Introduction to Network Layer

SIDDAGANGA INSTITUTE OF TECHNOLOGY

Department of CSE

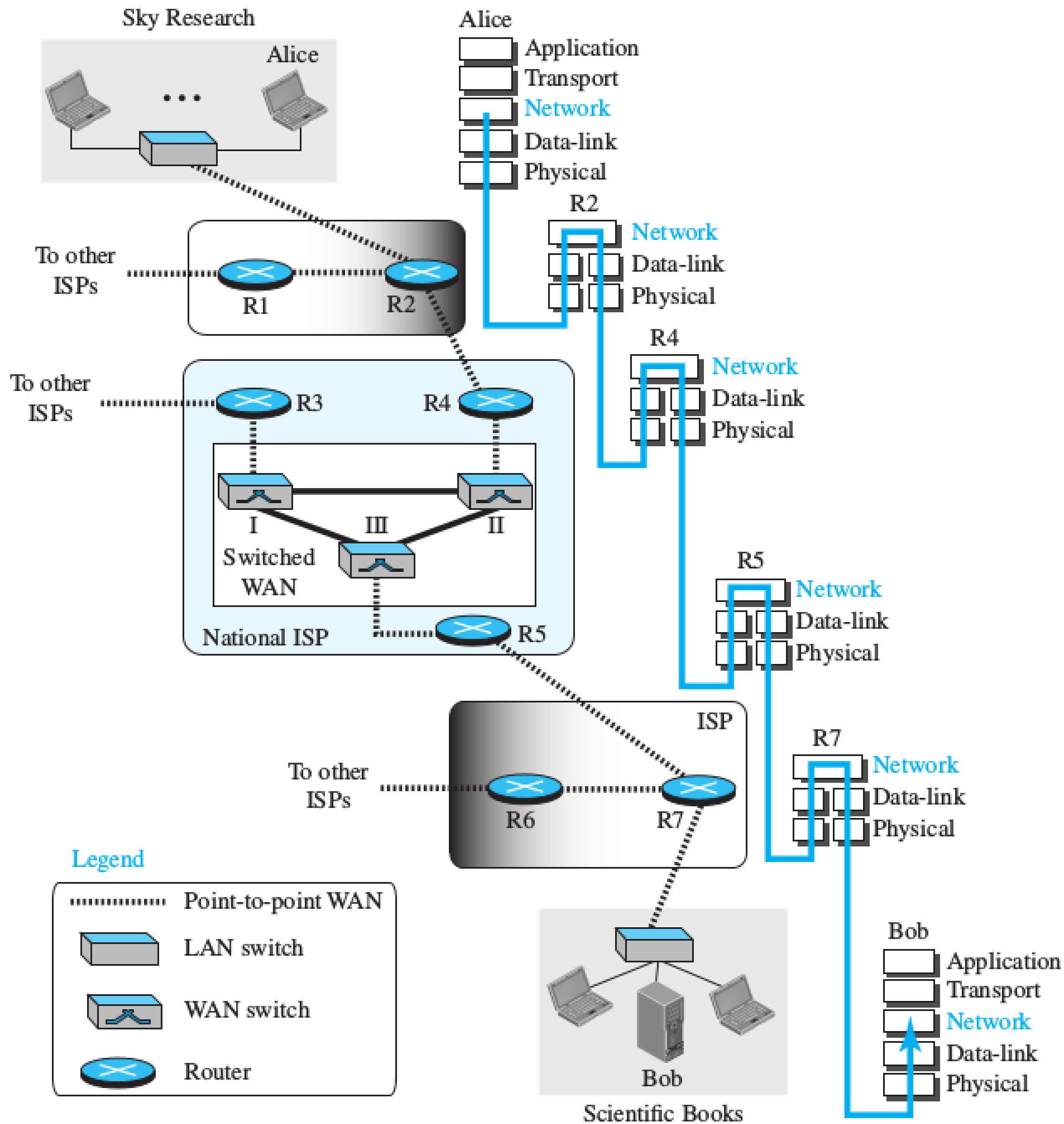
Prabodh C P

Contents

Network Layer

- The network layer is responsible for the host-to-host delivery of datagrams.
- It provides services to the transport layer
- It receives services from the data-link layer
- The network layer is responsible for creating a connection between the source computer and the destination computer.
- The network layer is responsible for host-to-host communication and routing the packet through possible routes.
- The network layer in the Internet includes the main protocol, Internet Protocol (IP).

