Computer Networks 1
(Mạng Máy Tính 1)

Lectured by: Dr. Phạm Trần Vũ

Lecture 5: Network Layer (cont')

Reference:

Chapter 5 - "*Computer Networks*",

Andrew S. Tanenbaum, 4th Edition, Prentice Hall, 2003.

Contents

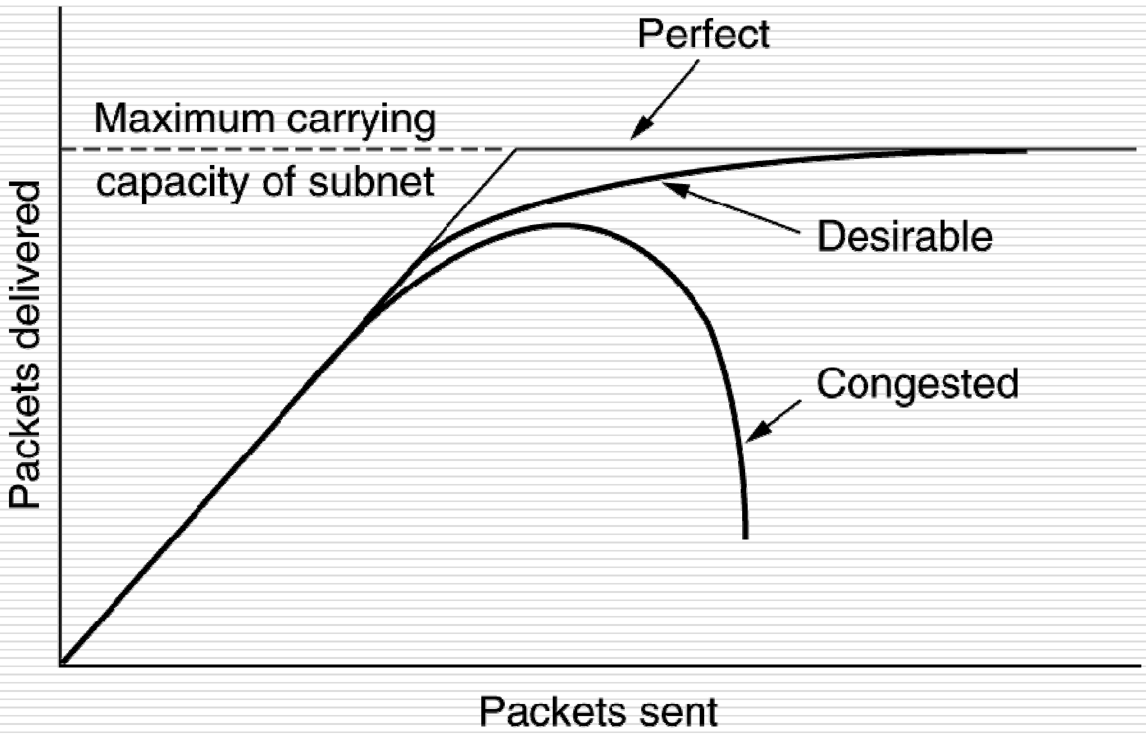
- The network layer design issues
- Routing algorithms
- **Congestion control algorithms**
- **Quality of services**
- **Internetworking**
- The network layer in the Internet

Congestion Control Algorithms

- General Principles of Congestion Control
- Congestion Prevention Policies
- Congestion Control in Virtual-Circuit Subnets
- Congestion Control in Datagram Subnets
- Load Shedding
- Jitter Control

Network Congestion

When too much traffic is offered, congestion sets in and performance degrades sharply.



General Principles of Congestion Control

- Open loop solutions
  - Solve the problems by good design
  - Prevent congestions from happening
  - Make decision without regard to state of the network
- Closed loop solutions
  - Using feedback loop

Closed Loop Solutions – Three Part Feedback Loop

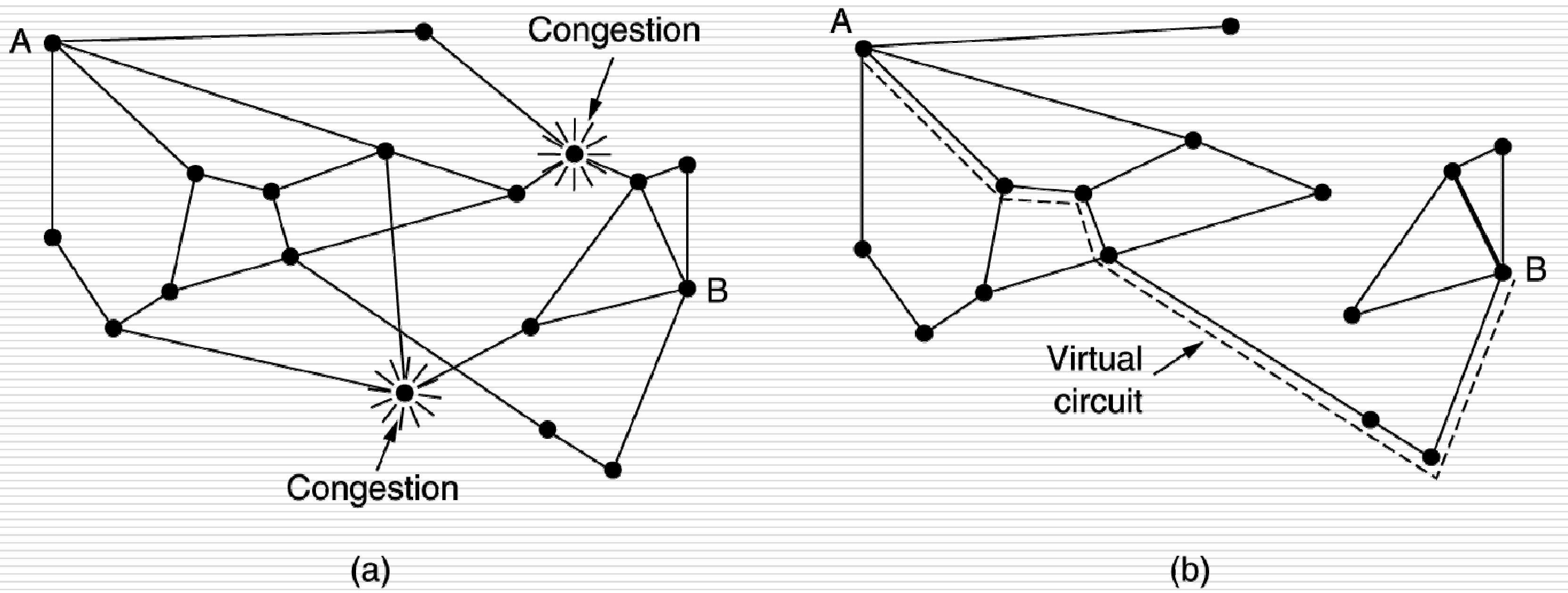
- Monitor the system
  - detect when and where congestion occurs.
- Pass information to where action can be taken.
- Adjust system operation to correct the problem.

Open Loop Solutions - Congestion Prevention Policies

Policies that affect congestion.

Layer	Policies
Transport	• Retransmission policy • Out-of-order caching policy • Acknowledgement policy • Flow control policy • Timeout determination
Network	• Virtual circuits versus datagram inside the subnet • Packet queueing and service policy • Packet discard policy • Routing algorithm • Packet lifetime management
Data link	• Retransmission policy • Out-of-order caching policy • Acknowledgement policy • Flow control policy

Congestion Control in Virtual-Circuit Subnets



(a) A congested subnet. (b) A redrawn subnet, eliminates congestion and a virtual circuit from A to B.

