CSC 138 Final Study Guide

Sunday, December 12, 2021 | 02:38 AM

Chapter 01

What's Internet protocol

Are specific messages sent and specific actions we take in response to the received reply messages or events; on the whole, protocols define how the format, the order, of the messages sent, and actions taken on transmission or received, receipt, message.

Network Core

The Network Core: The mesh of packet switches and links that interconnects the Internet's end systems.

Circuit switching networks VS Packet-switching networks have both traditionally occupied different spaces within corporations.

- Circuit-switched networks are ideal for communications which require data to be transmitted in real-time
    - Are normally used for traditional telephones calls
- Packet-switched networks are more flexible and more efficient if some amount of delay is acceptable
    - Are normally used to handle digital data

Packet Switching

1. In a network application end systems exchange **messages** with each other
    1. **Messages** can contain anything the application designer wants
    2. **Messages** can perform control functions ("handshake" between systems)
    3. **Messages** can contain data (e-mail message, JPEG image, or MP3 audio file)
2. To send a **message** between two systems (source and destination end system)
    1. **Packets**: The source system breaks messages into smaller chunks of data
    2. In travel each packet goes though communication links and **packet switches**
        1. **Packet Switches**: Two main types **routers** and **link-layer switches**
    3. **Packets** pass over each comm link equal to full transmission rate of the link
        1. If a source system or packet switch is sending *L*-bits over a link with transmission rate *R* bits/sec; then, the time to transmit the packet is

$$\frac{L}{R} seconds$$

Store and Forward

The entire packet must arrive at the router before it can be transmitted to the next link.

End-End Delay -

It takes

$$\frac{L}{R} seconds$$

to transmit, send-out, *L*-bit packet over communication link at a rate of

$$R \frac{bits}{sec}$$

Queuing and Loss -

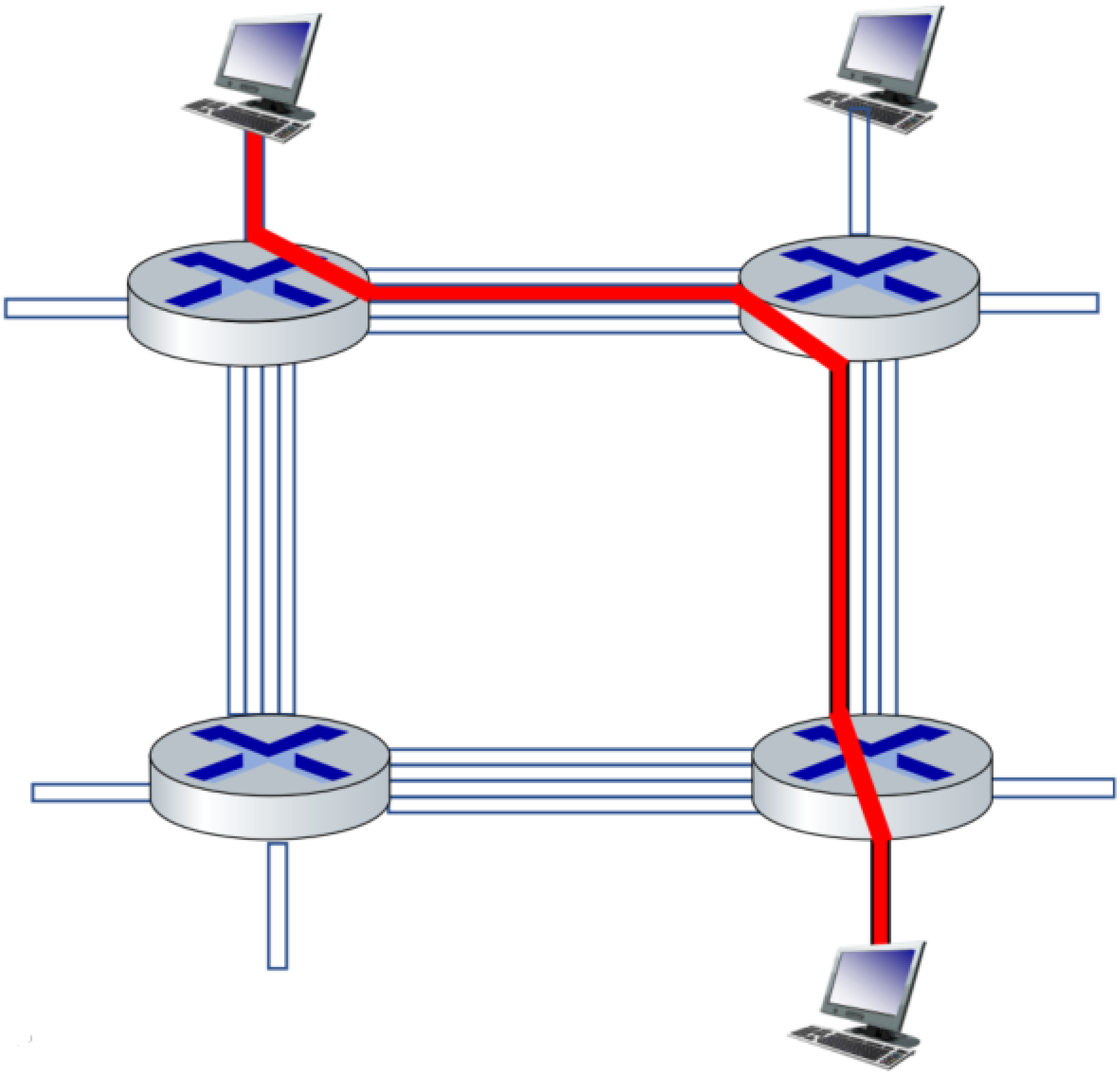
If the arrival rate, in bits/second, to the communication link exceeds transmission rate (bits/second) of the link for some period of time:

1. Packets will queue - waiting to be transmitted to the output link
2. Packets can be dropped (loss) when the memory (buffer) in the router fills up

Circuit Switching

Circuit switching is a type of switching in which a dedicated channel or circuit is established for the duration of communications. A method used by the old traditional telephone call where the call/signal is carried over the **Public Switched Telephone Network** (PSTN), or also known as the **Plain Old Telephone Service** (POTS).

In short: An end-to-end resources allocated, reserved (not shared), for the “call” between source and destination. *It works like a telephone switchboard*



TDM vs FDM

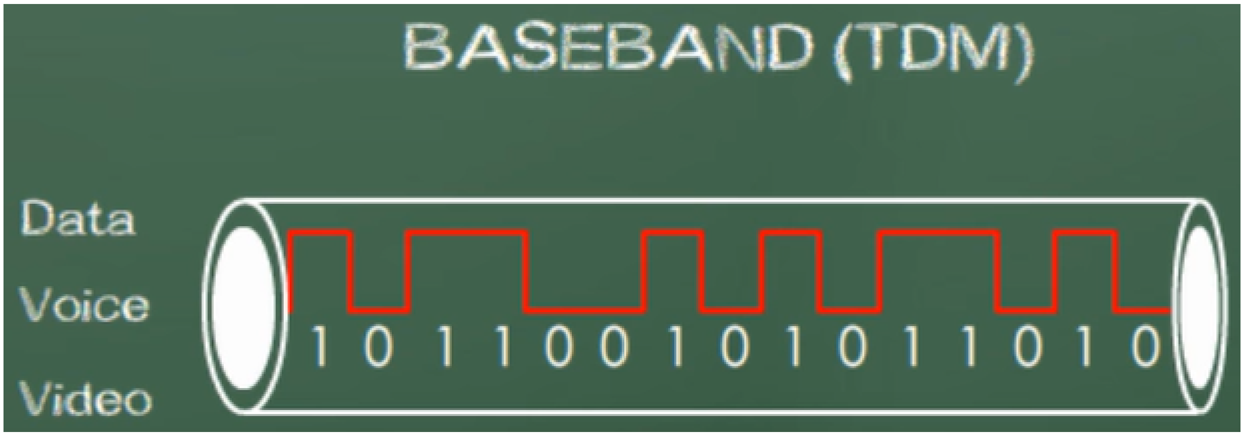
When do we use Time Division Multiplexing (TDM)?
When do we use Frequency Division Multiplexing (FDM)?

