



Wireless Communication Networks & Systems

Spring 2025

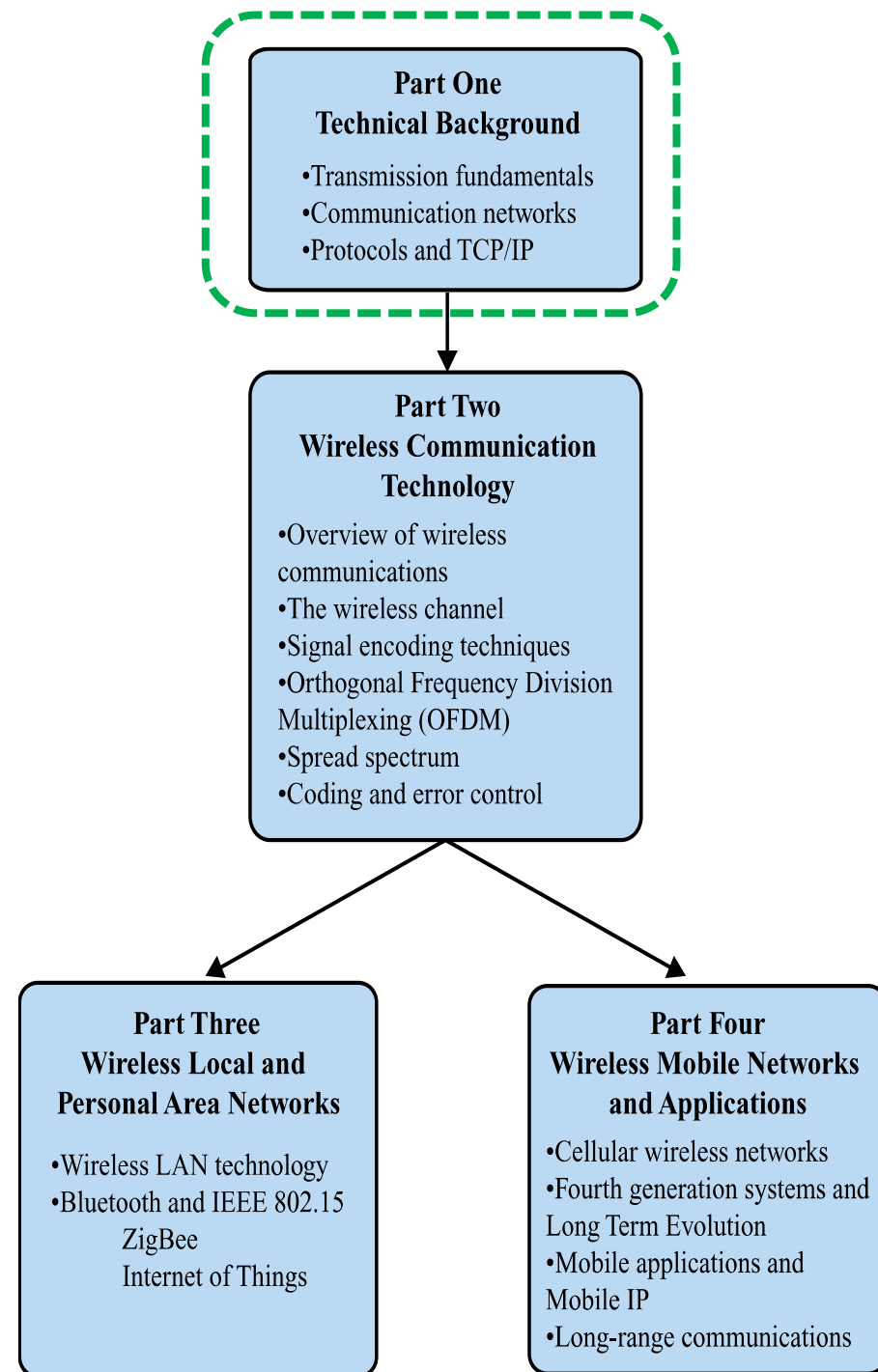
Week No. 02

Course Learning Outcomes (CLOs):




CLO # 01	Demonstrate an in-depth understanding of wireless network system's architecture, protocols, and Services.	Cog. 3
CLO # 02	Explore advanced technologies and features in wireless networks related to coverage, capacity, interference management, and mobility.	Cog. 3
CLO # 03	Examine the evolution of Wi-Fi networks, highlighting architectural differences across its various standards.	Cog. 4
CLO # 04	Analyze key cellular concepts used in cellular networks and the architectural advancements in 5G and beyond.	Cog. 4

WCNS Module- I



Textbook Reference

Module 01- Technical Background of Wireless Networks

- Chapter 02 – The Signals and Transmission Fundamentals
-  ▪ Chapter 03 – Communication Networks and QoS
- Chapter 04 – TCP/IP Network Model and & Admission/congestion Control

The Signals and Transmission Fundamentals

Quick recap of last week:

LEARNING OBJECTIVES

After studying this chapter, you should be able to:

- Distinguish between digital and analog information sources.
- Explain the various ways in which audio, data, image, and video can be represented by electromagnetic signals.
- Discuss the characteristics of analog and digital waveforms.
- Explain the roles of frequencies and frequency components in a signal.
- Identify the factors that affect channel capacity.
- Compare and contrast various forms of wireless transmission.

The Communication Networks

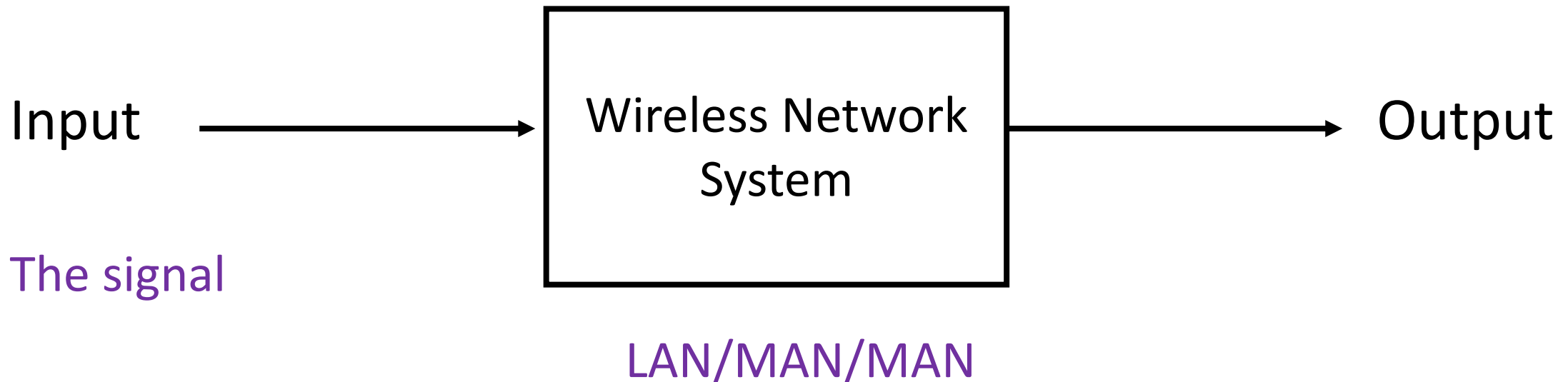
LEARNING OBJECTIVES

After studying this chapter, you should be able to:

- Explain the roles and scope of wide, local, and metropolitan area networks.
- Define circuit switching and describe the key elements of circuit-switching networks.
- Define packet switching and describe the key elements of packet-switching technology.
- Discuss the relative merits of circuit switching and packet switching and analyze the circumstances for which each is most appropriate.