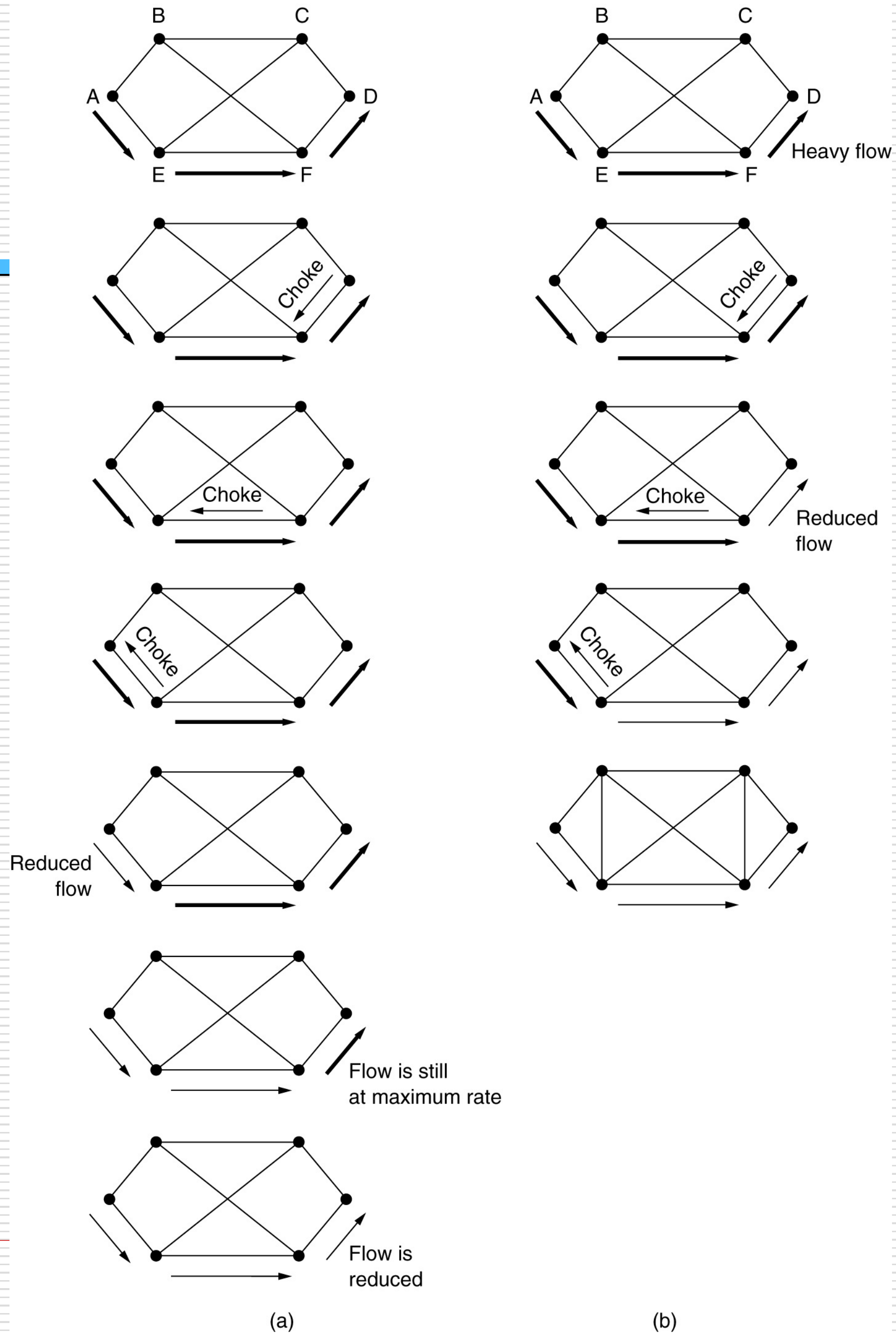
Congestion Control in Datagram Subnets

- Warning bit
  - Routers use a bit in the packet's header to signal the warning state.
  - The receiver copies the warning bit from the packet's header to the ACK message
  - The source, on receiving ACK with warning bit will adjust transmission rate accordingly
- Choke Packets
  - The router sends choke packet directly to the source host

Hop-by-Hop Choke Packets

(a) A choke packet that affects only the source.

(b) A choke packet that affects each hop it passes through.



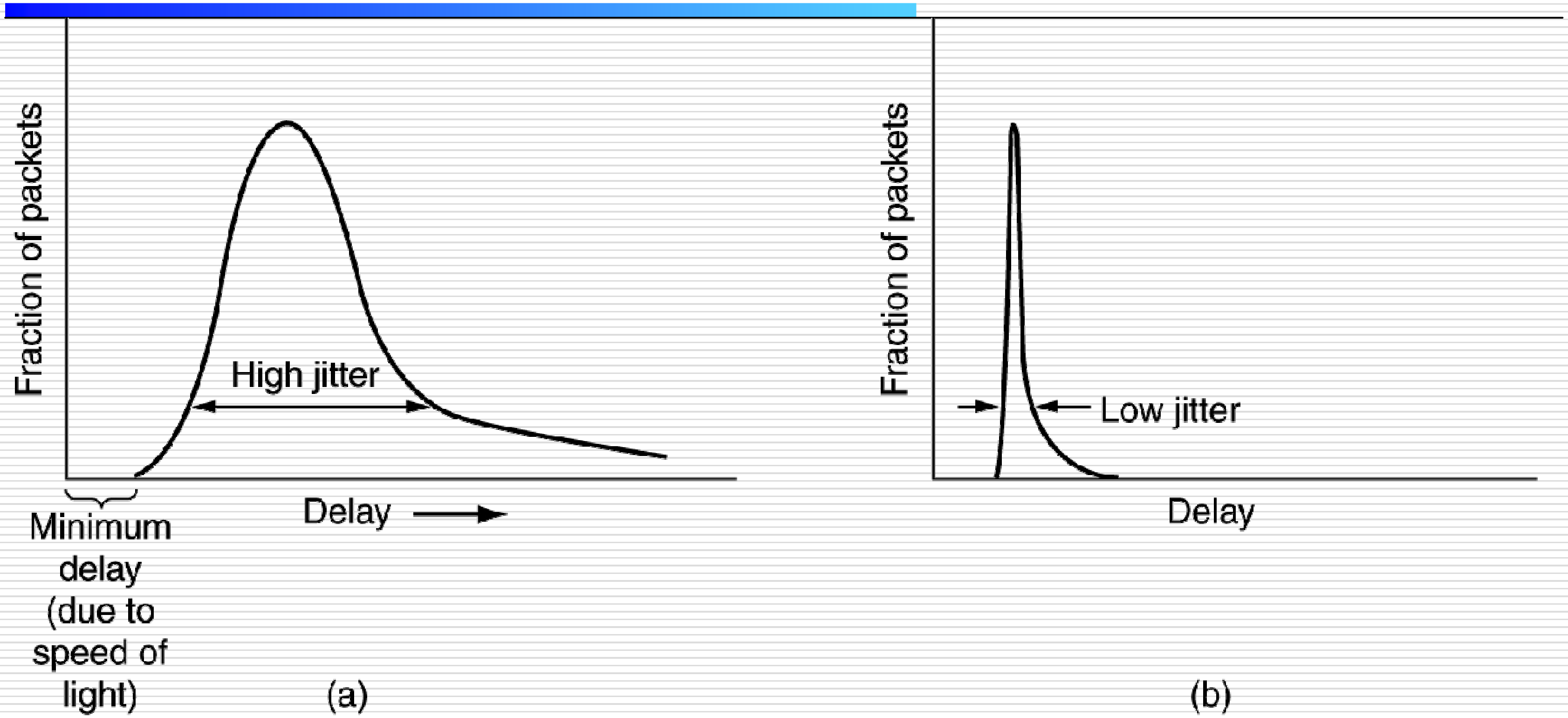
Load Shedding

- When routers are so heavily loaded with packets that they can't handle any more, they just throw them away
- Packets can be selected randomly or by using some selection strategy

Random Early Detection

- It is more effective to detect and prevent congestion from happening
- Routers monitor the network load on their queues, if they predict that congestion is about to happen, they start to drop packets

Jitter Control



Jitter: variation in packet arrival times

(a) High jitter. (b) Low jitter.

Quality of Service

- Requirements
- Techniques for Achieving Good Quality of Service
- Integrated Services
- Differentiated Services
- Label Switching and MPLS

Requirements

How stringent the quality-of-service requirements are.

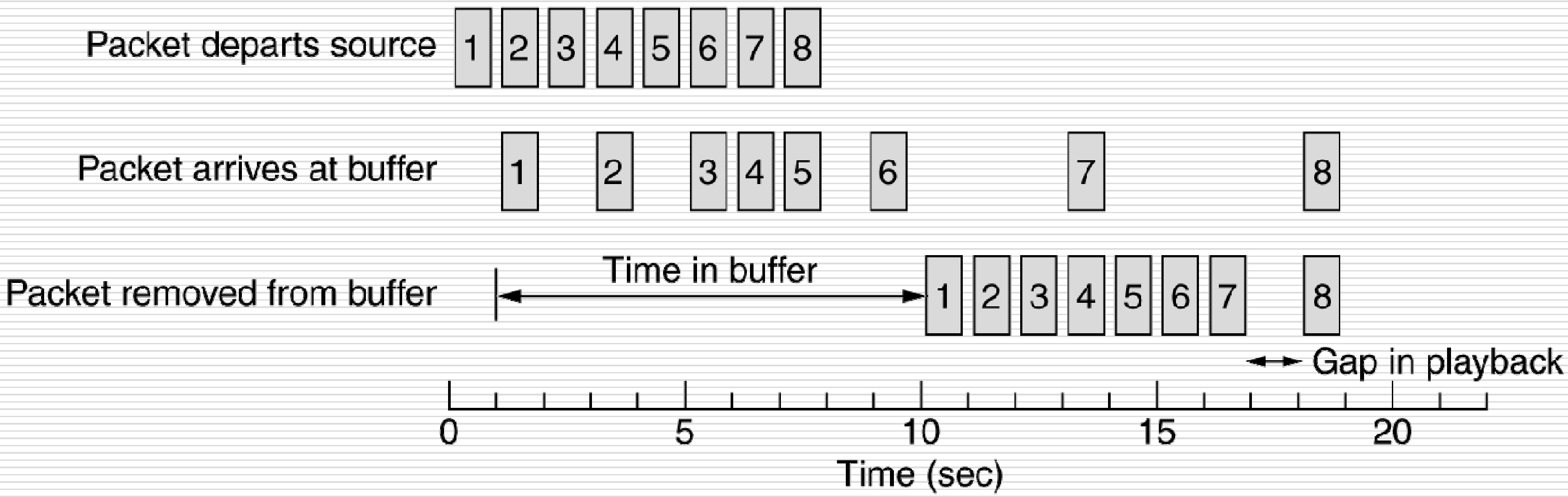
Application	Reliability	Delay	Jitter	Bandwidth
E-mail	High	Low	Low	Low
File transfer	High	Low	Low	Medium
Web access	High	Medium	Low	Medium
Remote login	High	Medium	Medium	Low
Audio on demand	Low	Low	High	Medium
Video on demand	Low	Low	High	High
Telephony	Low	High	High	Low
Videoconferencing	Low	High	High	High

