 - ▣ connectionless.



connection-oriented



connectionless

Connection-Oriented Vs. Connectionless Services

Criteria	Connection-Oriented	Connection-Less
Connection	Prior connection needs to be established.	No prior connection is established.
Resource Allocation	Resources need to be allocated.	No prior allocation of resource is required.
Reliability	It ensures reliable transfer of data.	Reliability is not guaranteed as it is a best effort service.
Congestion	Congestion is not at all possible.	Congestion can occur likely.
Transfer mode	It can be implemented either using Circuit Switching or VCs.	It is implemented using Packet Switching.
Retransmission	It is possible to retransmit the lost data bits.	It is not possible.
Suitability	It is suitable for long and steady communication.	It is suitable for bursty transmissions.
Signaling	Connection is established through process of signaling.	There is no concept of signaling.
Packet travel	In this packets travel to their destination node in a sequential manner.	In this packets reach the destination in a random manner.
Delay	There is more delay in transfer of information, but once connection established faster delivery.	There is no delay due absence of connection establishment phase.

Examples of Connection-Oriented and Connectionless Services

	Service	Example
Connection-oriented	Reliable message stream	Sequence of pages
	Reliable byte stream	Remote login
	Unreliable connection	Digitized voice
Connection-less	Unreliable datagram	Electronic junk mail
	Acknowledged datagram	Registered mail
	Request-reply	Database query

Service Primitives



- A service is formally specified by a set of primitives (operations).
- These primitives tell the service to perform some action or report on an action taken by a peer entity.
- If the protocol stack is located in the operating system, as it often is, the primitives are normally system calls.
- These calls cause a trap to kernel mode, which then turns control of the machine over to the operating system to send the necessary packets.
- The primitives for connection-oriented service are different from those of connection-less service.

Service Primitives

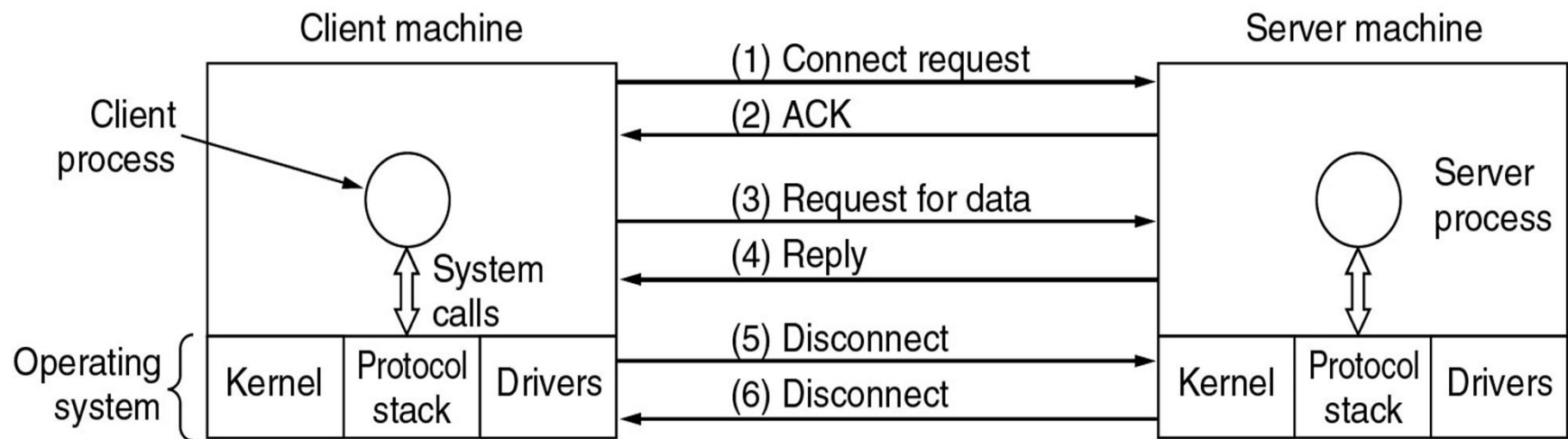
- There are five types of service primitives:
 - ▣ LISTEN: Executed at the server or communication initiator.
 - When a server is ready to accept an incoming connection it executes the LISTEN primitive.
 - It blocks waiting for an incoming connection.
 - ▣ CONNECT: Executed at the client or communication responder.
 - It connects the server by establishing a connection.
 - Response is awaited.
 - ▣ RECIEVE: Executed at the server or communication initiator.
 - The RECIEVE call blocks the server.

