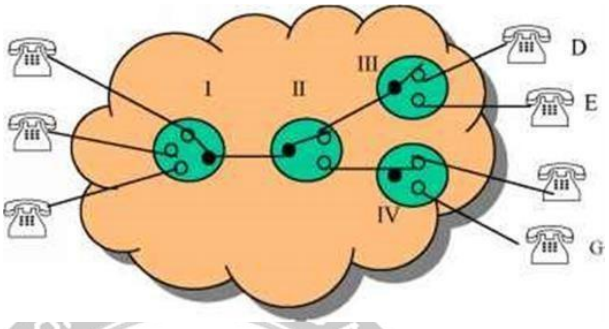
UNIT I

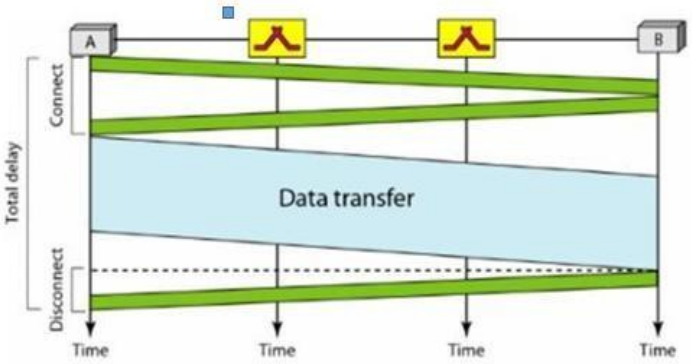
FOUNDATIONS OF COMPUTER NETWORKS

Circuit Switching

- Circuit switching is used in public telephone networks and is the basis for private networks built on leased-lines.
- Circuit switching was developed to handle voice traffic but also digital data (although inefficient)
- With circuit switching a dedicated path is established between two stations for communication.



- Switching and transmission resources within the network are reserved for the exclusive use of the circuit for the duration of the connection.
- The connection is transparent: once it is established, it appears to attach devices as if there were a direct connection.
- Communication via circuit switching involves three phases:
  1. Circuit Establishment
  2. Data Transfer
  3. Circuit Disconnect



- Connection path must be established before data transmission begins. Nodes must have switching capacity and channel capacity to establish connection.
- Circuit switching is inefficient
  1. Channel capacity dedicated for duration of connection
  2. If no data, capacity wasted
- Set up (connection) takes time
- Once connected, transfer is transparent to the users
  1. Data is transmitted at a fixed data rate with no delay (except for the propagation delay)
- Developed for voice traffic (phone)

1. May also be used for data traffic via modem

- Interconnection of telephones within a building or office.
- In circuit switching, a direct physical connection between two devices is created by space- division switches, time-division switches, or both OR Circuit switching use any of below two technologies:

Space Division Switching

- Developed for analog environment.
- In a space-division switch, the path from one device to another is spatially separate from other paths.
- A crossbar is the most common space-division switch. It connects n inputs to m outputs via n × m cross points.
- Crossbar switch.

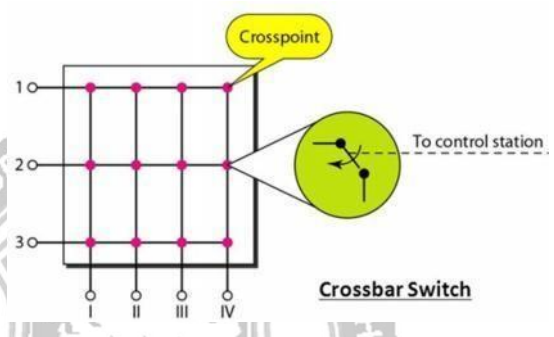


Figure 13: Space Division Switching

Time Division Switching

- In a time-division switch, the inputs are divided in time, using TDM. A control unit sends the input to the correct output device.
- Use digital time division techniques to set up and maintain virtual circuits.

