TCP/IP

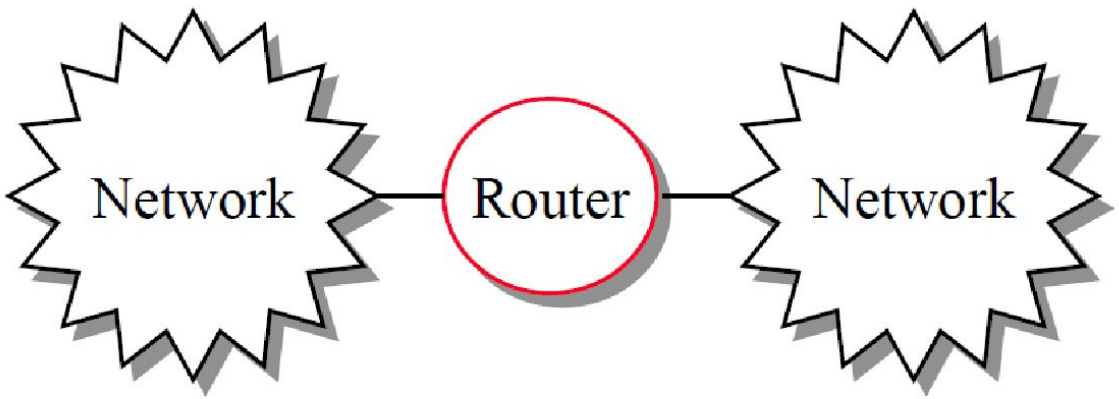
Internetworking

- The main design goal of TCP/IP was to build an interconnection of networks, referred to as an *internetwork*, or *internet*, that provided universal communication services over heterogeneous physical networks.

- The clear benefit of such an internetwork is the enabling of communication between hosts on different networks, perhaps separated by a large geographical area.

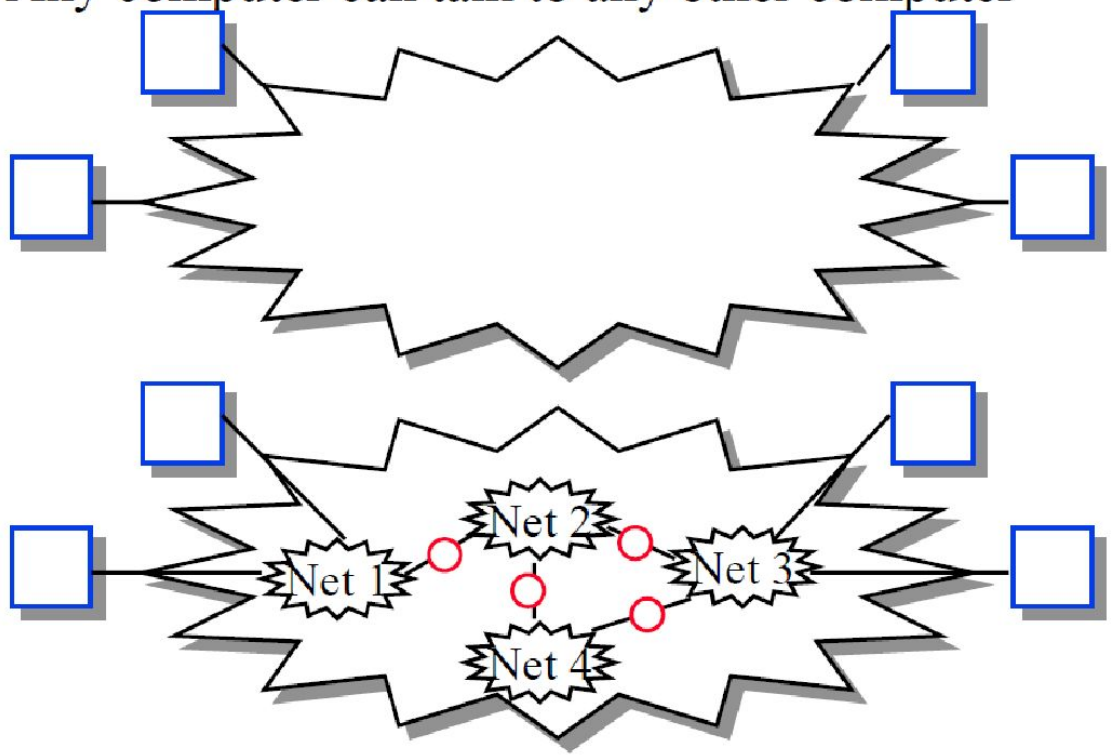
Internetworking

Inter-network = Collection of networks
Connected via routers



Internet = Collection of Networks

- Any computer can talk to any other computer



The Internet consists of the following groups of networks:

- Backbones: Large networks that exist primarily to interconnect other networks. Also known as network access points (NAPs) or Internet Exchange Points (IXPs). Currently, the backbones consist of commercial entities.

- Regional networks connecting, for example, universities and colleges.

- Commercial networks providing access to the backbones to subscribers, and networks owned by commercial organizations for internal use that also have connections to the Internet.