Service Primitives



- ▣ SEND: Executed at the client or communication responder.
 - Then client executes SEND primitive to transmit its request.
 - It is followed by the execution of RECEIVE call to wait for reply from the server.
- ▣ DISCONNECT: This primitive is used for terminating the connection.
 - After this primitive one can't send any message.
 - When the client sends DISCONNECT packet then the server also sends the DISCONNECT packet to acknowledge the client.
 - When the server packet is received by client then the process is terminated.

Service Primitives



Packets sent in a simple client-server interaction on a connection-oriented network.

The Relationship of Services to Protocols

□ Service

- A service is a set of primitives (operations) that a layer provides to the layer above it.
- The service defines what operations the layer is prepared to perform on behalf of its users, but it says nothing at all about how these operations are implemented.
- 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.

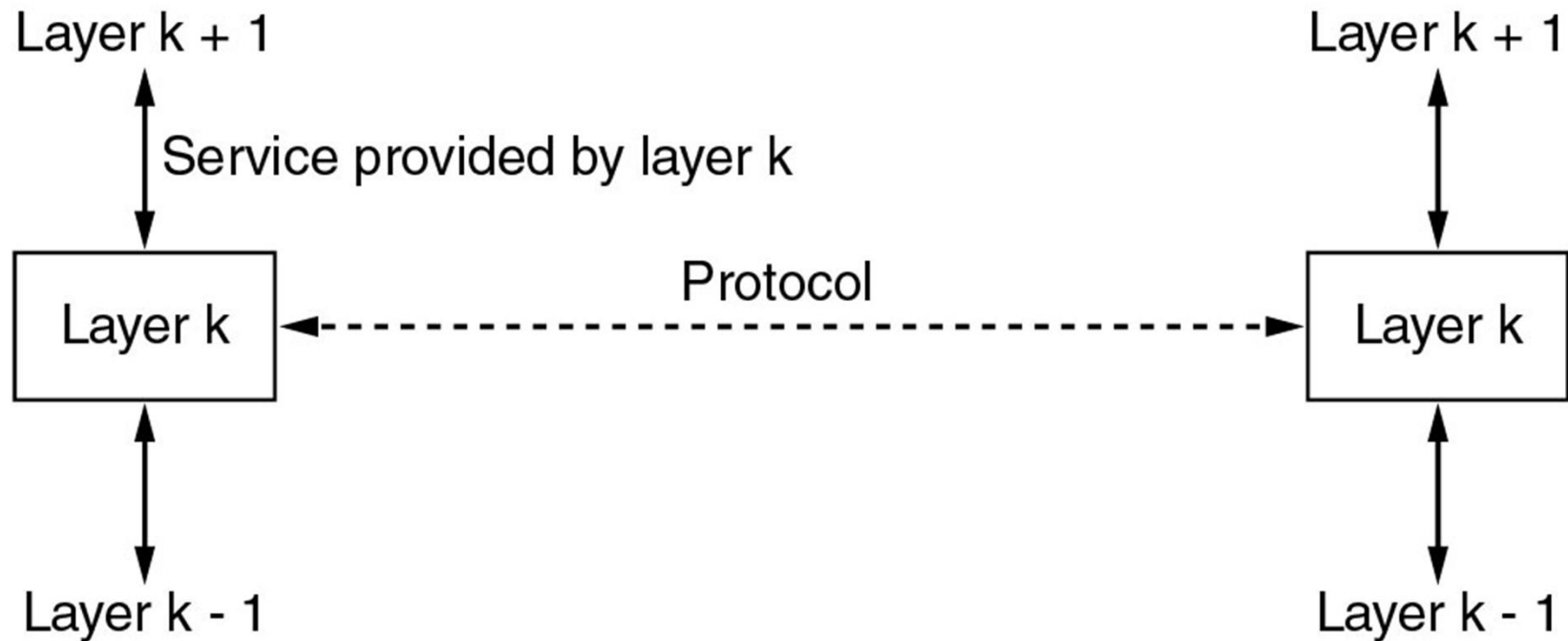
The Relationship of Services to Protocols



□ Protocol

- A protocol, in contrast, is a set of rules governing the format and meaning of the packets, or messages that are exchanged by the peer entities within a layer.
- Entities use protocols to implement their service definitions.
- They are free to change their protocols at will, provided they do not change the service visible to their users.
- In this way, the service and the protocol are completely decoupled.

