USN

Internal
Assessment Test 1

Sub:	**Computer Networks**					Sub Code:	**BCS502**	Branch:	**AINDS / CS (DS)**	
Date:		Duration:	**90 minutes**	Max Marks:	**50**	Sem	**V**		**OBE**	

		Answer any FIVE Questions	**MARKS**	**CO**	**RBT**
1	a	Explain guided transmission media used in networking(listing 0.5+explanation 4.5(1.5 for each type))	5	CO1	L1
	b	Explain Different Components of Communication System with neat diagram. 1 component 1 mark	5	CO1	L2
2		Explain, with the help of a diagram, how the TCP/IP protocol stack handles an HTTP request when a user communicates with a web server over a network(7+3 diagram)	10	CO2	L2
3	a	Compare and contrast byte-stuffing and bit-stuffing. Which technique is used in byte-oriented protocols? Which technique is used in bit-oriented protocols?(3+1+1)	5	CO2	L2
	b	Solve using Cyclic Redundancy Check. Dataword:100100, Divisor-1101 at sender side and find the value of CRC.	5	CO2	L3
4		A sender needs to send the four data items Ox4567, OxBCDE, Ox02BC, and Ox89AB. (5+5) Answer the following: i) Find the checksum at the sender site. ii) Find the checksum at the receiver site if the second data item is changed to OxABCE.	10	CO2	L3
5		Compare and contrast the Datagram approach with the Virtual Circuit approach in networking(5+5)	10	CO1	L1
6		A pure ALOHA network transmits 200-bit frames using a shared channel with a 200-kbps(1+3+3+3) bandwidth. Find the throughput if the system (all stations together) produces a. 1000 frames per second	10	CO2	L3

		b. 500 frames per second c. 250 frame+s per second			

CI CCI
HOD

Q 1a) Explain guided transmission media used in networking

Guided Transmission Media in Networking

Guided transmission media refers to wired communication channels where data signals are transmitted along a physical path (cables or wires). Unlike unguided media (wireless), here the transmission is directed and confined to the medium.

Types of Guided Transmission Media

1. Twisted Pair Cable

- Consists of pairs of insulated copper wires twisted together.
- Types:
    - Unshielded Twisted Pair (UTP): Cheaper, widely used in LANs, telephone lines, and Ethernet.
    - Shielded Twisted Pair (STP): Has an additional shielding layer to reduce interference.
- Advantages: Low cost, easy installation.
- Disadvantages: Limited bandwidth and distance, prone to electromagnetic interference (EMI).

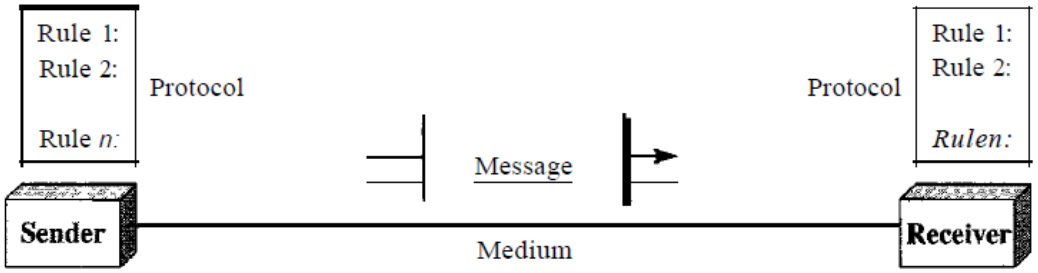
2. Coaxial Cable

- Has a central copper conductor surrounded by an insulating layer, a metallic shield, and an outer insulating cover.
- Provides better shielding than twisted pair.
- Used in cable TV networks, broadband internet, and older Ethernet connections.
- Advantages: Higher bandwidth than twisted pair, less noise.
- Disadvantages: Bulkier and more expensive than twisted pair.

3. Optical Fiber Cable

- Uses light signals instead of electrical signals.
- Made of a core (glass or plastic), cladding (reflects light back into core), and protective outer coating.
- Types:
    - Single-mode fiber: Small core, long-distance, higher bandwidth.
    - Multi-mode fiber: Larger core, shorter distance, lower cost.
- Advantages: Extremely high bandwidth, long-distance transmission, immune to EMI.
- Disadvantages: Expensive, requires specialized installation and maintenance.