- Local networks, such as campus-wide university networks.

- Another important aspect of TCP/IP internetworking is the creation of a standardized abstraction of the communication mechanisms provided by each type of network.

- Each physical network has its own technology-dependent communication interface, in the form of a programming interface that provides basic communication functions (primitives).

    - TCP/IP provides communication services that run between the programming interface of a physical network and user applications.

    - It enables a common interface for these applications, independent of the underlying physical network.

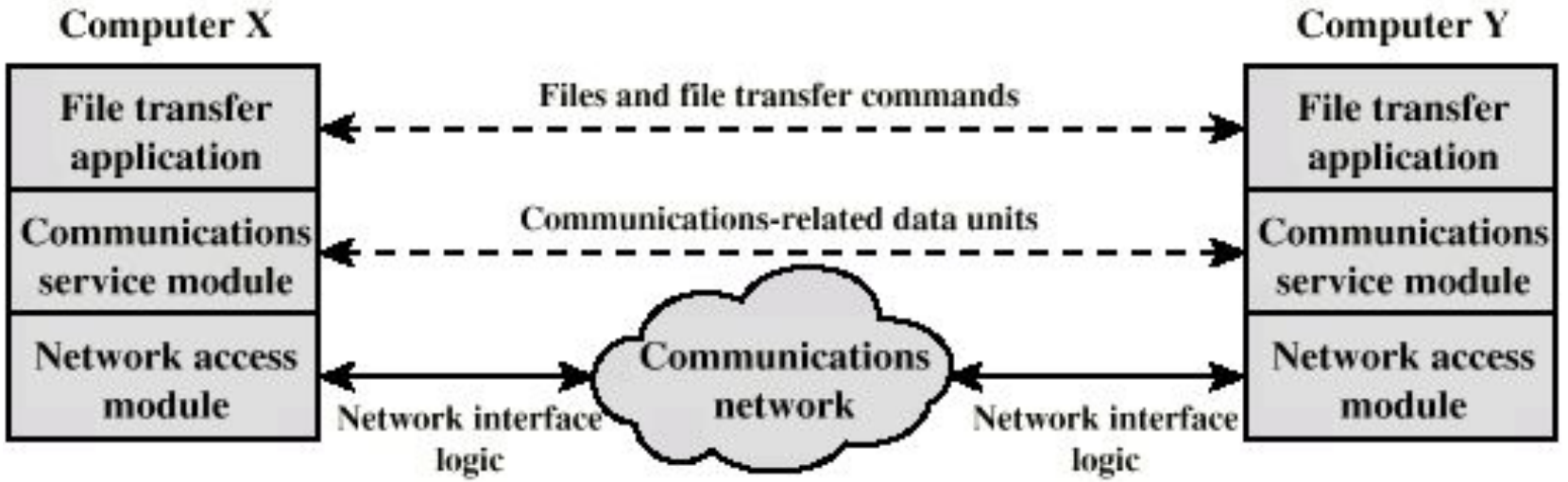
- The architecture of the physical network is therefore hidden from the user and from the developer of the application. The application need only code to the standardized communication abstraction to be able to function under any type of physical network and operating platform.

Simplified File Transfer Architecture

File Transfer Application Layer: Application specific commands, passwords and the actual file(s) – high level data

Communications Service Module: reliable transfer of those data – error detection, ordered delivery of data packets, etc.

Network Module: actual transfer of data and dealing with the network – if the network changes, only this module is affected, not the whole system



Network Access Layer

- Exchange of data between the computer and the network
- Sending computer provides address of destination so that network can route
- Different switching and networking techniques
  - Circuit switching
  - Packet switching
  - LANs
  - etc.
- This layer may need specific drivers and interface equipment depending on type of network used.
- But upper layers do not see these details
  - independence property

Transport Layer

- Reliable data exchange
  - to make sure that all the data packets arrived in the same order in which they are sent out
  - Packets not received or received in error are retransmitted
- Independent of network being used
- Independent of application

