INTRODUCTION

1. Uses of Computer Networks
2. Types of Computer Networks
3. Network Technology, From Local to Global
4. Examples of Networks
5. Network Protocols
6. Reference Models
7. Standardization

Introduction

- A computer network is a set of computers connected together for the purpose of sharing resources.
- The most common resource shared today is connection to the internet.
- ***Network:*** A set of computing devices connected together for the purpose of sharing information and resources.
- ***Networking:*** Total process of creating and using computer networks, w.r.t hardware, protocols, and software, including wired and wireless technology.

---

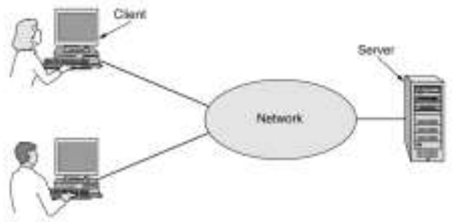
1. Uses of Computer Networks

i. Access to Information
ii. Person-to-Person Communication
iii. Electronic Commerce
iv. Entertainment
v. The Internet of Things

i. Access to Information

- Information can be accessed in various forms, particularly through the Internet.
- Web browsers are a common tool for retrieving information from websites, including social media sites.
- Mobile applications on smartphones also provide access to remote information.
- Information available covers a wide range of topics including arts, business, cooking, government, health, history, hobbies, science, sports, travel, and more.
- News organizations are increasingly moving online, with some ceasing print operations.
- Online news is becoming more personalizable, allowing users to choose specific interests.
- Social media platforms are increasingly curating news, where users can post and share content from various sources.

- The news seen by users is often personalized through algorithms based on user history.
- Organizations like ACM and IEEE Computer Society have made their journals and proceedings available online.
- Much of the information on the Internet is accessed via a client-server model shown in Figure 1.
- In this model, a client requests information from a server, which then responds as shown in Figure 2.
- This model is widely used, including for web applications, where a server generates web pages in response to client requests.
- Peer-to-peer (P2P) communication involves individuals communicating directly without a fixed division into clients and servers as shown in Figure 3.
- P2P communication became popular with music sharing services like Napster and is still used today for legal purposes, such as sharing public domain music and downloading software.



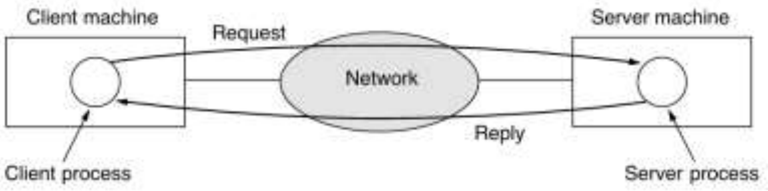


Figure 1: A network with two clients and one server

Figure 2: The client-server model involves requests and responses

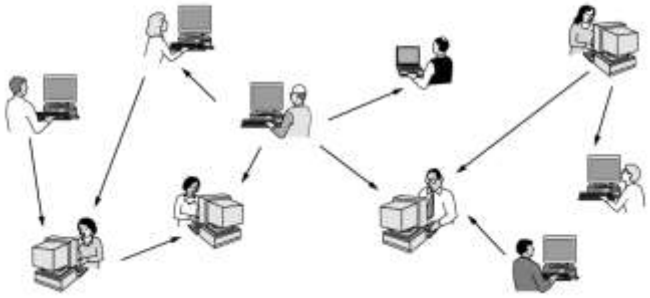


Figure 3: In a peer-to-peer system, there are no fixed clients and servers

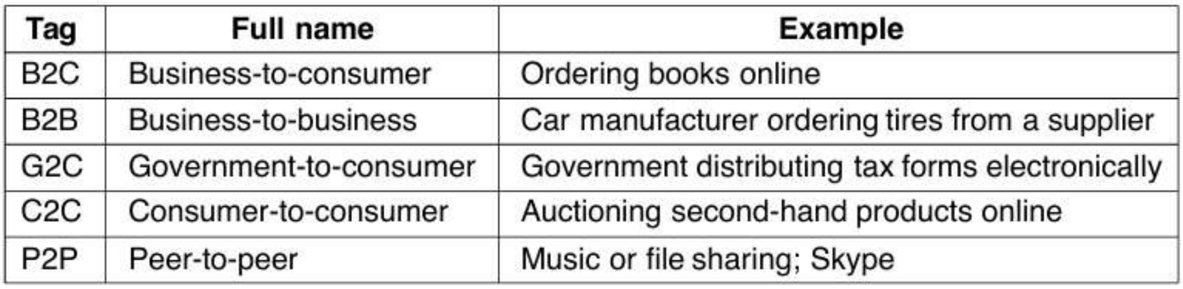
ii. Person-to-Person Communication

- Email is widely used globally, often including audio, video, text, and pictures.
- Instant messaging is popular, allowing real-time text communication between individuals.
- The Internet is used to carry audio (e.g., Internet radio, streaming music) and video (e.g., Netflix, YouTube).
- Internet-based communication can be crucial for those in remote areas, offering access to services comparable to those in urban centers.

- Social networks bridge person-to-person communication and information access, driven by user relationships.
- Facebook is a leading social networking site, allowing profile updates and sharing among friends.
- People can work together to create content, such as through wikis.
- Wikipedia is the most famous wiki, allowing anyone to read or edit content, with thousands of other wikis existing.

iii. Electronic Commerce

- **Online Shopping**: Online shopping is highly popular, allowing users to browse catalogs from thousands of companies and have products delivered to their homes.
- **E-commerce in Finance**: People pay bills, manage bank accounts, and handle investments electronically.
- **Online Auctions**: Online auctions for second-hand goods have become a massive industry. Unlike traditional e-commerce, online auctions are more peer-to-peer, where consumers can be both buyers and sellers.
- Certain forms of e-commerce have acquired terms or tags based on the pronunciation similarity between "to" and "2," with popular examples listed in the below figure 4.



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

Figure 4: Some forms of e-commerce

iv. Entertainment

- Entertainment at home has advanced significantly with the distribution of music, radio, TV programs, and movies over the Internet.
- Users can find, buy, and download MP3 songs and high-definition movies to add to their personal collections.
- Entertainment content can be moved around the home between different devices, displays, and speakers, typically through a wireless network.
- In the future, it may be possible to instantly search for and display any movie or TV program ever made.
- New films may become interactive, allowing viewers to influence the story direction, with alternative scenarios provided.

- Live television might become interactive, where audiences participate in quiz shows or choose among contestants.
- Multi-person real-time simulation games are already popular.

v. The Internet of Things

- Ubiquitous computing refers to computing embedded in everyday life, as envisioned by Mark Weiser in 1991.
- Many homes are equipped with security systems, including door and window sensors, and can integrate additional sensors for smart home monitoring.
- Smart electricity, gas, and water meters can report usage over the network, eliminating the need for manual meter reading.
- Smoke detectors can automatically alert the fire department, and smart refrigerators could reorder groceries when supplies are low.
- The IoT revolution is connecting nearly every electronic device to the Internet, enabling more measurement and reporting through networks.

---

2. Types of Computer Networks

i. Broadband Access Networks

ii. Mobile and Wireless Access Networks

iii. Content Provider Networks

iv. Transit Networks

v. Enterprise Networks

i. Broadband Access Networks

- In 1977, Ken Olsen of Digital Equipment Corporation claimed there was no need for personal computers at home, a prediction that proved incorrect as Digital eventually vanished.

- Initially used for word processing and games, home computers now primarily provide Internet access. Modern consumer electronics, including set-top boxes, game consoles, and televisions, feature embedded computers connected to networks.

- Home networks are widely used for managing entertainment content. Internet access allows users to connect to remote computers, access information, communicate, and shop.