Q 1 b) Explain Different Components of Communication System with neat diagram.



1) Message. The message is the information (data) to be communicated. Popular forms of information include text, numbers, pictures, audio, and video.

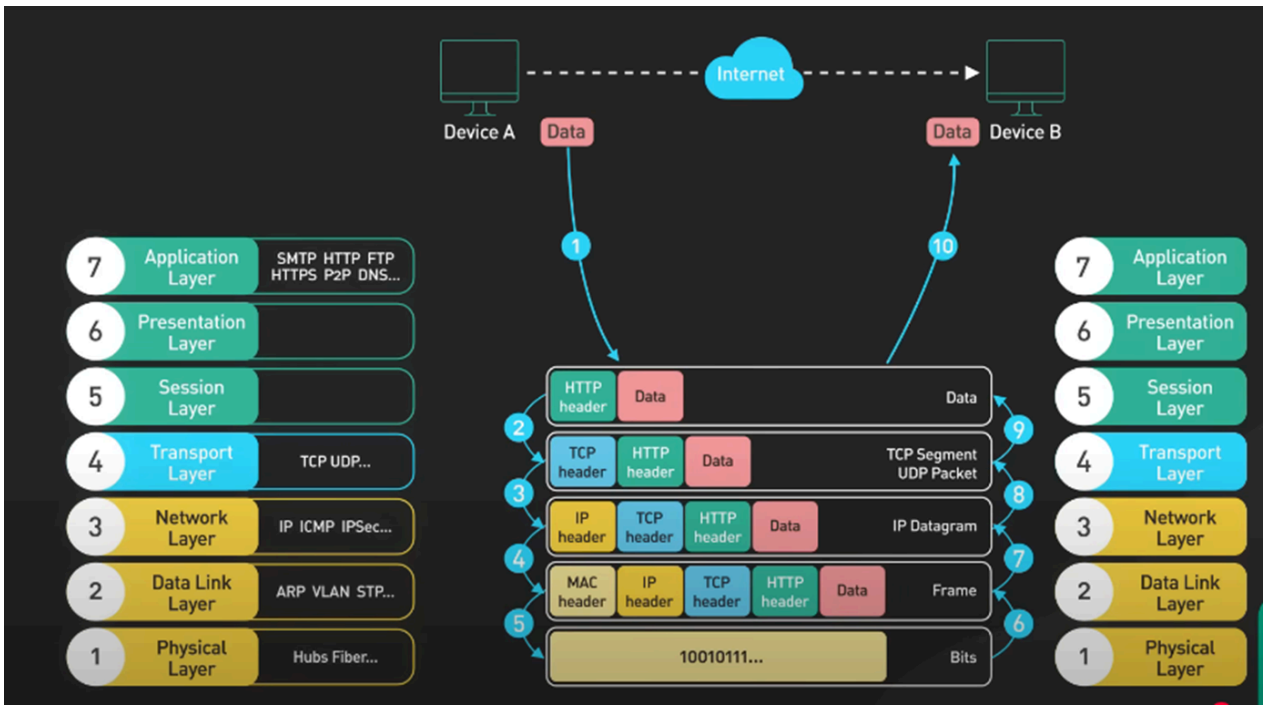
2) Sender. The sender is the device that sends the data message. It can be a computer, workstation, telephone handset, video camera, and so on.

3) Receiver. The receiver is the device that receives the message. It can be a computer, workstation, telephone handset, television, and so on.

4) Transmission medium. The transmission medium is the physical path by which a message travels from sender to receiver. Some examples of transmission media include twisted-pair wire, coaxial cable, fiber-optic cable, and radio waves.

5) Protocol. A protocol is a set of rules that govern data communications. It represents an agreement between the communicating devices. Without a protocol, two devices may be connected but not communicating, just as a person speaking French cannot be understood by a person who speaks only Japanese.