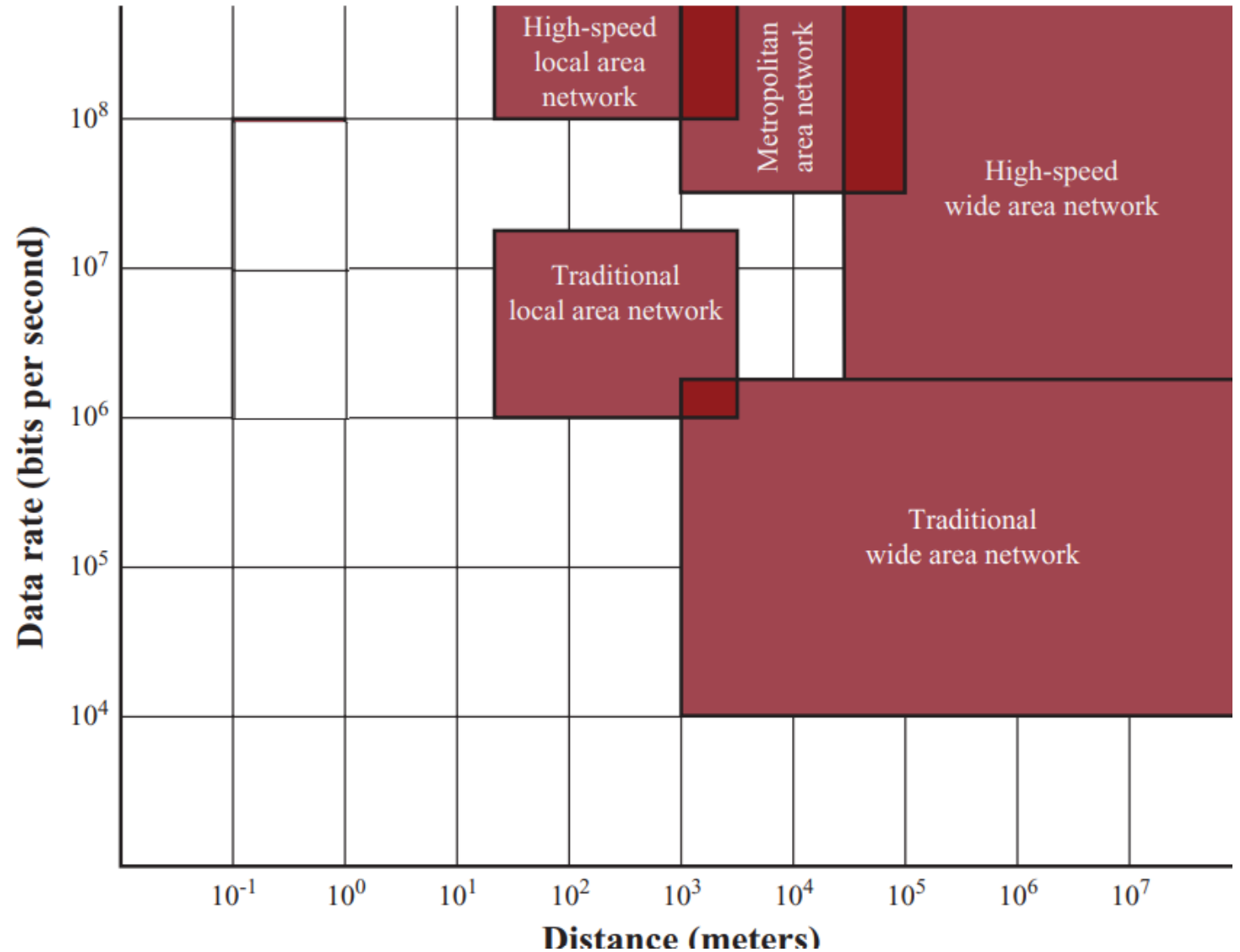
Wireless Networks Systems

- Input
- Output
- System's Main building Blocks



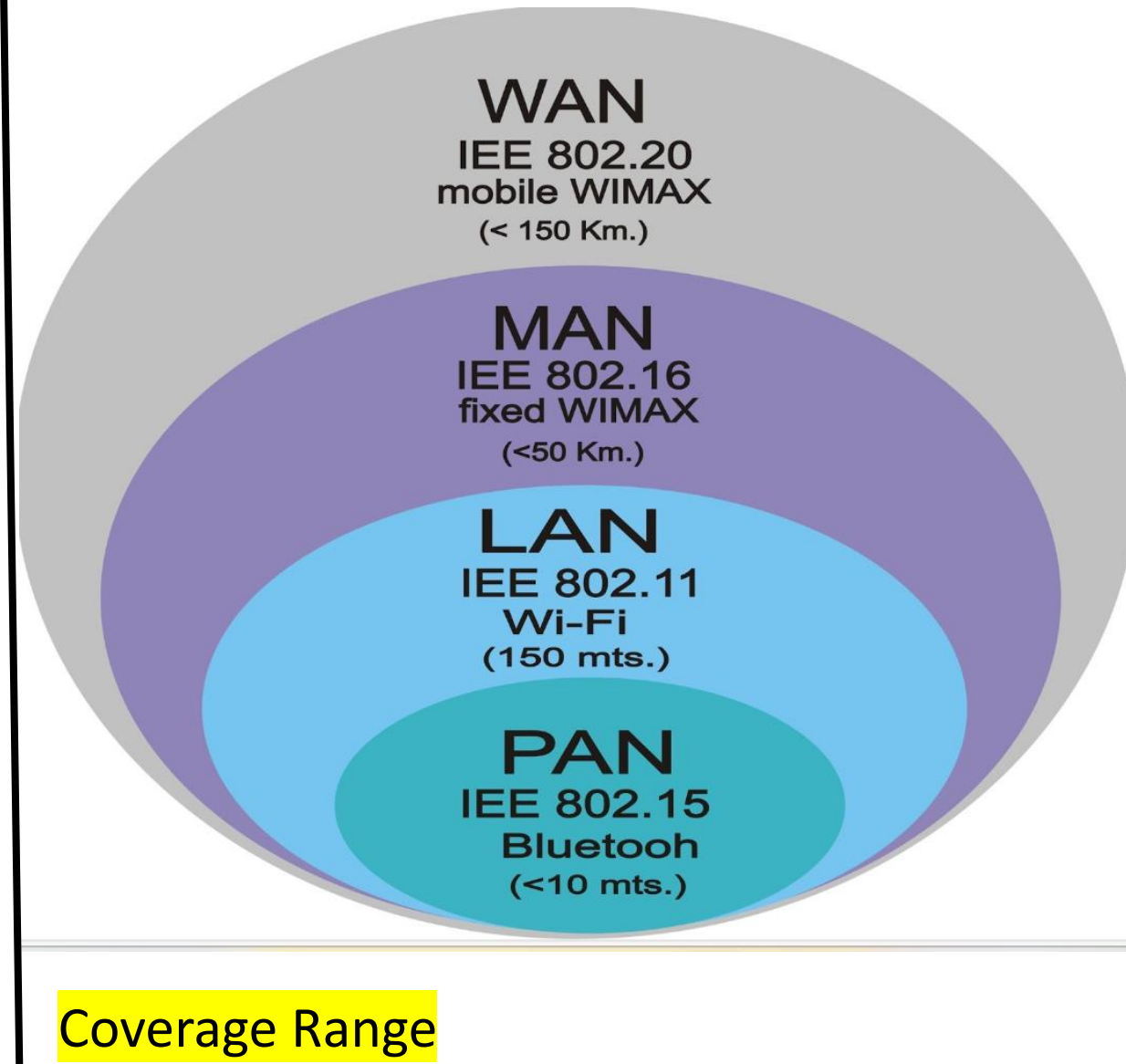
LAN, MAN, AND WAN

Local area networks (LANs), metropolitan area networks (MANs), and wide area networks (WANs) are all examples of communications networks.



LAN, MAN, AND WAN

- Traditional
 - Traditional local area network (LAN)
 - Traditional wide area network (WAN)
- Higher-speed
 - High-speed local area network (LAN)
 - Metropolitan area network (MAN)
 - High-speed wide area network (WAN)



Typical use cases

LAN:

- **Office Network:** Connecting computers, printers, and servers within an office or building.
- **Home Network:** Providing internet connectivity and connecting devices such as computers, smartphones, and smart appliances in a household.

MAN:

- **Connecting Multiple Branch Offices:** Interconnecting branch offices of businesses or organizations within a metropolitan area.
- **Public Safety Systems:** Connecting emergency services, such as police, fire, and healthcare facilities, across a city for coordinated responses.

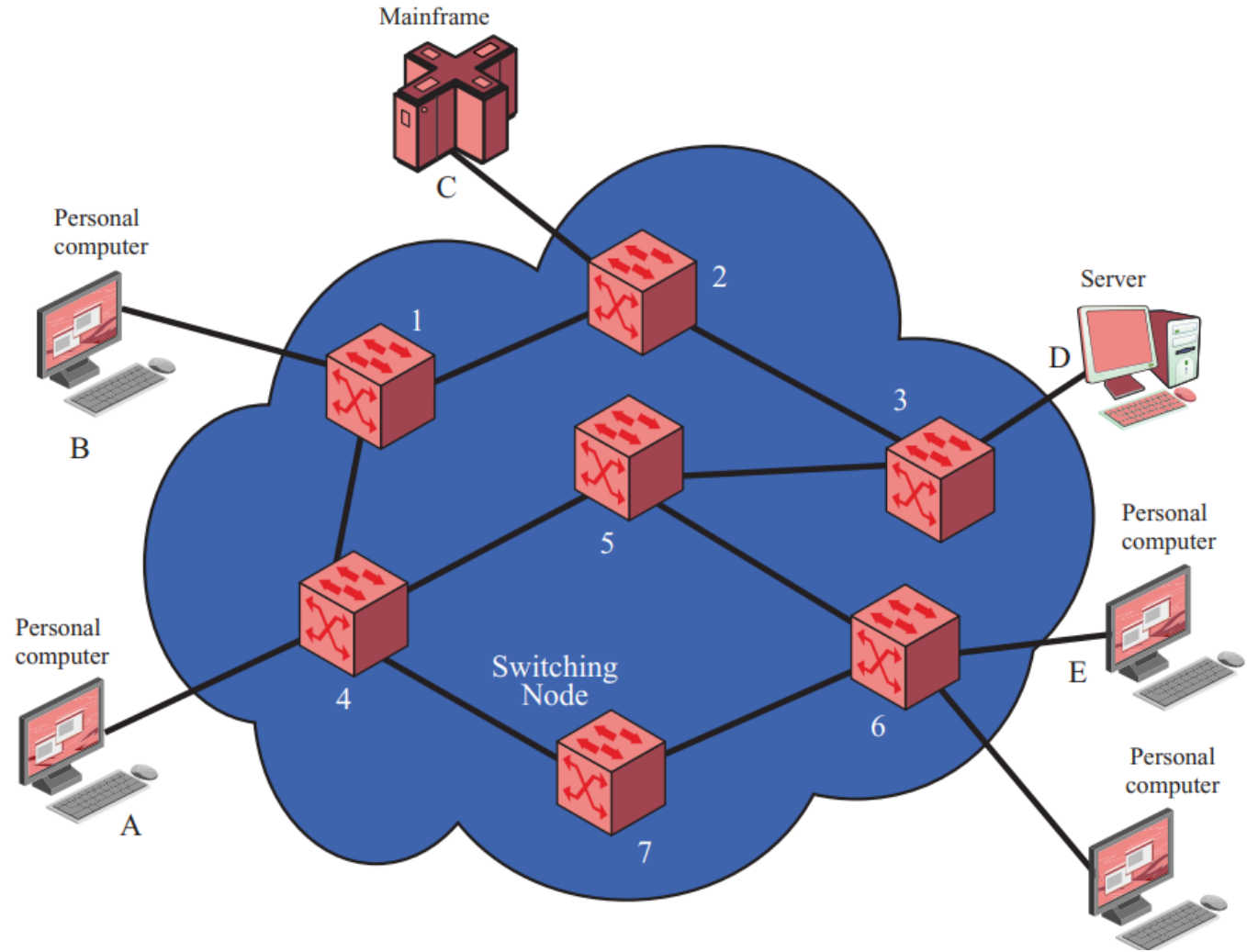
WAN:

- **Global Business Connectivity:** Connecting offices, data centers, and remote workers across cities, countries, or continents for large organizations.
- **Internet Backbone:** Providing long-distance connectivity between ISPs and major internet exchange points.