Communication at the network layer



Network Layer

- The network layer is involved at the source host, destination host, and all routers in the path.
- At the source host (Alice),
  - the network layer accepts a packet from a transport layer, encapsulates the packet in a datagram, and delivers the packet to the data-link layer.
- At the destination host (Bob),
  - the datagram is decapsulated, and the packet is extracted and delivered to the corresponding transport layer.
- Source and Destination are involved in all five layers of the TCP/IP suite, the routers use only three layers.

NETWORK-LAYER SERVICES

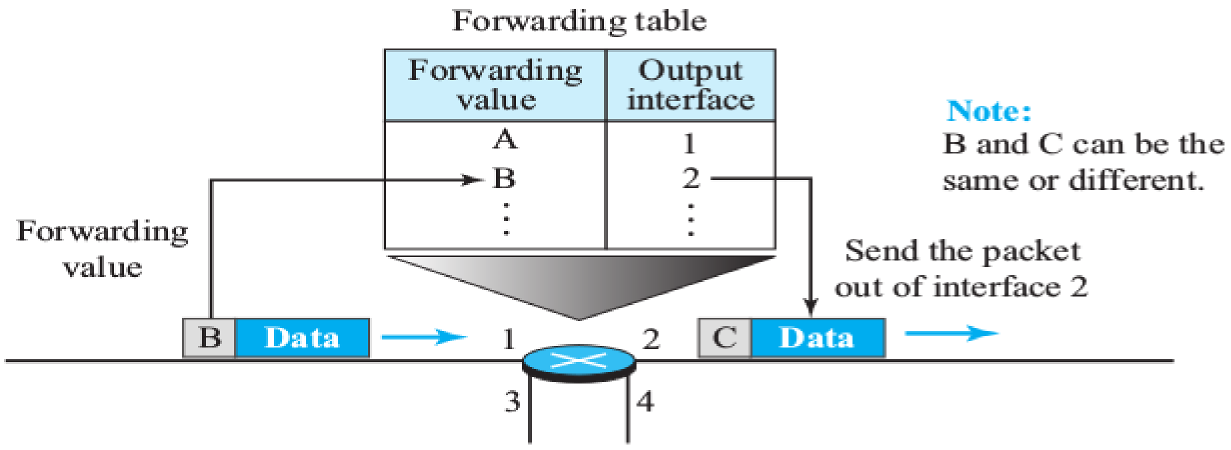
- Packetizing
- Routing and Forwarding
- Error Control
- Flow Control
- Congestion Control
- Quality of Service
- Security

Packetizing

- This involves encapsulating the payload (data received from upper layer) in a network-layer packet at the source and decapsulating the payload from the network-layer packet at the destination. (POST OFFICE)
- The source host receives the payload from an upper-layer protocol, adds a header that contains the source and destination addresses and sends to Data Link layer
- The destination host receives the network-layer packet from its data-link layer, decapsulates the packet, and delivers the payload to the corresponding upper-layer protocol.
- Routers on the way are not allowed to decapsulate the packets (fragmentation)

Routing and Forwarding

- Routing
  - Internet is a collection of several networks
  - Can have more than one path between two hosts
  - Network Layer is responsible for finding the best path using strategies implemented in routing protocols
- Forwarding
  - forwarding can be defined as the action applied by each router when a packet arrives at one of its interfaces based on the routing table



Other Services

- Error Control
  - Inefficient due to fragmentation
  - a checksum field to the datagram to control any corruption in the header, but not in the whole datagram.
- Flow Control
  - Flow control regulates the amount of data a source can send without overwhelming the receiver.
  - No flow control
  - left to the upper layers