Q 2) Explain, with the help of a diagram, how the TCP/IP protocol stack handles an HTTP request when a user communicates with a web server over a network



Step-by-step Process of an HTTP Request through TCP/IP Stack

1. Application Layer (HTTP request)

- The user (Device A) sends an HTTP request (e.g., opening a website in a browser).
- HTTP operates at the Application Layer of the OSI model.
- Data generated: `Data` (HTTP Request).

2. Transport Layer (TCP segment creation)

- The HTTP request is passed down to the Transport Layer.
- TCP adds a TCP header (with source port, destination port, sequence number, etc.).
- Now the packet is: `TCP header + HTTP header + Data`.

3. Network Layer (IP addressing)

- The Transport Layer hands the segment to the Network Layer.
- An IP header is added (with source and destination IP addresses).
- Now the packet is an IP Datagram:
  `IP header + TCP header + HTTP header + Data`.

4. Data Link Layer (framing)

- The Network Layer passes the IP Datagram to the Data Link Layer.
- A MAC (Media Access Control) header is added (with source and destination MAC addresses).
- Now it becomes a Frame:
  `MAC header + IP header + TCP header + HTTP header + Data`.

5. Physical Layer (bits transmission)

- Finally, the frame is converted into bits (0s and 1s).
- These bits are transmitted over the physical medium (cables, fiber, or wireless signals).

6. Data travels through the Internet

- The bits are transmitted from Device A → routers/switches → Internet → Device B (the web server).

7. Decapsulation at Device B (server)

- At the server (Device B), the reverse process happens:
  1. Physical Layer: Receives bits and converts them to frames.
  2. Data Link Layer: Removes MAC header.
  3. Network Layer: Removes IP header → identifies destination.
  4. Transport Layer: Removes TCP header → reassembles segments.
  5. Application Layer: Receives the original HTTP request.

8. Response

- The server processes the HTTP request and sends back an HTTP response using the same process in reverse.

Key Terms from the Diagram

- Encapsulation: Wrapping data with headers at each layer (steps 1–5).
- Decapsulation: Removing headers at each layer on the receiving side (steps 6–10).
- Data Units:
  - Application Layer → Data

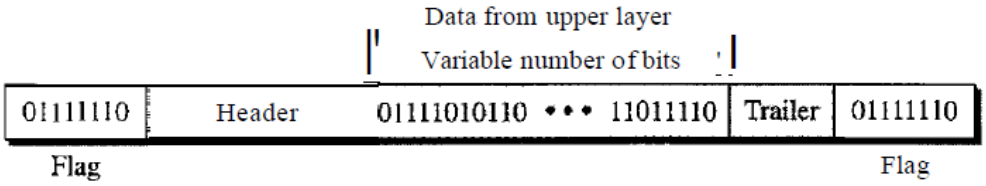
- Transport Layer → Segment
- Network Layer → Datagram/Packet
- Data Link Layer → Frame
- Physical Layer → Bits

Q 3a) Compare and contrast byte-stuffing and bit-stuffing. Which technique is used in byte-oriented protocols? Which technique is used in bit-oriented protocols?