To answer the questions above, we need to know about **baseband** and **broadband**

BASEBAND (TDM)

Baseband deals with digital signals. Baseband systems can transmit only one signal at a time. Digital signals occupy the entire bandwidth, which means baseband requires an exclusive use of the channel's capacity.

- When a user is sending a signal, no one else can use it at the same time.
    - For example: Ethernet



Baseband: Time Division Multiplexing (TDM)

TDM transmit different users' signals, the "call", over one link (the maximum rate of the frequency band) by dividing time into slots or intervals and assigning them equally among the users.

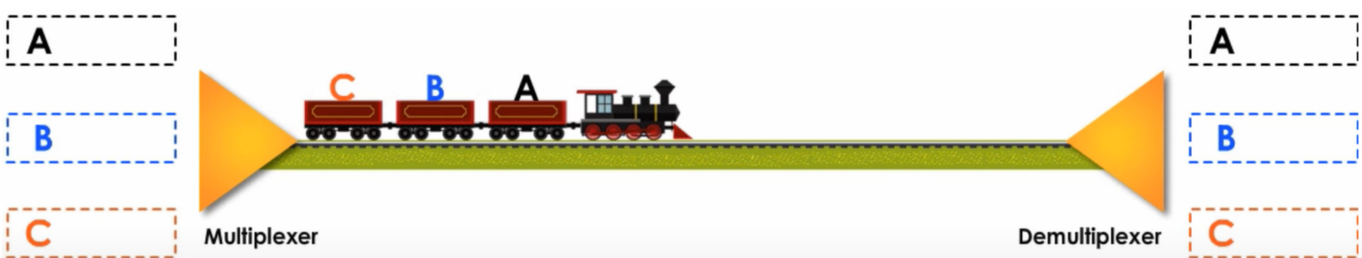
Main Feature quality of TDM: Every user is allocated with the same amount of time, but equality is not efficient in many situations.

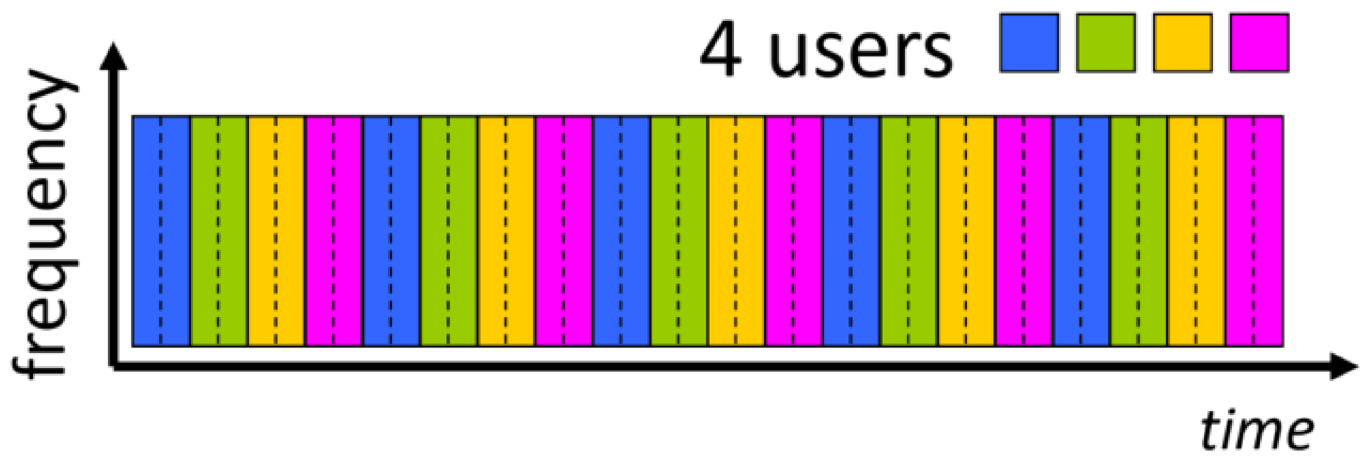
In summary: TDM, Time Division Multiplexing, is about time allocation. Every user is given the same amount of time in a "call".

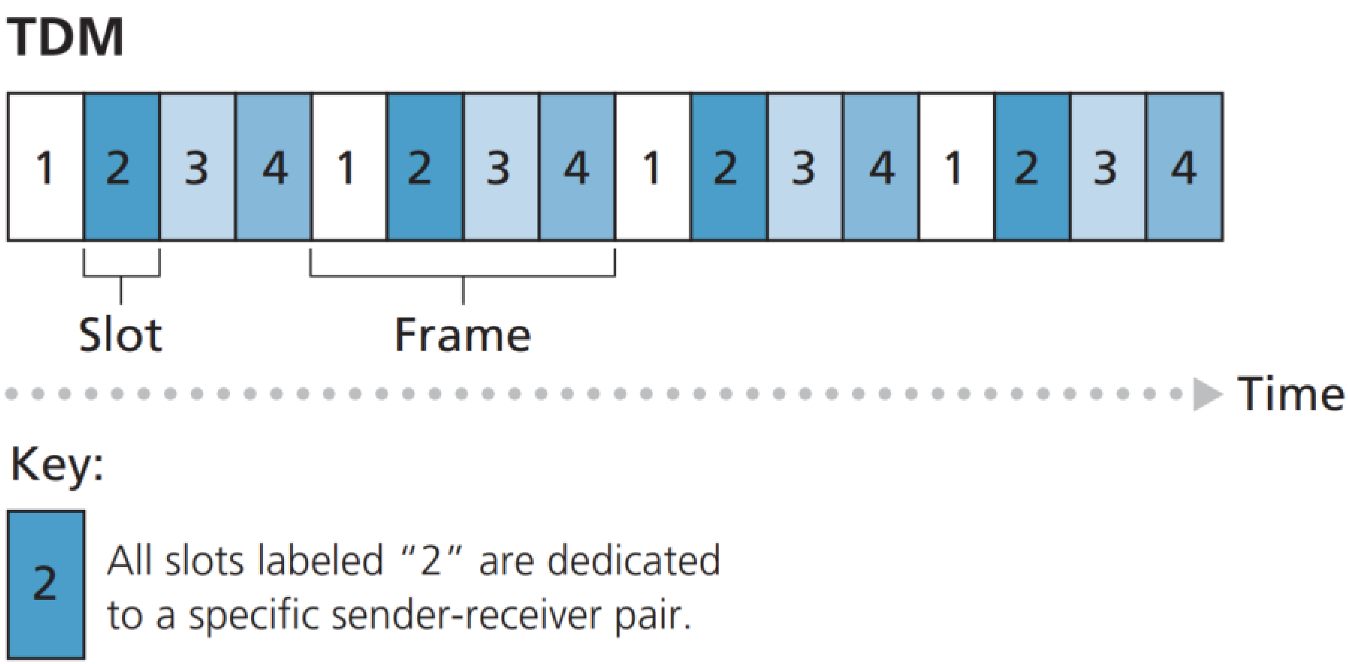
Example:

1. **Ethernet** is an example of baseband system.

Some users may have more data or a higher priority than others. Giving the same amount of time regardless of need or priority is not cost effective. As a result Statistical Time Division Multiplexing, or Statistical Multiplexing, is recommended.