Services to Protocols Relationship



The relationship between a service and a protocol.

Reference Models




- Two important network architectures:
 - ▣ The OSI reference model and (Model is useful)
 - ▣ The TCP/IP reference model.(Protocols are useful)
- Although the *protocols associated with the OSI model are not used any more, the model itself is actually quite general and still valid.*
- The TCP/IP model has the opposite properties: *the model itself is not of much use but the protocols are widely used.*

OSI Reference Model



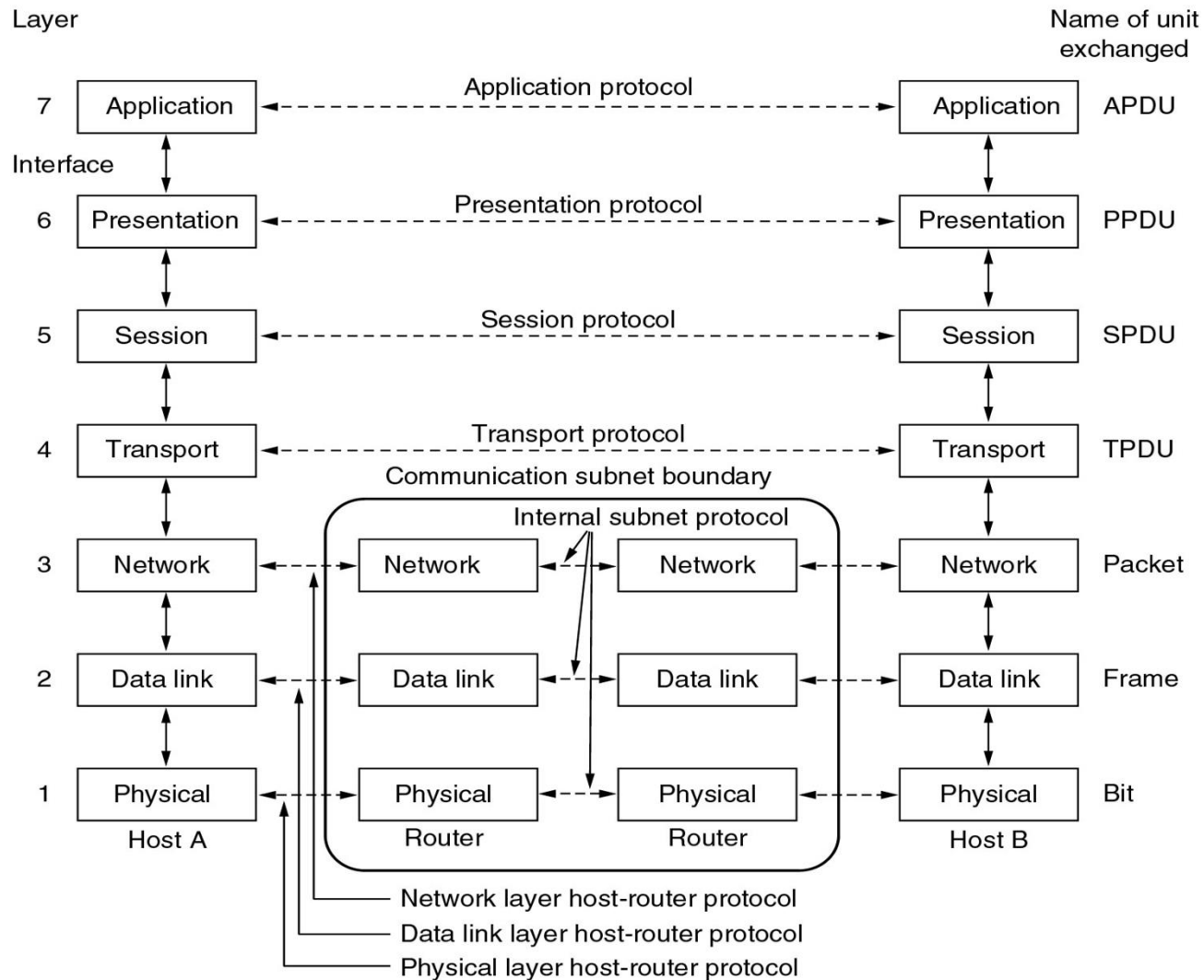
- The model is called the ISO OSI (Open Systems Interconnection) Reference Model because
 - ▣ it deals with connecting open systems (i.e. systems that are open for communication with other systems).
- It is called the OSI model for short.
- The OSI model has seven layers.