Application Layer

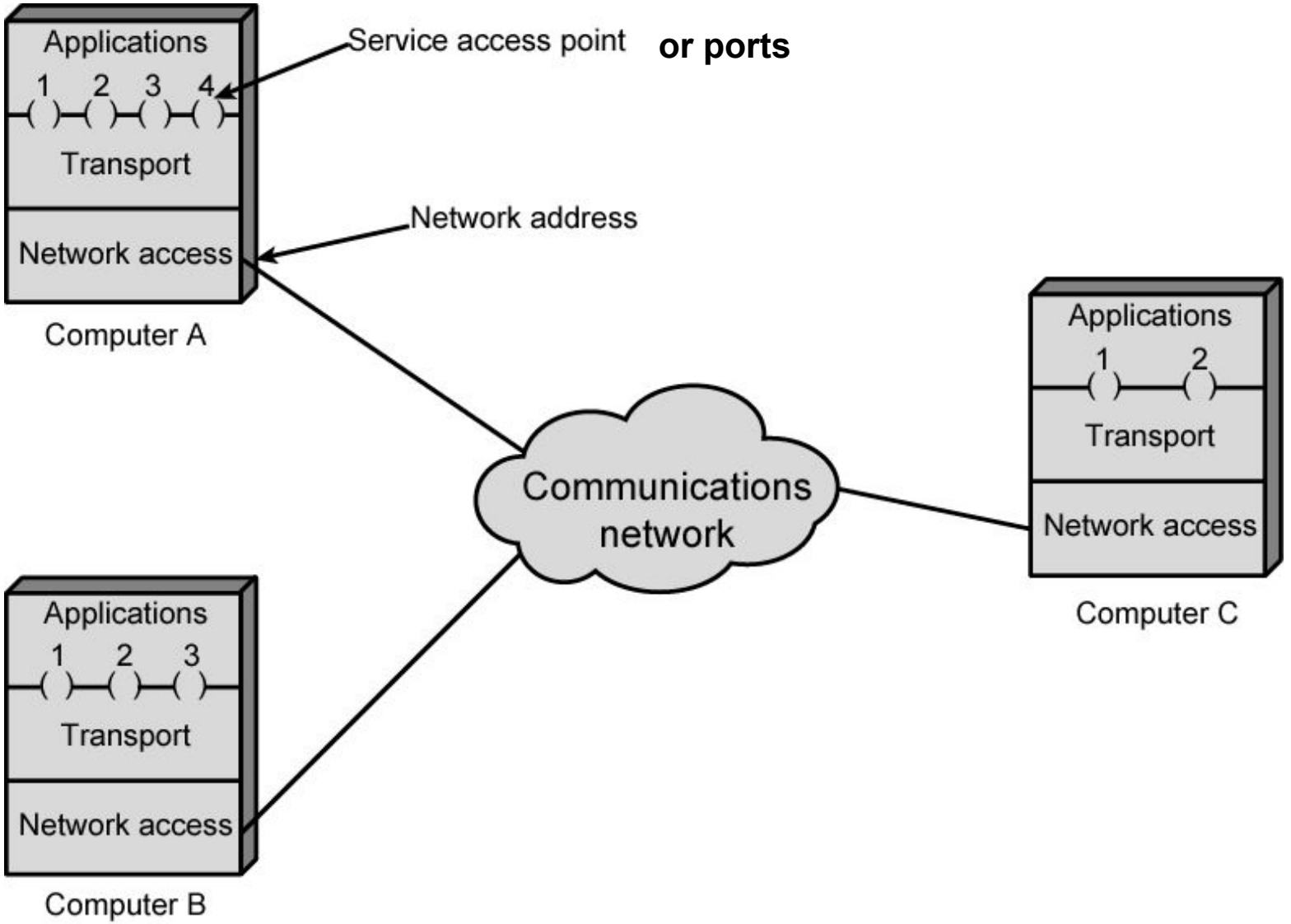
- Support for different user applications