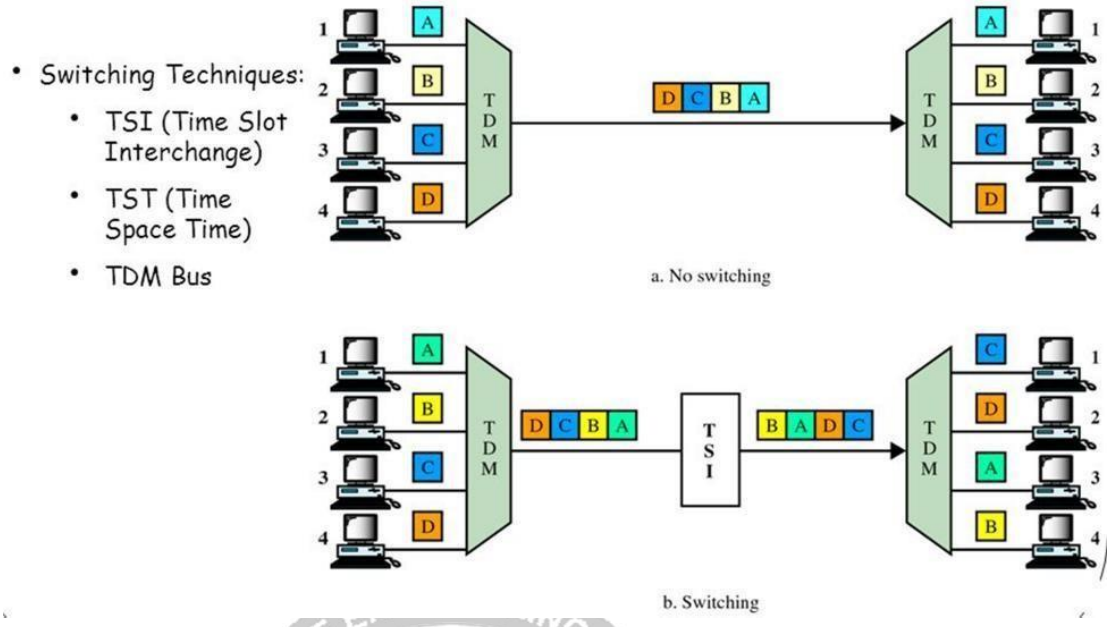


Figure 14: Time Division Switching

Packet Switching

- Packet switching was designed to provide a more efficient facility than circuit-switching for bursty data traffic.
- With packet switching, a station transmits data in small blocks, called packets.
- At each node packets are received, stored briefly (buffered) and passed on to the next node.
  1. Store and forward mechanism
- Each packet contains some portion of the user data plus control info needed for proper functioning of the network.
- A key element of packet-switching networks is whether the internal operation is datagram or virtual circuit (VC).
  1. With internal VCs, a route is defined between two endpoints and all packets for that VC follow the same route.
  2. With internal diagrams, each packet is treated independently, and packets intended for the same destination may follow different routes.
- Examples of packet switching networks are X.25, Frame Relay, ATM and IP.
- Station breaks long message into packets. Packets sent one at a time to the network.
- Packets handled in two ways:
  1. Datagram
     - Each packet treated independently
     - Packets can take any practical route
     - Packets may arrive out of order

- Packets may go missing
- Up to receiver to re-order packets and recover from missing packets

2. Virtual Circuit
   - Preplanned route established before any packets sent.
   - Once route is established, all the packets between the two communicating parties follow the same route through the network
   - Call request and call accept packets establish connection (handshake)
   - Each packet contains a Virtual Circuit Identifier (VCI) instead of destination address
   - No routing decisions required for each packet
   - Clear request to drop circuit
   - Not a dedicated path

Message Switching

- This technique was somewhere in middle of circuit switching and packet switching.
- In message switching, the whole message is treated as a data unit and is transferred in its entirety.
- A switch working on message switching, first receives the whole message and buffers it until there are resources available to transfer it to the next hop.
- If the next hop is not having enough resource to accommodate large size message, the message is stored and switch waits.

In 1983, the International Standards Organization (ISO) developed a model called Open Systems Interconnection (OSI) which is a standard reference model for communication between two end users in a network. The model is used in developing products and understanding networks. It is a prescription of characterizing and standardizing the functions of a communications system in terms of abstraction layers. Similar communication functions are grouped into logical layers. A layer serves the layer above it and is served by the layer below it.

Layers in the OSI Model

OSI divides Telecommunications into Seven Layers as shown below in the Figure 1 given below. Each layer is responsible for a particular aspect of data communication. For example, one layer may be responsible for establishing connections between devices, while another layer may be responsible for error checking during transfer.