- Metcalfe's Law explains the Internet's popularity by stating its value increases with the square of the number of users.

- Broadband access is expanding globally, with speeds rising to gigabit levels in developed countries and mobile access being more common in developing regions.

ii. ***Mobile and Wireless Access Network***

- Mobile computers like laptops, tablets, and smartphones are among the fastest-growing segments in the computer industry, surpassing desktop sales.

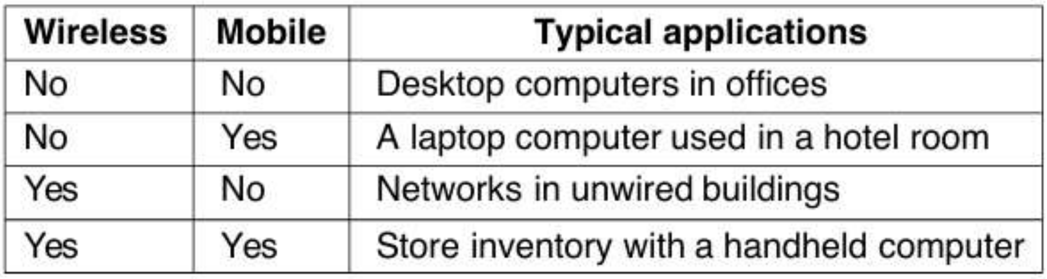
- People use these devices for a range of activities, including email, social media, streaming media, and web browsing from virtually anywhere.

- Connectivity is crucial, with wireless networks—cellular and Wi-Fi—providing access in places where wired connections are impractical, such as cars and airplanes.

- Wireless networks also support various applications, from fleet management to ride-sharing services.

- Additionally, mobile phones, which combine telephony and computing, have become central to mobile commerce (m-commerce), facilitating payments and transactions via SMS and NFC technology.

- The rise of mobile technology and wireless networks is driving innovations like sensor networks and wireless parking meters, promising to revolutionize both daily life and scientific research.



Wireless	Mobile	Typical applications
No	No	Desktop computers in offices
No	Yes	A laptop computer used in a hotel room
Yes	No	Networks in unwired buildings
Yes	Yes	Store inventory with a handheld computer

Figure 5: Combinations of wireless networks and mobile computing

iii. Content Provider Networks

- Many Internet services are hosted in large "cloud" data centers with thousands of servers, designed for high data transfer and energy efficiency.

- Early data center designs used a three-layer tree topology but had scalability issues. Content Delivery Networks (CDNs) help deliver content globally by placing servers close to users.

- Major providers like Google, Facebook, and Netflix operate their own CDNs, while services like Akamai and Cloudflare offer CDN solutions to others.

- CDNs manage content replication and selection based on proximity, server load, and network congestion.

iv. Transit Networks

- The Internet operates over multiple independently managed networks.
- Typically, your ISP's network differs from the one hosting website content. Content travels from data-center networks through transit networks to reach your ISP and device.
- Transit networks, historically profitable as backbone providers, charge ISPs and content providers for traffic.
- Recently, content consolidation with large providers and the expansion of access ISPs have reduced reliance on transit networks.
- Larger networks now often prefer direct interconnection, using transit networks primarily as a backup.

v. Enterprise Networks

- **Resource Sharing:** Efficiently share physical resources (e.g., printers) and crucial data across the network.
- **Remote Access:** Enable access to data and applications from various locations, overcoming geographical barriers.
- **Enhanced Communication:** Facilitate email, IP telephony, video conferencing, and desktop sharing to improve collaboration and reduce travel.
- **Electronic Business:** Conduct transactions and manage orders online to streamline operations and reduce inventory.

---

3. Network Technology, From Local to Global

i. Personal Area Networks
ii. Local Area Networks
iii. Home Networks
iv. Metropolitan Area Networks
v. Wide Area Networks
vi. Internetworks

i. Personal Area Networks

- Personal Area Networks (PANs) enable short-range communication between devices, such as connecting a computer to peripherals or linking wireless headphones and smartphones.

- Bluetooth is a common PAN technology that simplifies these connections without cables, using a master-slave model where the PC manages other devices.
- Other short-range communication technologies are also available and will be discussed further.

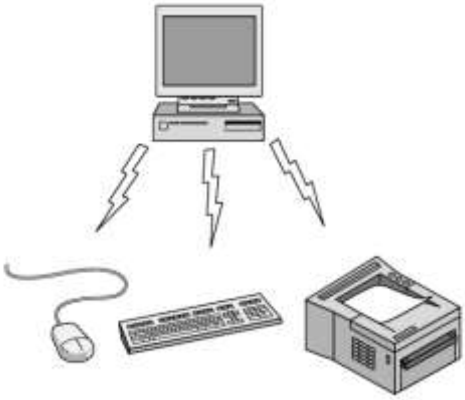


Figure 6: Bluetooth PAN configuration

ii. *Local Area Networks*

- Local Area Networks (LANs) are private networks used within a building, such as homes or offices, to connect and share resources like printers and information among computers and electronics.
- Wireless LANs, popular in various settings, use radio modems and antennas to communicate with Access Points (APs) or routers, which relay packets between devices and the Internet.
- Mesh networks, where devices relay packets for one another, are common in developing regions and large homes.

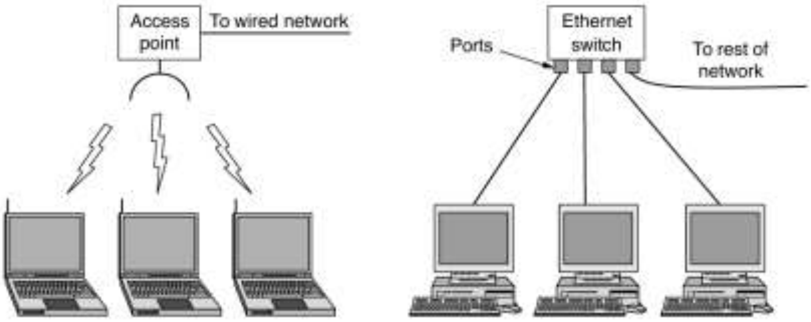


Figure 7: Wireless and wired LANs (a) 802.11 (b) Switched Ethernet

- The IEEE 802.11 standard, commonly known as WiFi, supports speeds from 11 Mbps to 7 Gbps.
- Wired LANs, using technologies like copper, coaxial cable, and optical fiber, generally offer higher speeds (100 Mbps to 40 Gbps), lower latency, and fewer errors compared to wireless LANs.
- Ethernet, governed by IEEE 802.3, is the most common wired LAN type, using switches to relay packets between connected computers.
- Ethernet switches use an anti-looping algorithm to manage packet routing effectively.
- LANs can be divided into logical networks, called VLANs (Virtual LANs), to match organizational structures.
- VLANs allow for traffic separation within a physical LAN, enhancing management.

- Traditional Ethernet used a single linear cable for broadcasting packets, while modern switched Ethernet does not.
- Resource allocation in LANs can be static or dynamic, with dynamic methods being centralized (controlled by a single entity) or decentralized (where each machine manages its transmission).

iii. ***Home Networks***

- Home networks, a type of LAN, connect a wide range of Internet-enabled devices, including smartphones, smart appliances, and security systems.
- They must be user-friendly, secure, and reliable due to the diverse and growing number of connected devices.
- Wireless networks are commonly used for their convenience and low cost but face challenges like performance bottlenecks and security risks.
- With devices evolving organically and needing to interoperate, ensuring compatibility and security while keeping costs low is crucial.
- Power-line networks are an alternative for extending connectivity but come with their own limitations.

iv. ***Metropolitan Area Network***

- A Metropolitan Area Network (MAN) covers an entire city and includes systems like cable television networks.
- Originally, these networks were used for TV reception via community antennas but evolved to include Internet service by utilizing unused parts of the spectrum.
- Cable TV systems transformed into MANs by providing both television and Internet services.
- Another example of a MAN is WiMAX (IEEE 802.16), a high-speed wireless Internet technology, though it has not become widespread.
- Other wireless technologies, such as LTE and 5G, also serve as MANs.