Other Services

- Congestion Control
  - Congestion in the network layer is a situation in which too many datagrams are present in an area of the Internet
  - Congestion may occur if the number of datagrams sent by source computers is beyond the capacity of the network or routers.
- Quality of Service
  - With new applications such as multimedia communication the quality of service (QoS) has become more and more important.
  - However this is left to the upper layer
- Security

PACKET SWITCHING

- A router, in fact, is a switch that creates a connection between an input port and an output port.
- Only packet switching is used at the network layer
- We use two different approaches to route the packets in a Packet Switched Network
  - datagram approach
  - virtual circuit approach

NETWORK-LAYER PERFORMANCE

- The performance of a network can be measured in terms of
  - Delay
  - Throughput
  - Packet loss.
- Congestion control is an issue that can improve the performance.

Delay

- The delays in a network can be divided into four types:
  - transmission delay
  - propagation delay
  - processing delay
  - queuing delay
- **Transmission Delay**
  - Difference between the time of first and last bits of a packet
  - **$Delay_{tr}$ = (Packet length) / (Transmission rate).**
- **Propagation Delay**
  - Propagation delay is the time it takes for a bit to travel from point A to point B in the transmission media.
  - **$Delay_{pg}$ = (Distance) / (Propagation speed).**

Delay

- **Processing Delay**
  - time required for a router or a destination host to receive a packet from its input port, remove the header, perform an error detection procedure, and deliver the packet to the output port (in the case of a router) or deliver the packet to the upper-layer protocol (in the case of the destination host).
  - **Delay_{pr} = Time required to process a packet in a router or a destination host**
- **Queuing Delay**
  - **Delay_{qu} = The time a packet waits in input and output queues in a router**

Total Delay

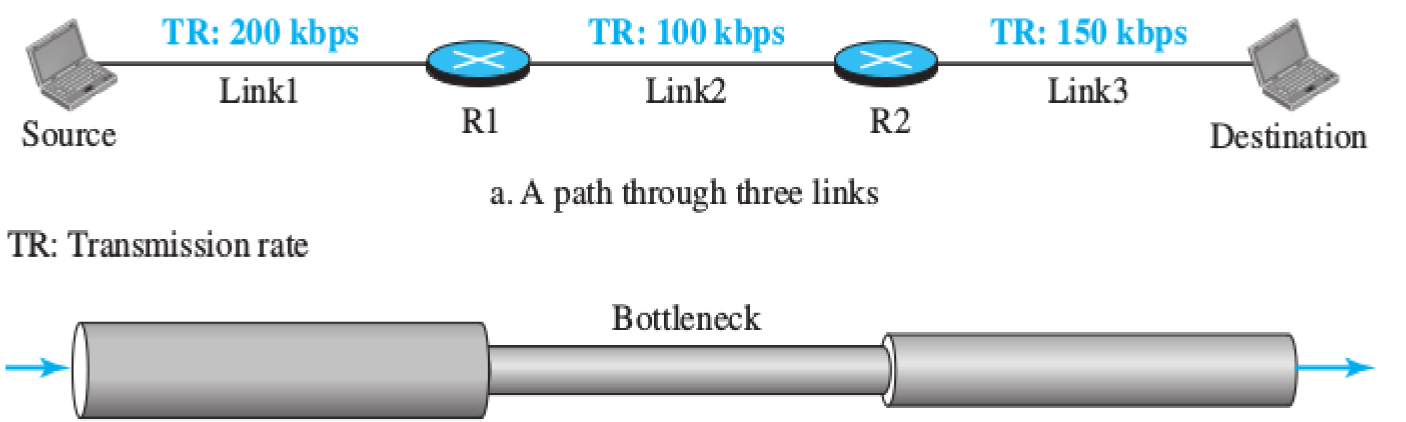
The total delay (source-to-destination delay) a packet encounters can be calculated if we know the number of routers, n, in the whole path.

$$\textbf{Total delay} = (n + 1)\,(\text{Delay}_{tr} + \text{Delay}_{pg} + \text{Delay}_{pr}) + (n)\,(\text{Delay}_{qu})$$

if we have n routers, we have (n + 1) links.