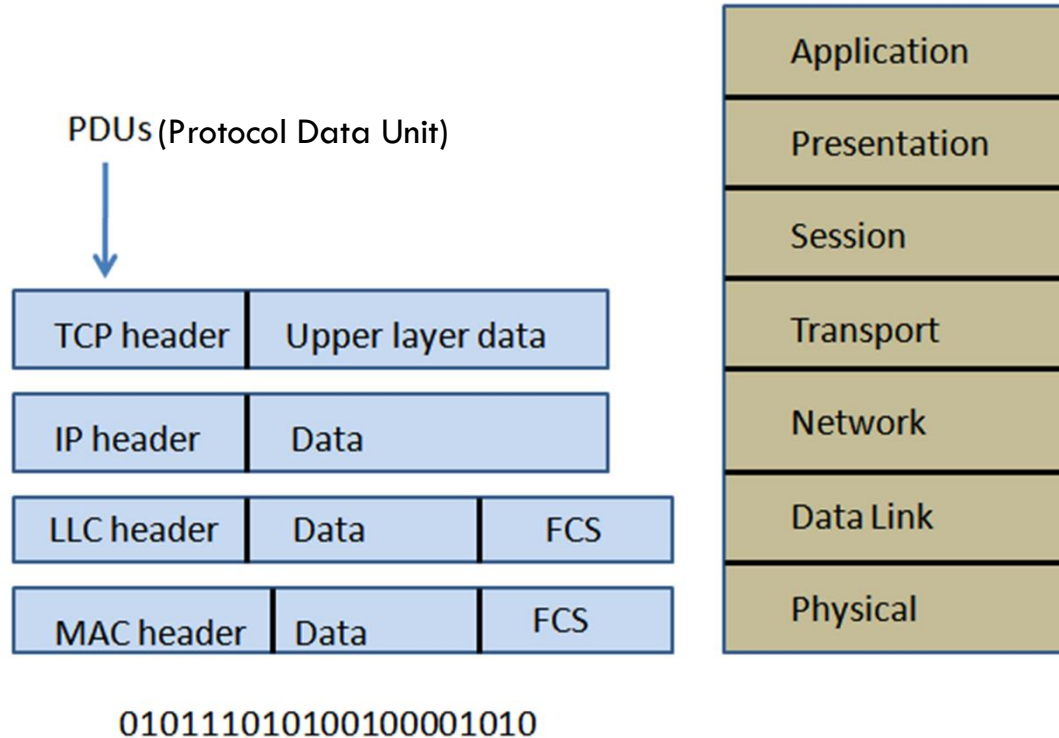
□ The principles that were applied to arrive at the seven layers can be briefly summarized as follows:

- A layer should be created where a different abstraction is needed.
- Each layer should perform a well-defined function.
- The function of each layer should be chosen with an eye toward defining internationally standardized protocols.
- The layer boundaries should be chosen to minimize the information flow across the interfaces.
- The number of layers should be large enough that distinct functions need not be thrown together in the same layer out of necessity and small enough that the architecture does not become unwieldy.

The OSI reference model.



The OSI reference model.



TCP: Transmission Control Protocol IP: Internet Protocol

LLC: Logical Link Layer

MAC: Multiple Access Control /

FCS: Frame Check Sequence

Media Access Control

The OSI reference model.