  e.g. e-mail, file transfer

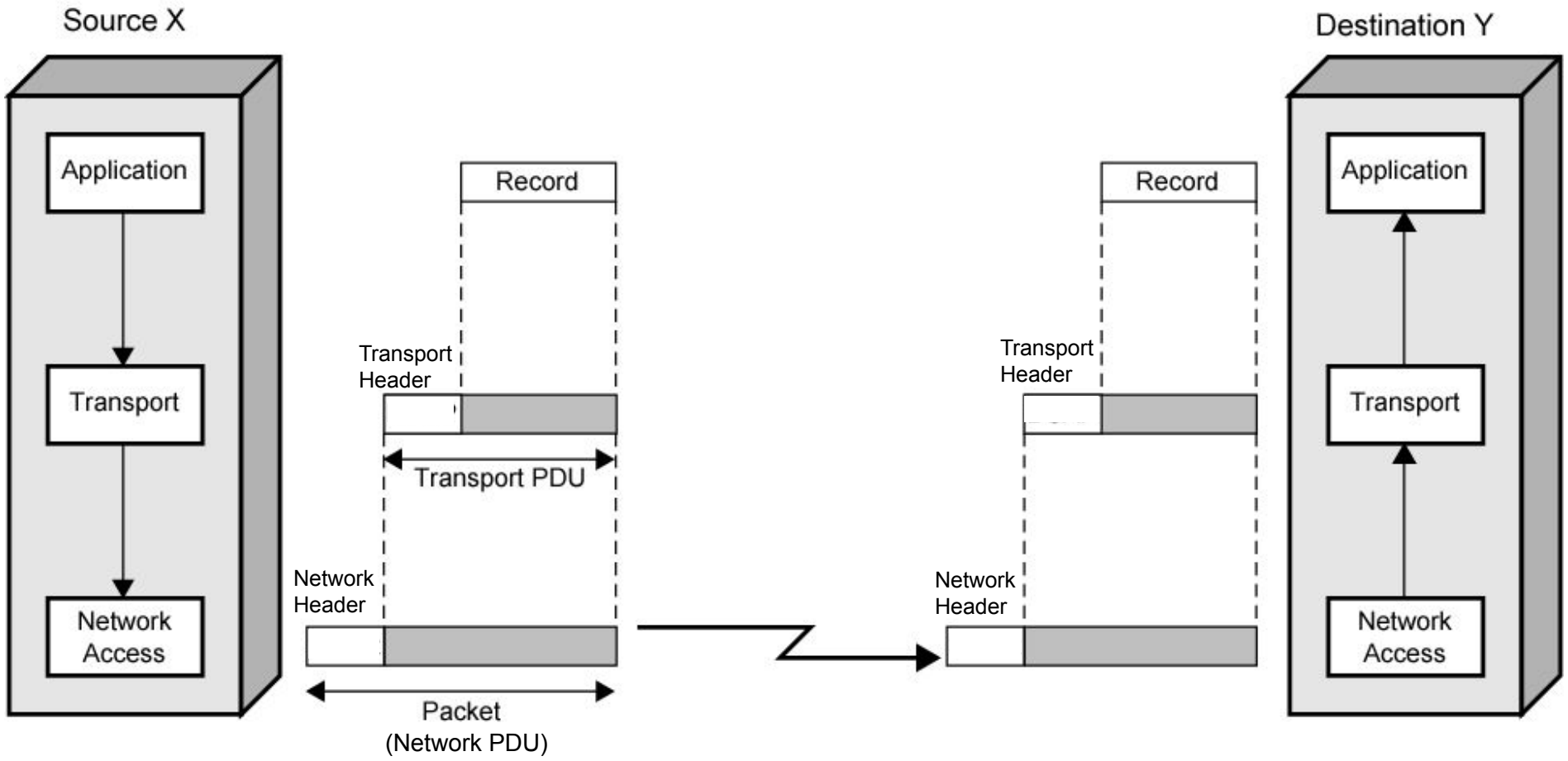
Addressing Requirements

- Two levels of addressing required
- Each computer needs unique network address
- Each application on a (multi-tasking) computer needs a unique address within the computer
  - The *service access point* or SAP
  - The *port number* in TCP/IP protocol stack

Protocol Architectures and Networks



Operation of a Protocol Architecture



TCP/IP Protocol Suite

The TCP/IP Model, or Internet Protocol Suite, describes a set of general design guidelines and implementations of specific networking protocols to enable computers to communicate over a network.

It is the set of computer network communications protocols and a description framework used for the Internet and other similar networks.

It provides end-to-end connectivity specifying how data should be formatted, addressed, transmitted, routed and received at the destination. Protocols exist for a variety of different types of communication services between computers.

TCP/IP Protocol Suite

The TCP/IP Model was created in the 1970s by Defense Advanced Research Project Agency (DARPA), an agency of the United States Department of Defense (DOD).

It evolved from ARPANET, which was the world's first wide area network and

predecessor of the Internet.

Specified and extensively used before OSI

Funded by the US - DARPA for its packet switched network (ARPANET)- DOD automatically created an enormous market for TCP/IP

Most widely used interoperable network protocol architecture i.e.

Used by the Internet and WWW

TCP/IP Protocol Suite

Target goals

The DOD wanted to build a network to connect a number of military sites. The key requirements for the network were as follows:

It must continue to function during nuclear war .

It must be completely decentralized with no key central installation that could be destroyed and bring down the whole network.

It must be fully redundant and able to continue communication between A and B even though intermediate sites and links might stop functioning during the conversation.

The architecture must be flexible as the envisaged range of applications for the network was wide: from file transfer to time sensitive data such as voice.

TCP/IP Protocol Suite

TCP/IP has evolved. The protocols within the TCP/IP Suite have been tested, modified, and improved over time. The original TCP/IP protocol suite targeted the management of large, evolving internetwork.

Some TCP/IP goals included:

Hardware independence - A protocol suite that could be used on a Mac, PC, mainframe, or any other computer.

Software independence - A protocol suite that could be used by different software vendors and applications. This would enable a host on one site to communicate with a host on another site, without having the same software configuration: heterogeneous networks.

Failure recovery and the ability to handle high error rates - A protocol suite that featured automatic recovery from any dropped or lost data. This protocol must be able to recover from an outage of any host on any part of the network and at any point in a data transfer.

TCP/IP Protocol Suite

- Efficient protocol with low overhead - A protocol suite that had a minimal amount of “extra” data moving with the data being transferred. This extra data called overhead, functions as packaging for the data being transferred and enables the data transmission. Overhead is similar to an envelope used to send a letter, or a box used to send a bigger item.
- Ability to add new networks to the internetwork without service disruption - A protocol suite that enabled new, independent networks to join this network of networks without bringing down the larger internetwork.
- Routable Data - A protocol suite on which data could make its way through an internetwork of computers to any possible destination. For this to be possible, a single and meaningful addressing scheme must be used so that every computer that is moving the data can compute the best path for every piece of data as it moves through the network.