Throughput

- Throughput at any point in a network is defined as the number of bits passing through the point in a second.
- In a path from source to destination, a packet may pass through several links (networks), each with a different transmission rate.
- How, then, can we determine the throughput of the whole path?



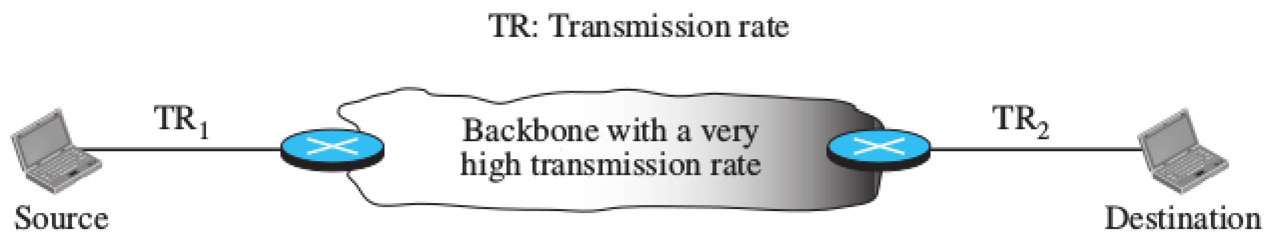
a. A path through three links

b. Simulation using pipes

Throughput

Throughput = minimum {TR_1 , TR_2 , . . . TR_n }.

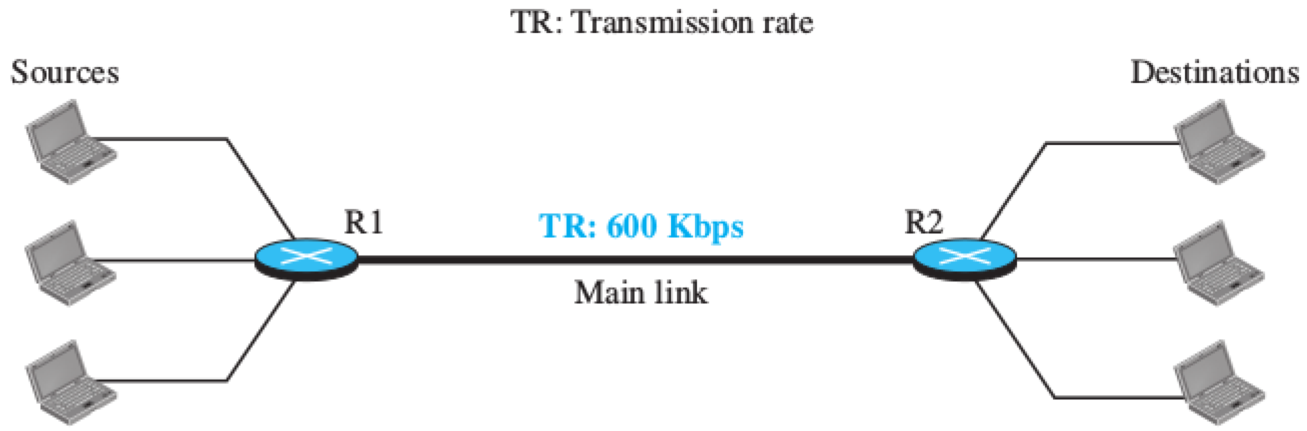
- the actual situation in the Internet is that the data normally passes through two access networks and the Internet backbone



- The Internet backbone has a very high transmission rate
- The throughput is normally defined as the minimum transmission rate of the two access links that connect the source and destination to the backbone

Throughput

- Sometimes a link can be shared or having multiple flows
- In the example the transmission rate of the link is is divided among flows