The layers of the OSI model are divided into two groups: the upper layers and lower layers. The upper layers (Host layers) focus on user applications and how files are represented on the computers prior to transport. The lower layers (Media Layers) concentrate on how the communication across a network actually occurs. Each layer has a set of functions that are to be performed by a specific protocol(s). The OSI reference model has a protocol suit for all of its layers.

In computing, a protocol is a convention or standard that controls or enables the connection, communication, and data transfer between two computing endpoints. In its simplest form, a protocol can be defined as the rules governing the syntax, semantics, and synchronization of communication.

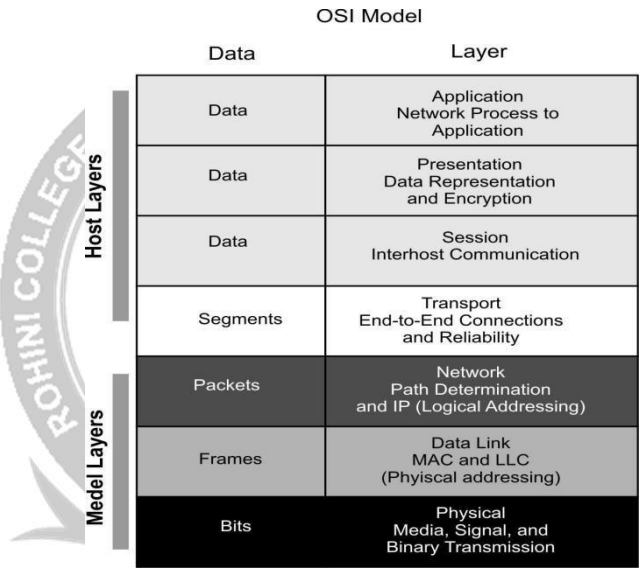


Figure 1: The OSI Model

Layer 1: The Physical Layer

The physical layer, the lowest layer of the OSI model, is concerned with the transmission and reception of the unstructured raw bit stream over a physical medium. It describes the electrical/optical, mechanical, and functional interfaces to the physical medium, and carries the signals for all of the higher layers. It provides :

- Data encoding: modifies the simple digital signal pattern (1s and 0s) used by the PC to better accommodate the characteristics of the physical medium, and to aid in bit and frame synchronization.
- Transmission technique: determines whether the encoded bits will be transmitted by baseband (digital) or broadband (analog) signaling.

- Physical medium transmission: transmits bits as electrical or optical signals appropriate for the physical medium, and determines: What physical medium options can be used? And How many volts/db should be used to represent a given signal state, using a given physical medium?
- Layer 2: The data-link layer: The data link layer provides error-free transfer of data frames from one node to another over the physical layer, allowing layers above it to assume virtually error-free transmission over the link. To do this, the data link layer provides:
- Frame Traffic Control: tells the transmitting node to "stop‖ when no frame buffers are available.
- Frame Sequencing: transmits/receives frames sequentially.
- Frame Acknowledgment: provides/expects frame acknowledgments. Detects and recovers from errors that occur in the physical layer by retransmitting non-acknowledged frames and handling duplicate frame receipt.
- Frame Delimiting: creates and recognizes frame boundaries.
- Link Establishment and Termination: establishes and terminates the logical link between two nodes.
- Frame Error Checking: checks received frames for integrity.
- Media access management: determines when the node "has the right" to use the physical medium.
- Data Link Sub layers
  - The Data Link Layer is described in more detail with Media Access Control (MAC) and Logical Link Control (LLC) sub layers; where LLC is consider as upper data link layer and MAC as lower data link layer as shown below in the Figure 2.
  - Logical Link Control (LLC): The LLC is concerned with managing traffic (flow and error control) over the physical medium and may also assign sequence numbers to frames and track acknowledgements. LLC is defined in the IEEE
  - 802.2 specification and supports both connectionless and connection-oriented services used by higher-layer protocols.
  - Media Access Control (MAC): The MAC sub layer controls how a computer on the network gains access to the data and permission to transmit it.