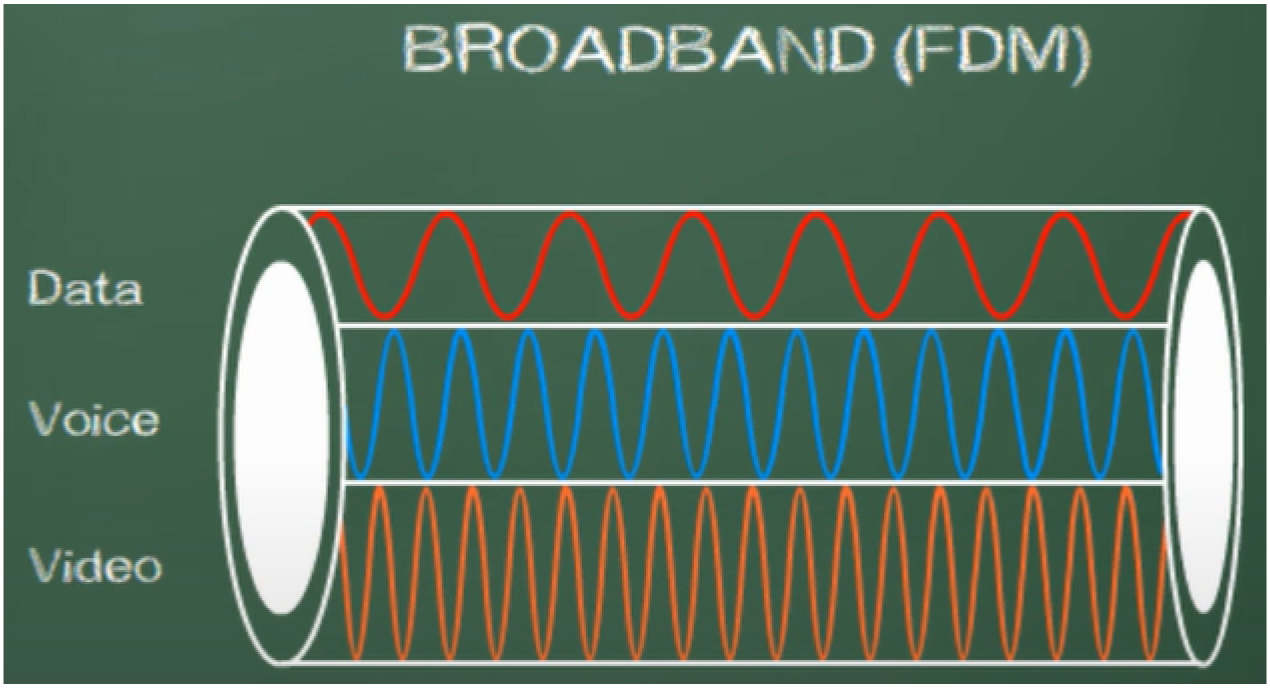






BROADBAND (FDM)

Broadband transmissions deal with analog signals which are in the form of optical or Radio Frequency, RF, waves. Broadband allows multiple transmissions at the same time. They can share one channel by using different frequency range. Thus, FDM, Frequency Division Multiplexing, is used in the broadband system.



Broadband: Frequency Division Multiplexing (FDM)

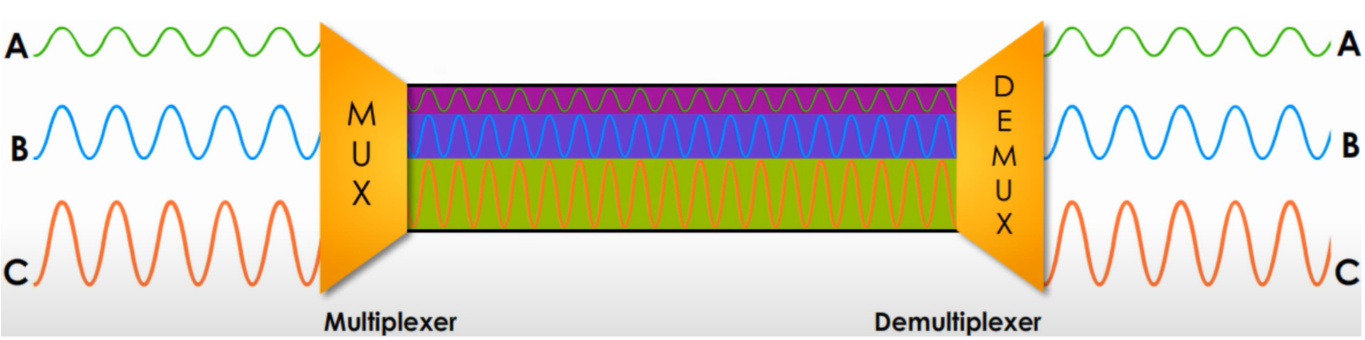
The optical electromagnetic frequencies, analog signals (not digital signals), are divided (narrowed) into frequency bands; where, each call gets its own band, and can only transmit at the max rate of the narrow band.

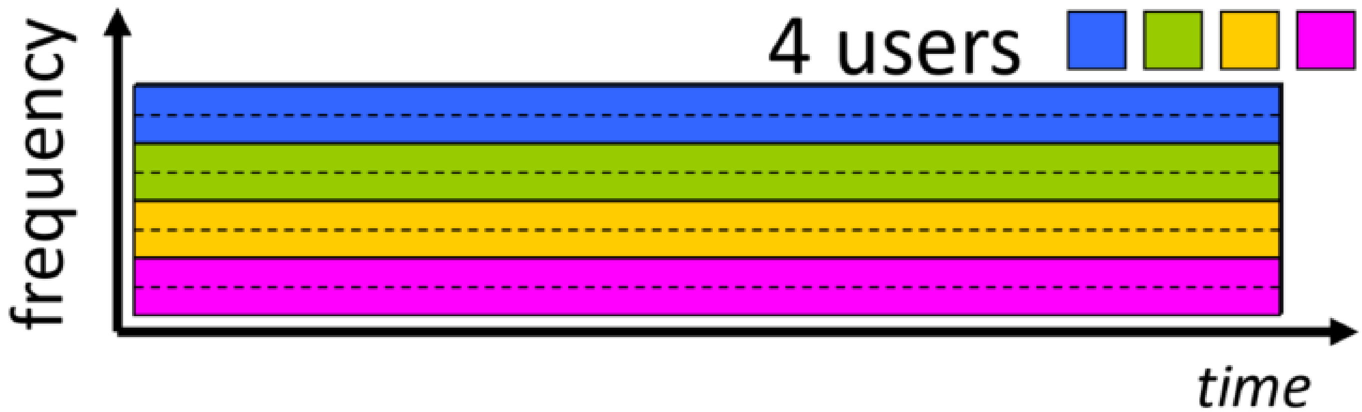
1. Optical electromagnetic frequencies are divided (narrowed) into frequency bands
2. Each call gets its own band and can only transmit at the max rate of the narrow band

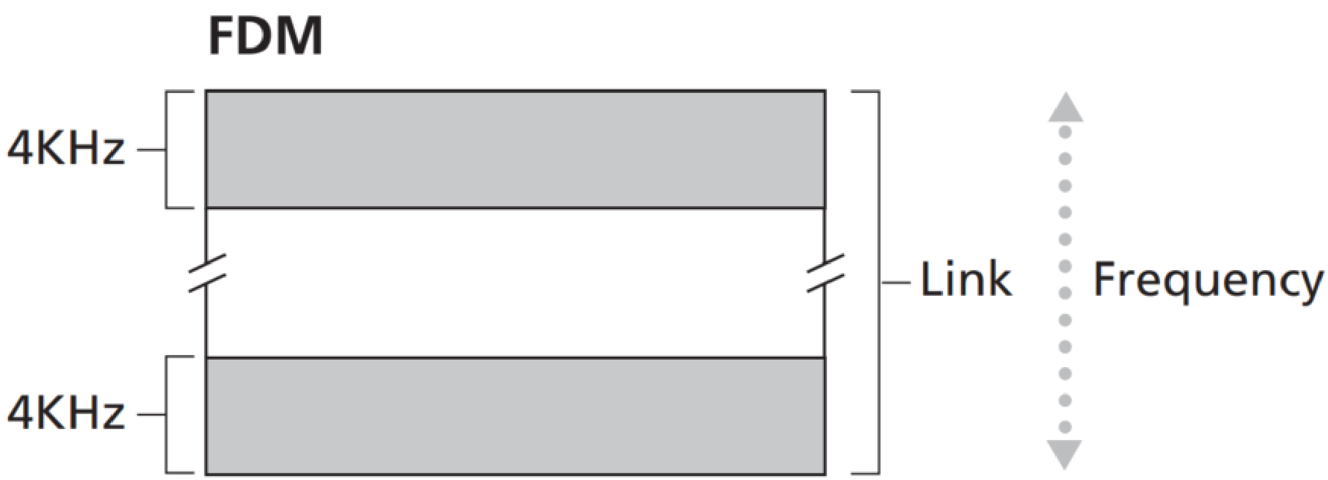
In Summary: FDM, Frequency Division Multiplexing, is about frequency channel and each user used their own non-overlapping frequency channel.