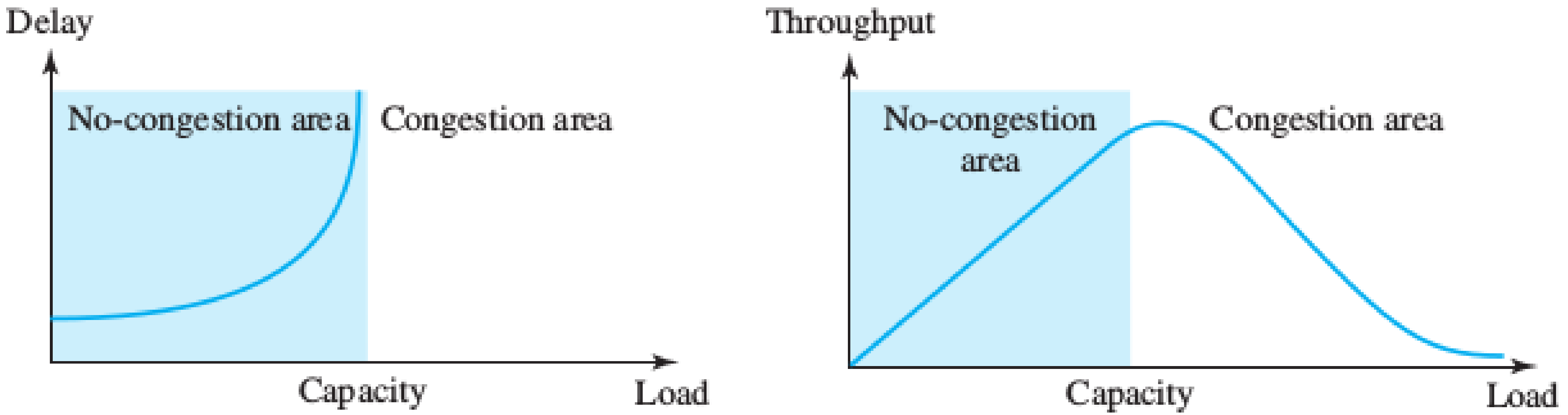
Packet Loss

- Another issue that severely affects the performance of communication is the number of packets lost during transmission.
- This may result when the buffer is full.
- The effect of packet loss on the Internet network layer is that the packet needs to be resent, which in turn may create overflow and cause more packet loss.

Congestion Control

- Congestion control is a mechanism for improving performance.
- Congestion is dealt at the transport layer.
- But study of congestion at network layer helps us understand and solve it better.
- Congestion at the network layer is related to throughput and delay.

Packet delay and throughput as functions of load



a. Delay as a function of load

b. Throughput as a function of load

Load and Delay

- When the load is much less than the capacity of the network, the delay is at a minimum.
- This minimum delay is composed of propagation delay and processing delay, both of which are negligible.
- However, when the load reaches the network capacity, the delay increases sharply because we now need to add the queuing delay to the total delay.
- Note that the delay becomes infinite when the load is greater than the capacity.

Load and Throughput

- When the load is below the capacity of the network, the throughput increases proportionally with the load.
- We expect the throughput to remain constant after the load reaches the capacity, but instead the throughput declines sharply.
- The reason is the discarding of packets by the routers.
- This will result in the source resending packets due to time out mechanisms.

Congestion Control

- Congestion control refers to techniques and mechanisms that can either prevent congestion before it happens or remove congestion after it has happened.
- In general, we can divide congestion control mechanisms into two broad categories:
  - open-loop congestion control (prevention)
  - closed-loop congestion control (removal).