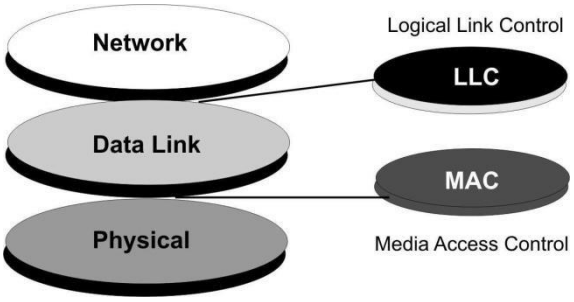


Figure 2: Data Link Sub-Layers

Layer 3: The Network Layer

The network layer provides the functional and procedural means of transferring variable length data sequences from a source host on one network to a destination host on a different network. The network layer performs network routing functions, and might also perform fragmentation and reassembly, and report delivery errors. Routers operate at this layer, sending data throughout the extended network and making the Internet possible.

Functions of the network layer include:

- Connection setup
- Addressing
- Routing
- Security
- Quality of Service
- Fragmentation

The Network Layer identifies computers on a network. Two types of packets are used at the Network layer; Data packets and Route update packets. Data packets are used to transport user data through the Internet work. Protocols used to support data traffic are called routed protocols. Route update packets are used to update neighboring routers about the network connected to all routers within the internet work. Protocols that send route updates are called routing protocols. This layer is concerned with two functions Routing and Fragmentation / Reassembly:

Routing: It is the process of selecting the best paths in a network along which to send data on physical traffic as shown in Figure 3.

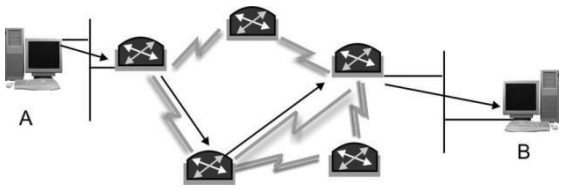


Figure 3: Routing at Network Layer

Fragmentation / Reassembly: if the network layer determines that a next router's maximum transmission unit (MTU) size is less than the current frame size, a router can fragment a frame for transmission and re-assembly at the destination station.

Layer 4: The Transport Layer

The transport layer provides transparent transfer of data between end users, providing reliable data transfer services to the upper layers. The transport layer controls the reliability of a given link through flow control, segmentation/de-segmentation, and error control. This layer manages the end-to-end control (for example, determining whether all packets have arrived). It ensures complete data transfer. The Basic Transport Layer Services are:

- Resource Utilization (multiplexing): Multiple applications run on the same machine but use different ports.
- Connection Management (establishing & terminating): The second major task of Transport Layer is establishing connection between sender & the receiver before data transmission starts & terminating the connection once the data transmission is finished
- Flow Control (Buffering / Windowing): Once the connection has occurred and transfer is in progress, congestion of the data flow can occur at a destination for a variety of reasons. Possible options include:

o The destination can become overwhelmed if multiple devices are trying to send it data at the same time.

o The destination can become overwhelmed if the source is sending faster than it can physically receive.

The Transport Layer is responsible for providing flow control to alleviate the issue of congestion in the data transfer. Two main methods for flow control include:

Buffering: Buffering is a form of data flow control regulated by the Transport Layer as depicted in Figure 4. It is responsible for ensuring that sufficient buffers (Temporary Memory) are available at the destination for the processing of data and that the data is transmitted at a rate that does not exceed what the buffer can handle.

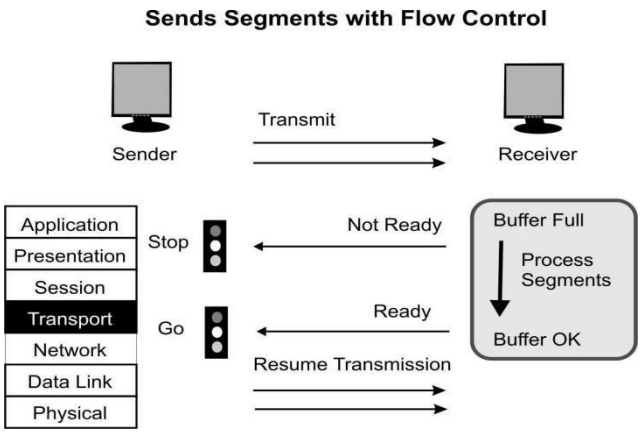


Figure 4: Buffering at Work

Windowing: Windowing is a flow control scheme in which the source computer will monitor and make adjustments to the amount of information sent based on successful, reliable receipt of data segments by the destination computer as shown in Figure 5. The size of the data transmission, called the "window size", is negotiated at the time of connection establishment, which is determined by the amount of memory or buffer that is available.