Switching Techniques

Switching Techniques:

- For transmission of data beyond a local area, communication is typically achieved by transmitting data from source to destination through a network of intermediate switching nodes.
- The switching nodes will move the data from node to node until they reach their destination.
- Two quite different technologies are used in wide area switched networks: **circuit switching** and **packet switching**.

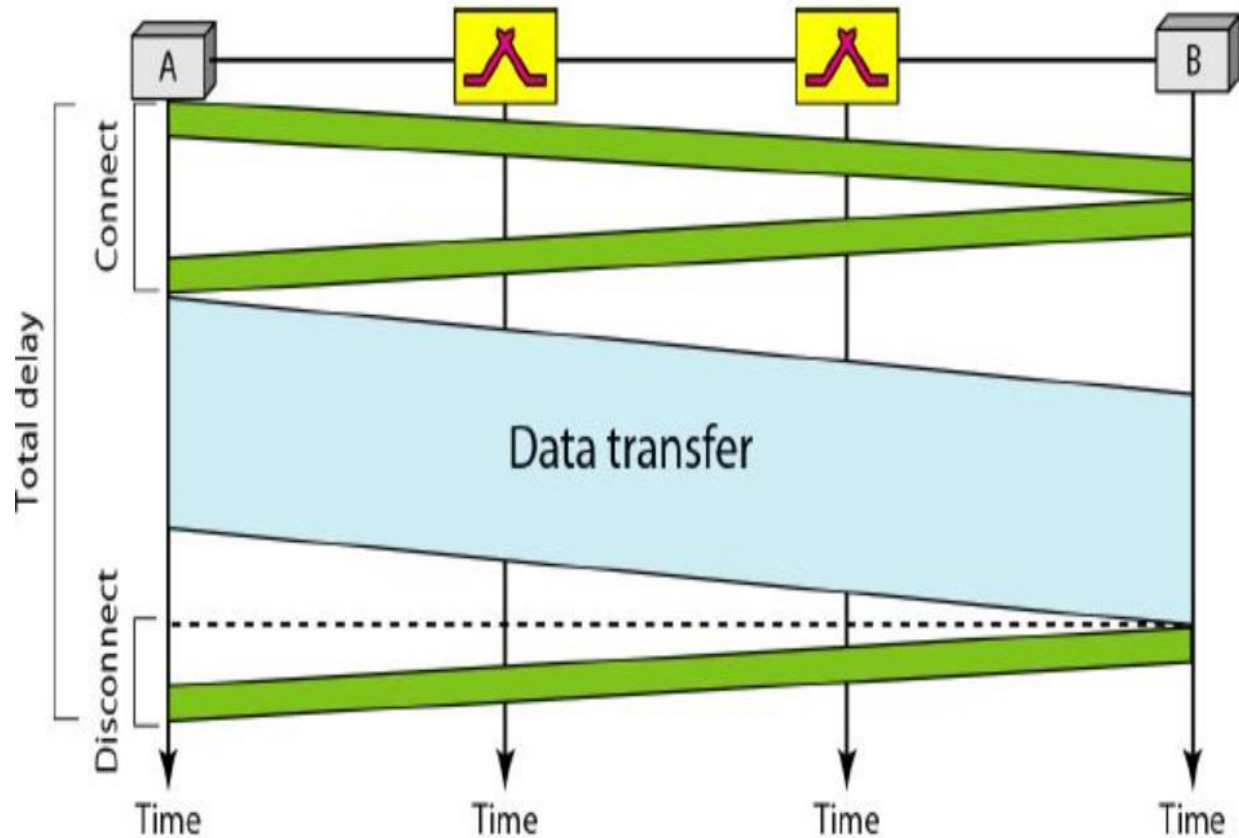


Techniques Used in Switched Networks

- Circuit switching
 - Dedicated communications path between two stations
 - E.g., public telephone network, Voice call on Mobile phones
- Packet switching
 - Message is broken into a series of packets, each switching node determines next leg of transmission for each packet
 - E.g., Internet

Circuit Switching

- Circuit establishment
 - An end to end circuit is established through switching nodes
- Information Transfer
 - Information transmitted through the network
 - Data may be analog voice, digitized voice, or binary data
- Circuit disconnect
 - Circuit is terminated
 - Each node deallocates dedicated resources



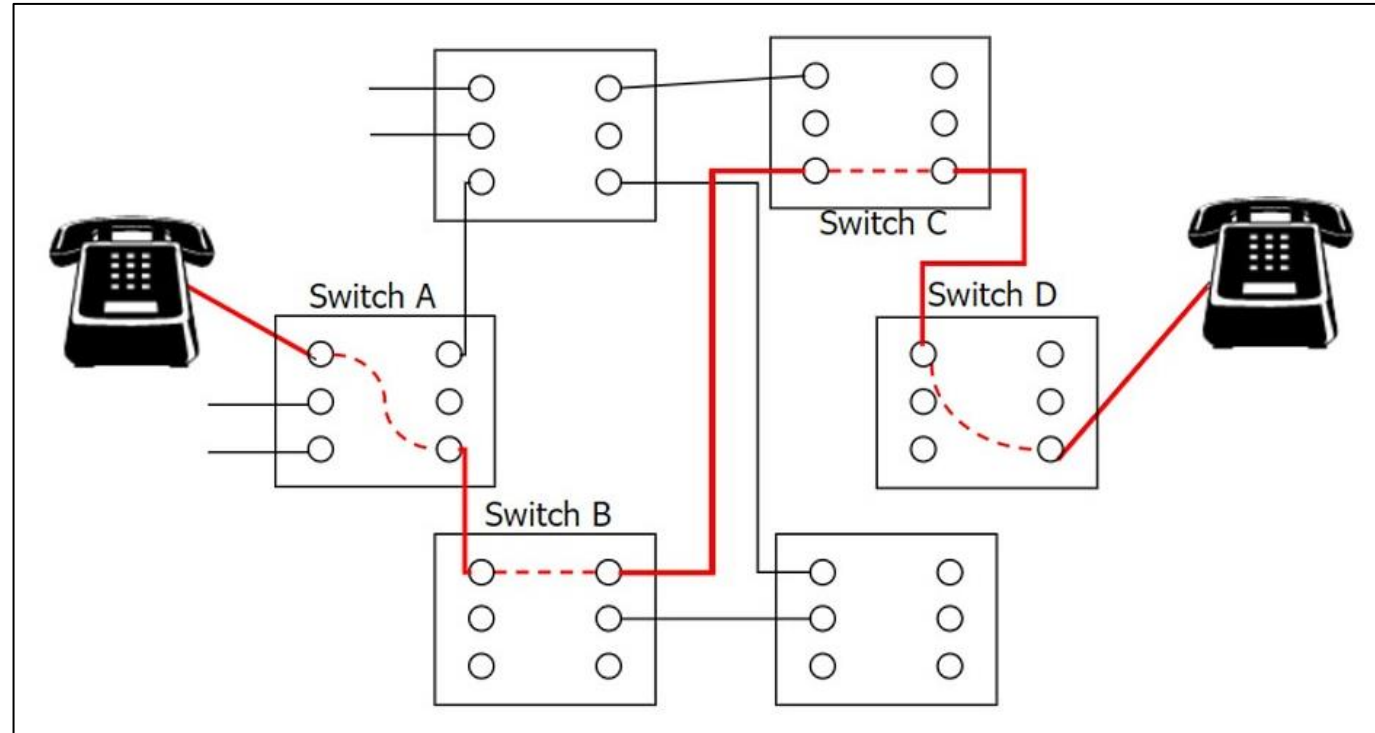
Circuit Switching

Cons:

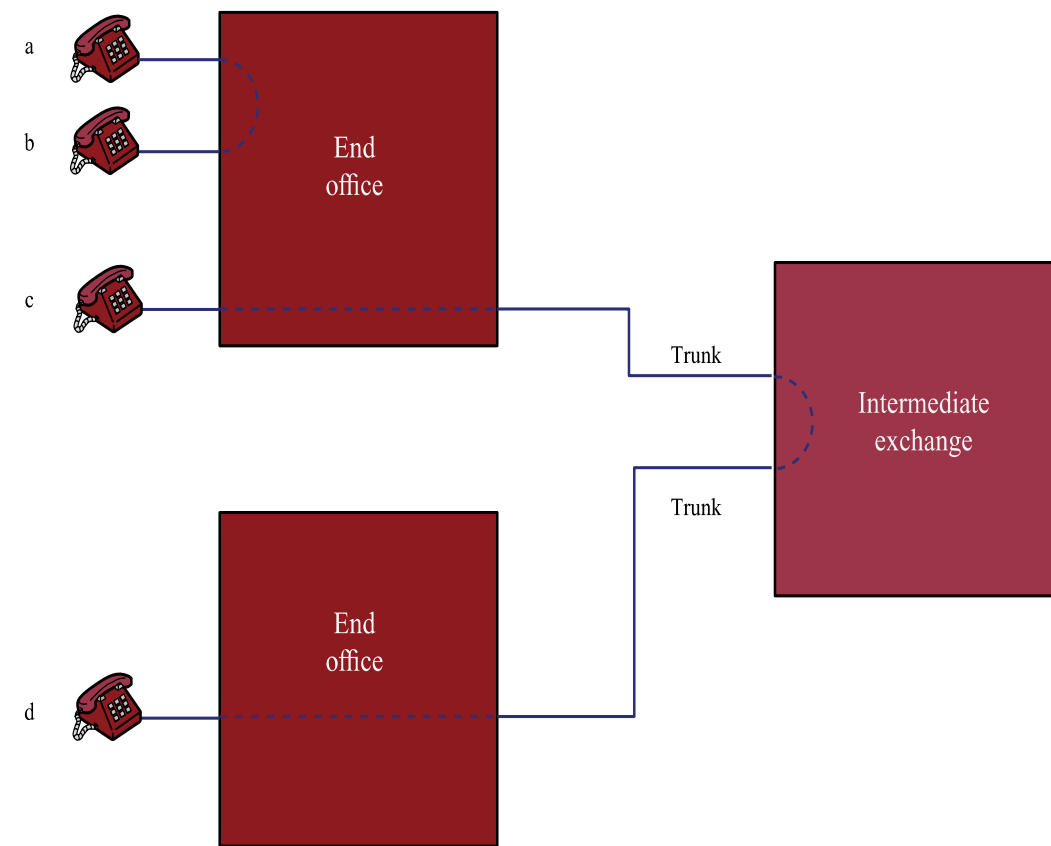
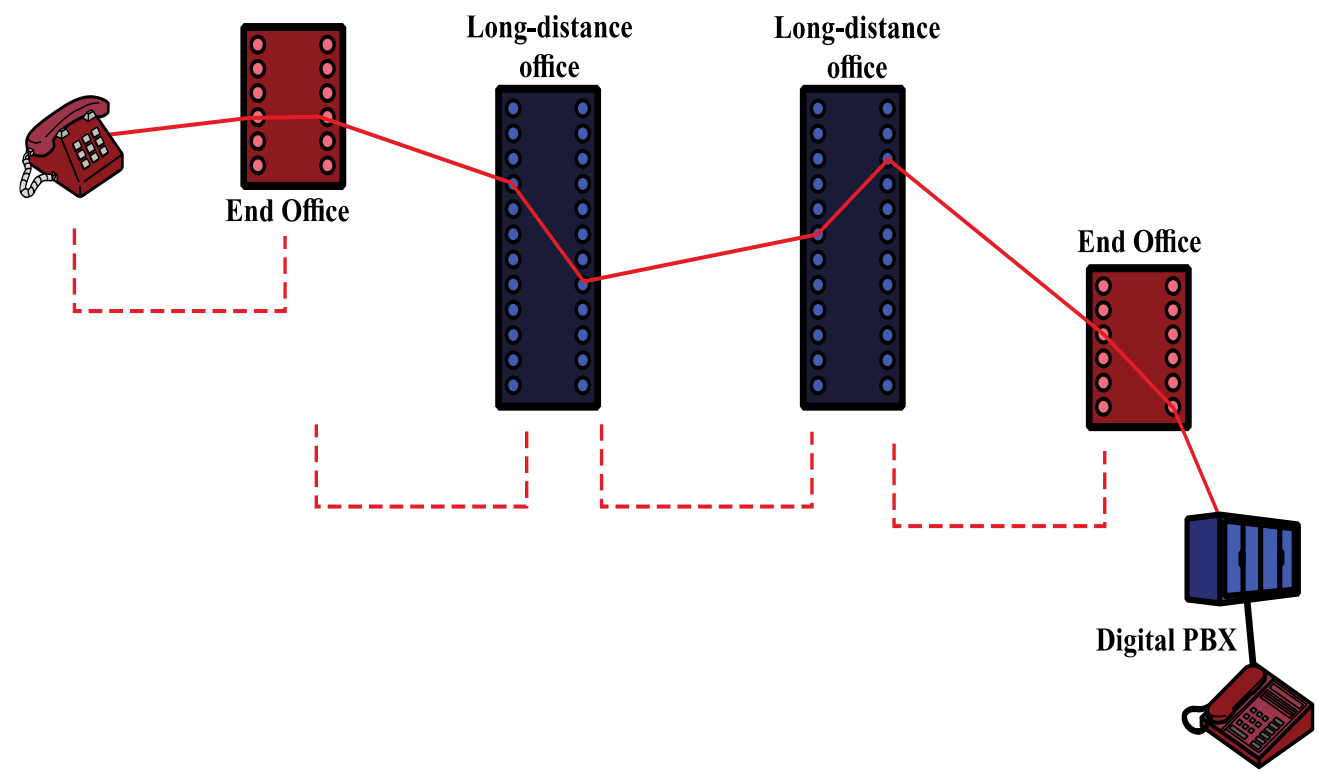
- Channel capacity dedicated for the duration of the connection
- Utilization not 100%
- Delay prior to signal transfer for establishment

Pros:

- Information transmitted at a guaranteed fixed rate.

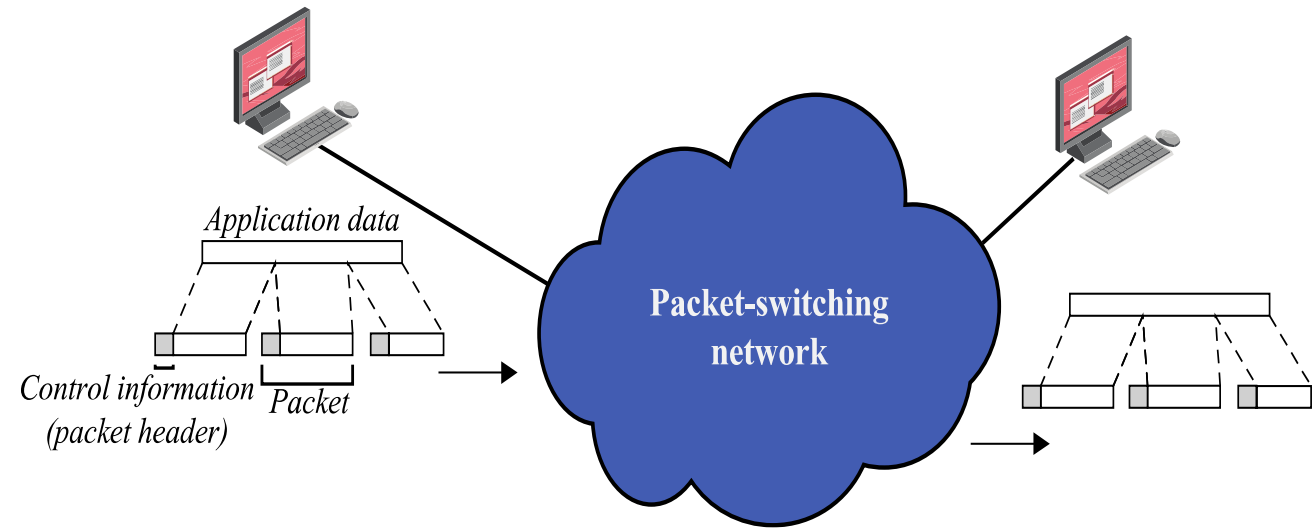


Circuit Switching



Packet Switching

- Data is transmitted in blocks, called packets
- Before sending, the message is broken into a series of packets
- Packets consist of a portion of data plus a packet header that includes control information
- At each switching node, packet is received, stored briefly and passed to the next node



Packet Switching

- Line efficiency is greater
 - Many packets over time can dynamically share the same node-to-node link
- Packet-switching networks can carry out data-rate conversion
 - Two stations with different data rates can exchange information
- Unlike circuit-switching networks that block calls when traffic is heavy, packet-switching still accepts packets, but with increased delivery delay
- QoS is used to meet specific requirements of the user/application.

A packet-switched network can use two different approaches to route the packets:

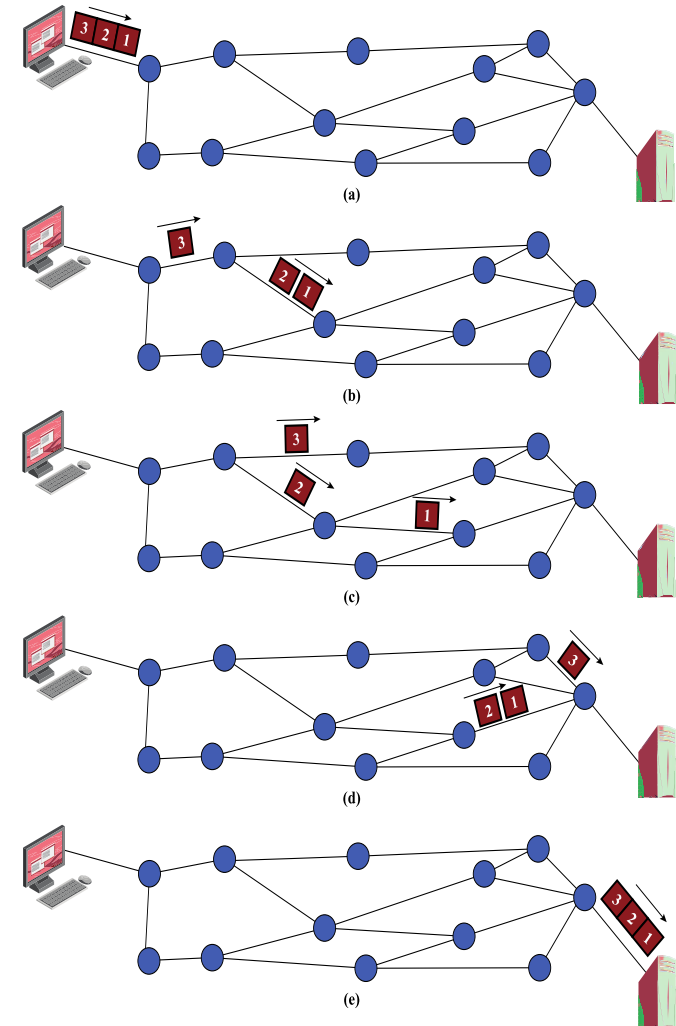
1. The datagram approach
2. The virtual-circuit approach.