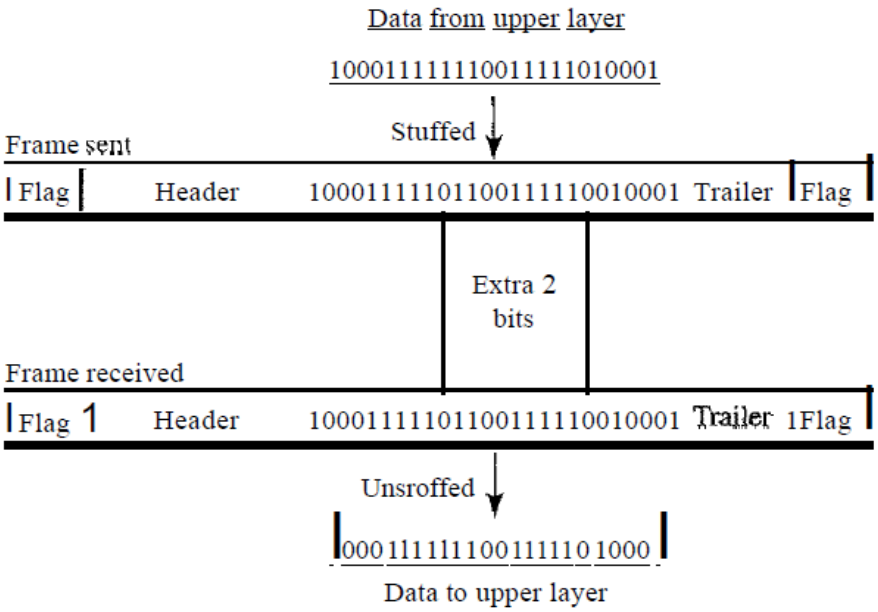
Ans: In byte stuffing (or character stuffing), a special byte is added to the data section of the frame when there is a character with the same pattern as the flag. The data section is stuffed with an extra byte. This byte is usually called the escape character (ESC), which has a predefined bit pattern. Whenever the receiver encounters the ESC character, it removes it from the data section and treats the next character as data, not a delimiting flag. Byte stuffing by the escape character allows the presence of the flag in the data section of the frame, but it creates another problem. What happens if the text contains one or more escape characters followed by a flag? The receiver removes the escape character, but keeps the flag, which is incorrectly interpreted as the end of the frame. To solve this problem, the escape characters that are part of the text must also be marked by another escape character. In other words, if the escape character is part of the text, an extra one is added to show that the second one is part of the text.

Bit-Oriented Protocols

In a bit-oriented protocol, the data section of a frame is a sequence of bits to be interpreted by the upper layer as text, graphic, audio, video, and so on. However, in addition to headers (and possible trailers), we still need a delimiter to separate one frame from the other. Most protocols use a special 8-bit pattern flag 01111110 as the delimiter to define the beginning and the end of the frame