Example:

1. FM radio stations also use Frequency Division Multiplexing (FDM) to share the frequency spectrum between 88 MHz and 108 MHz, with each station being allocated a specific frequency band.
2. The broadband system is an example of Frequency Division Multiplexing (FDM)







Packet Delay -

Four Sources of Packet Delay -

1. Nodal Processing
2. Queuing Delay
3. Transmission Delay
4. Propagation Delay

Packet Loss -

If a router is queuing packets because of high congestion, and the queue is full, the packets will be dropped.

Throughput

The rate (bits per second / time unit) at which bits are being sent from sender to receiver.

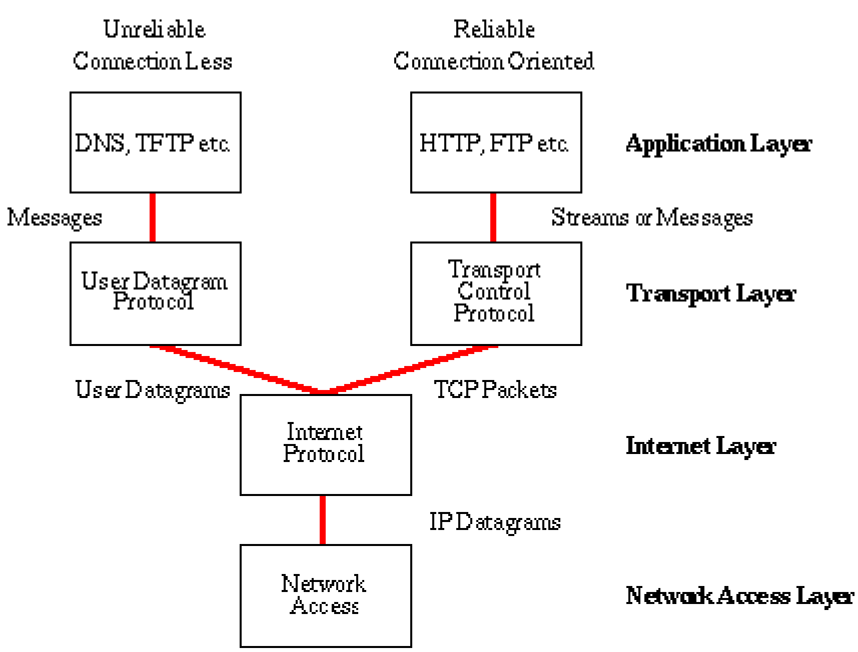
1. Instantaneous: rate at given point in time
2. Average: rate over longer period of time

Protocol Layer

1. Network designers organize protocols including the hardware and software that implement the protocols in **layers**, so to provide structure.
2. Each protocol belongs to one of the layers

Internet Protocol Stack

1. Application Layer (**message**): Applications implement services of the Transport Layer
2. Packets of information at the Application Layer are referred to as **messages**
3. Transport Layer (**segment**): Encapsulates the application layer message and integrates the protocol type (UDP, TCP, etc...)
4. The book refers to a transport-layer packet as a **segment**
5. Network Layer (**datagrams**): Transfers messages from one host to another using link layer.
6. The internet's network layer is responsible for moving network-layer packets known as **datagrams** from one host to another.
7. Link Layer (**frames**): Transfers datagrams from host to neighboring host using the network layer
8. The book refers to the link-layer packets as **frames**
9. Physical Layer: The physical layer includes the physical medium of transfer (twisted-pair copper wire, single-mode fiber optics, coaxial cable) and protocols to handle that transfer