Packet Switching: Datagram Approach

- Each packet is treated independently, without reference to previous packets. Each node chooses the next node on the packet's path
- Packets don't necessarily follow same route and may arrive out of sequence
- Responsibility of exit node or destination to detect loss of packet and how to recover
- The Delivery of packets from the source to the destination is with **BEST EFFORT QoS**

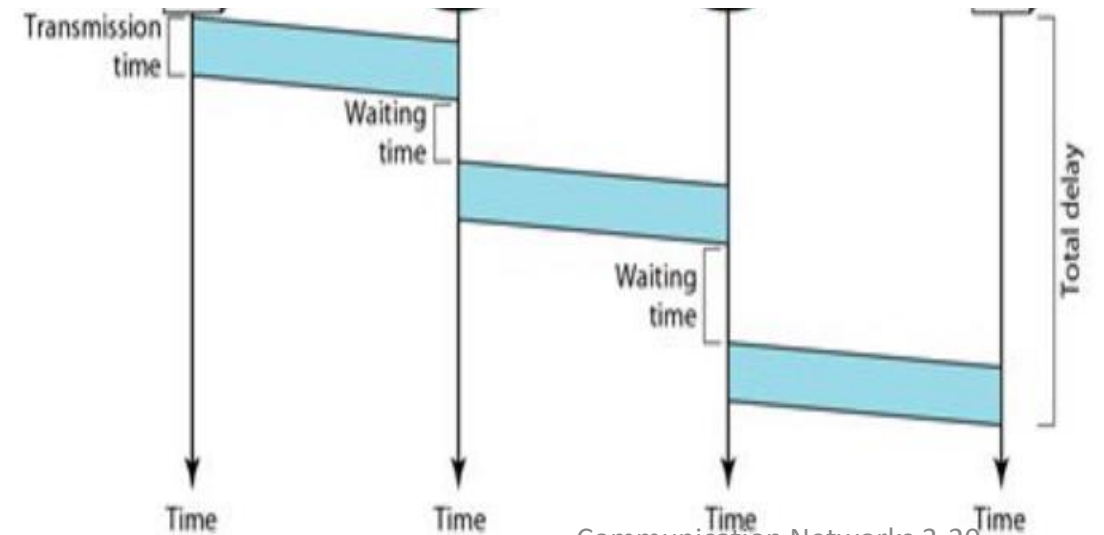
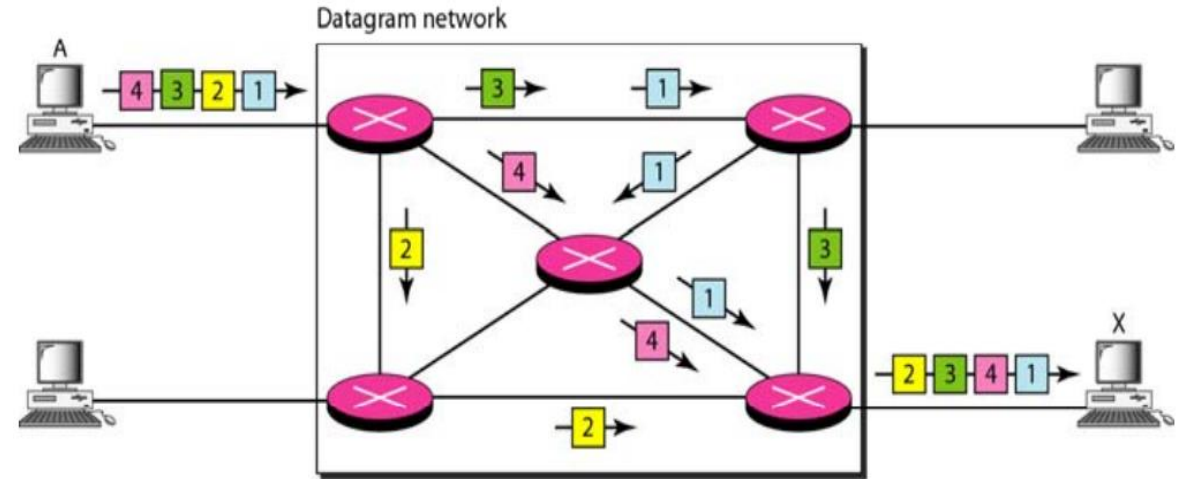
Advantages:

- Call setup phase is avoided
- Flexible and scalable



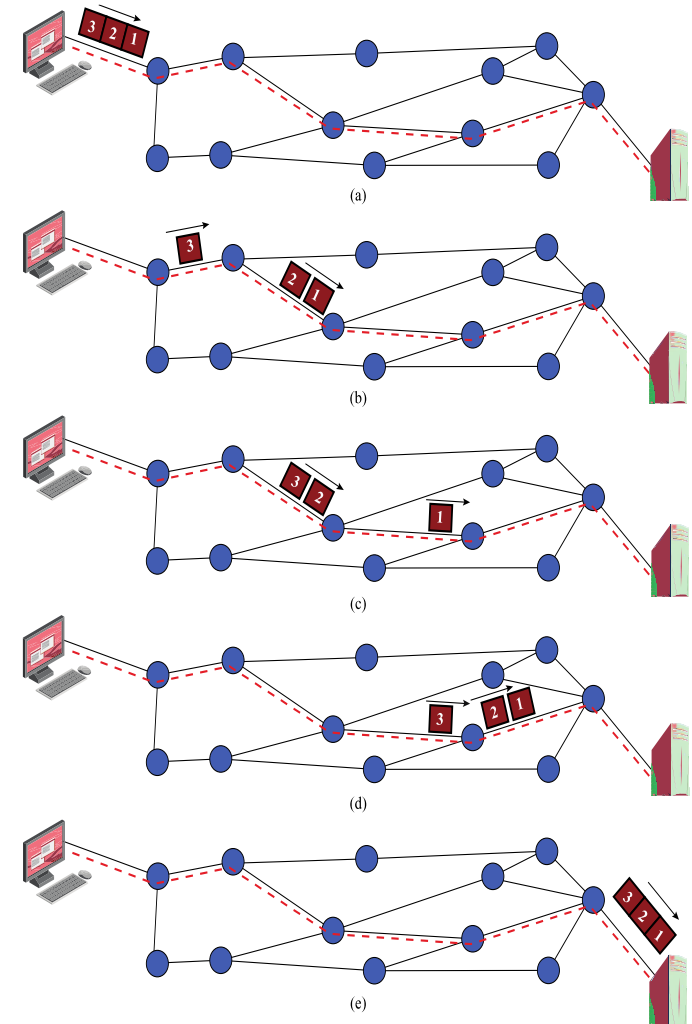
Packet Switching: Datagram Approach

- Each packet-switching node introduces a delay
- Overall packet delay can vary substantially, this is referred to as jitter
- Each packet requires overhead information includes destination and sequencing information it reduces communication capacity
- More processing required at each node



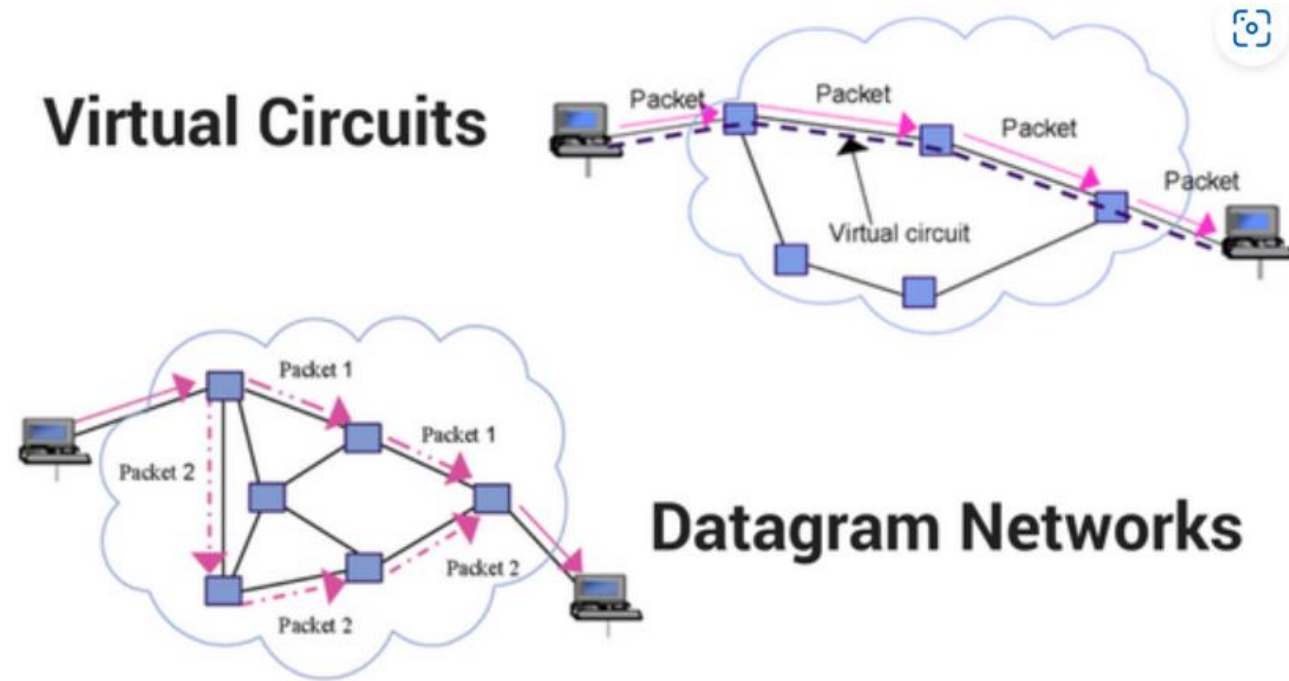
Packet Switching: Virtual Circuit Approach

- Preplanned route established before packets sent
- All packets between source and destination follow this route
- Routing decision not required by nodes for each packet
- Emulates a circuit in a circuit switching network but is not a dedicated path but packets still buffered at each node and queued for output over a line



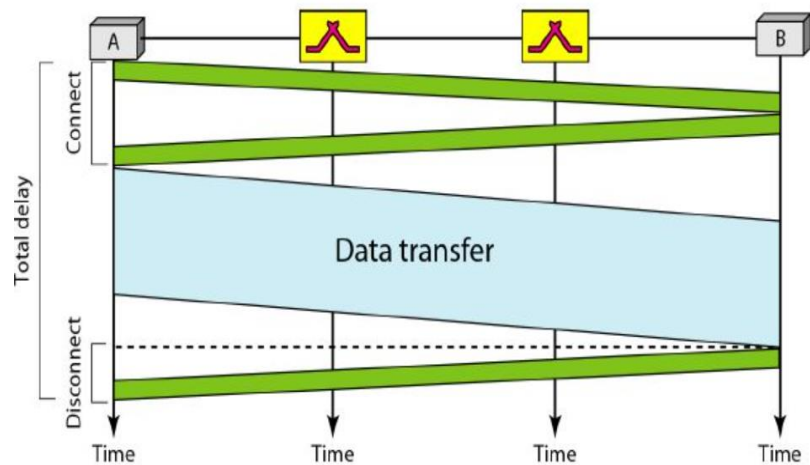
Packet Switching: Virtual Circuit Approach