TCP/IP Protocol Suite

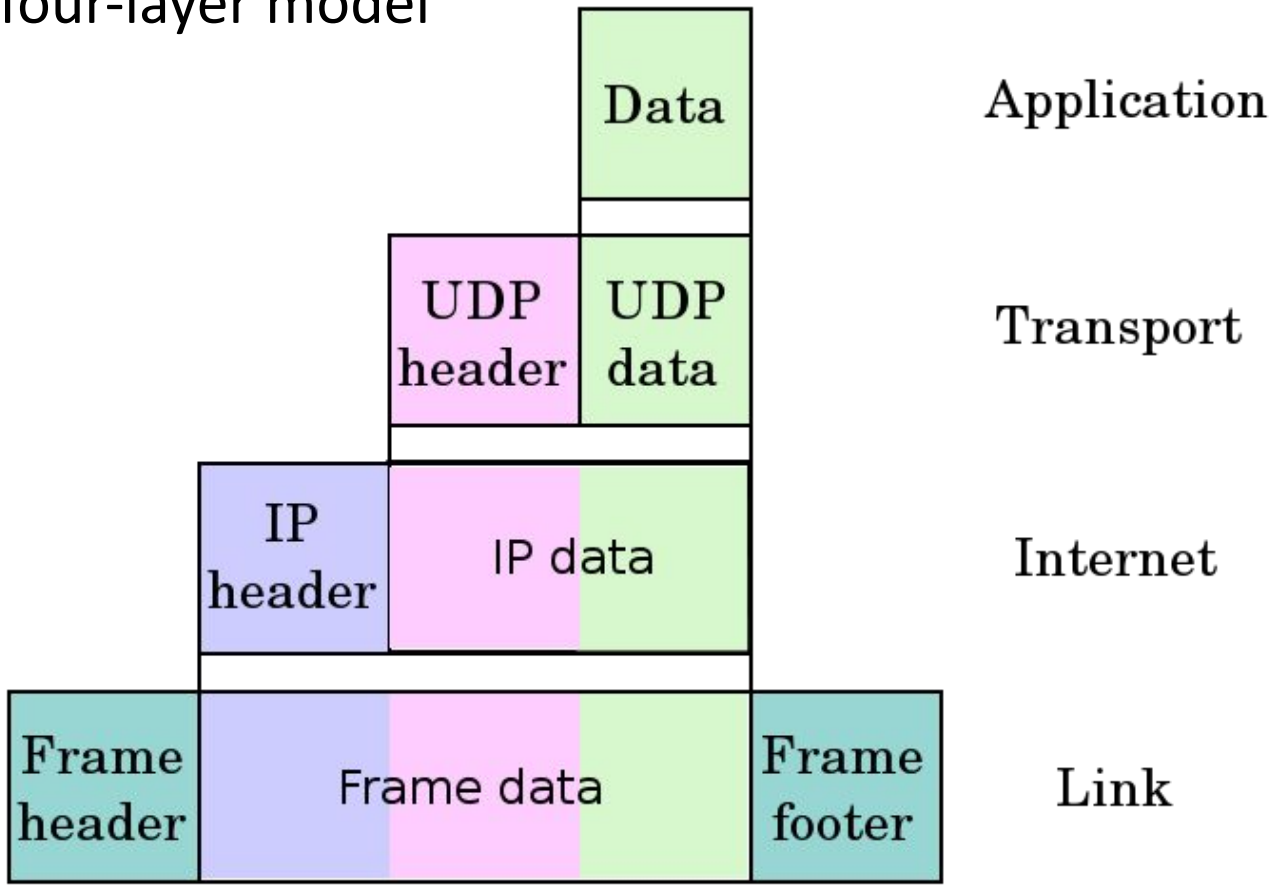
The TCP/IP protocol suite was developed before the OSI model was published. As a result, it does not use the OSI model as a reference. An early architectural document, RFC 1122, emphasizes architectural principles over layering.

End-to-End Principle: This principle has evolved over time. Its original expression put the maintenance of state and overall intelligence at the edges, and assumed the Internet that connected the edges retained no state and concentrated on speed and simplicity. Real-world needs for firewalls, network address translators, web content caches and the like have forced changes in this principle.