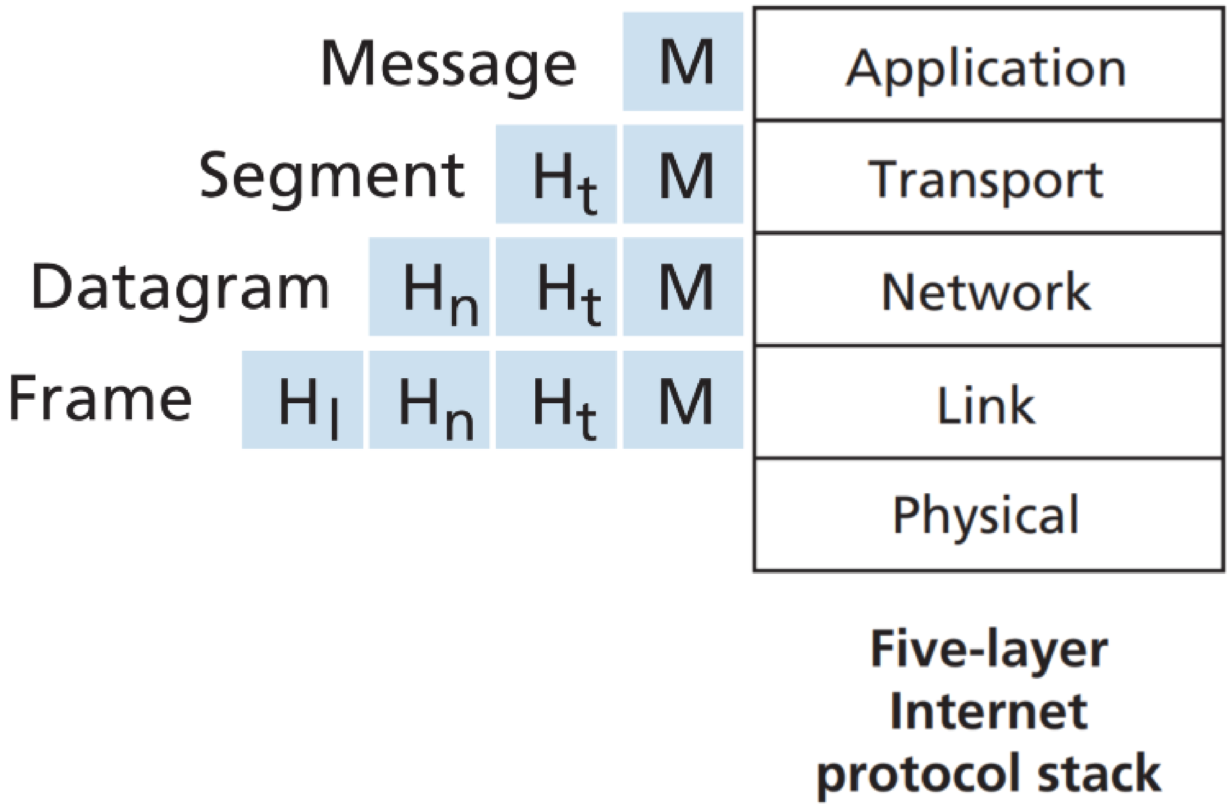


Figure 1.23 ♦ The Internet protocol stack

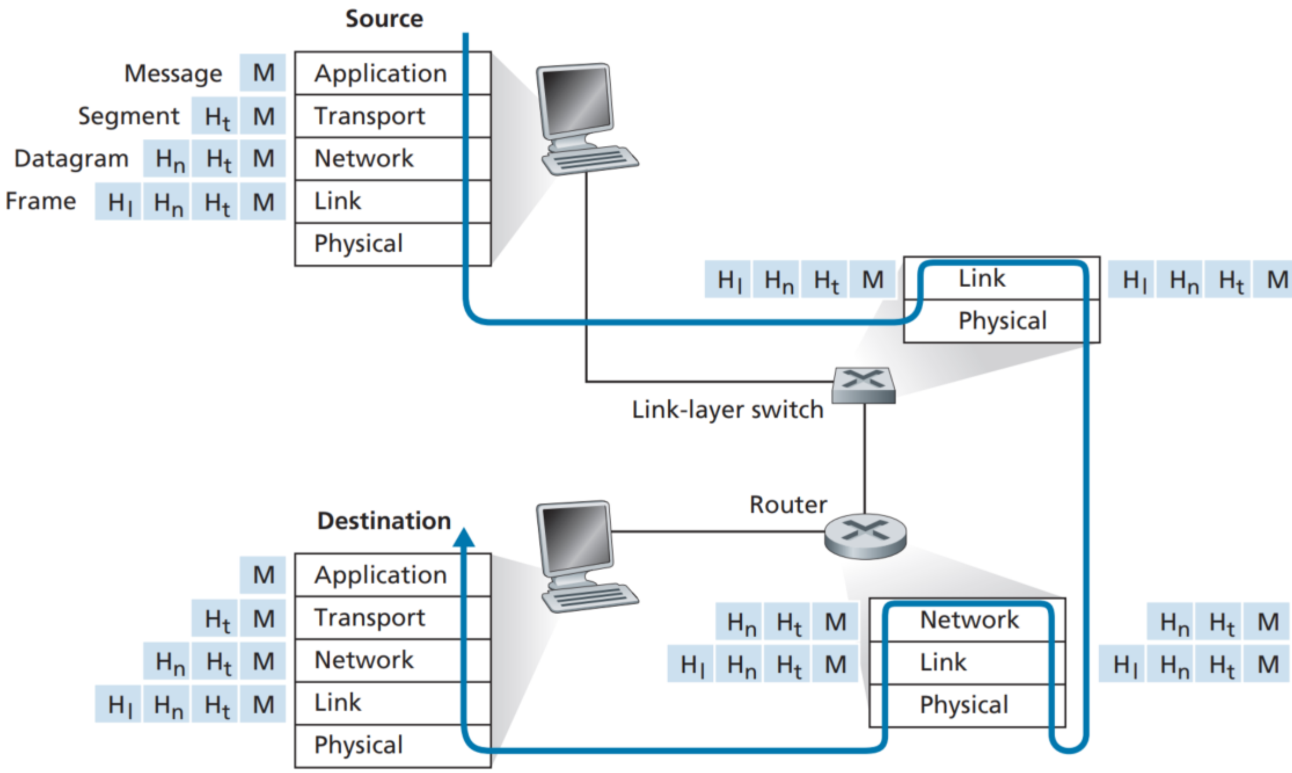


Figure 1.24 ♦ Hosts, routers, and link-layer switches; each contains a different set of layers, reflecting their differences in functionality

Network Security

Denial-of-Service (DoS) Attacks / Distributed DoS (DDoS) Attacks

Purposeful overloading of a server with requests (usually through multiple machines controlled by one attacker) to prevent legitimate access

Categories of DoS attacks

1. **Vulnerability attack**: Sending a few well-crafted messages to a vulnerable application or Operating System running on the targeted system, so if the right sequence of packets sent will stop service or crash the host system
2. **Bandwidth flooding**: Send a deluge of packets to the targeted host, so that the target's access link becomes clogged
3. **Connecting flooding**: Establishes a large number of half-open or fully open TCP connections at the target host, so the host system will become bogged down with bogus connections it will stop accepting ones from legitimate connections

Packet Sniffing

Intercept and copy packets via an application where unencrypted info can be displayed and inspected

IP Spoofing

Creation of packets with a modified source address to hide the identity of the sender or impersonate another sender

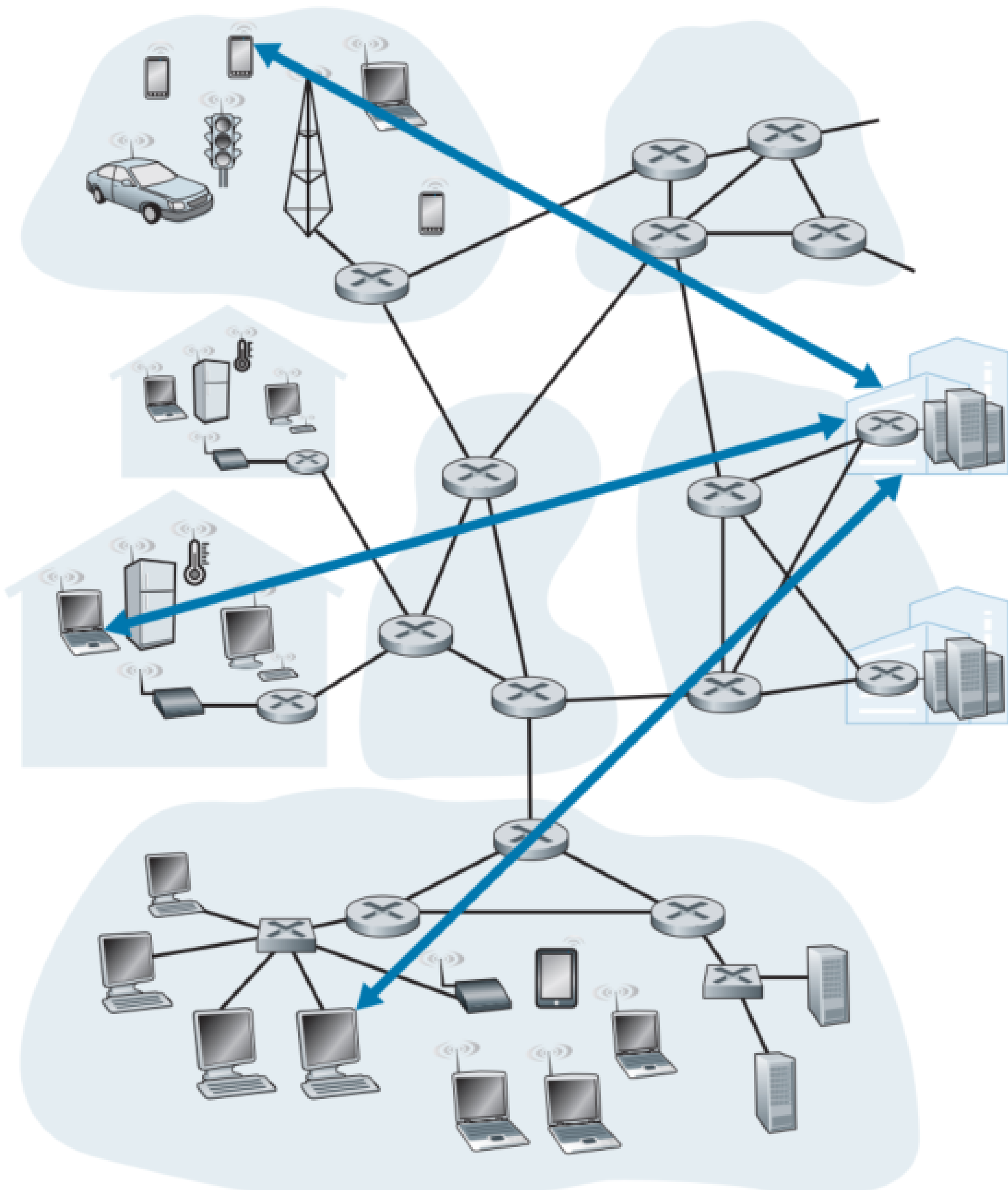
Chapter 02

Application Models

Client-server

Clients do not directly talk to each other and is mediated by an always-on host (a server)