Techniques for Good QoS

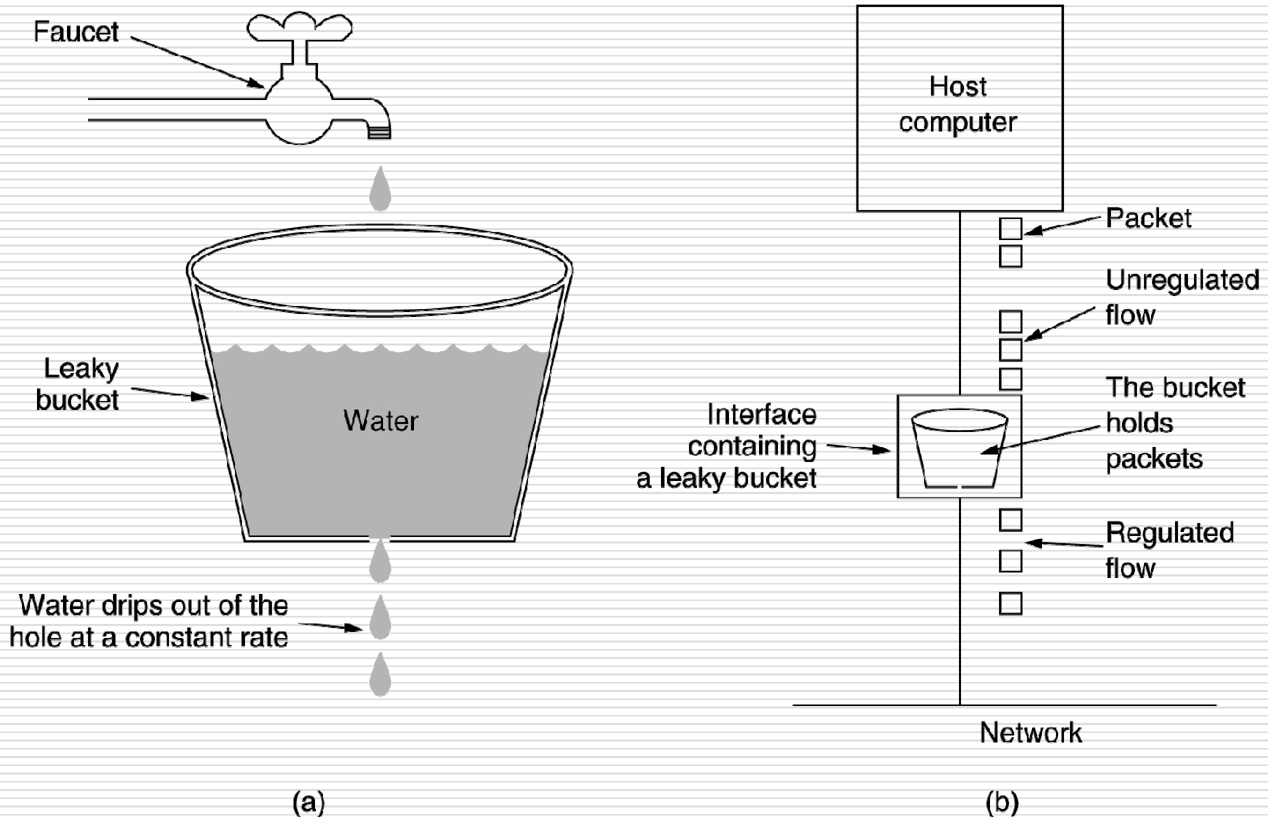
- Overprovisioning
- Buffering
- Traffic shaping
- The leak bucket algorithm
- Token bucket algorithm
- Resource reservation
- Admission control
- Proportional routing
- Packet scheduling

Buffering

Smoothing the output stream by buffering packets.

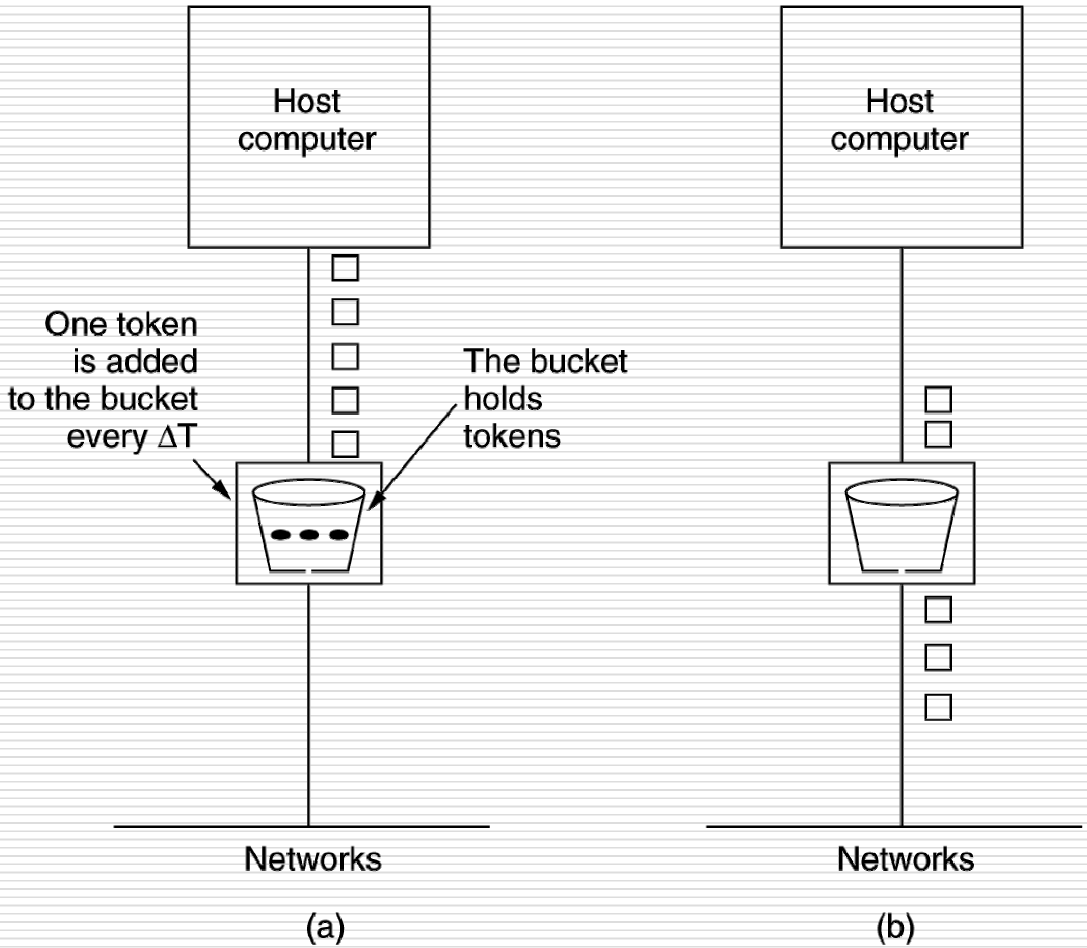


The Leaky Bucket Algorithm



(a) A leaky bucket with water. (b) a leaky bucket with packets.

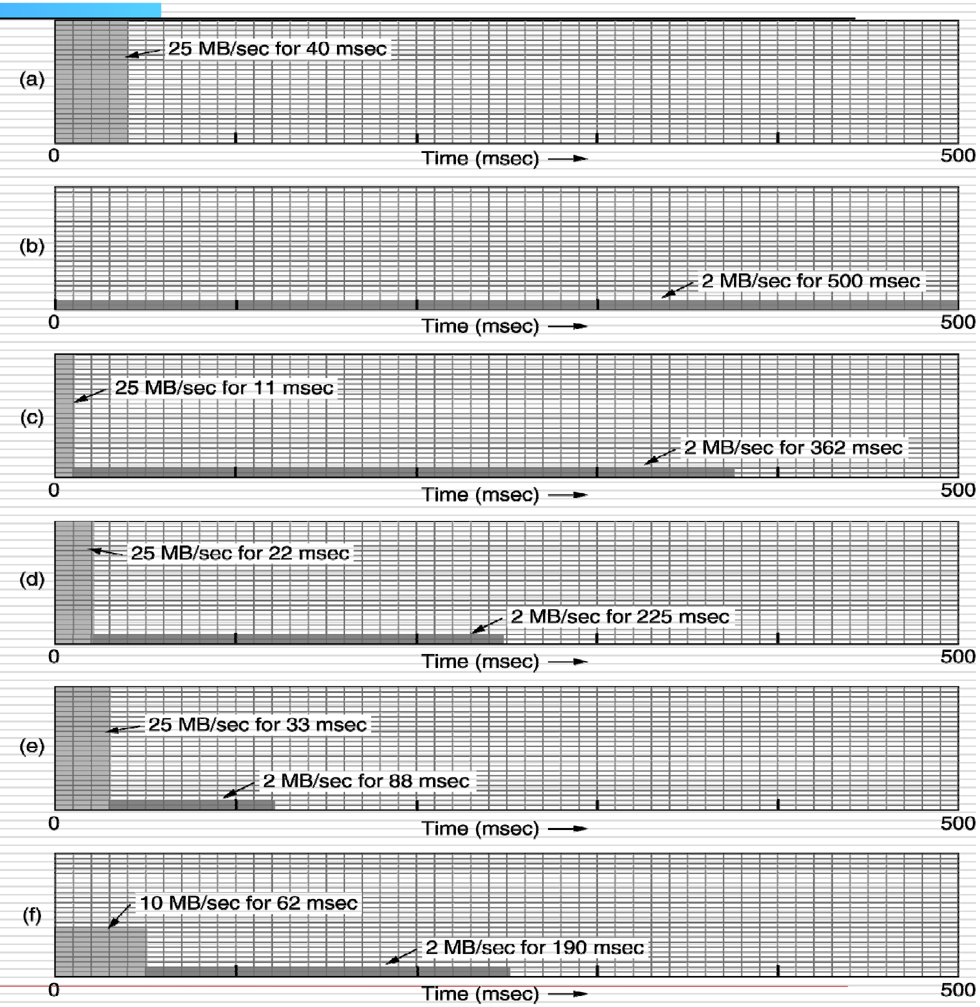
The Token Bucket Algorithm



(a) Before. (b) After.