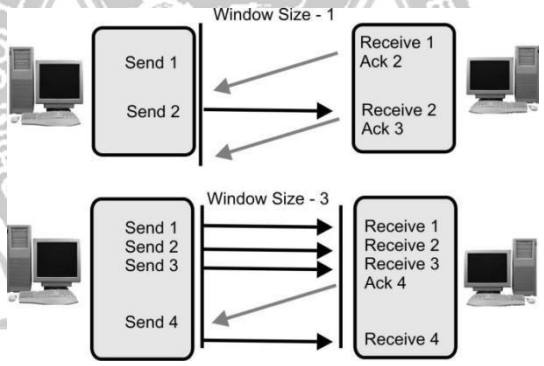


Figure 5: Flow Control & Reliability through Windowing

Reliable Transport (positive acknowledgment): Transport layer provides reliable transport of data by sending positive acknowledgements back to the sender once the data has reached the receiving side, if the data is lost or is corrupted, a negative acknowledgement is sent.

Layer 5: The Session Layer

The session Layer establishes, manages, and terminates sessions (different from connections) between applications as they interact on different hosts on a network. Its main job is to coordinate the service requests and responses between different hosts for applications.

The session established between hosts can be Simplex, half duplex and full duplex:

 Simplex: Simplex transmission is like a one-way street where traffic moves in only one direction. Simplex mode is a one-way-only transmission,

which means that data can flow only in one direction from the sending device to the receiving device.

 Half Duplex: Half Duplex is like the center lane on some three-lane roads. It is a single lane in which traffic can move in one direction or the other, but not in both directions at the same time. Half-duplex mode limits data transmission because each device must take turns using the line. Therefore, data can flow from A to B and from B to A, but not at the same time.

 Full Duplex: is like a major highway with two lanes of traffic, each lane accommodating traffic going in opposite directions. Full-duplex mode accommodates two-way simultaneous transmission, which means that both sides can send and receive at the same time. In full-duplex mode, data can flow from A to B and B to A at the same time.

Note: Full-duplex transmission is, in fact, two simplex connections: One connection has traffic flowing in only one direction; the other connection has traffic flowing in the opposite direction of the first connection.

Layer 6: The Presentation Layer

The presentation layer transforms data into the form that the application accepts. This layer formats and encrypts data to be sent across a network. This layer, usually part of an operating system, that converts incoming and outgoing data from one presentation format to another (for example, from a text stream into a popup window with the newly arrived text). This layer is sometimes called the syntax layer. The Presentation Layer is responsible for the following services:

- Data representation:

The presentation layer of the OSI model at the receiving computer is also responsible for the conversion of ―the external format‖ with which data is received from the sending computer to one accepted by the other layers in the host computer. Data formats include postscript, ASCII, or BINARY such as EBCDIC (fully Extended Binary Coded Decimal Interchange Code).

 Data security: Some types of encryption (and decryption) are performed at the presentation layer. This ensures the security of the data as it travels down the protocol stack.

 Data compression: Compression (and decompression) may be done at the presentation layer to improve the throughput of data.

Layer 7: The Application Layer

The application layer is closest to the end user, which means that both the OSI application layer and the user interact directly with the software application.

This layer interacts with software applications that implement a communicating component.