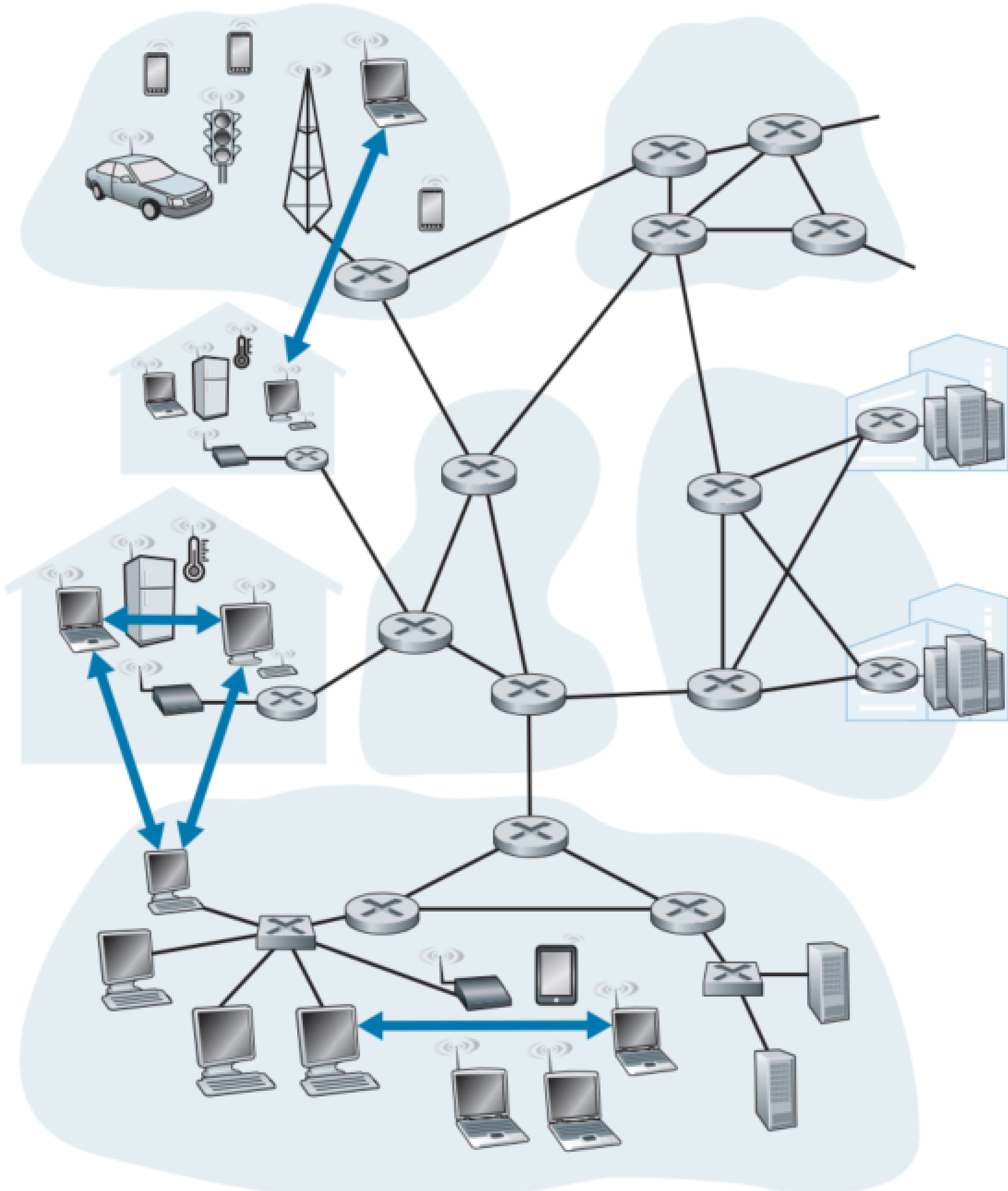
Managing a client-server connection is far simpler than Peer-to-Peer (P2P)



a. Client-server architecture

Peer-to-Peer (P2P)

In a P2P architecture, there is minimal (or no) reliance on dedicated servers in data centers. Instead the application exploits direct communication between pairs of intermittently connected hosts, called peers. The peers are not owned by the service provider, but are instead desktops and laptops controlled by users, with most of the peers residing in homes, universities, and offices.



b. Peer-to-peer architecture

Transport protocols -

There are two transport protocols **TCP** and **UDP**, and either of which can transport application-layer messages.

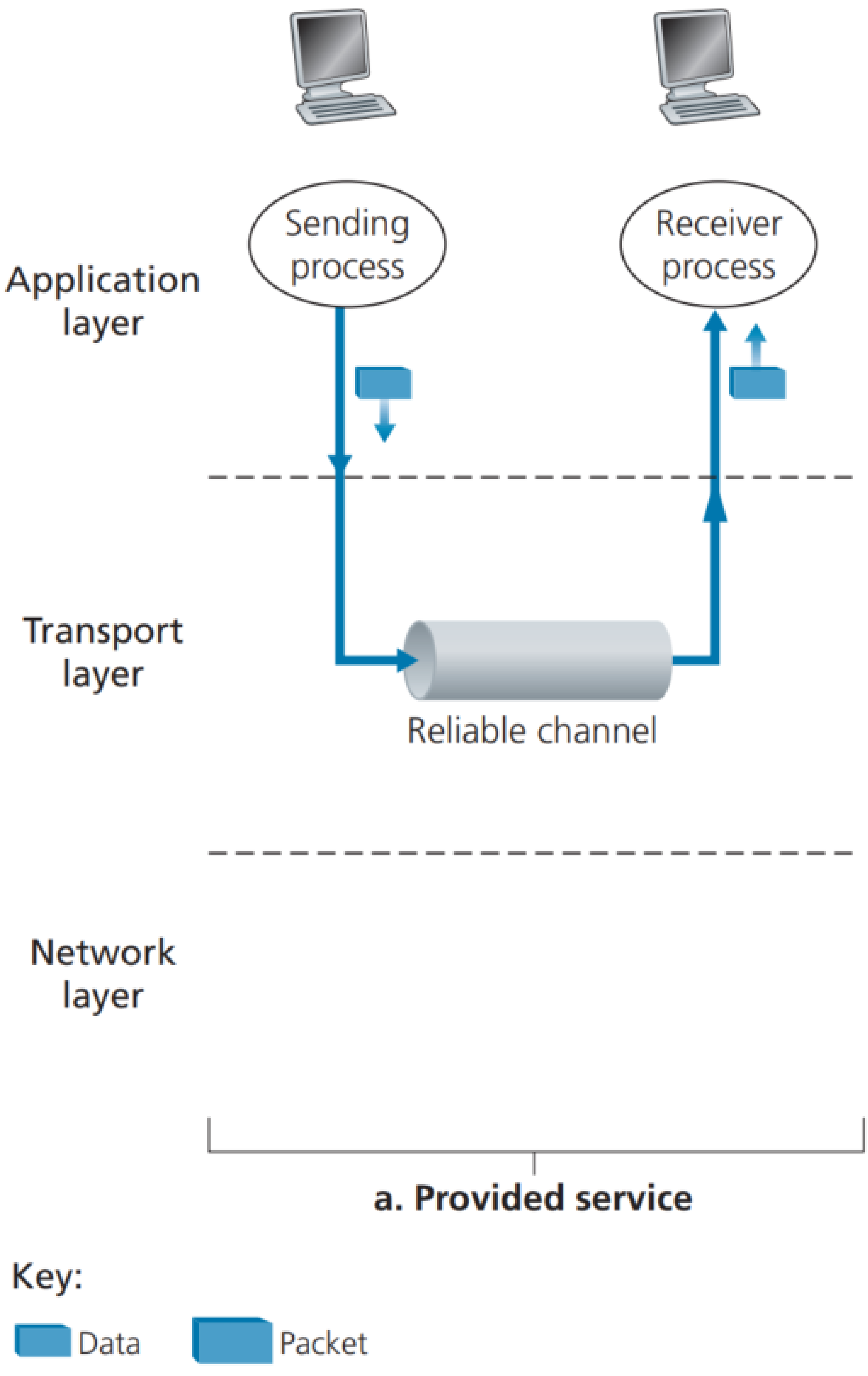
TCP

1. **TCP** provides a connection-oriented service to its applications.
2. **TCP** guaranties delivery of application-layer messages to the destination and flow control (sender/receiver speed matching)

3. **TCP** Breaks long messages into shorter segments and provides a congestion control mechanism
    1. so the source throttles its transmission rate when the network is congested

TL;DR

- Reliable transport
- Flow control; sender will not overwhelm receiver
- Congestion control; sender can be throttled
- No timing, security, or minimum throughput
- Setup is required to establish connection


Sending process
Receiver process
Application layer
Transport layer
Reliable channel
Network layer
a. Provided service
Key:
Data
Packet