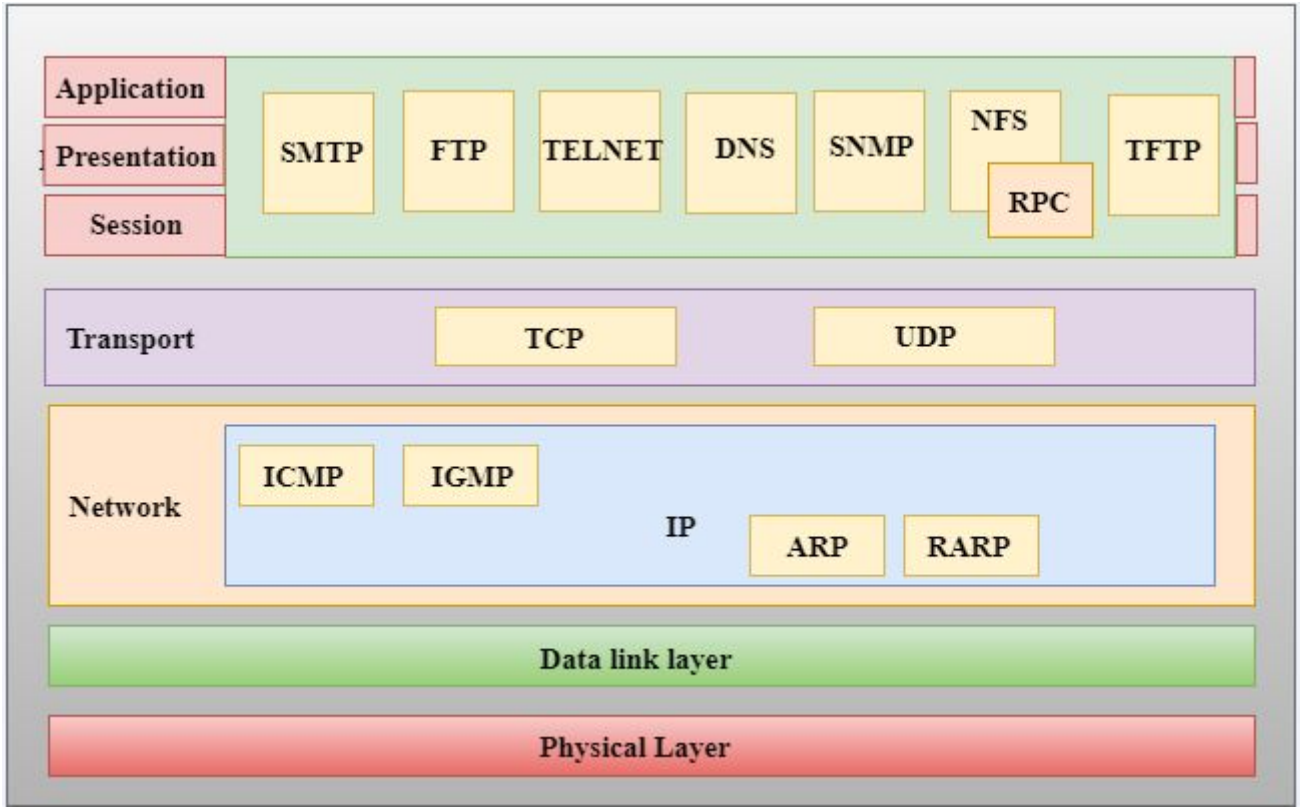
- Robustness Principle: In general, an implementation must be conservative in its sending behavior, and liberal in its receiving behavior.
- That is, it must be careful to send well-formed datagrams, but must accept any datagram that it can interpret.

TCP/IP Protocol Suite

RFC 1122 defines a four-layer model



TCP/IP Protocol Suite



Application (process-to-process) Layer

- An application layer is the topmost layer in the TCP/IP model.
- This is the scope within which applications create user data and communicate this data to other processes or applications on another or the same host.
- The communications partners are often called peers.
- It is responsible for handling high-level protocols, issues of representation.
- This layer allows the user to interact with the application.

Application Layer of TCP/IP Model encompasses same functions as these OSI Model layers : Application, Presentation, Session

Application Layer

- When one application layer protocol wants to communicate with another application layer, it forwards its data to the transport layer.
- There is an ambiguity that occurs in the application layer. Every application cannot be placed inside the application layer except those who interact with the communication system.
- For example: text editor cannot be considered in application layer while web browser using **HTTP** protocol to interact with the network where **HTTP** protocol is an application layer protocol.

Main protocols used in the application layer

- **HTTP:** HTTP stands for Hypertext transfer protocol. This protocol allows us to access the data over the world wide web. It transfers the data in the form of plain text, audio, video. It is known as a Hypertext transfer protocol as it has the efficiency to use in a hypertext environment where there are rapid jumps from one document to another.
- **SNMP:** SNMP stands for Simple Network Management Protocol. It is a framework used for managing the devices on the internet by using the TCP/IP protocol suite.
- **SMTP:** SMTP stands for Simple mail transfer protocol. The TCP/IP protocol that supports the e-mail is known as a Simple mail transfer protocol. This protocol is used to send the data to another e-mail address.

- **DNS:** DNS stands for Domain Name System. An IP address is used to identify the connection of a host to the internet uniquely. But, people prefer to use the names instead of addresses. Therefore, the system that maps the name to the address is known as Domain Name System.
- **TELNET:** It is an abbreviation for Terminal Network. It establishes the connection between the local computer and remote computer in such a way that the local terminal appears to be a terminal at the remote system.
- **FTP:** FTP stands for File Transfer Protocol. FTP is a standard internet protocol used for transmitting the files from one computer to another computer.

Transport (host-to-host) Layer

- The Transport Layer constitutes the networking regime between two network hosts, either on the local network or on remote networks separated by routers.
- The Transport Layer provides a uniform networking interface that hides the actual topology (layout) of the underlying network connections.
- This layer deals with opening and maintaining connections between Internet hosts.
- Functions the same as the Transport layer in OSI Model and part of Session layer

- TCP and other similar protocols take on some of the function of the Session layer
  - Synchronize source and destination computers to set up the session between the respective computers
- The transport layer is responsible for the reliability, flow control, and correction of data which is being sent over the network.
- The two protocols used in the transport layer are **User Datagram protocol and Transmission control protocol**.

