MODULE 1

INTERNET: The Internet is a computer network that interconnects hundreds of millions of computing devices throughout the world – Nuts and Bolts description

In Internet jargon, all of the devices are called hosts or end systems.

End systems are connected together by a network of **communication links** and **packet switches.**

When one end system has data to send to another end system, the sending end system segments the data and adds header bytes to each segment. The resulting packages of information, known as packets in the jargon of computer networks, are then sent through the network to the destination end system, where they are reassembled into the original data.

Examples of packet switches: Routers and Link Layer Switches.

Routers are used in the network core whereas link layer switches are used in access networks.

Route/Path through the network: The sequence of communication links and packet switches traversed by a packet while travelling from starting end system to destination end system.

End systems access the Internet through Internet Service Providers (ISPs).

Each ISP is in itself a network of packet switches and communication links.

PROTOCOL: Protocols control the sending and receiving of information within the Internet.

Example: Transmission Control Protocol (TCP) and Internet Protocol (IP).

INTERNET: Infrastructure that provides services to applications.

API: End systems attached to the Internet provide an Application Programming Interface (API) that specifies how a program running on one end system asks the Internet infrastructure to deliver data to a specific destination program running on another end system. This Internet API is a set of rules that the sending program must follow so that the Internet can deliver the data to the destination program.

PROTOCOL: A protocol defines the format and the order of messages exchanged between two or more communicating entities, as well as the actions taken on the transmission and/or receipt of a message or other event.

Host = End system.

Hosts are sometimes further divided into two categories: clients and servers.

NETWORK EDGE

frequency division multiplexing (FDM): The technique of combining different frequency signals over a common medium and transmitting them simultaneously.

HFC: hybrid fiber coax

The two most prevalent types of broadband residential access are digital subscriber line (DSL) and cable.

The residential telephone line carries both data and traditional telephone signals simultaneously, which are encoded at different frequencies:

• A high-speed downstream channel, in the 50 kHz to 1 MHz band

• A medium-speed upstream channel, in the 4 kHz to 50 kHz band

• An ordinary two-way telephone channel, in the 0 to 4 kHz band

This approach makes the single DSL link appear as if there were three separate links, so that a telephone call and an Internet connection can share the DSL link at the same time.

Fiber to the Home (FTTH): FTTH concept is simple, provide an optical fiber path from the Central Office directly to the home.

host sending function:

- takes application message
- breaks into smaller chunks, known as *packets*, of length *L* bits
- transmits packet into access network at *transmission rate R*
    - link transmission rate, aka link *capacity, aka link bandwidth*

Packet transmission delay = Time needed to transmit L bit packet into link = L/R

Physical Media:

- guided media:
    - signals propagate in solid media: copper, fiber, coax
- unguided media:
    - signals propagate freely, e.g., radio

NETWORK CORE

- mesh of interconnected routers

- packet-switching: hosts break application-layer messages into *packets*
- network forwards packets from one router to the next, across links on path from source to destination

Two key network core functions:

1] Forwarding

- aka “switching”
- *local* action: move arriving packets from router’s input link to appropriate router output link

2] Routing

- *global* action: determine source-destination paths taken by packets
- routing algorithms

Packet Switching – Store and forward

Packet transmission delay: takes *L*/*R* seconds to transmit (push out) *L*-bit packet into link at *R* bps

1] Most packet switches use store and forward transmission at the inputs to the link.

2] It means that the packet switch must receive the entire packet before it can begin to transmit the first bit of the packet onto the outbound link.

3] The packet switch must buffer(store) the bits till all the bits of the packet are received then only it will start transmitting the packet onto the outbound link.