The Leaky Bucket Algorithm

(a) Input to a leaky bucket. (b) Output from a leaky bucket. Output from a token bucket with capacities of (c) 250 KB, (d) 500 KB, (e) 750 KB, (f) Output from a 500KB token bucket feeding a 10-MB/sec leaky bucket.



Resource Reservation

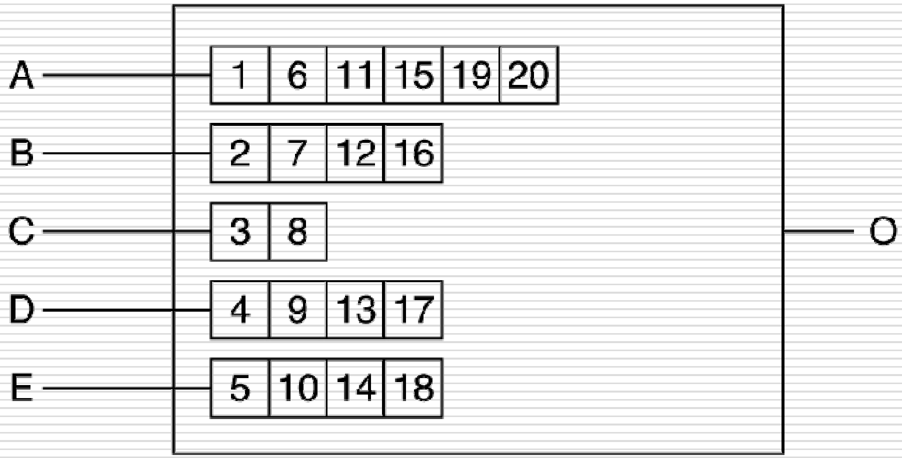
- Packets of a flow have to follow the same route, similar to a virtual circuit
- Resources can be reserved
  - Bandwidth
  - Buffer space
  - CPU cycles (of routers)

Admission Control

An example of flow specification.

Parameter	Unit
Token bucket rate	Bytes/sec
Token bucket size	Bytes
Peak data rate	Bytes/sec
Minimum packet size	Bytes
Maximum packet size	Bytes

Packet Scheduling



(a)

Packet	Finishing time
C	8
B	16
D	17
E	18
A	20

(b)

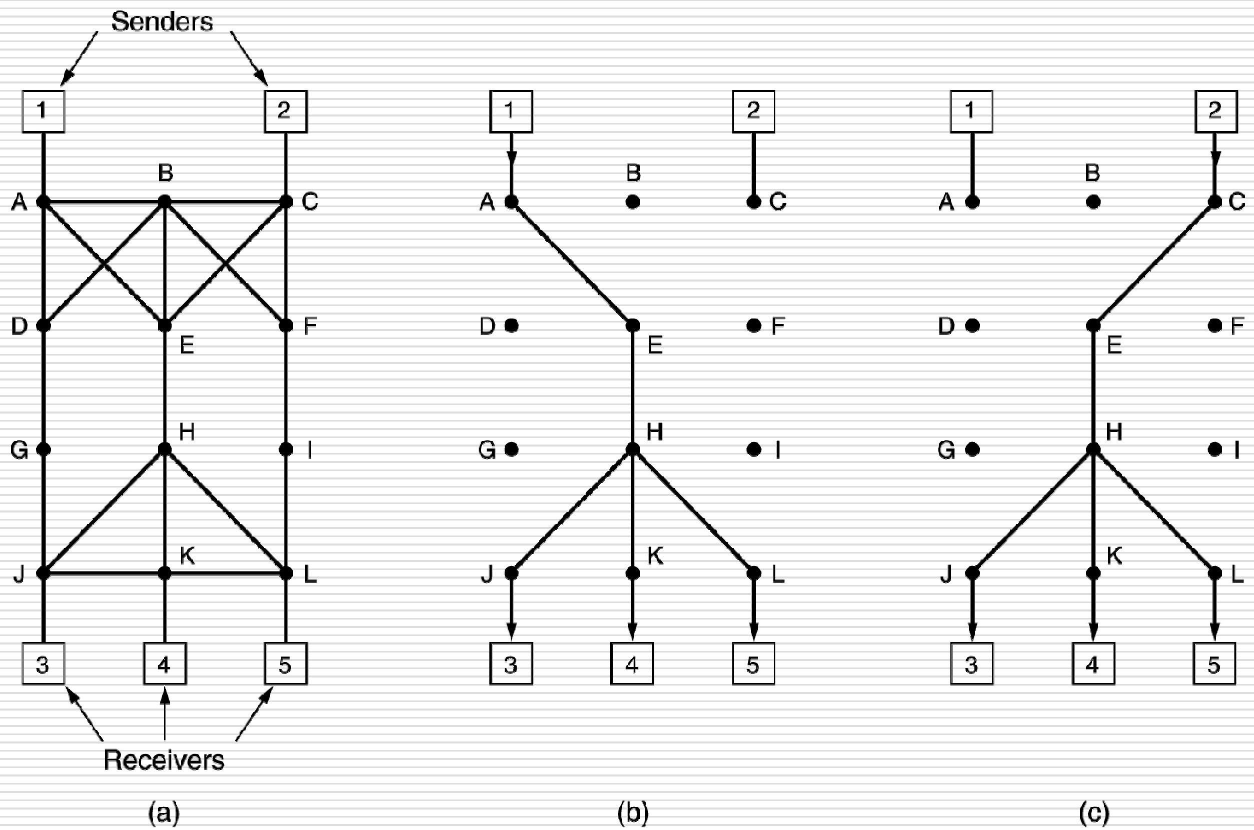
(a) A router with five packets queued for line O.

(b) Finishing times for the five packets.

Integrated Services

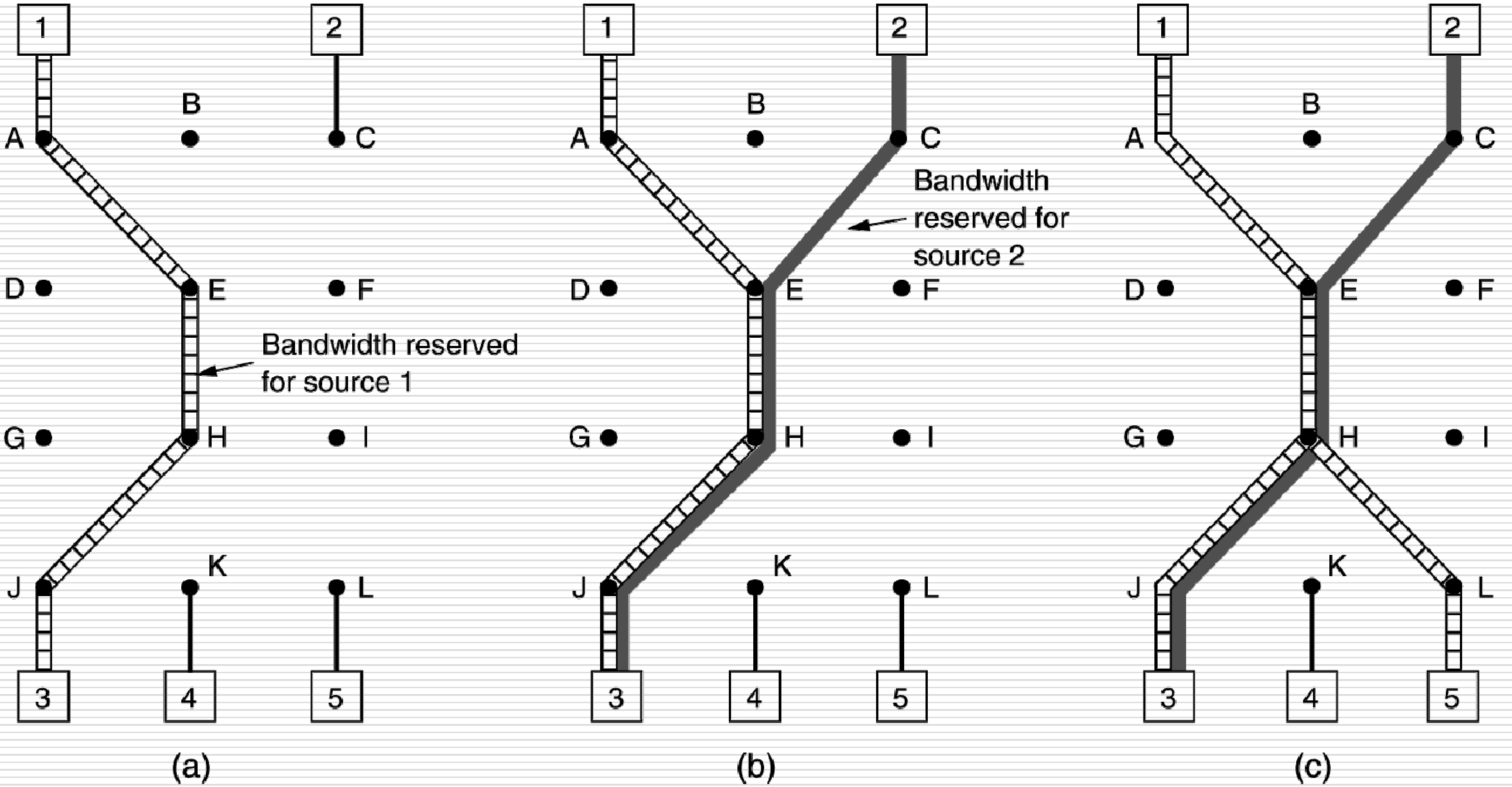
- An architecture for streaming multimedia
- Flow-based reservation algorithms
- Aimed at both unicast and multicast application
- Main protocol: RSVP – Resource reSerVation Protocol