User Datagram Protocol (UDP)

- It provides connectionless service and end-to-end delivery of transmission.
- It is an unreliable protocol as it discovers the errors but not specify the error.
- User Datagram Protocol discovers the error, and ICMP protocol reports the error to the sender that user datagram has been damaged.
- **UDP consists of the following fields:**
  Source port address: The source port address is the address of the application program that has created the message.
  Destination port address: The destination port address is the address of the application program that receives the message.
  Total length: It defines the total number of bytes of the user datagram in bytes.
  Checksum: The checksum is a 16-bit field used in error detection.
- UDP does not specify which packet is lost. UDP contains only checksum; it does not contain any ID of a data segment.

Transmission Control Protocol (TCP)

- It provides a full transport layer services to applications.
- It creates a virtual circuit between the sender and receiver, and it is active for the duration of the transmission.
- TCP is a reliable protocol as it detects the error and retransmits the damaged frames. Therefore, it ensures all the segments must be received and acknowledged before the transmission is considered to be completed and a virtual circuit is discarded.
- At the sending end, TCP divides the whole message into smaller units known as segment, and each segment contains a sequence number which is required for reordering the frames to form an original message.
- At the receiving end, TCP collects all the segments and reorders them based on sequence numbers.

Internet (internetworking) Layer

- The Internet Layer has the task of exchanging datagrams across network boundaries. It is therefore also referred to as the layer that establishes internetworking; indeed, it defines and establishes the Internet. An internet layer is also known as the network layer.
- The main responsibility of the internet layer is to send the packets from any network, and they arrive at the destination irrespective of the route they take.
- This layer defines the addressing and routing structures used for the TCP/IP protocol suite.
- Its function in routing is to transport datagrams to the next IP router that has the connectivity to a network closer to the final data destination.
- It performs same functions as OSI Model Network Layer, many of the functions of the Logical Link Control sublayer of the OSI Model's Data Link layer

Protocols used in this layer

- The primary protocol in this scope is the Internet Protocol, which defines IP addresses.
- Also uses Address Resolution Protocol (ARP), which performs much of the LLC sublayer’s job in the area of physical addressing

IP Protocol

Following are the responsibilities of this protocol:

- **IP Addressing:** This protocol implements logical host addresses known as IP addresses. The IP addresses are used by the internet and higher layers to identify the device and to provide internetwork routing.
- **Host-to-host communication:** It determines the path through which the data is to be transmitted.
- **Data Encapsulation and Formatting:** An IP protocol accepts the data from the transport layer protocol. An IP protocol ensures that the data is sent and received securely, it encapsulates the data into message known as IP datagram.

- **Fragmentation and Reassembly:**
  - The limit imposed on the size of the IP datagram by data link layer protocol is known as Maximum Transmission unit (MTU).
  - If the size of IP datagram is greater than the MTU unit, then the IP protocol splits the datagram into smaller units so that they can travel over the local network.
  - Fragmentation can be done by the sender or intermediate router. At the receiver side, all the fragments are reassembled to form an original message.
- **Routing:** When IP datagram is sent over the same local network such as LAN, MAN, WAN, it is known as direct delivery. When source and destination are on the distant network, then the IP datagram is sent indirectly. This can be accomplished by routing the IP datagram through various devices such as routers.

ARP Protocol

- ARP stands for **Address Resolution Protocol**.
- ARP is a network layer protocol which is used to find the physical address from the IP address.
- **The two terms are mainly associated with the ARP Protocol**
  - **ARP request:** When a sender wants to know the physical address of the device, it broadcasts the ARP request to the network.
  - **ARP reply:** Every device attached to the network will accept the ARP request and process the request, but only recipient recognize the IP address and sends back its physical address in the form of ARP reply. The recipient adds the physical address both to its cache memory and to the datagram header