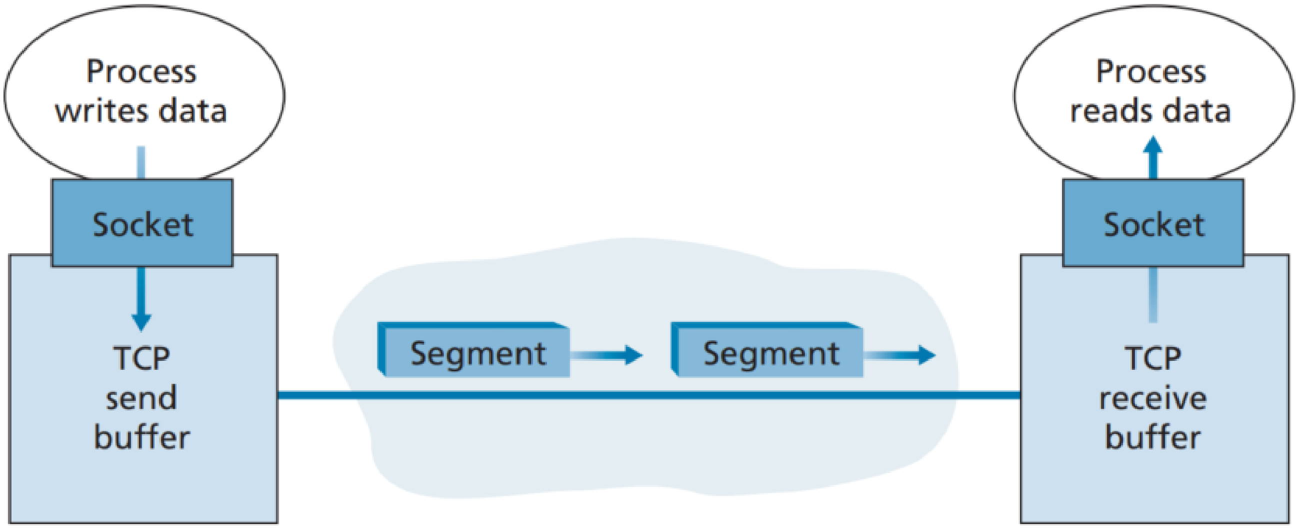


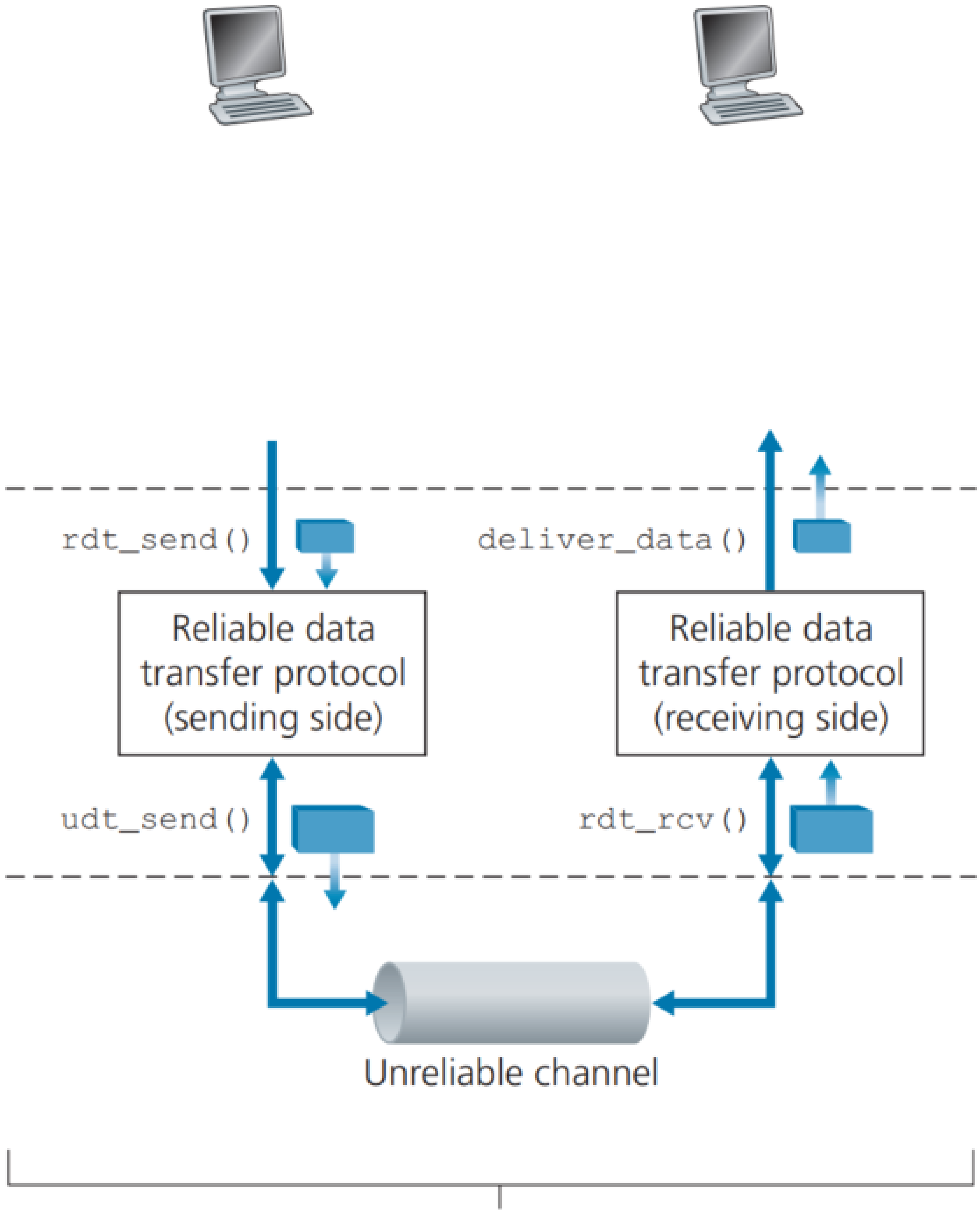
Figure 3.28 ♦ TCP send and receive buffers

UDP

1. **UDP** provides a connectionless service to its applications
2. **UDP** DOES NOT provide reliability, flow control, and congestion control

TL;DR

- Unreliable transport
- No flow control, congestion control, timing, minimum throughput, security, or setup



b. Service implementation

Web and HTTP-

HTTP protocol-

Persistence and non-persistence HTTP-

Cookies-

Web caches-

Conditional GET-

Electronic mail

Three major components

SMTP

Mail access protocols

SMTP vs HTTP

DNS

Definition

Services

Different Tiers of servers

Video Steaming

DASH: server and client

Content distribution networks

Chapter 03

Transport-layer services

Multiplexing and demultiplexing

UDP

Internet checksum

Rdt1.0 to 3.0

Pipelined protocols

Go-Back N

Selective repeat

TCP overview

Seq and ack

RTT

Retransmission

Flow control

3-way handshake

TCP congestion control

AIMD

RENO and Tahoe

ECN

Chapter 04 and Chapter 05

Forwarding and routing

Data plane and control plane

What’s inside a router

Longest prefix matching

Switching fabrics

IP datagram

IP addressing

Subnets

DHCP

NAT

IPv6 Format

Tunneling

Routing protocols

Classification

Link-state routing

Distance vector

Intra-AS routing (RIP, OSPF, IS-IS, IGRP)

Inter-AS routing (BGP)

Chapter 06

Link Layer

Error Detection (CRC)

Multiple Access protocols

TDMA and FDMA

Slotted ALOHA, Pure ALOHA, CSMA/CD

MAC addresses and ARP

Ethernet (switch)

Putting all together

Chapter 07

Wireless

Wireless links and network characteristics

WiFi

Cellular network: 4G LTE

Chapter 08

Network Security

Principles of cryptography

Symmetric key cryptography

Public Key Cryptography

Authentication, message integrity

Securing e-mail

Part 1: 15 Short-answer questions (carefully, briefly and clearly)

EXAMPLE

1. > What is the main reason that packet loss may occur in computer network?