RSVP-The Resource reSerVation Protocol



(a) A network, (b) The multicast spanning tree for host 1.
(c) The multicast spanning tree for host 2.

RSVP-The Resource reSerVation Protocol (2)



(a) Host 3 requests a channel to host 1. (b) Host 3 then requests a second channel, to host 2. (c) Host 5 requests a channel to host 1.

RSVP-The Resource reSerVation Protocol (3)

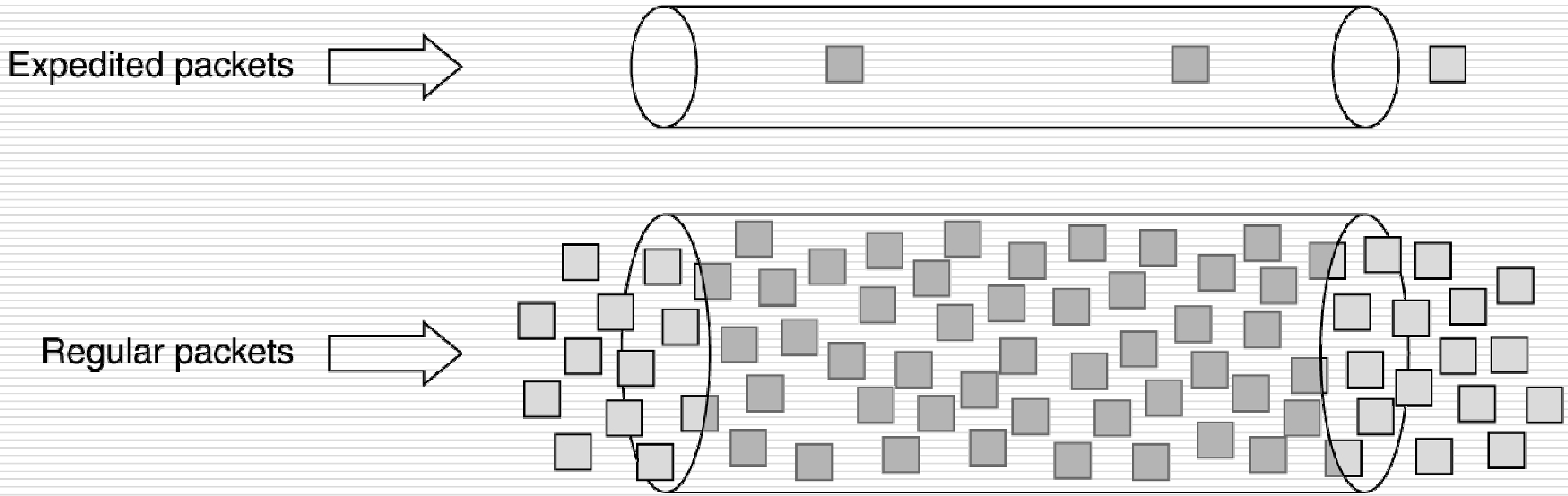
- Flow-based algorithms (e.g. RSVP) have the potential to offer good quality of service
- However:
  - Require advanced setup to establish each flow
  - Maintain internal per-flow state in routers
  - Require changes to router code and involve complex router-to-router exchanges
- Very few, or almost no implementation, of RSVP

Differentiated Services

- Class-based quality of service
- Administration defines a set of service classes with corresponding forwarding rules
- Customers sign up for service class they want
- Similar to postal mail services: Express or Regular
- Examples: expedited forwarding and assured forwarding

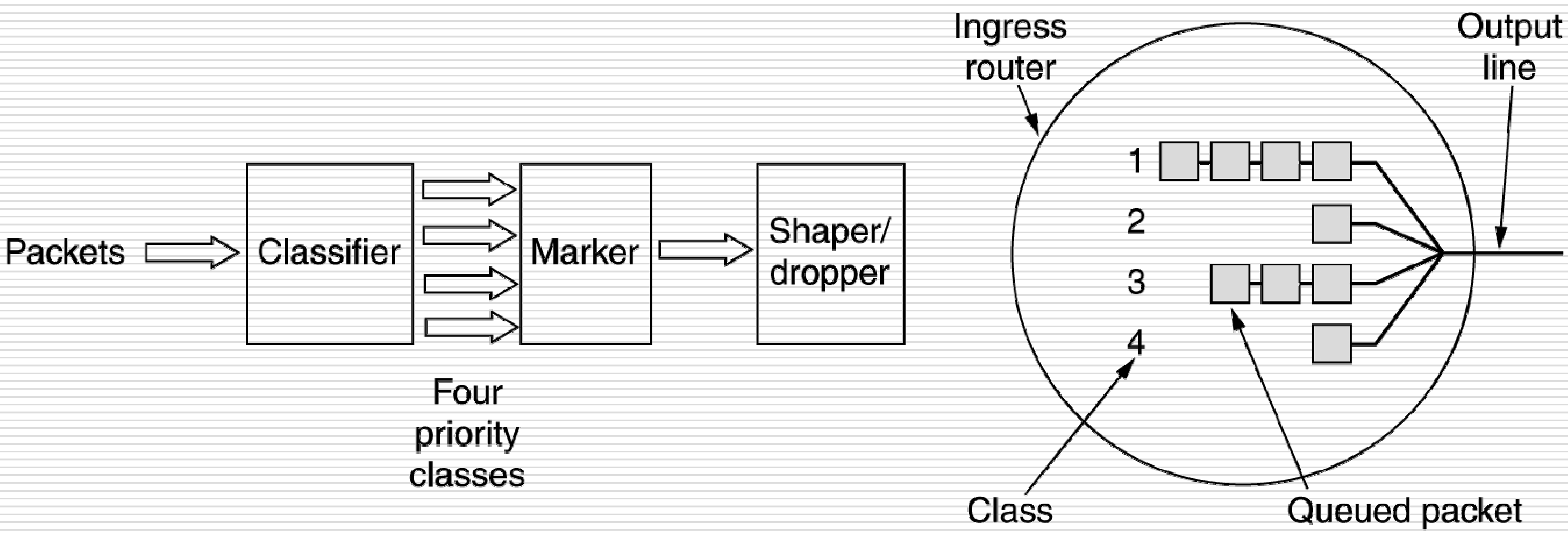
Expedited Forwarding

Expedited packets experience a traffic-free network.