- In a connection-oriented service (also called virtual-circuit approach), there is a relationship between all packets belonging to a message.
- Before all datagrams in a message can be sent, a virtual connection should be set up to define the path for the datagrams. After connection setup, the datagrams can all follow the same path.
- Advantages:
 - Packets arrive in original order
 - Packets arrive correctly
 - Packets transmitted more rapidly without routing decisions made at each node

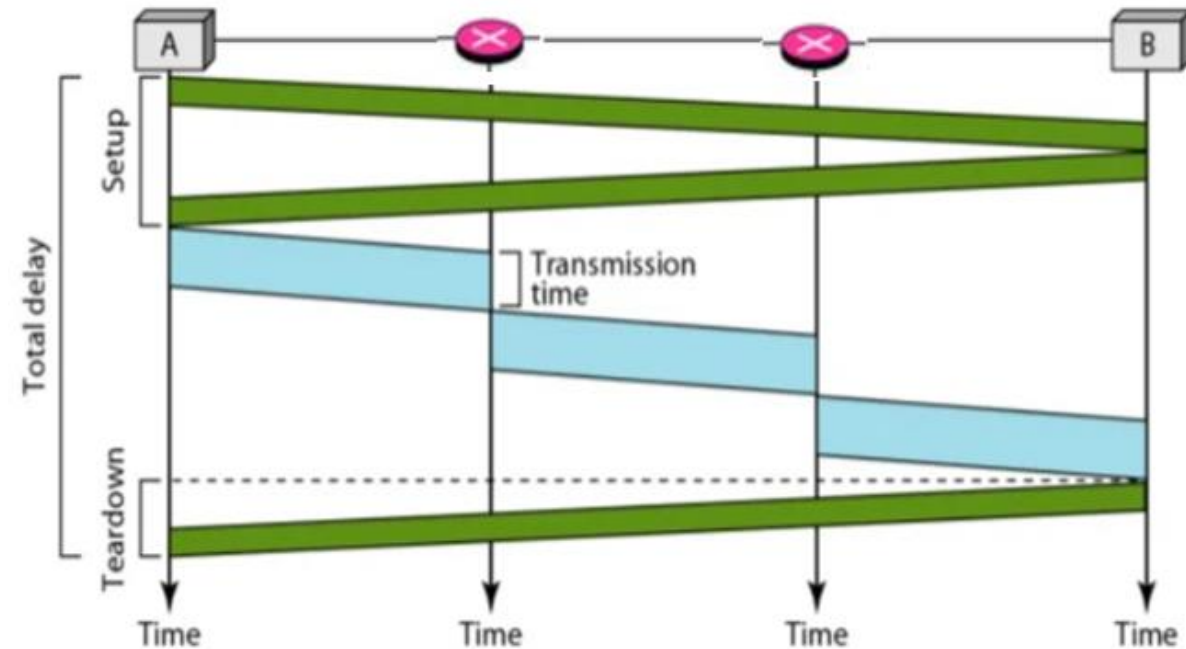
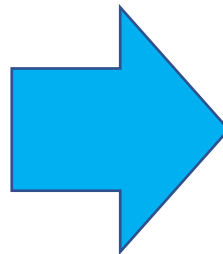
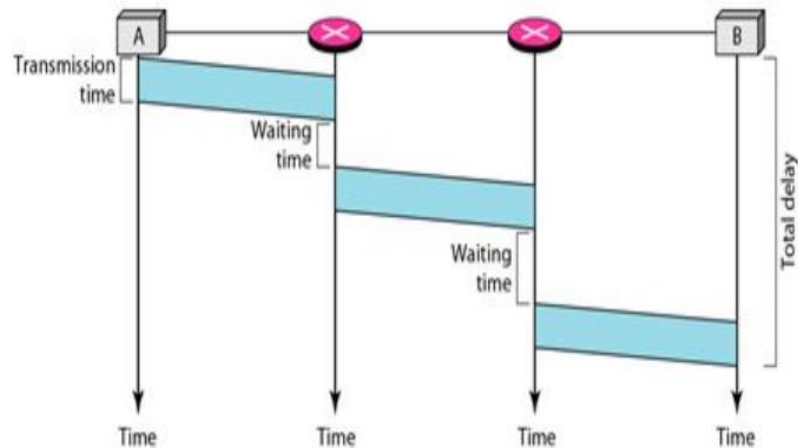


Packet Switching: Virtual Circuit Approach

CS



PS



In VC, resource availability is checked during the setup phase to avoid waiting time. Then, the resource can be reserved on demand during data transfer mode.


Packet Switching: Virtual Circuit Approach

- Unlike PS, where each data packet is treated independently, Virtual Circuit Networks establish a **predetermined** "virtual circuit" between sender and receiver for the duration of a session.
- In VC, a connection is established before data transfer begins which involves allocating resources (bandwidth, buffer spaces), and verifying the availability of the route between the sender and receiver. This ensures **guaranteed quality of service (QoS)** for the data transfer unlike the 'Best effort' PS scenario.
- Virtual Circuit networks guarantee that data packets will arrive at the destination in the **same order** they were sent this ensures predictability.
- Virtual Circuit Networks are very efficient for certain types of services having **predictable and constant data flows** such as voice and video streaming.
- For critical data transfers, where low latency and guaranteed delivery are essential, VCs can be employed to establish dedicated communication paths.

End of Session # 01

Textbook Reference

Module 01- Technical Background of Wireless Networks

- Chapter 02 – The Signals and Transmission Fundamentals
-  ▪ Chapter 03 – Communication Networks and QoS
- Chapter 04 – TCP/IP Network Model and Admission/congestion Control

The Communication Networks

LEARNING OBJECTIVES

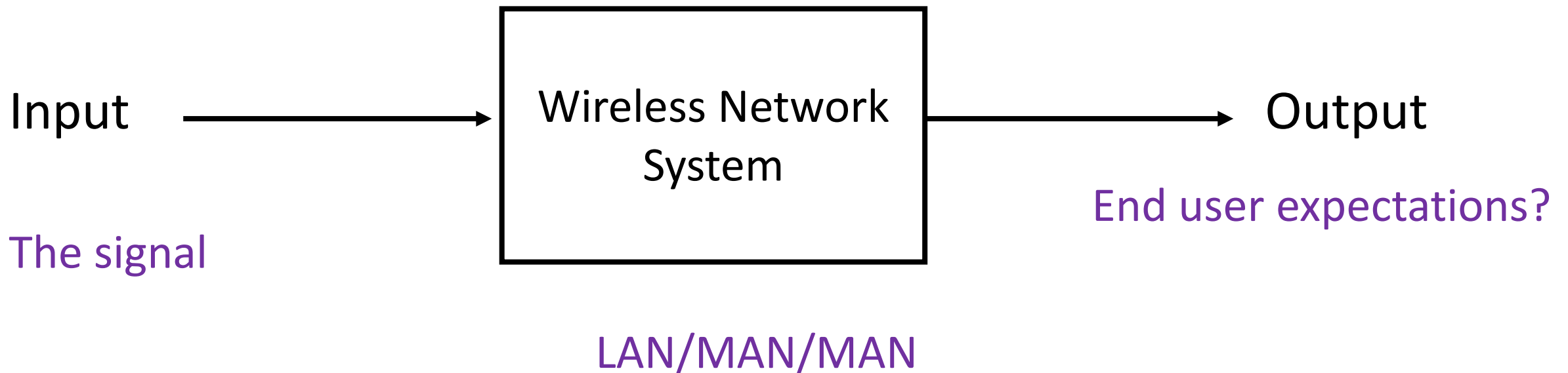
After studying this chapter, you should be able to:

- Explain the roles and scope of wide, local, and metropolitan area networks.
- Define circuit switching and describe the key elements of circuit-switching networks.
- Define packet switching and describe the key elements of packet-switching technology.
- Discuss the relative merits of circuit switching and packet switching and analyze the circumstances for which each is most appropriate.

Output of the Wireless Networks

Wireless Networks Systems

- Input
- Output
- System's Main building Blocks



Wireless Networks Systems - Output

- High Data rate - throughput
- Low delay
- High reliability, availability of good signals
- High reliability, low packet drop rate
- Support to provide a large number of users, Capacity
- Seamless Mobility

Quality of Service

- In packet-switched networks, data is broken into packets and each packet may take different routes to reach the destination. Therefore, packets can experience delays, loss, or variations in transmission time, leading to poor performance specifically for time-sensitive applications (e.g., voice calls, video streaming, online gaming). **Therefore, QoS is essential to address these challenges.**
- Quality of Service (QoS) refers to the set of technologies, policies, and mechanisms used to manage network traffic to ensure that specific types of user data can receive the appropriate level of service and performance based on their requirements.
- On a broader level, data is divided into two parts:
 - Voice, Audio, and Video Traffic
 - Data Traffic

Quality of Service

Voice, Audio, and Video Traffic

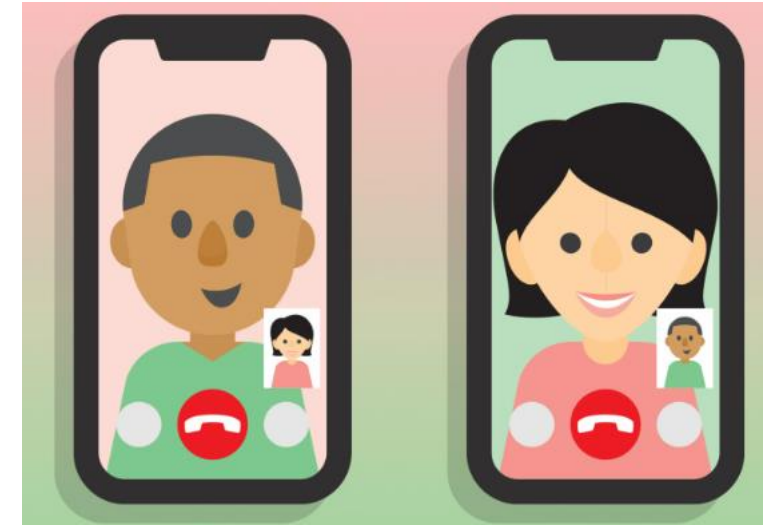
Voice, audio, and video traffic can be generalized under the term of real-time traffic, in which the **delay constraints are of paramount importance**.