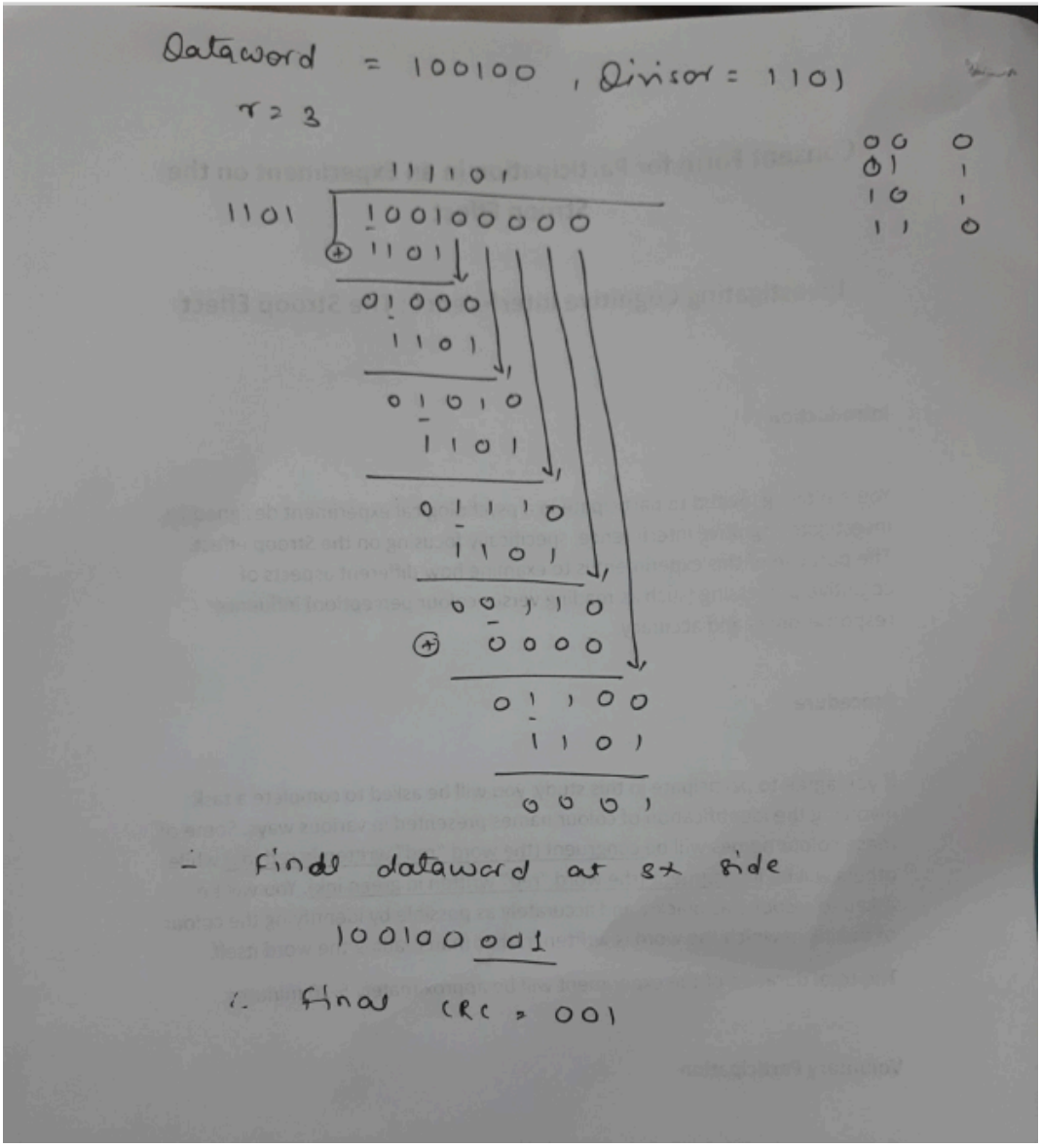


This flag can create the same type of problem we saw in the byte-oriented protocols. That is, if the flag pattern appears in the data, we need to somehow inform the receiver that this is not the end of the frame. We do this by stuffing 1 single bit (instead of I byte) to prevent the pattern from looking like a flag. The strategy is called bit stuffing. In bit stuffing, if a 0 and five consecutive I bits are encountered, an extra 0 is added. This extra stuffed bit is eventually removed from the data by the receiver.