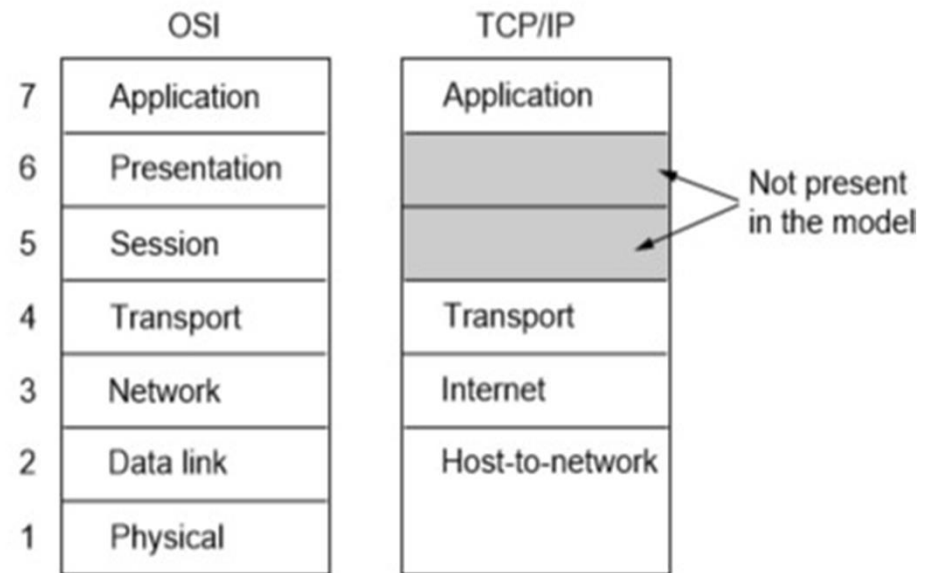
1. **Physical layer:** is concerned with the transmission of raw bits, and deals with mechanical, electrical and procedural interfaces, and physical transmission medium
2. **Data link layer:** describes how a shared communication medium can be accessed, and how to make an unreliable noisy link reliable
3. **Network layer:** is concerned with controlling the operation of subnet, for example, how routing is done
4. **Transport layer:** provides the actual network interface to applications, jobs like making network connections, multiplexing, flow control. It is a true end-to-end layer, from source to destination
5. **Session layer:** tells how to set up “long-lasting” communications (sessions). This is the dumbest and ill-defined
6. **Presentation layer:** describes everything that is needed to exchange data in a platform-independent way. An example is data encoding
7. **Application layer:** contains the stuff that user can see, such as e-mail, file transfer, remote login, web’s exchange protocols

Note that the **user-network interaction** occurs at the bottom three-layer levels: the “net” is essentially unconcerned with higher layers

The TCP/IP reference model.

- This is where Internet started: used to be a wild cowboy's world but now is better standardised

1. **Application layer:** does similar things as OSI application layer
2. **Transport layer:** does similar things as OSI transport layer
Two end-to-end protocols are defined:
TCP – transmission control protocol (for reliable connection-oriented) and
UDP – user datagram protocol (for unreliable connectionless)
3. **Internet layer:** similar in functionality to OSI network layer