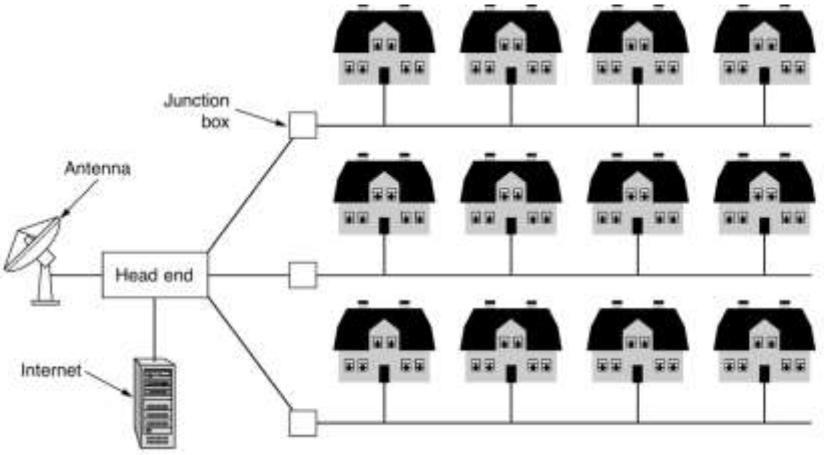


Figure 8: A metropolitan area network based on cable TV

v. *Wide Area Network*

- A Wide Area Network (WAN) spans large areas like countries or continents, connecting multiple locations. It includes:

1. Subnet: The communication part of the WAN, consisting of transmission lines (e.g., fiber, copper) and routers that direct data traffic.
2. Routing and Forwarding: Routers determine the best data paths and send packets to their destinations.
3. Management: In WANs, hosts and the subnet are often managed separately, with WANs connecting different networking technologies and sometimes entire LANs.
4. Internetworks: Many WANs combine various networks and technologies into one system.

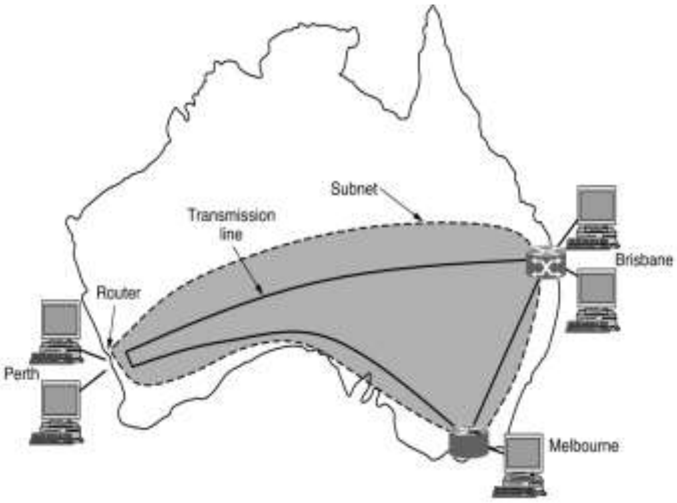


Figure 9: A metropolitan area network based on cable TV

vi. *Internetworks*

- To connect different networks, which often use various hardware and software technologies, an internetwork (or internet) is created. This term generally refers to a collection of interconnected networks, as opposed to the specific global Internet.
- Internetworks: These connect distinct networks, such as LANs and WANs, or two LANs, often involving different technologies.
- Gateways: Devices that connect networks and handle necessary translations are called gateways.
- Routers: These are network-layer gateways that direct packets between networks. Large networks often use many routers to manage data traffic.

---

4. Network Technology, From Local to Global

i. The Internet

   a. The ARPANET

   b. NSFNET

c. The Internet Architecture

ii. Mobile Networks

a. Mobile Network Architecture

b. Packet Switching and Circuit Switching

c. Early Generation Mobile Networks: 1G, 2G and 3G

d. Modern Mobile Networks: 4G and 5G

iii. Wireless Networks (WiFi)

i. The Internet

- ➢ The Internet is a vast network of interconnected systems using common protocols and services.

a. The ARPANET

- ➢ It is abbreviated as "Advanced Research Project Agency Network".
- ➢ In mid 60's Department of Defense (DoD) started ARPANET to build a network that could resist any attacks from USSR and help academicians share research.
- ➢ ARPANET used the packet-switching technology to interconnect four nodes.
- ➢ Hence DoD divided the network into subnets and host computers.
- ➢ The subnet software consisted of the IMP end of the host-IMP connection, the IMP-IMP protocol, and a source IMP to destination IMP protocol designed to improve reliability.
- ➢ Subnet would consist of minicomputers called "Interface Message Processors" (IMPs) connected by transmission lines.

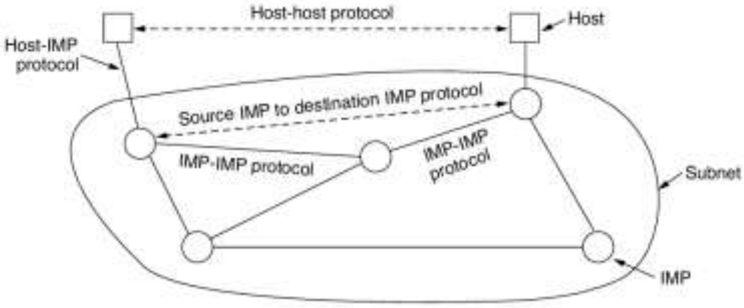


Figure 10: WAN using an ISP network

b. NFSNET

- ➢ By the late 1970s, the NSF recognized the value of ARPANET for research but needed a broader network. In 1981, NSF funded CSNET to connect computer science departments to ARPANET.
- ➢ Later, they developed NSFNET, connecting six supercomputers with TCP/IP, marking the first large-scale TCP/IP network.

- As NSFNET expanded, it transitioned to commercial operation, leading to the creation of ANS and multiple NAPs to support competitive internet services.
- This shift laid the foundation for the modern Internet. The World Wide Web's rise in the 1990s fueled exponential growth, with the Internet now dominated by streaming and social media, drastically increasing traffic and reshaping its architecture.

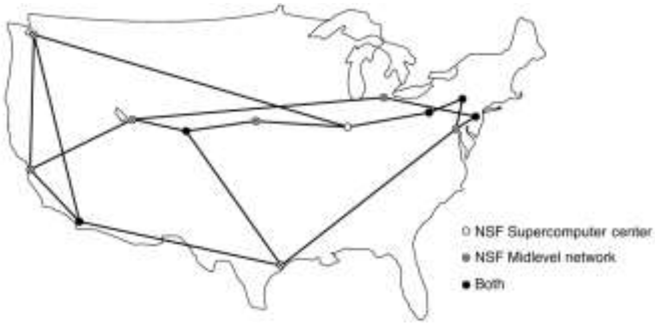


Figure 11: The NSFNET backbone in 1988

c. <u>The Internet Architecture</u>

- The Internet's architecture has evolved significantly due to growth and industry convergence, such as "triple play" services.
- A home computer connects to the Internet through an ISP, often via cable (HFC networks) or fiber (FTTH).
- ISPs operate POPs (Points of Presence) for packet entry, and they connect at IXPs (Internet Exchange Points) to exchange traffic.
- Peering agreements between ISPs determine packet paths, with tier-1 ISPs like AT&T forming the backbone of the Internet.
- Content providers, such as Facebook and Netflix, host servers in data centers, often directly connected to ISPs, bypassing traditional hierarchies.
- The rise of "hyper-giant" content providers and CDNs has flattened the Internet's architecture, allowing direct connections between access ISPs and content providers.

ii. ***<u>Mobile Networks</u>***

- Mobile networks have over five billion subscribers, about 65% of the global population, with most having Internet access on their devices.
- In 2018, mobile Internet traffic surpassed half of global online traffic, making the study of mobile phone systems essential.

a. <u>Mobile Network Architecture</u>

i. The architecture of mobile phone networks, particularly 4G LTE, differs significantly from the Internet.

ii. The radio communication protocol between mobile devices and base stations, known as E-UTRAN, forms the wireless side, while the core network, EPC (Evolved Packet Core), handles data traffic.

iii. Mobile networks have evolved to fully packet-switched systems, supporting higher data rates than earlier generations.

iv. Mobility is managed through handovers between base stations, ensuring seamless connectivity.

v. Security is also a priority, with SIM cards used for authentication and encryption, providing better privacy than earlier systems.