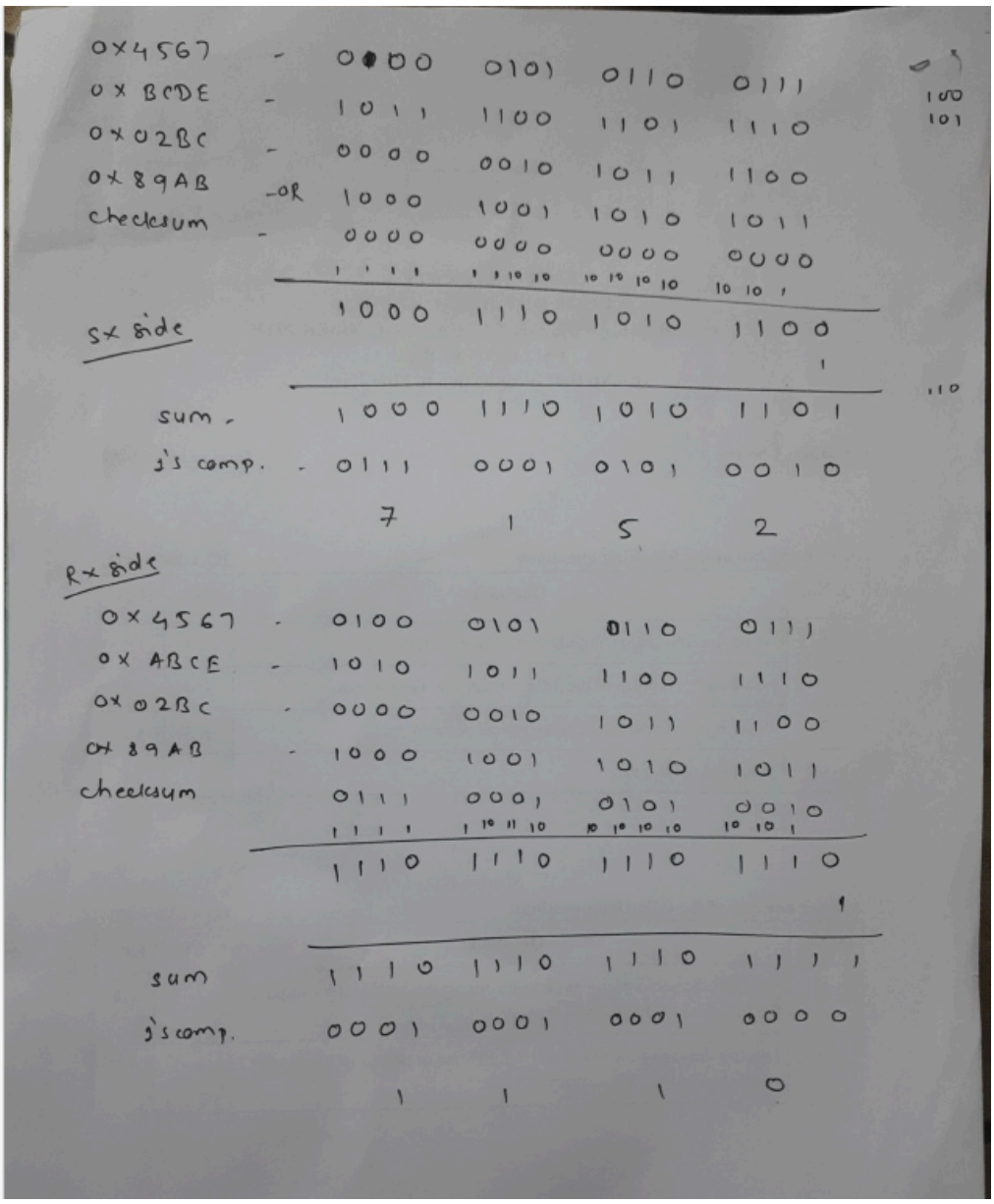


Q 3b) Solve using Cyclic Redundancy Check. Dataword:100100, Divisor-1101 at sender side and find the value of CRC.

Ans:



Q 4) A sender needs to send the four data items Ox4567, OxBCDE, Ox02BC, and Ox89AB. Answer the following:
i) Find the checksum at the sender site.
ii) Find the checksum at the receiver site if the second data item is changed to OxABCE.
Ans:



Q 5) Compare and contrast the Datagram approach with the Virtual Circuit approach in networking
Ans:

Datagram vs. Virtual Circuit Approach in Networking

These are two **connection services** provided at the **Network Layer** to deliver packets between sender and receiver.

1. Datagram Approach (Connectionless Service)

- Each packet is treated independently.
- No need to establish a connection before sending data.
- Packets may take different routes to reach the destination.
- Each packet carries complete addressing information (source & destination).

- Delivery is not guaranteed (packets may be delayed, lost, or arrive out of order).
- Example: IP protocol (Internet).

2. Virtual Circuit Approach (Connection-Oriented Service)

- A connection (path) is established before communication.
- All packets follow the same route through the network.
- Each packet carries only a virtual circuit identifier (VCI) instead of full addressing.
- Delivery is reliable and ordered.
- Example: ATM, Frame Relay, MPLS.