Types

- Streaming live video – such as a live sporting event
- Streaming stored video – such as Youtube, that uses buffering
- Video conferencing – interactive and has additional requirements for round-trip delay

Requirements

- Strict Bounds on **delay**
- Some packet loss is acceptable



Quality of service

Data Traffic

While some packet loss is tolerable for real-time traffic, **data traffic** requires packets to eventually arrive **free from error**.

Data traffic is considered elastic, i.e. Data is typically delivered in files and it is the final delivery time of those files which is important, not the steady delivery of bits in the middle. This is in definite contrast to real-time traffic, so data traffic is also commonly called non-real-time traffic

Types

- Interactive – such as transactions or web page interactions
- Non-interactive – background downloads of files or email

Requirements

- Eventual error-free delivery after retransmissions
- The higher **throughput/ data rate**

Generic Framework of QoS

to meet diverse requirements of different
application

PROVISIONING OF QoS

There are three fundamental methods by which different technologies provide support for **Quality of Service (QoS)** to ensure that critical network traffic receives the appropriate treatment in terms of performance (e.g., reduced latency, minimized packet loss).

These methods are:

- Overprovisioning
- Prioritization without guarantees
- Prioritization with guarantees



PROVISIONING OF QoS

Overprovisioning

- Overprovisioning involves increasing the capacity of the network (by adding more bandwidth) beyond the expected demand to accommodate high traffic loads.
- Overprovisioning minimizes congestion by providing abundant resources, which allows the network to handle all traffic without performance degradation.
- This method doesn't require any specific management of traffic types or priorities but instead ensures that there are more resources than necessary to handle all traffic.
- Overprovisioning is the concept of best-effort where the network does nothing special with particular traffic but does its best to make timely deliveries
- While overprovisioning can prevent congestion and service degradation, it can be inefficient and costly because it often involves excess infrastructure that may remain underutilized most of the time.

PROVISIONING OF QoS

Prioritization without guarantees

- In this method, traffic is **classified into different categories** or classes (e.g., voice, video, data) based on their performance needs.
- Traffic is **prioritized**, meaning that more time-sensitive or important traffic (like VoIP or real-time video) is given preference over less critical traffic (like email or file downloads) when the network is congested.
- In this method, **high-priority user** packets are marked as higher priority and scheduling schemes give those packets higher priority when making decisions and hence the higher priority packet will receive relatively better service.
- Although high-priority traffic is given preference, there is **no guarantee of performance under heavy congestion**. It's possible that even prioritized traffic may experience delays or packet loss if the network becomes too congested.

PROVISIONING OF QoS

Prioritization with guarantees

- In this scheme, the high-priority traffic is not only given preferential treatment but also receives **a guaranteed level of performance**, such as a minimum amount of bandwidth, maximum latency, or no packet loss.
- Prioritization with guarantees provides **numerical bounds** on performance, also possibly with some statistical reliability. For example, packets might receive a delay less than 100 ms 99.9% of the time.
- This method is more advanced and provides both prioritization and performance guarantees for specific traffic classes.

Practical QoS Implementation

Practical QoS Models

The important QoS models are:

Best-Effort Model: The Best-Effort model is the default QoS model in most networks. It provides no specific QoS treatment, meaning all traffic is treated equally without prioritization. This model doesn't guarantee performance for any type of traffic, and in case of network congestion, packets may be dropped or delayed.

Integrated Services (IntServ) Model: The IntServ model provides end-to-end service guarantees for traffic flows. It uses the Resource Reservation Protocol (RSVP) to reserve network resources (like bandwidth) for each flow to ensure that specific QoS parameters (such as latency, jitter, and bandwidth) are met. IntServ is ideal for applications requiring strict QoS, such as real-time voice and video communications.

Practical QoS Models

Differentiated Services (DiffServ) Model:

The DiffServ model provides traffic classification and prioritization using **Differentiated Services Code Points (DSCP)**.

- Traffic is classified into different classes, and each class is treated according to its priority level.
- The DiffServ allows for scalable and simplified management of QoS without requiring resource reservation as IntServ.
- DiffServ is widely used in enterprise and service provider networks where traffic is categorized into various levels of priority
 - Class Selector (CS)
 - Assured Forwarding (AF)
 - Expedited Forwarding (EF)

Precedence/DSCP			
	Binary	DSCP	Prec.
56	111000	Reserved	7
48	110000	Reserved	6
46	101110	EF	5
32	100000	CS4	4
34	100010	AF41	
36	100100	AF42	
38	100110	AF43	
24	011000	CS3	3
26	011010	AF31	
28	011100	AF32	
30	011110	AF33	
16	010000	CS2	2
18	010010	AF21	
20	010100	AF22	
22	010110	AF23	
8	001000	CS1	1
10	001010	AF11	
12	001100	AF12	
14	001110	AF13	
0	000000	BE	0

Practical QoS Models

Traffic Classes of DiffServ:

Class Selector (CS) – Default/ Basic Class:

This is the default class for best-effort traffic that does not require any specific QoS treatment. It is typically used for general internet traffic and services with no particular QoS requirements.

Expedited Forwarding (EF) - Premium Class :

This class is designed for low-loss, low-latency traffic, such as voice and video. Packets in this class are forwarded with minimal delay and jitter.

Assured Forwarding (AF):

These classes provide assured delivery under prescribed conditions and are suitable for applications that require predictable and assured service.

Key techniques used in QoS Models

Key techniques used in QoS Models

Queuing and Scheduling Models:

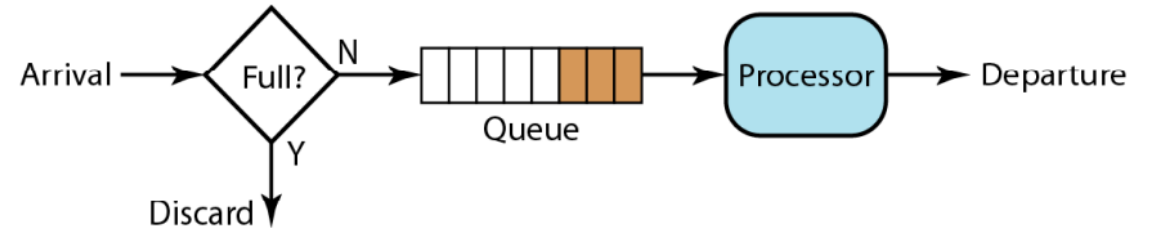
Here packets are placed in different queues based on priority, and scheduling algorithms determine the order in which packets are sent.

The Common techniques include:

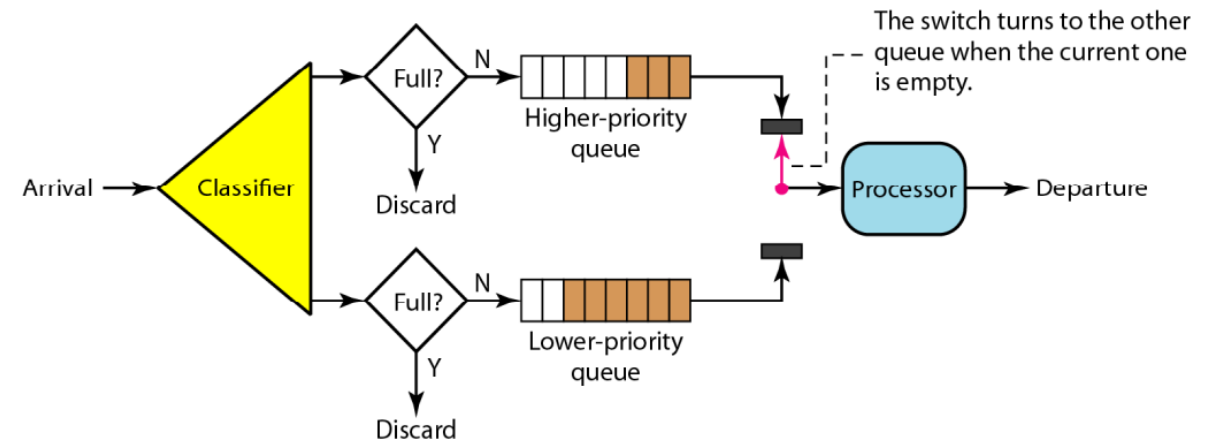
- **Weighted Fair Queuing (WFQ)**
- **Priority Queuing (PQ)**
- **Class-Based Queuing (CBQ)**
- **Random Early Detection (RED)**

Queuing and Scheduling Models used to ensure that critical traffic, like voice or video, is processed before other traffic, ensuring low latency for time-sensitive applications.