The Application Layer is the highest layer in the protocol stack and the layer responsible for introducing data into the OSI stack. The functions of Application Layer are:

- Resource sharing and device redirection
- Remote file access
- Remote printer access
- Network management
- Directory services
- Electronic messaging (such as mail) etc

TCP/IP Addressing

TCP/IP Reference Model (Internet Protocol Stack layers)

- Transmission Control Protocol/Internet Protocol (TCP/IP) protocol suite is the engine for the Internet and networks worldwide.
- TCP/IP either combines several OSI layers into a single layer, or does not use certain layers at all.
- TCP/IP is a set of protocols developed to allow cooperating computers to share resources across the network.
- The TCP/IP model has five layers.
  1. Application Layer
  2. Transport Layer
  3. Internet Layer
  4. Data Link Layer
  5. Physical Network

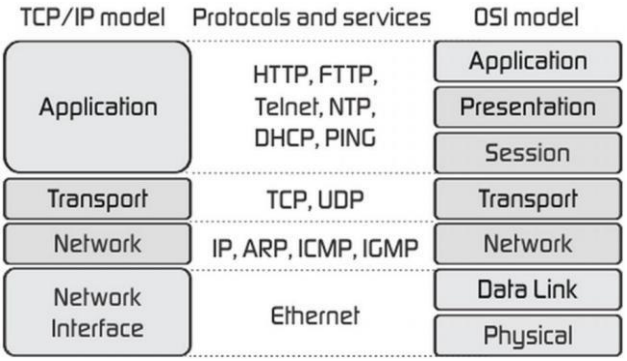


Figure 16: TCP/IP Reference Model

As we can see from the above figure, presentation and session layers are not there in TCP/IP model. Also note that the Network Access Layer in TCP/IP model combines the functions of Data link Layer and Physical Layer.

Application Layer

- Application layer is the top most layer of four layer TCP/IP model.
- Application layer is present on the top of the Transport layer.
- Application layer defines TCP/IP application protocols and how host programs interface with Transport layer services to use the network.
- Application layer includes all the higher-level protocols like DNS (Domain Naming System), HTTP (Hypertext Transfer Protocol), Telnet, SSH, FTP (File Transfer Protocol), TFTP (Trivial File Transfer Protocol), SNMP (Simple Network Management Protocol), SMTP (Simple Mail Transfer Protocol), DHCP (Dynamic Host Configuration Protocol), X Windows, RDP (Remote Desktop Protocol) etc.

Transport Layer

- The purpose of Transport layer is to permit devices on the source and destination hosts to carry on a conversation.
- Transport layer defines the level of service and status of the connection used when transporting data.
- The transport layer provides the end-to-end data transfer by delivering data from

an application to its remote peer.

- The most-used transport layer protocol is the Transmission Control Protocol (TCP), which provides:
  - Reliable delivery data
  - Duplicate data suppression
  - Flow control Congestion control

- Another transport layer protocol is the User Datagram Protocol (UDP), which provides:
  - Connectionless
  - Unreliable
- UDP is used by applications that need a fast transport mechanism and can tolerate the loss of some data.
  - Best-effort service

Network Layer (Internet Layer)

- The internet layer also called the network layer.
- Internet layer pack data into data packets known as IP datagrams, which contain source and destination address (logical address or IP address) information that is used to forward the datagrams between hosts and across networks.
- The Internet layer is also responsible for routing of IP datagrams.
- Internet Protocol (IP) is the most important protocol in this layer.
- It is a connectionless protocol that does not assume reliability from lower layers. IP does not provide reliability, flow control or error recovery.
- IP provides a routing function that attempts to deliver transmitted messages to their destination.
- These message units in an IP network are called an IP datagram.
- Example: IP, ICMP, IGMP, ARP, and RARP.

Network Interface Layer (Network Access Layer)

- Network Access Layer defines details of how data is physically sent through the network, including how bits are electrically or optically signalled by hardware devices that interface directly with a network medium, such as coaxial cable, optical fiber, or twisted pair copper wire.

- The protocols included in Network Access Layer are Ethernet, Token Ring, FDDI, X.25, Frame Relay etc.

OSI(Open System	TCP/IP (Transmission Control Protocol/ Internet Protocol)
OSI provides layer functioning and also defines functions of all	TCP/IP model is more based on protocols and protocols are not
In OSI model the transport layer guarantees the delivery of packets	In TCP/IP model the transport layer does not guarantees
Follows horizontal approach	Follows vertical approach
OSI model has a separate	TCP/IP doesn't have a
OSI is a general model.	TCP/IP model cannot be used in any other application
Network layer of OSI model	The Network layer in TCP/IP
OSI model has a problem of fitting the protocols in	TCP/IP model does not fit any protocol
Protocols are hidden in OSI model and are easily replaced as the	In TCP/IP replacing protocol is not easy.
OSI model defines services, interfaces and protocols very clearly	In TCP/IP it is not clearly separated its services,
It has 7 layers	It has 4 layers