Figure 18.3 *A connectionless packet-switched network*

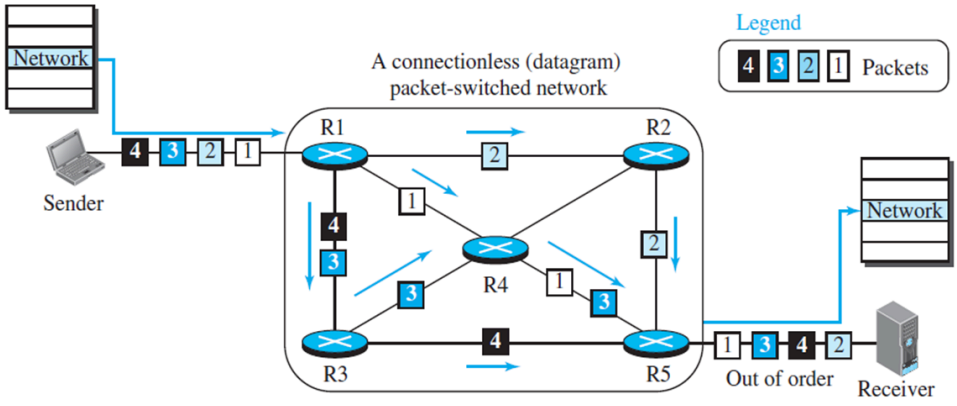
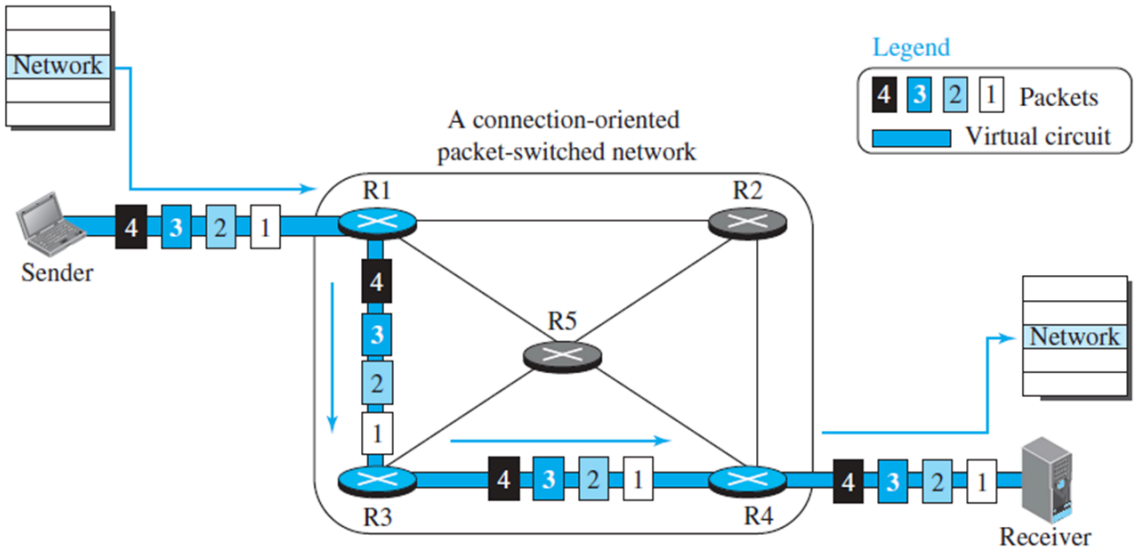


Figure 18.5 *A virtual-circuit packet-switched network*



Comparison Table

Feature	Datagram Approach	Virtual Circuit Approach
Connection setup	No setup needed (connectionless).	Setup required before data transfer.
Routing	Each packet may take a different path.	All packets follow the same path.
Addressing	Full source & destination address in each packet.	Uses a Virtual Circuit Identifier (VCI).
Delivery	Unreliable, may be out of order or lost.	Reliable, ordered delivery.

Q 6) A pure ALOHA network transmits 200-bit frames using a shared channel with a 200-kbps bandwidth. Find the throughput if the system (all stations together) produces
a. 1000 frames per second
b. 500 frames per second
c. 250 frames per second

Ans:
The frame transmission time is *2001200* kbps or 1 ms.
a. If the system creates 1000 frames per second, this is 1 frame per millisecond. The load is 1. In this case S =G x *e-2G* or S =0.135 (13.5 percent). This means that the throughput is 1000 x 0.135 =135 frames. Only 135 frames out of 1000 will probably survive.
b. If the system creates 500 frames per second, this is (1/2) frame per millisecond. The load is *(112)*. In this case S = G x *e-2G* or S = 0.184 (18.4 percent). This means that the throughput is 500 x 0.184 =92 and that only 92 frames out of 500 will probably survive. Note that this is the maximum throughput case, percentagewise.
c. If the system creates 250 frames per second, this is (1/4) frame per millisecond. The load is (1/4). In this case S = G x *e-2G* or S =0.152 (15.2 percent). This means that the throughput is 250 x 0.152 = 38. Only 38 frames out of 250 will probably survive.