End-to-end delay = N (L/R)

Packet Switching – Queueing

Packet queuing and loss: If arrival rate (in bps) to link exceeds transmission rate (bps) of link for some period of time:

- packets will queue, waiting to be transmitted on output link
- packets can be dropped (lost) if memory (buffer) in router fills up

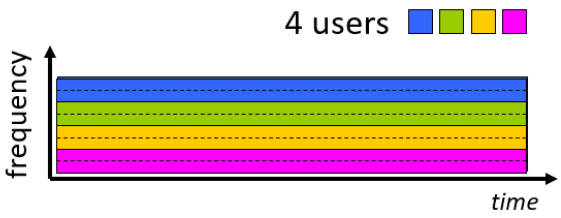
In link attached to packet switch, there is an output buffer queue which stores the packet which the packet switch is about to send to the link. If a packet arrives at the packet switch and it finds the buffer full, then packet loss can occur.

CIRCUIT SWITCHING

In circuit-switched networks, the resources needed along a path (buffers, link transmission rate) to provide for communication between the end systems are reserved for the duration of the communication session between the end systems. In packet-switched networks, these resources are not reserved; a session’s messages use the resources on demand, and as a consequence, may have to wait (that is, queue) for access to a communication link.

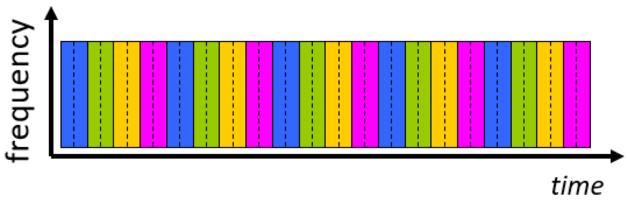
Frequency Division Multiplexing (FDM)

- optical, electromagnetic frequencies divided into (narrow) frequency bands
- each call allocated its own band, can transmit at max rate of that narrow band



Time Division Multiplexing (TDM)

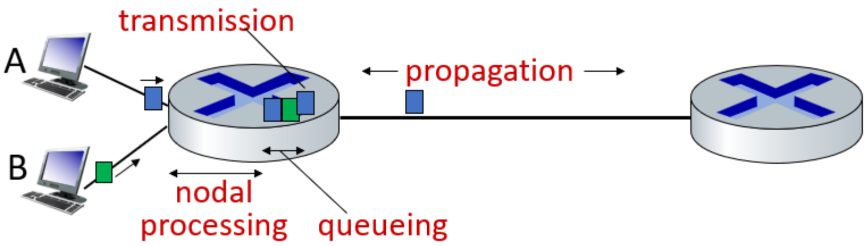
- time divided into slots.
- each call allocated periodic slot(s), can transmit at maximum rate of (wider) frequency band (only) during its time slot(s).



Differences Between TDM and FDM

TDM	FDM
TDM stands for Time division multiplexing.	FDM stands for Frequency division multiplexing.
TDM works with digital signals as well as analog signals.	While FDM works with only analog signals.
TDM has low conflict.	While it has high conflict.
Wiring or chip of TDM is simple.	While it's wiring or chip is complex rather than simple.
TDM is efficient.	While it is inefficient.
In TDM, time sharing takes place.	While in this, frequency sharing takes place.
In TDM, synchronization pulse is necessary.	While in it Guard band is necessary.

Packet delay: four sources

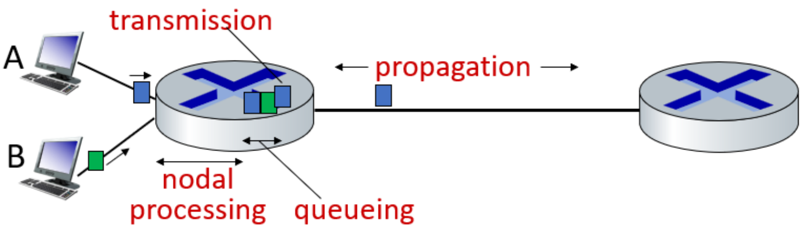


$$d_{nodal} = d_{proc} + d_{queue} + d_{trans} + d_{prop}$$

d_{proc}: nodal processing
- check bit errors
- determine output link
- typically < microsecs

d_{queue}: queueing delay
- time waiting at output link for transmission
- depends on congestion level of router