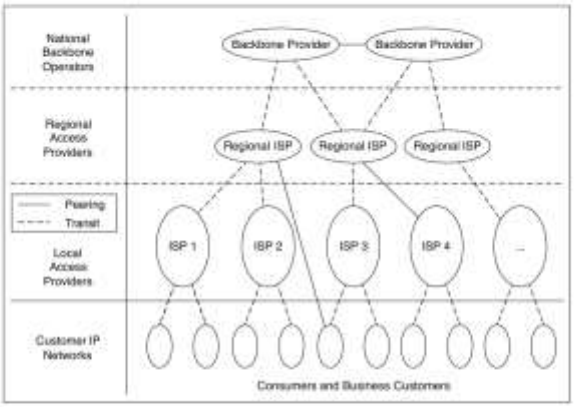


Figure 12: The Internet architecture through the 1990s followed a hierarchical structure

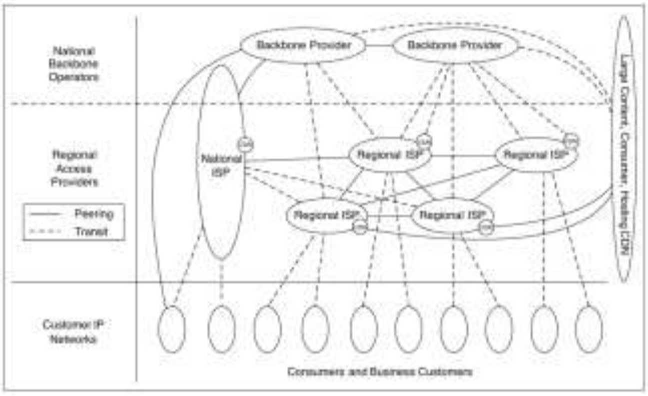
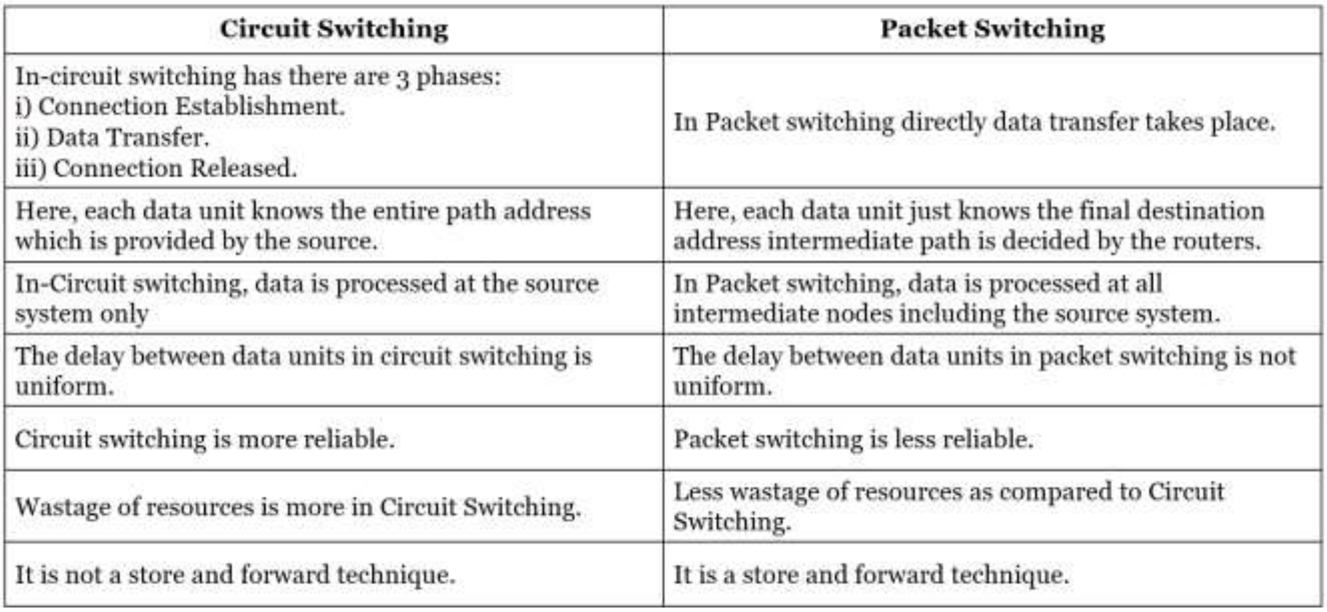


Figure 13: Flattening of the Internet hierarchy

b. Packet Switching and Circuit Switching



Circuit Switching	Packet Switching
In-circuit switching has there are 3 phases: i) Connection Establishment. ii) Data Transfer. iii) Connection Released.	In Packet switching directly data transfer takes place.
Here, each data unit knows the entire path address which is provided by the source.	Here, each data unit just knows the final destination address intermediate path is decided by the routers.
In-Circuit switching, data is processed at the source system only	In Packet switching, data is processed at all intermediate nodes including the source system.
The delay between data units in circuit switching is uniform.	The delay between data units in packet switching is not uniform.
Circuit switching is more reliable.	Packet switching is less reliable.
Wastage of resources is more in Circuit Switching.	Less wastage of resources as compared to Circuit Switching.
It is not a store and forward technique.	It is a store and forward technique.

c. Early Generation Mobile Networks: 1G, 2G, and 3G

➢ Mobile networks have evolved significantly over 50 years:

- **1G** (e.g., AMPS, 1982): Used analog signals for voice.
- **2G** (e.g., GSM, 1991): Introduced digital voice and text messaging.
- **3G** (e.g., UMTS, 2001): Added broadband data services with speeds up to 14 Mbps downlink.

- To manage radio spectrum scarcity, mobile networks use a cellular design that reuses frequencies while minimizing interference. Spectrum licensing, often through expensive auctions, is crucial for network operation.

d. Modern Mobile Networks: 4G and 5G

Future mobile networks are focused on mobile broadband rather than just voice calls.

- **4G LTE**: Launched in the late 2000s, offering faster speeds and became dominant over alternatives like WiMAX.
- **5G**: Set for early 2020s, promises speeds up to 10 Gbps and operates at higher frequencies (up to 6 GHz). Higher frequencies face challenges such as shorter signal range and increased susceptibility to interference and weather conditions. To address these, 5G uses advanced technologies like MIMO antennas and improved algorithms.

iii. Wireless Networks (WiFi)

- The IEEE 802.11 standard, developed in the mid-1990s, unified wireless LANs, addressing earlier compatibility issues.
- Operating in unlicensed ISM bands, it avoids the cost of licensed spectrum but faces potential interference.
- The standard includes infrastructure mode with access points and ad hoc mode for direct client communication.
- It evolved from initial speeds of 1-2 Mbps to 54 Mbps with 802.11a/g, and now supports up to 3.5 Gbps with 802.11ac and 7 Gbps with 802.11ad, though the latter is limited to indoor use.
- It uses CSMA for managing interference and collisions, with security improving from WEP to WPA2 and WPA3.
- Today, 802.11 is widespread, extending to various devices and vehicles, and integrating with technologies like LTE-U for unlicensed spectrum use.