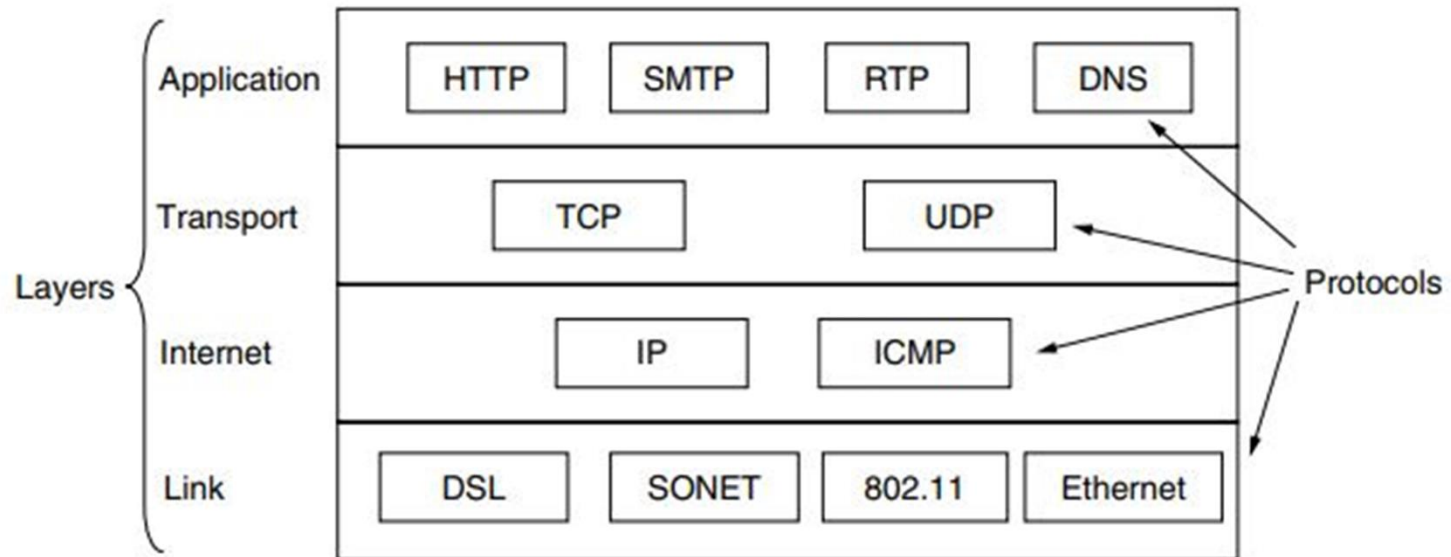


4. **Host-to-network layer:** anything below the internet layer, not very well defined

- Two reference models represent two different views of the world: telecommunication camp and computer camp. OSI camp views the world (i.e. the network) as rigid, well defined and organised, TCP/IP camp historically views the world as hostile and chaotic

New standards are now often defined with **best** of **both** reference models

The TCP/IP model with some protocols



PDUs names at various layers

OSI Model	PDU	TCP/IP Stack
Application	Data	Application
Presentation		
Session		
Transport	Segment	Transport
Network	Packet	Internet
Data Link	Frame	Network Access/Link
Physical	Bits	

PDUs names at various layers

Comparison of OSI and TCP/IP Model

- Three important concepts, **services**, **interfaces** and **protocols**, are well defined in OSI model, but not in original TCP/IP model
- **Transport** layer does the hardest job, dealing with end-to-end “connection”
- **Data link** layer is also very important: An end-to-end “connection” consists of many “links”, and each possibly noisy link need to be made reliable
- On the other hand, no one really knows precisely what **session** layer does
- It may also be argued that a separate **presentation** layer is not strictly necessary
- Based on comparison, we will adopt the hybrid **5-layer reference model**:

This is a good **framework** for discussion of computer networks

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


Comparison of OSI and TCP/IP Model

- The OSI reference model was devised before the corresponding protocols were invented.
- With TCP/IP the reverse was true: the protocols came first, and the model was really just a description of the existing protocols
- The OSI model supports both connectionless and connection oriented communication in the network layer, but only connection-oriented communication in the transport layer,
- The TCP/IP model supports only one mode in the network layer (connectionless) but both in the transport layer.

Example Networks:

Internet and its history, evolution, and technology.

- 1957:
 - The Department of Defense's Advanced Research Projects Agency founded, or ARPA (later referred to as DARPA.)
- 1962:
 - An ARPA affiliated scientist proposed an "intergalactic network" of linked computers.
- 1968:
 - ARPA put out a request for proposals to actually build a network of computers.
 - The first two computers were connected in 1969.
 - One computer was located at UCLA, and a second at Stanford.
- 1970:
 - The Network Working Group finished the initial ARPAnet protocol called the Network Control Protocol.
- 1972:
 - A new application of electronic mail, allowing messages to be sent and received was developed.
- 1973:
 - ARPAnet expanded to Europe.

- 
- 1976:
 - The first known use of the word “internet”, Specification of Internet Transmission Control Program.
 - 1979:
 - The Usenet bulletin board system allows the users on the ARPAnet network to easily engage in “non-work” activities like message posts.
 - 1983:
 - ARPAnet began using the TCP/IP protocol
 - The Domain Name System (DNS) was established
 - 1985:
 - The First Domain Symbolics.com becomes the first ever registered domain.
 - 1990:
 - A CERN scientist named Tim Berners-Lee develops Hyper-Text Markup Language, or HTML.
 - 1993:
 - University of Illinois develops Mosaic, an internet browser that allows users to display web pages and images.
 - 1994:
 - Netscape, the first commercial browser.