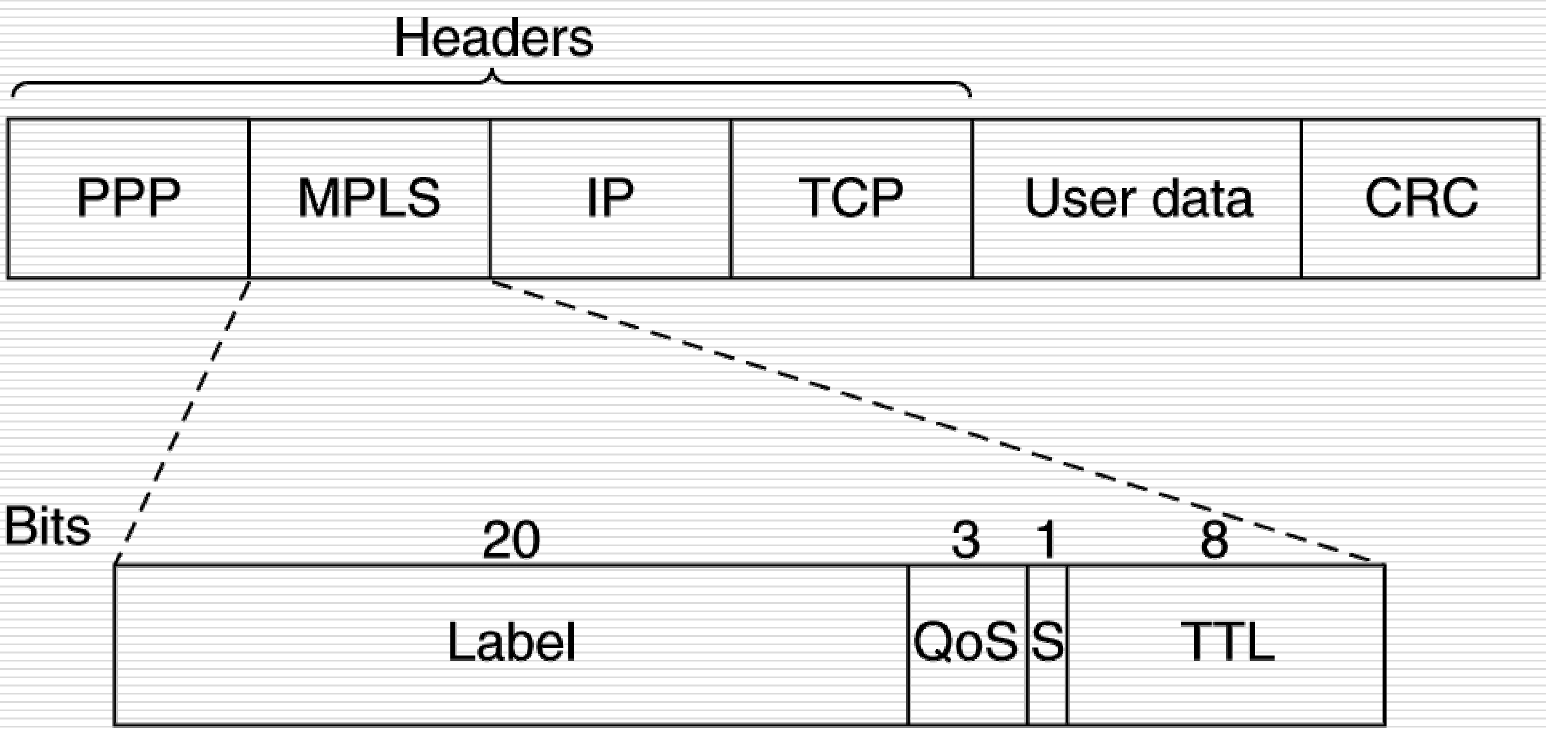
Assured Forwarding

A possible implementation of the data flow for assured forwarding.



Label Switching and MPLS

Transmitting a TCP segment using IP, MPLS, and PPP.

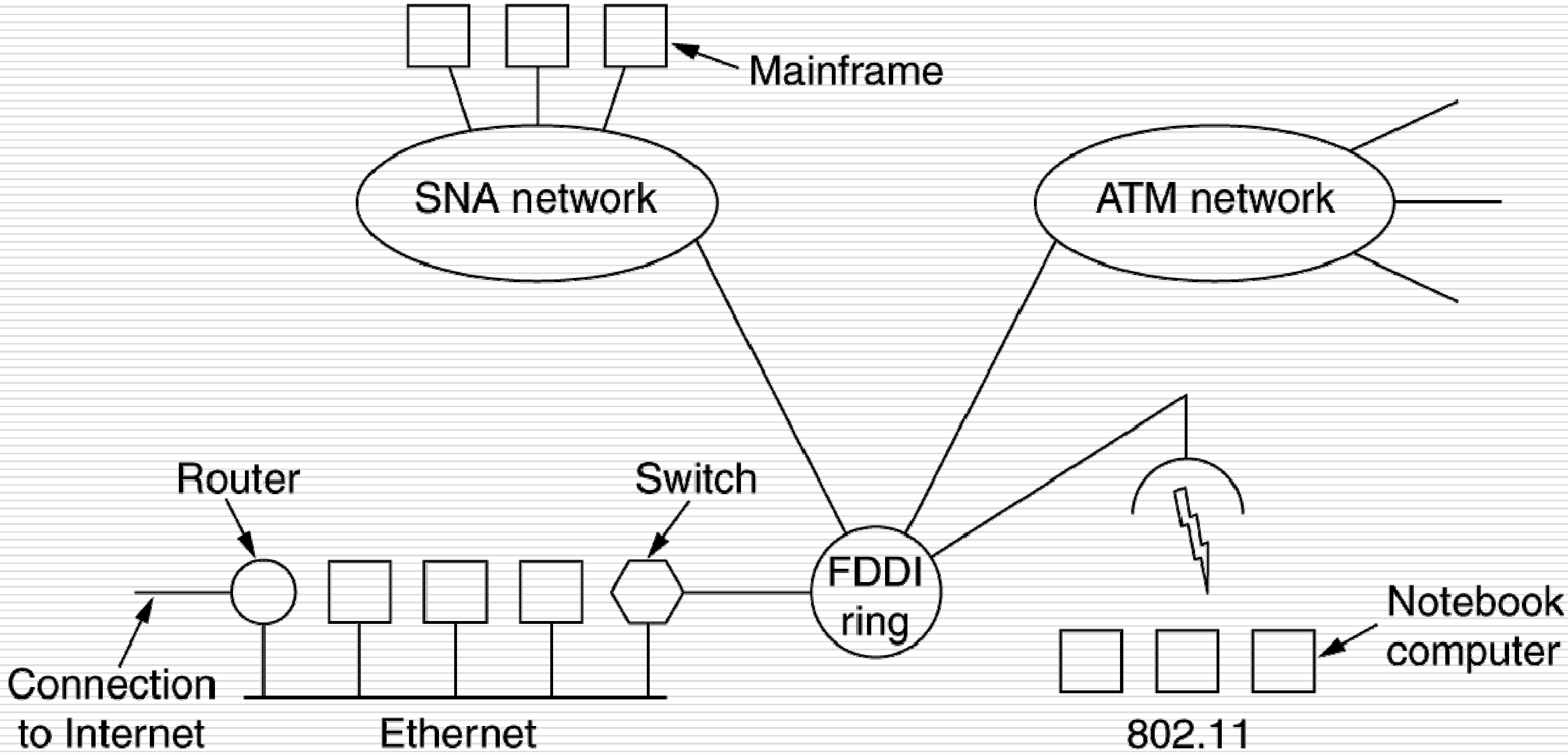


Internetworking

- How Networks Differ
- How Networks Can Be Connected
- Concatenated Virtual Circuits
- Connectionless Internetworking
- Tunneling
- Internetwork Routing
- Fragmentation

Connecting Networks

A collection of interconnected networks.



How Networks Differ

Some of the many ways networks can differ.

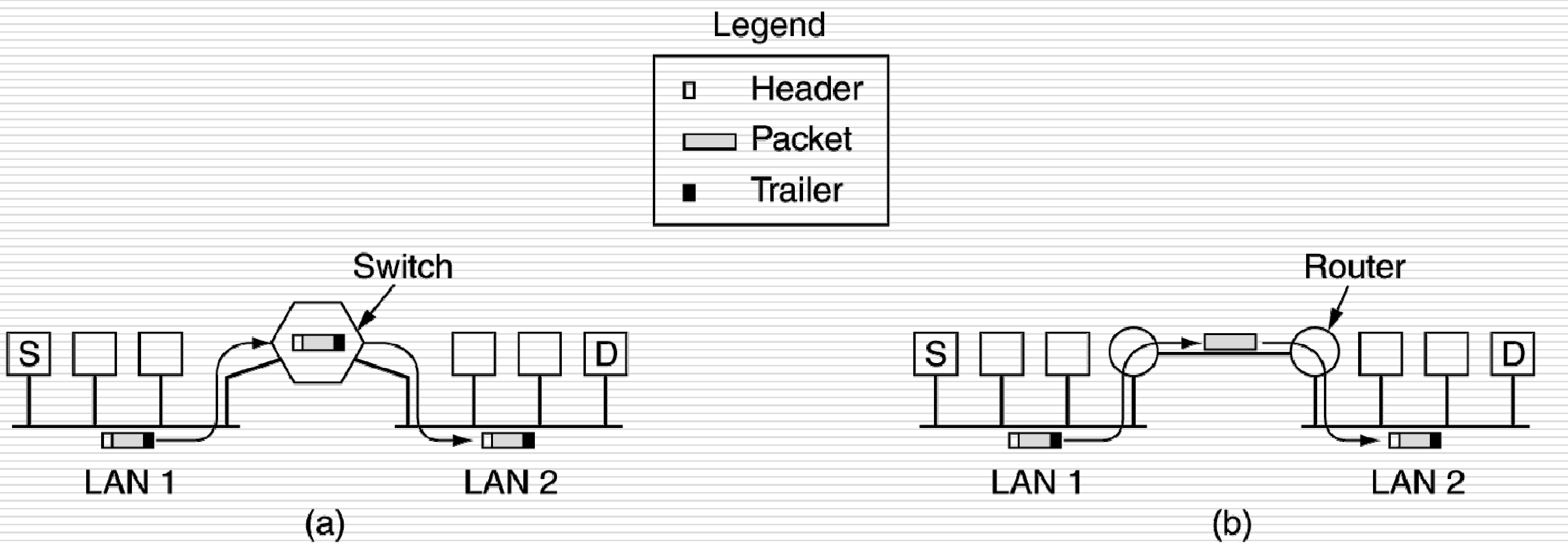
Item	Some Possibilities
Service offered	Connection oriented versus connectionless
Protocols	IP, IPX, SNA, ATM, MPLS, AppleTalk, etc.
Addressing	Flat (802) versus hierarchical (IP)
Multicasting	Present or absent (also broadcasting)
Packet size	Every network has its own maximum
Quality of service	Present or absent; many different kinds
Error handling	Reliable, ordered, and unordered delivery
Flow control	Sliding window, rate control, other, or none
Congestion control	Leaky bucket, token bucket, RED, choke packets, etc.
Security	Privacy rules, encryption, etc.
Parameters	Different timeouts, flow specifications, etc.
Accounting	By connect time, by packet, by byte, or not at all