5. Network Protocols

i. Design goals

   a. Reliability

   b. Resource Allocation

   c. Evolvability

   d. Security

ii. Protocol Layering

iii. Connections and Reliability

a. Connection-Oriented Service

b. Connectionless Service

c. Reliability

iv. Service Primitives

v. The Relationship of Services to protocols

i. ***Design Goals***

a. Reliability

- Reliability involves ensuring the network operates correctly despite unreliable components. Bits in a packet may be damaged due to noise, signals, or faults.
- Error detection codes can identify errors, and retransmission ensures correct receipt.
- Error correction codes can recover the original message from incorrect bits.
- These methods use redundant information and are applied both at low layers for individual links and high layers for overall data integrity.
- Another issue is finding a working path through the network.
- Multiple paths often exist, and some links or routers may be down.
- For example, if the network is down in Berlin, packets from London to Rome can be rerouted through Paris.
- This process is known as routing, which the network should handle automatically.

b. Resource Allocation

- In large networks, challenges similar to city traffic jams and shortages arise. Scalable designs continue to work well as networks grow. Networks manage resources like transmission line capacity to ensure one host doesn’t interfere too much with another.
- Statistical multiplexing is a method where network bandwidth is shared dynamically based on short-term demand, rather than fixed allocations. This can be applied at both low and high layers.
- Flow control addresses the issue of fast senders overwhelming slow receivers, typically through feedback mechanisms. Congestion occurs when too many devices demand more resources than the network can provide, leading to strategies for reducing demand during overload.
- Beyond bandwidth, networks must also address timeliness for real-time applications. Quality of service mechanisms balance real-time delivery with high throughput needs.

c. Evolvability

- Another design issue is network evolution. As networks grow and new designs emerge, they need to connect with existing infrastructure.

- Protocol layering is a key strategy for managing change by dividing the problem and hiding implementation details.
- Additionally, each layer requires addressing or naming mechanisms to identify message senders and receivers.
- Different network technologies have varied limitations.
- For instance, some channels do not preserve message order, requiring numbering solutions.
- Variations in maximum message size necessitate mechanisms for breaking down, transmitting, and reassembling messages.
- This overall process is known as internetworking.

d. Security

- The final major design issue is network security.
- Key threats include eavesdropping on communications.
- Confidentiality mechanisms protect against this by ensuring data privacy across multiple layers.
- Authentication mechanisms prevent impersonation, helping to distinguish legitimate sites and verify caller identities.
- Integrity mechanisms guard against unauthorized changes to messages, such as altering transaction amounts.

ii. Protocol Layering

- To manage design complexity, networks use a layered structure, where each layer builds on the one below it.
- The number, names, functions, and contents of layers vary by network.
- Each layer provides services to the layer above while hiding implementation details.
- This concept, known as information hiding or encapsulation, is common in computer science.
- When layers on different machines communicate, they follow specific rules and conventions known as the layer's protocol.
- A protocol is an agreement on how communication should proceed. For example, in social interactions, the choice of greeting depends on the context, similar to how adhering to protocol ensures effective communication.
- The entities comprising the corresponding layers on different machines are called **peers.** The peers may be software processes, hardware devices, or even human beings.
- Between each pair of adjacent layers is an **interface.** The interface defines which primitive operations and services the lower layer makes available to the upper one.
- A set of layers and protocols is called a **network architecture.**
- A list of the proto cols used by a certain system, one protocol per layer, is called a **protocol stack.**

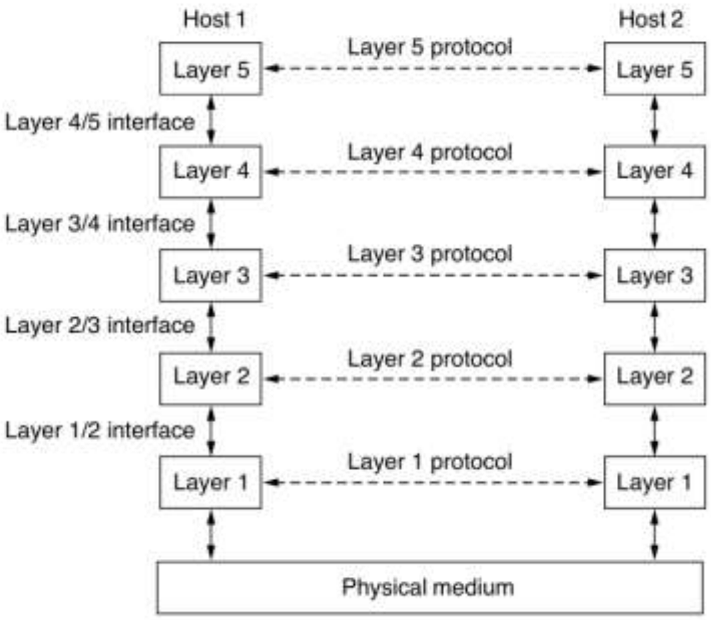
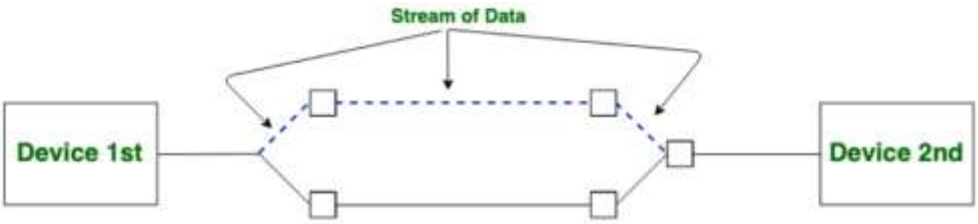


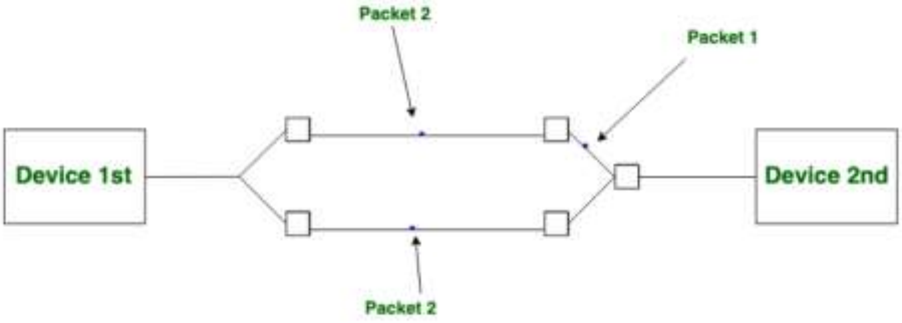
Figure 14: Layers, protocols, and interfaces