Packet delay: four sources



$$d_{nodal} = d_{proc} + d_{queue} + d_{trans} + d_{prop}$$

d_{trans}: transmission delay:
- L: packet length (bits)
- R: link *transmission rate (bps)*
- $d_{trans} = L/R$

d_{prop}: propagation delay:
- d: length of physical link
- s: propagation speed (~2×10^8 m/sec)
- $d_{prop} = d/s$

d_{trans} and d_{prop}
very different

1] <u>Processing Delay:</u> The time required to examine a packet header and determine where to direct it.

2] <u>Queueing Delay:</u> If a packet is stuck in the buffer queue, it is called queueing delay.

3] <u>Transmission Delay:</u> It is the amount of time required to push all of the packet bits into the link.

4] <u>Propagation Delay:</u> The time required to propagate from one end of the link to another is propagation delay.

5] <u>End-to-end delay:</u> Total delay from source to destination.

6] <u>Throughput:</u> Rate (bits/time unit) at which bits are being sent from sender to receiver

- *instantaneous:* rate at given point in time
- *average:* rate over longer period of time

PROTOCOL LAYERS

To provide structure to the design of network protocols, network designers organize protocols—and the network hardware and software that implement the protocols— in layers.

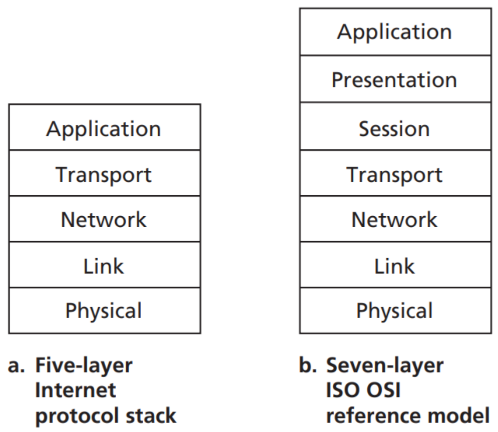


Figure 1.23 ♦ The Internet protocol stack (a) and OSI reference model (b)

1] <u>Application Layer:</u>

The application layer is where network applications and their protocols reside. It includes HTTP for web document transfer, SMTP for email, and FTP for file transfer. Functions like translating domain names to network addresses use specific protocols like DNS. Application-layer protocols facilitate communication between end systems by exchanging packets of information, known as messages.

2] <u>Transport Layer:</u>

The transport layer is responsible for transferring messages between applications. In the Internet, there are two main protocols: TCP and UDP. TCP ensures reliable delivery, flow control, and congestion control, while UDP offers a simpler, connectionless service. Each message transmitted at this layer is called a segment.

3] Network Layer:

The network layer manages the transfer of datagrams between hosts using the Internet Protocol (IP). It includes routing protocols that determine the paths datagrams take between source and destination hosts. IP is the fundamental protocol, and it ensures the delivery of segments across the network.

4] Link Layer:

The link layer facilitates the movement of datagrams between nodes within a network. It relies on specific protocols like Ethernet and WiFi, which may provide services such as reliable delivery. Different links in the network may use different protocols, and each packet transmitted at this layer is called a frame.

5] Physical Layer:

The physical layer handles the transmission of individual bits within frames between network elements. Protocols at this layer depend on the transmission medium, such as copper wire or fiber optics. For example, Ethernet employs various physical-layer protocols tailored to different transmission mediums to ensure efficient data transfer.

ENCAPSULATION:

In networking, encapsulation refers to the process of adding protocol-specific headers and trailers to data at each layer of the network protocol stack as it traverses from the source to the destination. These headers and trailers contain control information necessary for routing, error detection and correction, addressing, and other network functions. Encapsulation ensures that data transmitted over a network is correctly handled and delivered to the intended recipient by encapsulating it within a series of nested protocol headers.