5-43

How Networks Can Be Connected

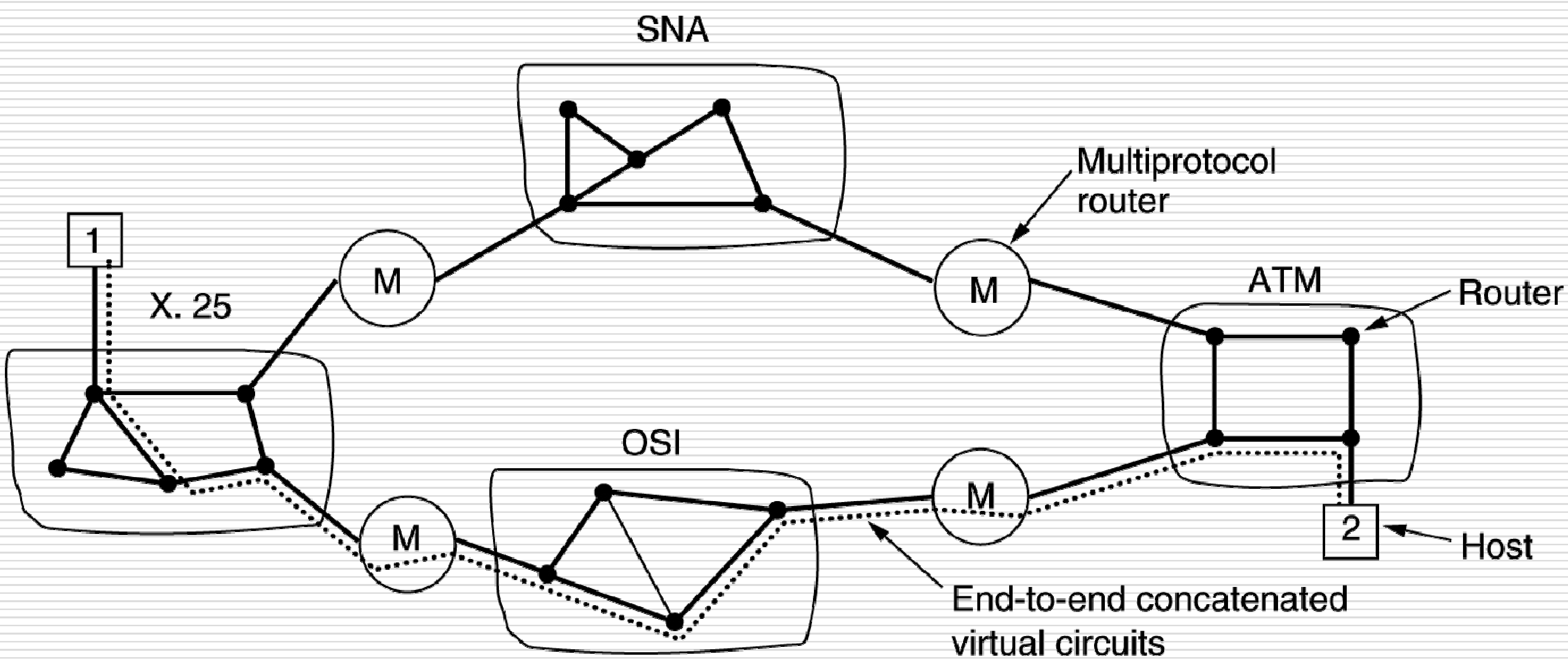
(a) Two Ethernets connected by a switch.

(b) Two Ethernets connected by routers.



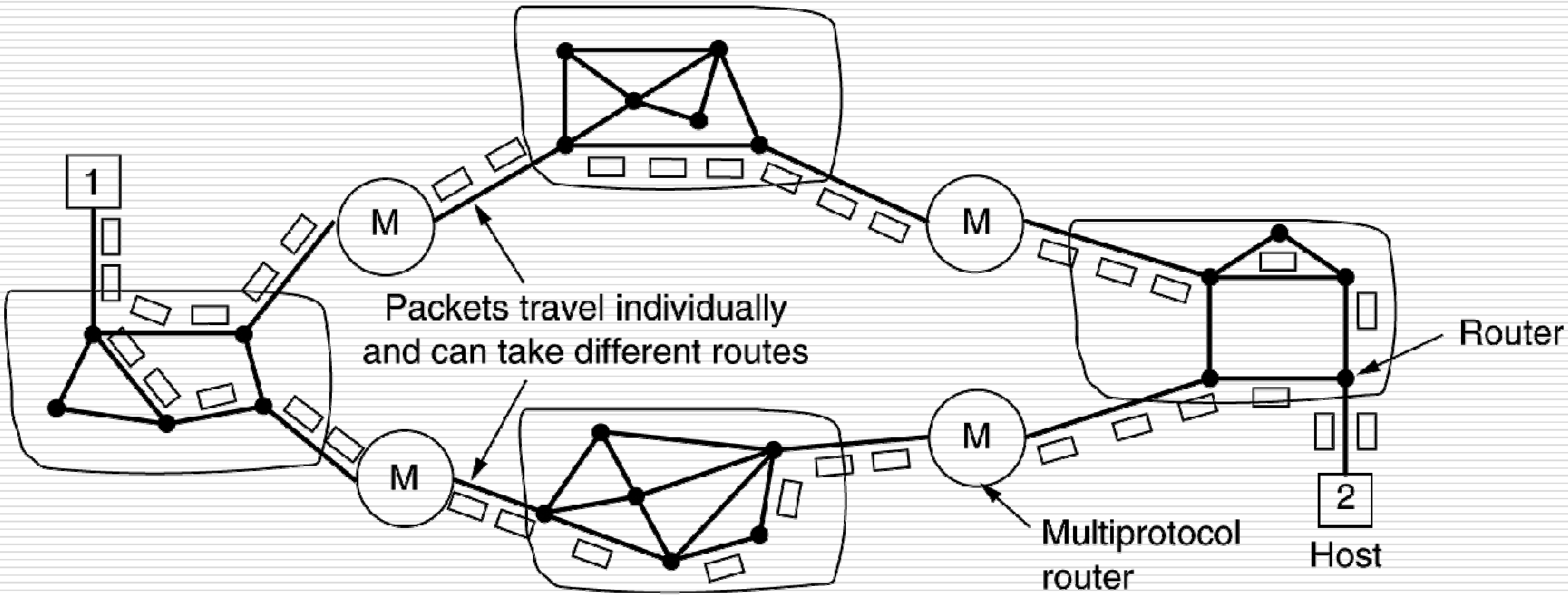
Concatenated Virtual Circuits

Internetworking using concatenated virtual circuits.



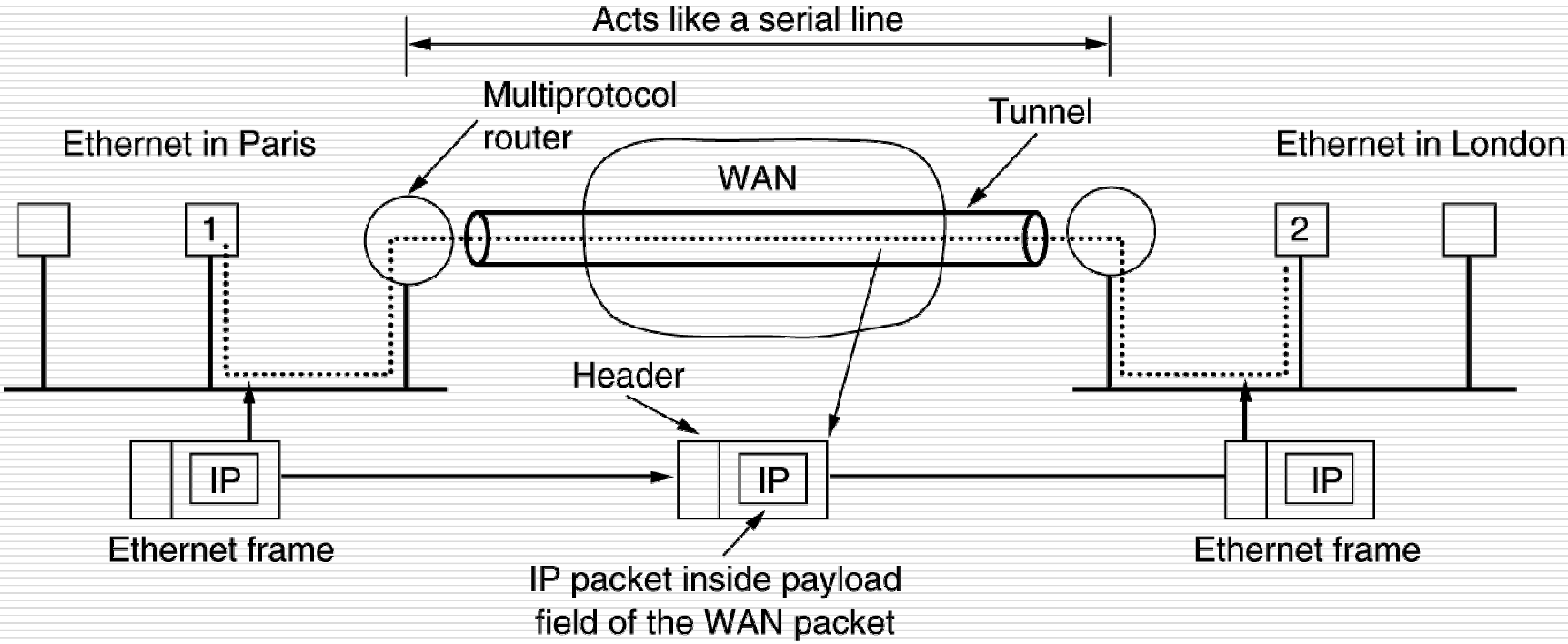
Connectionless Internetworking

A connectionless internet.