Open-Loop Congestion Control

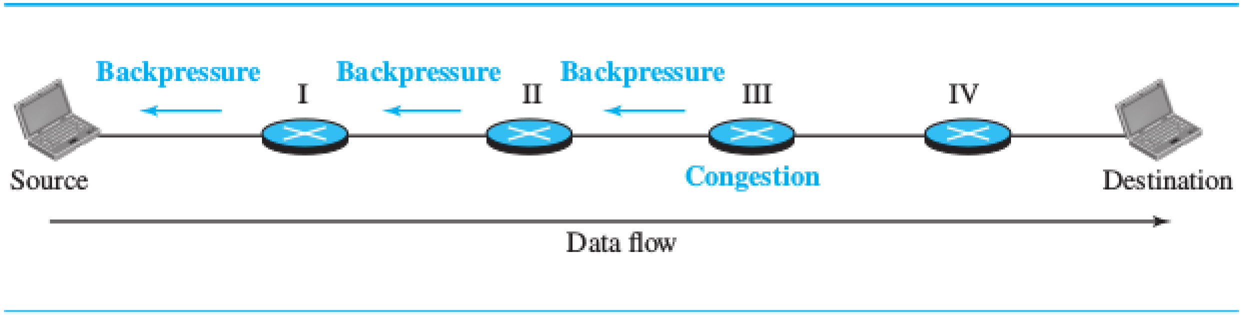
- Retransmission Policy
  - good retransmission policy can prevent congestion.
  - The retransmission policy and the retransmission timers must be designed to optimize efficiency and at the same time prevent congestion.
- Window Policy
  - Size of the window
  - Selective Repeat vs Go-Back-N
- Acknowledgment Policy
  - Timing and number of acknowledgments can influence the congestion

Open-Loop Congestion Control

- Discarding Policy
  - Dropping less priority packets
- Admission Policy
  - Allot resources only if available
  - Deny connection establishment if there is congestion

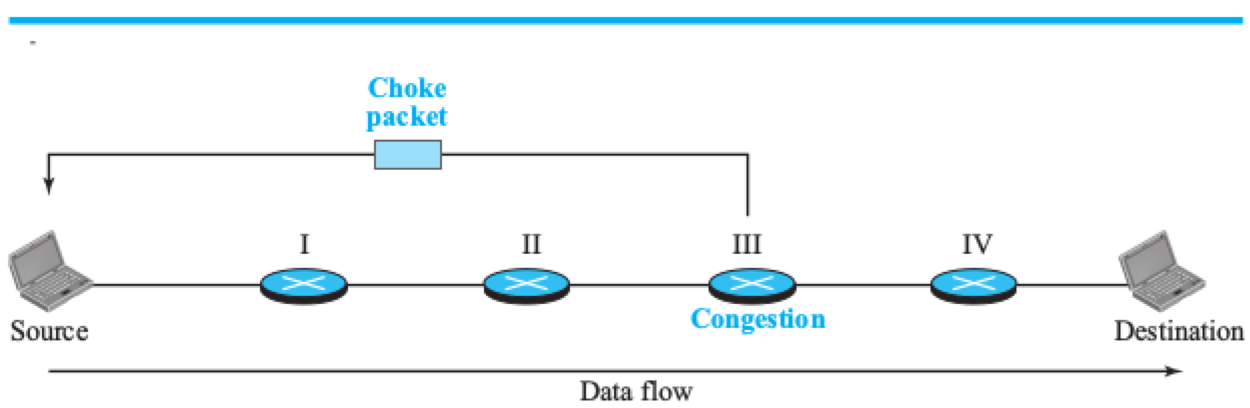
Closed-Loop Congestion Control

- Backpressure
  - The technique of backpressure refers to a congestion control mechanism in which a congested node stops receiving data from the immediate upstream node or nodes.



Closed-Loop Congestion Control

- Choke Packet
  - A choke packet is a packet sent by a node to the source to inform it of congestion. Note the difference between the backpressure and choke-packet methods.
  - In backpressure, the warning is from one node to its upstream node, although the warning may eventually reach the source station.
  - In the choke-packet method, the warning is from the router, which has encountered congestion, directly to the source station.
  - The intermediate nodes through which the packet has traveled are not warned.



Closed-Loop Congestion Control

- Implicit Signalling
  - In implicit signaling, there is no communication between the congested node or nodes and the source. The source guesses that there is congestion somewhere in the network from other symptoms.
  - The delay in receiving an acknowledgment is interpreted as congestion in the network
- Explicit Signalling
  - The node that experiences congestion can explicitly send a signal to the source or destination.
  - The explicit-signaling method, however, is different from the choke-packet method. In the choke-packet method, a separate packet is used for this purpose; in the explicit-signaling method, the signal is included in the packets that carry data.