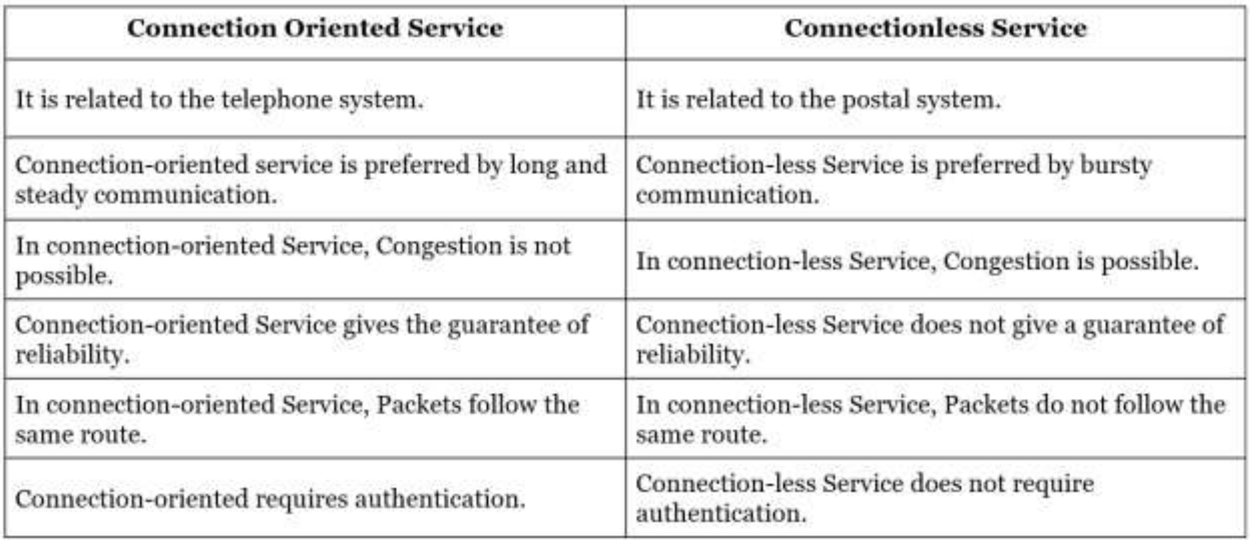
iii. Connections and Reliability

a. **Connection-Oriented Service:** Connection-oriented service is related to the telephone system. It includes connection establishment and connection termination. In a connection-oriented service, the Handshake method is used to establish the connection between sender and receiver.



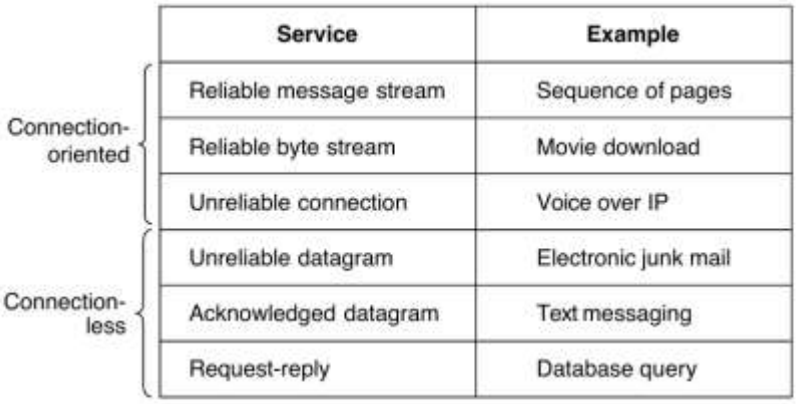
b. **Connectionless Service: Connection-less service** is related to the postal system. It does not include any connection establishment and connection termination. Connection-less Service does not give a guarantee of reliability. In this, Packets do not follow the same path to reach their destination. There are different names for messages in different contexts; a packet is a message at the network layer. When the intermediate nodes receive a message in full before sending it on to the next node, this is called **store-and-forward switching.**





Connection Oriented Service	Connectionless Service
It is related to the telephone system.	It is related to the postal system.
Connection-oriented service is preferred by long and steady communication.	Connection-less Service is preferred by bursty communication.
In connection-oriented Service, Congestion is not possible.	In connection-less Service, Congestion is possible.
Connection-oriented Service gives the guarantee of reliability.	Connection-less Service does not give a guarantee of reliability.
In connection-oriented Service, Packets follow the same route.	In connection-less Service, Packets do not follow the same route.
Connection-oriented requires authentication.	Connection-less Service does not require authentication.

c. **Reliability:** Connection-oriented and connectionless services can each be characterized by their reliability. Some services are reliable in the sense that they never lose data. Usually, a reliable service is implemented by having the receiver acknowledge the receipt of each message so the sender is sure that it arrived. The acknowledgement process introduces overhead and delays, which are often worth it but sometimes the price that has to be paid for reliability is too high.

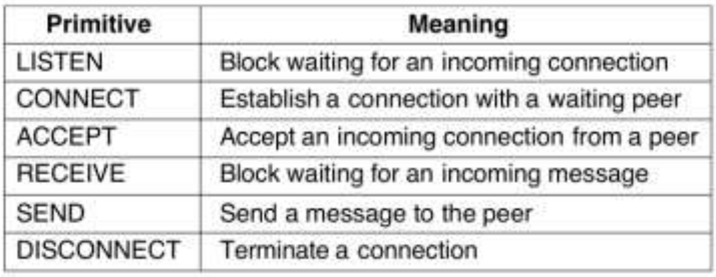


	Service	Example
Connection-oriented	Reliable message stream	Sequence of pages
	Reliable byte stream	Movie download
	Unreliable connection	Voice over IP
Connection-less	Unreliable datagram	Electronic junk mail
	Acknowledged datagram	Text messaging
	Request-reply	Database query

Figure 15: Six different types of service

iv. *Service Primitives*

➢ A service is formally specified by a set of primitives (operations) available to user processes to access the service. These primitives tell the service to perform some action or report on an action taken by a peer entity.



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

Figure 16: Six service primitives that provide a simple connection-oriented service

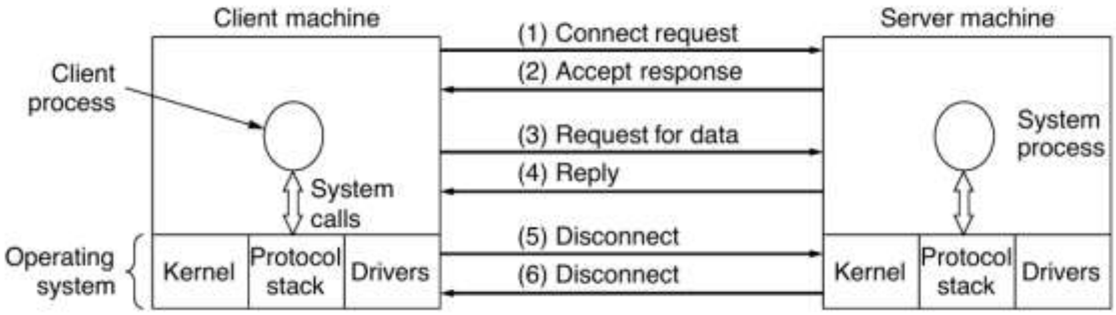


Figure 17: A simple client-server interaction using acknowledged datagrams

v. *The Relationship of Services to Protocols*

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 in order 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. This is a key concept that any network designer should understand well.

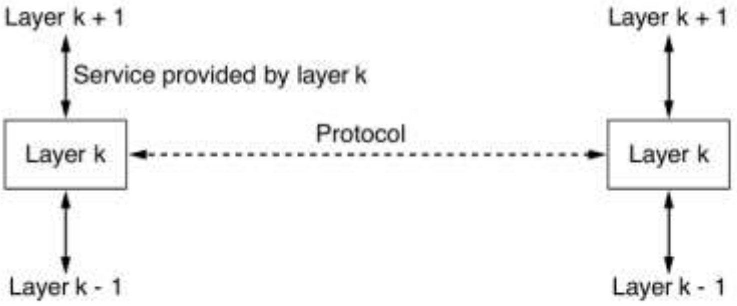


Figure 18: The relationship between a service and a protocol

6. Reference Models

a. The OSI Reference Model

- It is called the ISO OSI (Open Systems Interconnection) Reference Model because it deals with connecting open systems—that is, systems that are open for communication with other systems.
- The OSI model has seven layers. The principles that were applied to arrive at the seven layers can be briefly summarized as follows:

1. A layer should be created where a different abstraction is needed.
2. Each layer should perform a well-defined function.
3. The function of each layer should be chosen with an eye toward defining internationally standardized protocols.
4. The layer boundaries should be chosen to minimize the information flow across the interfaces.