FIFO Queue



Priority Queuing

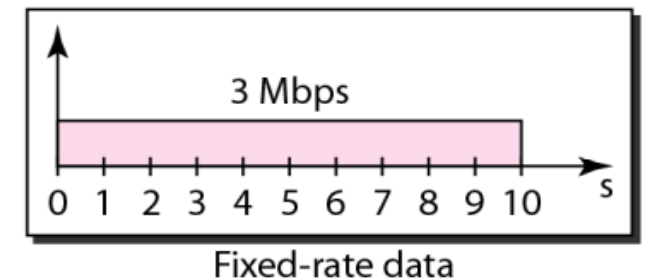
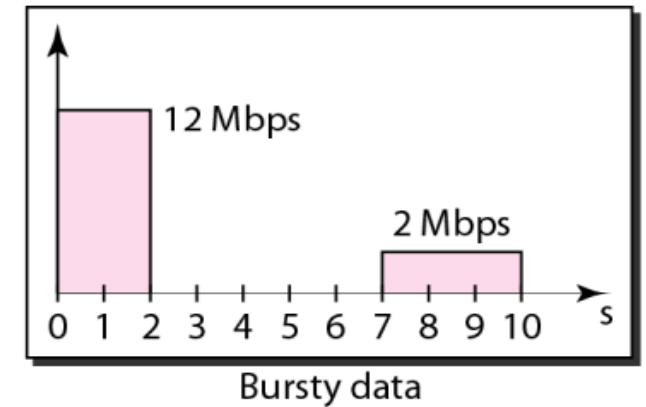
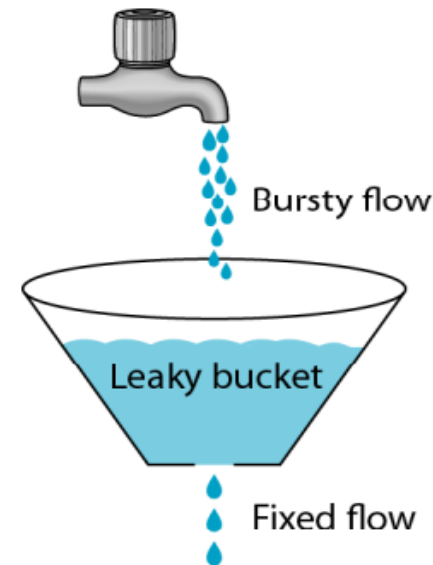


Key techniques used in QoS Models

Traffic Shaping or Policing Models:

- A leaky bucket technique is used to smooth out burst traffic.
- In this scheme, bursty traffic is stored in the bucket and sent out at an average rate.
- It helps regulate the flow of data to prevent bursts of traffic that could lead to congestion and ensure a more consistent and controlled usage of network resources.
- A leaky bucket algorithm shapes bursty traffic into fixed-rate traffic by averaging the data rate.

Leaky bucket



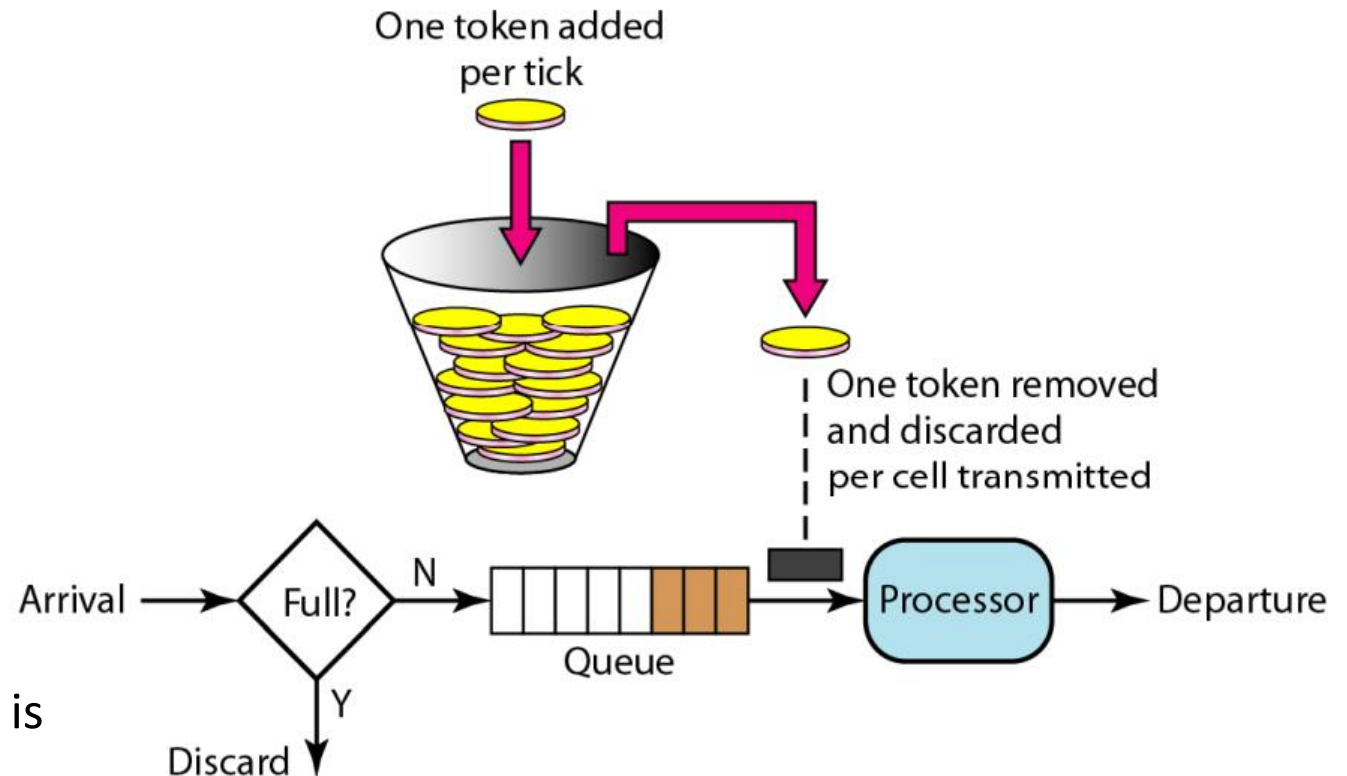
Key techniques used in QoS Models

Traffic Shaping or Policing Models:

Token bucket

The leaky does not credit an idle host, while the token bucket algorithm allows the idle host to accumulate credit for the future in the form of a token.

The token bucket is implemented by a counter operation. Each time token is added, the counter is incremented by one. Each time a unit is sent, the counter is decremented by 1. When the counter is zero, the host cannot send data.



Key techniques used in QoS Models

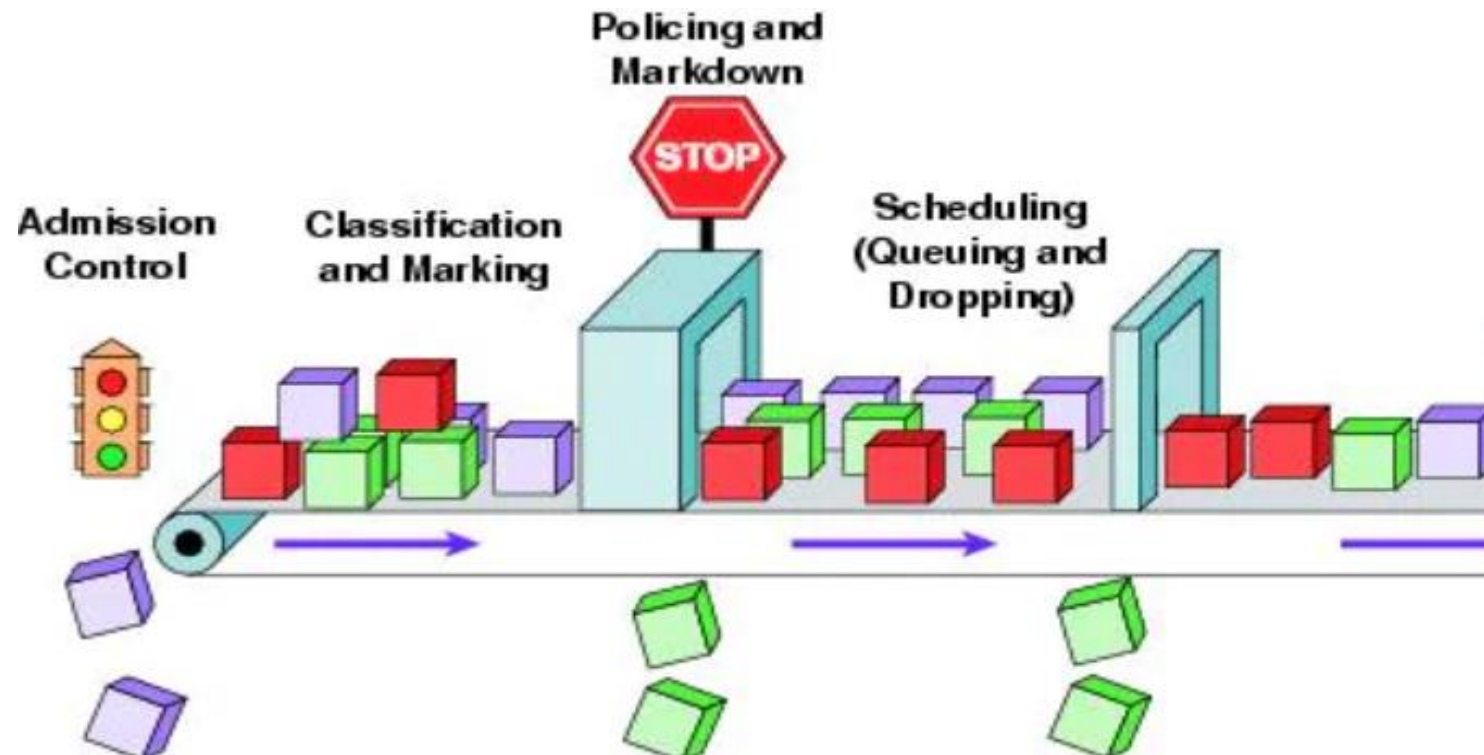
Traffic Shaping or Policing Models:

Token bucket

- Tokens are generated at a fixed rate and are placed in the bucket. Each token represents the ability to transmit one packet.
- When a packet arrives for transmission, the system checks if there are tokens available in the bucket.
- If there are enough tokens, the packet is allowed to be transmitted, and the corresponding number of tokens is removed from the bucket.
- If there are not enough tokens, the packet may be delayed or discarded. This helps to control the rate of traffic and prevents bursts that could lead to congestion.

Key techniques used in QoS Models

Admission Control: If resources are insufficient or accepting the new traffic would degrade QoS for existing flows, the request is rejected.



Practical QoS Models

Admission Control:

- Admission control is the process of determining whether a new request or flow of traffic should be accepted into the network based on the available resources and the network's ability to meet certain QoS requirements.
- The goal of admission control is to prevent network congestion and ensure that the existing and new traffic can be handled within the network's capacity.
- Whenever a new request for network resources is initiated, it goes through the admission control process. The admission control system evaluates the availability of resources (for instance, bandwidth, and buffer space) in the network.
- The Admission control checks whether accepting the new request would meet the QoS requirements specified for that type of traffic. Based on the resource availability and QoS requirements, the admission control system decides to either accept or reject the new request.

Thanks!