ICMP Protocol

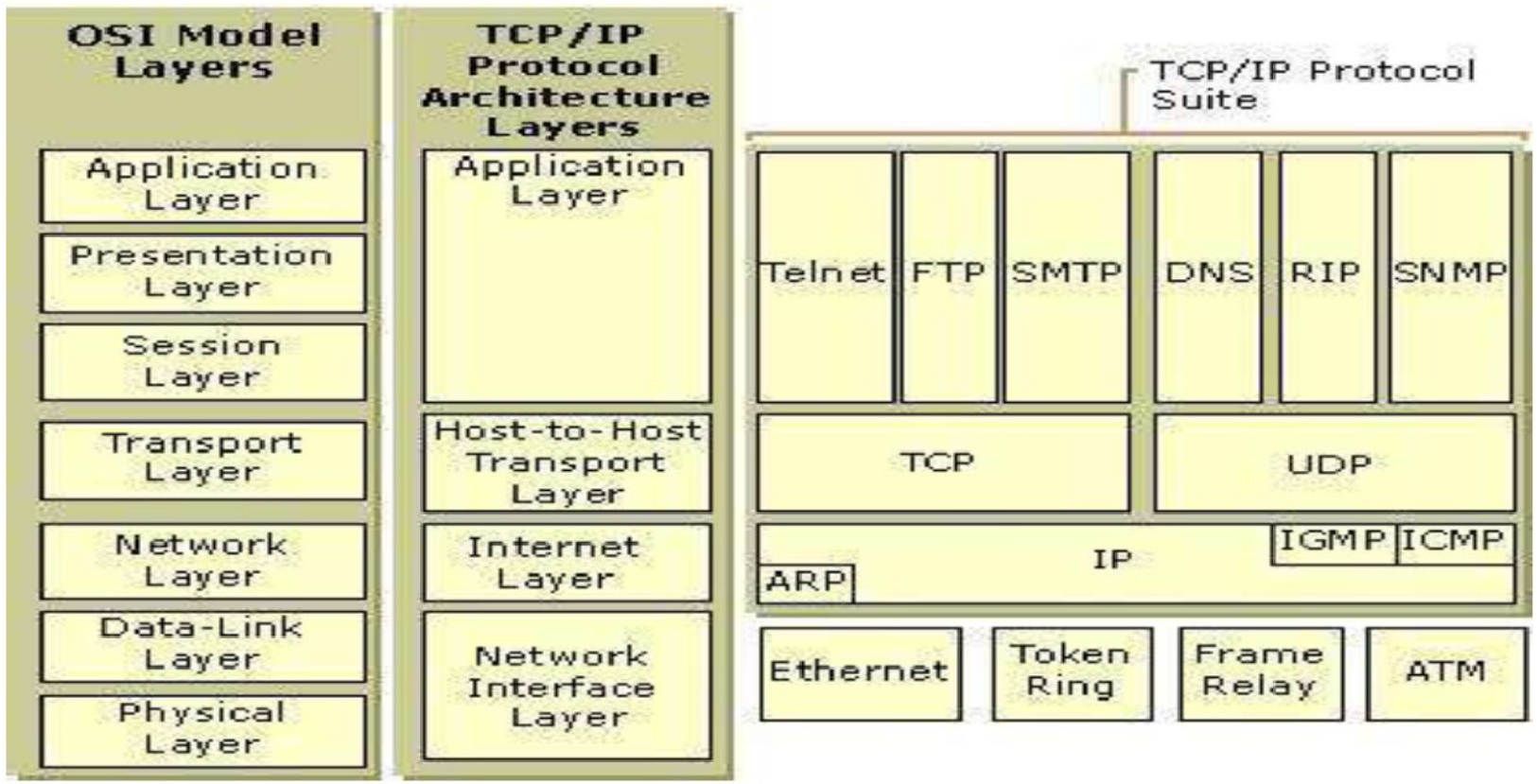
- **ICMP** stands for Internet Control Message Protocol.
- It is a mechanism used by the hosts or routers to send notifications regarding datagram problems back to the sender.
- A datagram travels from router-to-router until it reaches its destination. If a router is unable to route the data because of some unusual conditions such as disabled links, a device is on fire or network congestion, then the ICMP protocol is used to inform the sender that the datagram is undeliverable.

- An ICMP protocol mainly uses two terms:
  - **ICMP Test:** ICMP Test is used to test whether the destination is reachable or not.
  - **ICMP Reply:** ICMP Reply is used to check whether the destination device is responding or not.
- The core responsibility of the ICMP protocol is to report the problems, not correct them. The responsibility of the correction lies with the sender.
- ICMP can send the messages only to the source, but not to the intermediate routers because the IP datagram carries the addresses of the source and destination but not of the router that it is passed to.

Link Layer / Interface /Network Access Layer

- This layer defines the networking methods with the scope of the local network link on which hosts communicate without intervening routers.
- It is the combination of the Physical layer and Data Link layer defined in the OSI reference model. It performs much of the job of the MAC portion of the Data Link and Physical layers of the OSI Model
- It defines how the data should be sent physically through the network.
- This layer describes the protocols used to describe the local network topology and the interfaces needed to affect transmission of Internet Layer datagrams to next-neighbor hosts.
- TCP/IP protocol suite relies on standards created by the various standards organizations concerning how to encode bits onto media to do the work on this layer

- This layer is mainly responsible for the transmission of the data between two devices on the same network.
- The functions carried out by this layer are encapsulating the IP datagram into frames transmitted by the network and mapping of IP addresses into physical addresses.
- The protocols used by this layer are ethernet, token ring, FDDI, X.25, frame relay.


OSI Model Layers
Application Layer
Presentation Layer
Session Layer
Transport Layer
Network Layer
Data-Link Layer
Physical Layer
TCP/IP Protocol Architecture Layers
Application Layer
Host-to-Host Transport Layer
Internet Layer
Network Interface Layer
TCP/IP Protocol Suite
Telnet
FTP
SMTP
DNS
RIP
SNMP
TCP
UDP
IP
IGMP
ICMP
ARP
Ethernet
Token Ring
Frame Relay
ATM