Understanding of Delay, Loss and Throughput in the Packet Switching Network

Basics

- Recall that a packet starts in a host (the source), passes through a series of routers, and ends its journey in another host (the destination).
- As a packet travels from one node (host or router) to the subsequent node (host or router) along this path, the packet suffers from several types of delays at each node along the path.
- The most important of these delays are the
  - Nodal processing delay
  - Queuing delay
  - Transmission delay
  - Propagation delay
- Together, these delays accumulate to give a total nodal delay.
- The performance of many Internet applications—such as search, Web browsing, email, maps, instant messaging, and voice-over-IP—are greatly affected by network delays.

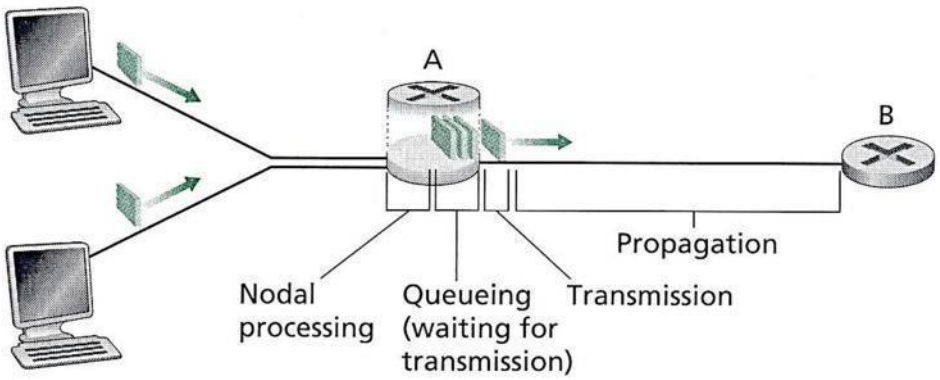


Figure 17: Delay in Packet Switched Network

Processing Delay

- The time required to examine the packet's header and determine where to direct the packet is part of the processing delay.
- The processing delay can also include other factors, such as the time needed to check for bit- level errors in the packet that occurred in transmitting the packet's bits from the upstream node to router.

 It is typically on the order of microseconds or less.

Queuing Delay

- At the queue, the packet experiences a queuing delay as it waits to be transmitted onto the link.
- The length of the queuing delay of a specific packet will depend on the number of earlier- arriving packets that are queued and waiting for transmission onto the link.
- If the queue is empty and no other packet is currently being transmitted, then our packet's queuing delay will be zero.
- On the other hand, if the traffic is heavy and many other packets are also waiting to be transmitted, the queuing delay will be long.

 Queuing delays can be on the order of microseconds to milliseconds in practice.

Transmission Delay

- Assuming that packets are transmitted in a first-come-first-served manner like packet-switched networks.
- Now packet can be transmitted only after all the packets that have arrived before it have been transmitted.
- Denote the length of the packet by L bits, and denote the transmission rate of the link from router to router by R bits/sec.
- The transmission delay is L/R.
- Transmission delays are typically on the order of microseconds to milliseconds in practice.

Propagation Delay

- Once a bit is pushed into the link, it needs to propagate to router B. The time required to propagate from the beginning of the link to router B is the propagation delay.
- The bit propagates at the propagation speed of the link.
- The propagation speed depends on the physical medium of the link.
- Propagation delays are on the order of milliseconds.
- Propagations delay=d (Length of Physical Link) /s (Propagation speed in medium).

Packet Loss

- Packet loss is the failure of one or more transmitted packets to arrive at their destination.
- This event can cause noticeable effects in all types of digital communications.
- The loss of data packets depends on the switch queue. The loss of data packets increases with the increases in the traffic intensity.
- It affects the performance of the network.

Throughput

- Throughput or Network Throughput is the rate of successful message delivery over a communication channel.
- The data these messages belong to may be delivered over a physical or logical link or it can pass through a certain network node.
- Throughput is usually measured in bits per second (bit/s or bps), and sometimes in

  data packets per second (p/s or pps) or data packets per time slot.