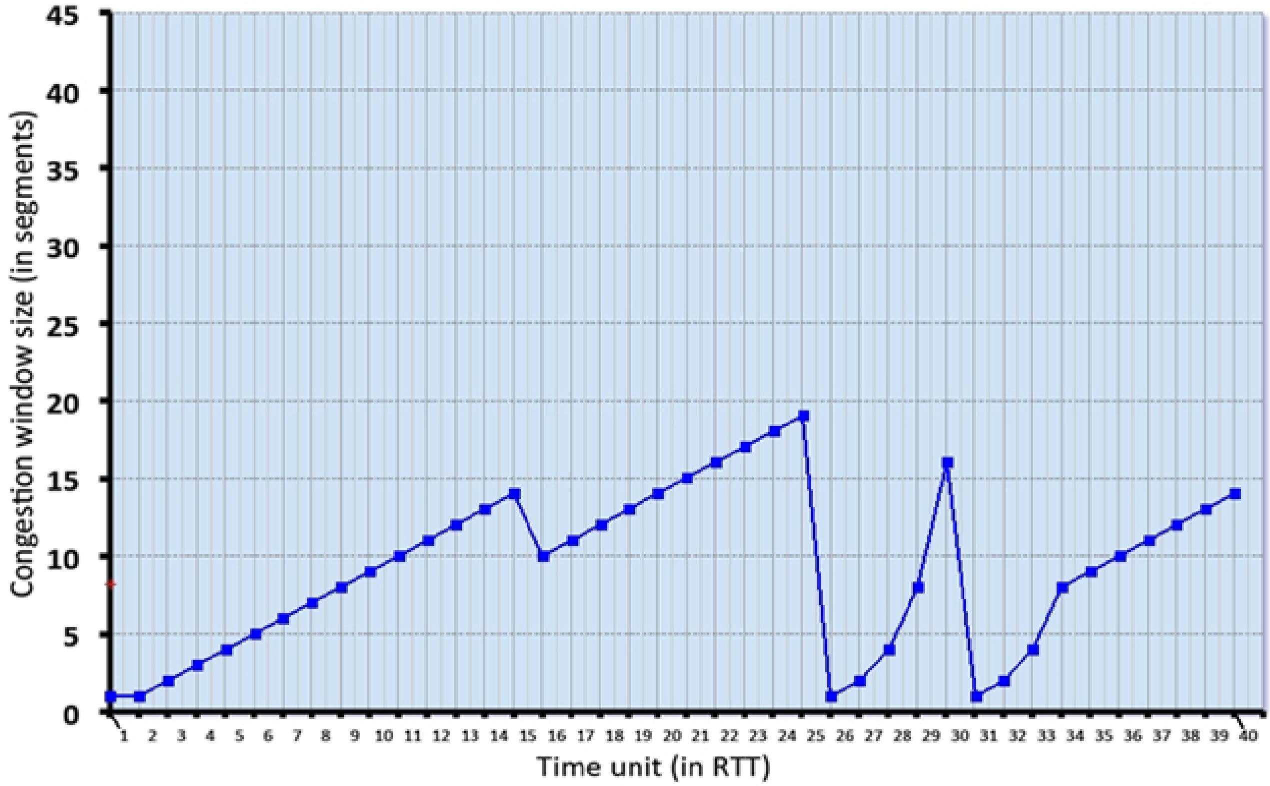
Part 2: 10 Multiple-choice questions (Single answer) please circle it

EXAMPLE

1. 5. Which of the following about SMTP is false?
   (a) It enables a mail server to send email messages to another mail server
   (b) User agent cannot use it to retrieve email
   (c) It typically uses a connectionless protocol such as UDP
   (d) Unlike FTP it uses a single port number

Part 3: 5 Long-answer questions

EXAMPLE

1. 

2) Consider the Cyclic Redundancy Check (CRC) algorithm discussed in Section 5.2.3 of the text. Suppose that the 4-bit generator (G) is 1001, that the data payload (D) is 10011101 and that r=3. What are the CRC bits R?

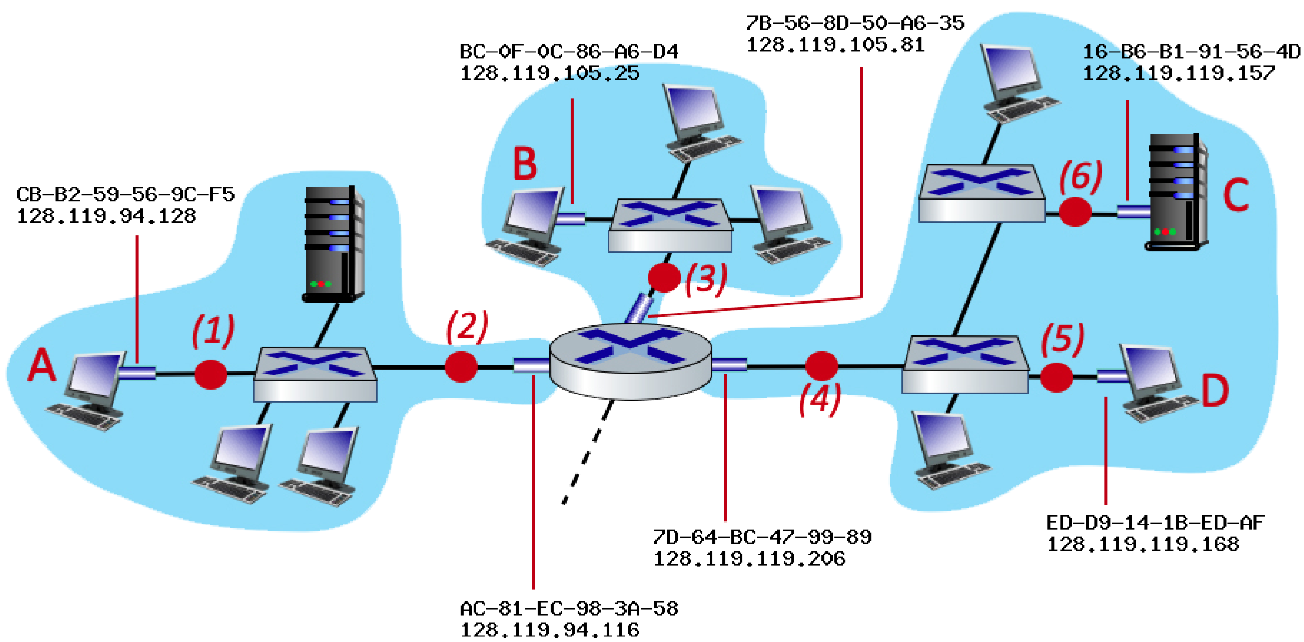
Recall from the text that in calculating the CRC bits, all CRC calculations are done in modulo-2 arithmetic without carries in addition or borrows in subtraction. This means that addition and subtraction are identical and both equal to the bitwise exclusive-OR (XOR) of the operands.

To compute the CRC, we begin by taking the value of D, 10011101, and multiplying it by 2^3, giving 10011101000. We then divide this number by the generator bits [G] = 1001, using modulo-2 arithmetic. The final remainder, R, after this division are then the CRC bits. Here is that calculation:

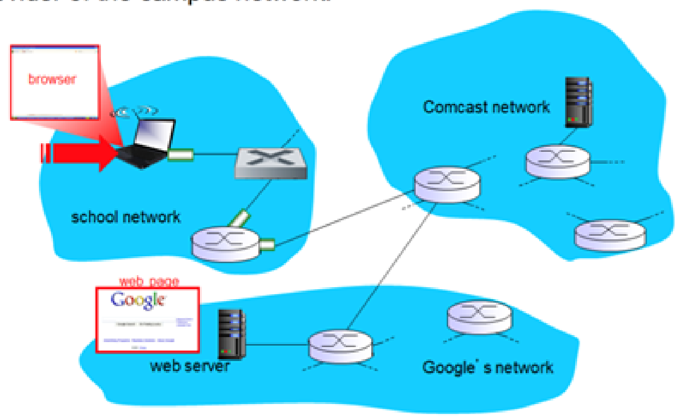
```
        10001100
      -------------
1001 ) 10011101000
       1001
       ----
          1101
          1001
          ----
           1000
           1001
           ----
             100------->R
```

We've computed the remainder as R = 100 and the quotient n = 10001100. You should verify that n*G XOR R is indeed equal to 10011101000. You can use [this calculator] to do the modulo-2 arithmetic if you don't want to do it by hand.

3) The IP and MAC addresses are shown for nodes A, B, C and D, as well as for the router interfaces. Consider an IP datagram being sent from NODE C to NODE B. Give the source and destination Ethernet address, as well as the source and destination address of the IP datagram encapsulated within the Ethernet frame at points `(6)`, `(4)`, and `(3)` in the figure



Let's use the following scenario to journey down the protocol stack completely: a student attaches laptop to campus network, requests the homepage from www.google.com web server. Suppose Comcast is the Internet Service Provider of the campus network.



5.

Bob chooses $p=5$, $q=7$. Then $n=35$, $z=24$.

$e=5$ (so e, z relatively prime).

$d=29$ (so $ed-1$ exactly divisible by z).

encrypting 8-bit messages.

encrypt:	bit pattern	m	m^e	$c = m^e \bmod n$
	00001000	12	24832	17
decrypt:	c	c^d		$m = c^d \bmod n$
	17	481968572106750915091411825223071697		12

6.

---

course:

- CSC 138-06 - Computer Network Fundamentals

HELPFUL RESOURCE:

https://gaia.cs.umass.edu/kurose_ross/interactive/index.php