5. 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.

- Three concepts are central to the OSI model:

1. Services
2. Interfaces
3. Protocols

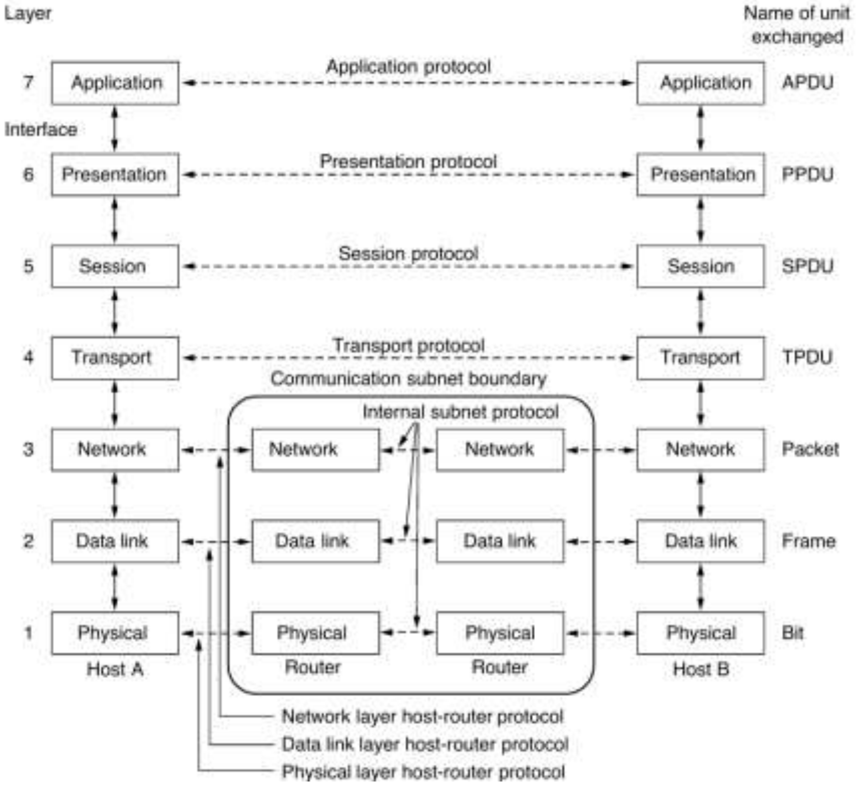


Figure 19: The OSI reference model

Physical Layer

- Deals with all aspects of physically moving data from one computer to the next
- Converts data from the upper layers into 1s and 0s for transmission over media
- Defines how data is encoded onto the media to transmit the data
- Defined on this layer: Cable standards, wireless standards, and fiber optic standards.
- Copper wiring, fiber optic cable, radio frequencies, anything that can be used to transmit data is defined on the Physical layer of the OSI Model
- Device example: Hub
- Used to transmit data

Data Link Layer

- Is responsible for moving frames from node to node or computer to computer
- Can move frames from one adjacent computer to another, cannot move frames across routers
- Encapsulation = frame

- ➢ Requires MAC address or physical address
- ➢ Protocols defined include Ethernet Protocol and Point-to-Point Protocol (PPP)
- ➢ Device example: Switch
- ➢ Two sublayers: Logical Link Control (LLC) and the Media Access Control (MAC)
- ✓ Logical Link Control (LLC) – Data Link layer addressing, flow control, address notification, error control
- ✓ Media Access Control (MAC) –Determines which computer has access to the network media at any given time. Determines where one frame ends and the next one starts, called frame synchronization

Network Layer

- ➢ Responsible for moving packets (data) from one end of the network to the other, called end-to-end communications
- ➢ Requires logical addresses such as IP addresses
- ➢ Device example: Router
- ➢ Routing is the ability of various network devices and their related software to move data packets from source to destination

Transport Layer

- ➢ Takes data from higher levels of OSI Model and breaks it into segments that can be sent to lower-level layers for data transmission
- ➢ Conversely, reassembles data segments into data that higher-level protocols and applications can use
- ➢ Also puts segments in correct order (called sequencing) so they can be reassembled in correct order at destination
- ➢ Concerned with the reliability of the transport of sent data
- ➢ May use a connection-oriented protocol such as TCP to ensure destination received segments
- ➢ May use a connectionless protocol such as UDP to send segments without assurance of delivery
- ➢ Uses port addressing

Session Layer

- ➢ Responsible for managing the dialog between networked devices
- ➢ Establishes, manages, and terminates connections
- ➢ Provides duplex, half-duplex, or simplex communications between devices
- ➢ Provides procedures for establishing checkpoints, adjournment, termination, and restart or recovery procedures

Presentation Layer

- Concerned with how data is presented to the network
- Handles three primary tasks: –Translation, –Compression, –Encryption
  - ✓ Translation: Changes data so another type of computer can understand it
  - ✓ Compression: Makes data smaller to send more data in same amount of time
  - ✓ Encryption: Encodes data to protect from interception or eaves dropping

Application Layer

- Contains all services or protocols needed by application software or operating system to communicate on the network
- Examples
- ✓ Firefox web browser uses HTTP (Hyper-Text Transport Protocol)
- ✓ E-mail program may use POP3 (Post Office Protocol version 3) to read e-mails and SMTP (Simple Mail Transport Protocol) to send e-mails

b. The TCP/IP Reference Model

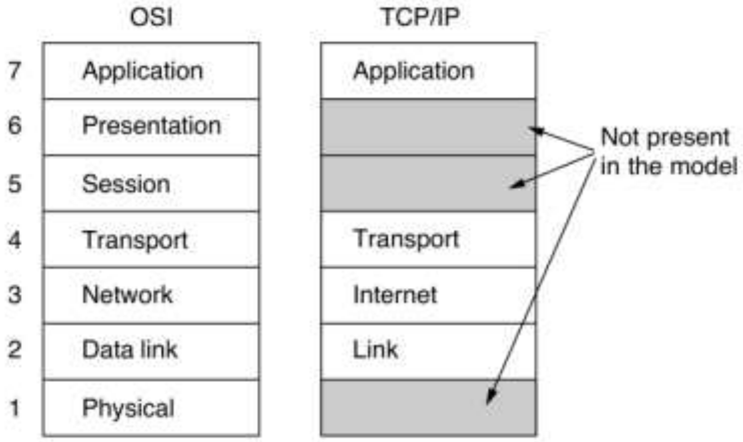


Figure 20: The TCP/IP reference model

i. ***The Link Layer:*** The lowest layer in the model, the link layer, describes what links such as serial lines and classic Ethernet must do to meet the needs of this connectionless internet layer.

ii. ***The Internet Layer:*** Its job is to permit hosts to inject packets into any network and have them travel independently to the destination. The internet layer defines an official packet format and protocol called IP (Internet Protocol), plus a companion protocol called ICMP (Internet Control Message Protocol) that helps it function. The job of the internet layer is to deliver IP packets where they are supposed to go.

iii. ***The Transport Layer:*** Two end to-end transport protocols have been defined here. The first one, TCP (Transmission Control Protocol), is a reliable connection-oriented protocol that allows a byte stream originating on one machine to be delivered without error on any other machine in the internet. It segments the incoming byte stream into discrete messages and passes each one on to the internet layer. At the destination, the receiving TCP process reassembles the received messages into the output stream. UDP (User Datagram Protocol), is an unreliable, connectionless protocol for applications that do not want TCP’s sequencing or flow control and wish to provide their own (if any). It is also widely used for one-shot, client-server-type request-reply queries and applications in which prompt delivery is more important than accurate delivery, such as transmitting speech or video.

iv. ***<u>The Application Layer:</u>*** Application layer include any session and presentation functions that they require. It contains all the high er-level protocols. The early ones included virtual terminal (TELNET), file trans fer (FTP), and electronic mail (SMTP). Many other protocols have been added to these over the years.

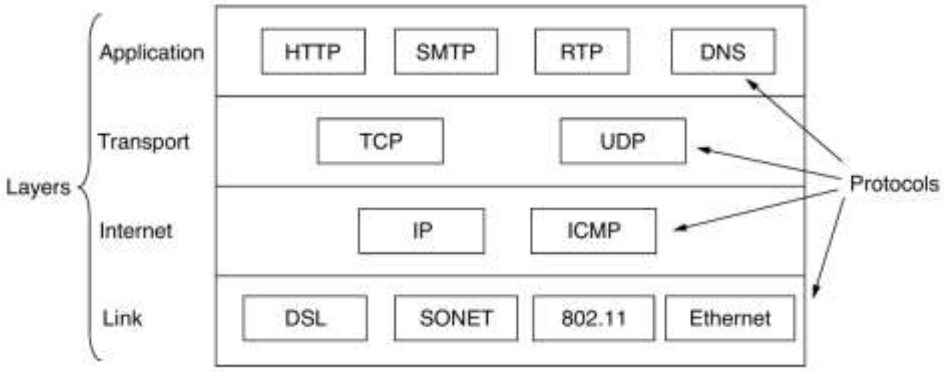
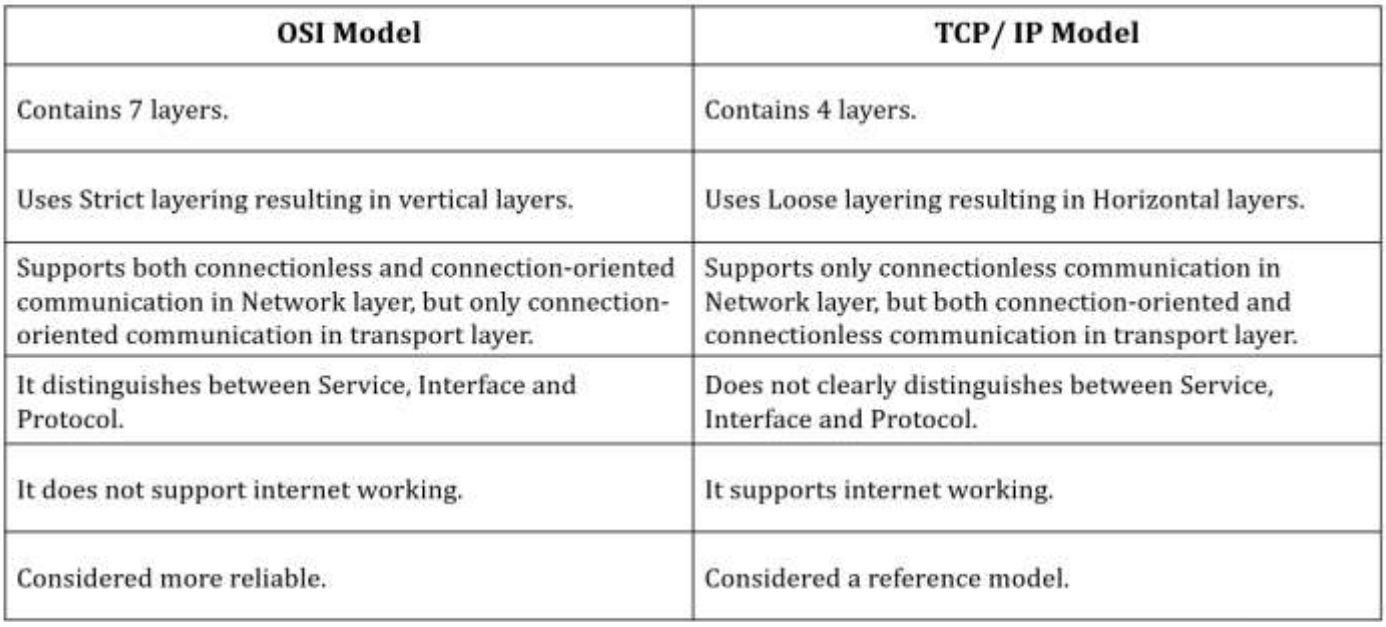


Figure 21: The TCP/IP model with some protocols

<u>Differences</u>



OSI Model	TCP/ IP Model
Contains 7 layers.	Contains 4 layers.
Uses Strict layering resulting in vertical layers.	Uses Loose layering resulting in Horizontal layers.
Supports both connectionless and connection-oriented communication in Network layer, but only connection-oriented communication in transport layer.	Supports only connectionless communication in Network layer, but both connection-oriented and connectionless communication in transport layer.
It distinguishes between Service, Interface and Protocol.	Does not clearly distinguishes between Service, Interface and Protocol.
It does not support internet working.	It supports internet working.
Considered more reliable.	Considered a reference model.

7. Standardization

- ➢ The Internet, with its roots primarily in the research domain.
- ➢ Various groups that coordinate Internet issues have guided this growth and development.

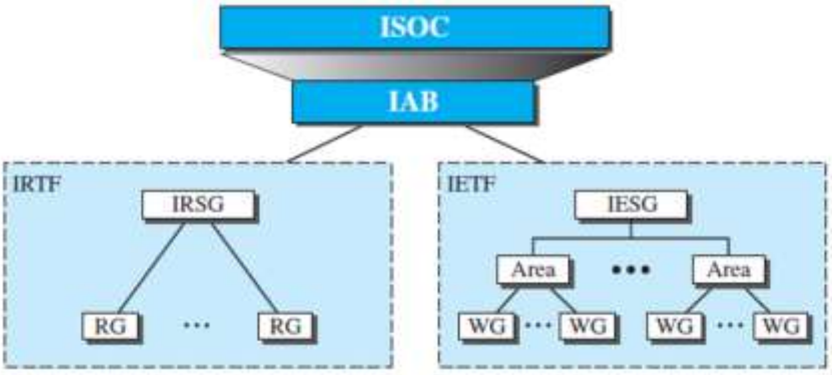


Figure 22: Internet Administration

i. **Internet Society (ISOC):** ISOC is an international, nonprofit organization formed in 1992 to provide support for the Internet standards process. ISOC accomplishes this through maintaining and supporting other. Internet administrative bodies such as IAB,IETF, IRTF, and IANA. Also promotes research and other scholarly activities relating to the Internet.

ii. **Internet Architecture Board (IAB):** The IAB is the technical advisor to the ISOC. Purposes: oversee the continuing development of the TCP/IP Protocol Suite and serve in a technical advisory capacity to research members of the Internet community. IAB accomplishes this through its two primary components: 1.Internet Engineering Task Force (IETF) 2.Internet Research Task Force (IRTF). Another responsibility of the IAB is the editorial management of the RFCs.

iii. **Internet Engineering Task Force(IETF):** Forum of working groups managed by the Internet Engineering Steering Group (IESG). Responsible for identifying operational problems and proposing solutions to these problems. Also develops and reviews specifications intended as Internet standards.

iv. **Internet Research Task Force (IRTF):** Forum of working groups managed by Steering Group (IRSG). It focus on long-term research topics related to Internet protocols, applications, architecture and technology.

v. **W3C:** For Web standards, the World Wide Web Consortium (W3C) develops protocols and guidelines to facilitate the long-term growth of the Web. W3C now has almost 500 companies, universities, and other organizations as members and has produced well over 100 W3C Recommendations, as its standards are called, covering topics such as HTML and Web privacy.