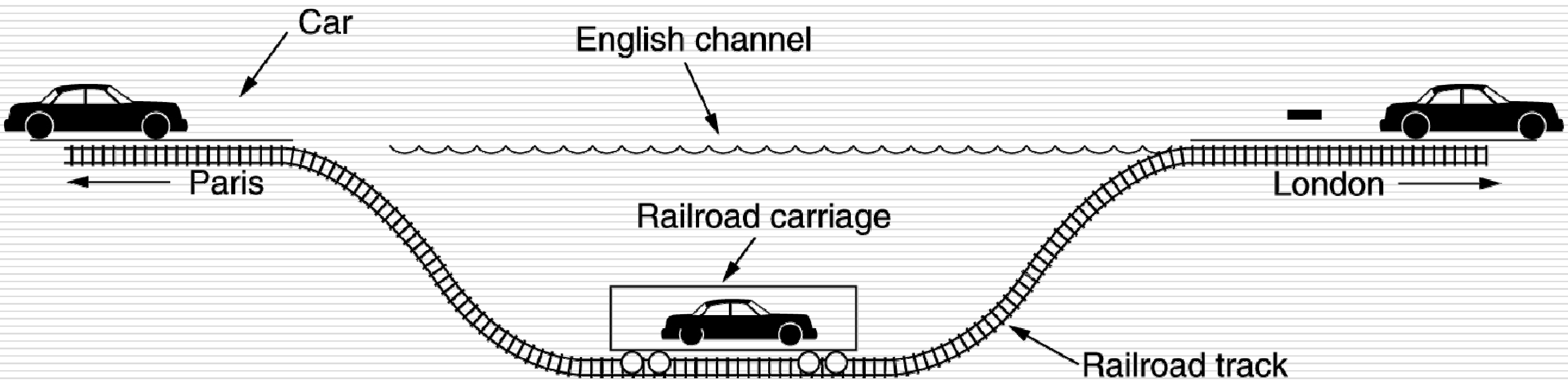
Tunneling

Tunneling a packet from Paris to London.



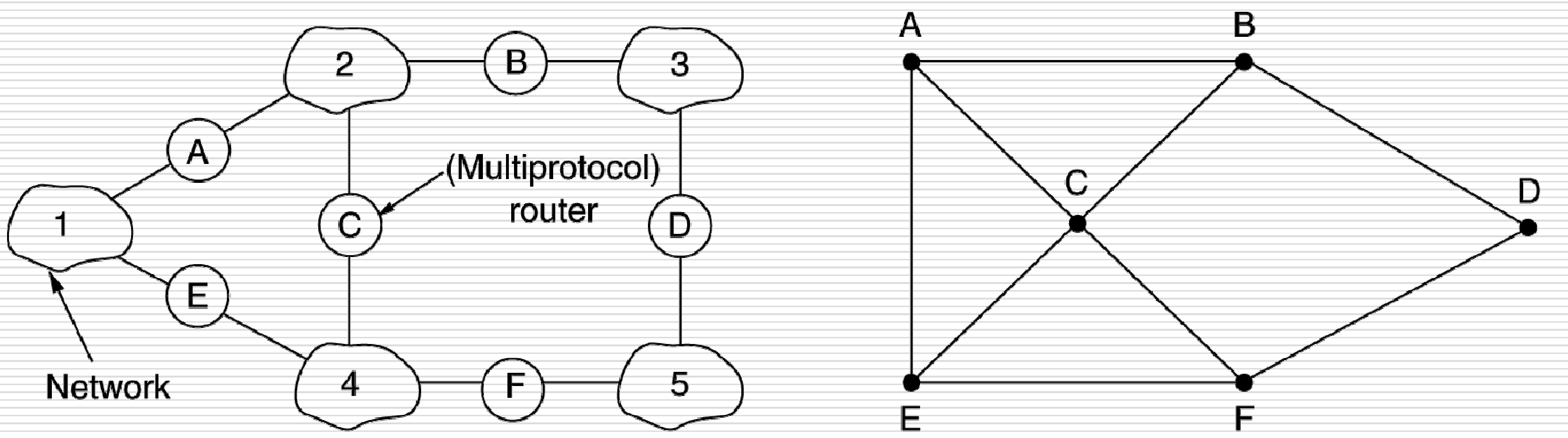
Tunneling (2)

Tunneling a car from France to England.



Internetwork Routing

(a) An internetwork. (b) A graph of the internetwork.

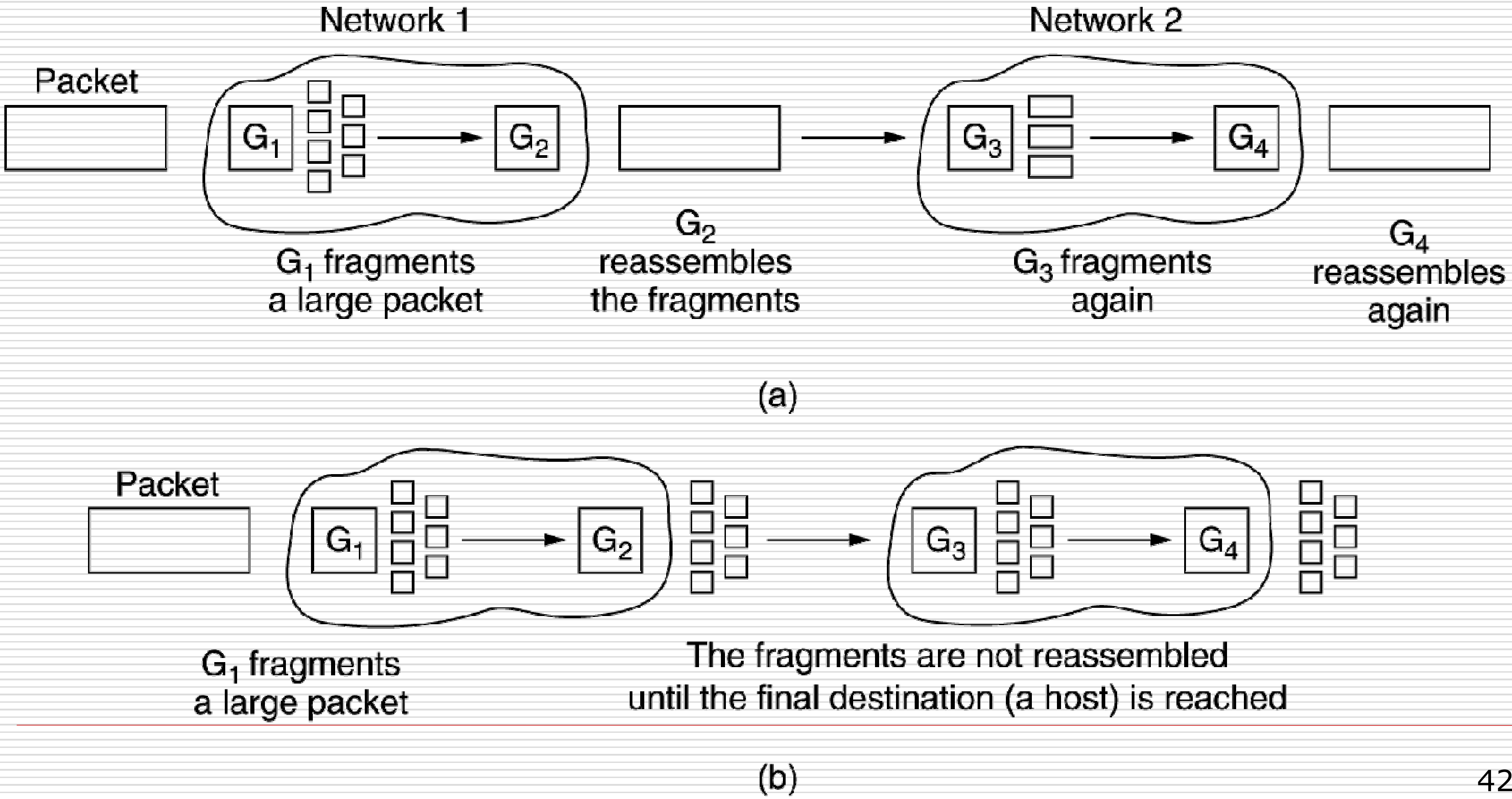


(a) (b)

Fragmentation (1)

(a) Transparent fragmentation.

(b) Nontransparent fragmentation.



Fragmentation (2)

Fragmentation when the elementary data size is 1 byte.
(a) Original packet, containing 10 data bytes.
(b) Fragments after passing through a network with maximum packet size of 8 payload bytes plus header.
(c) Fragments after passing through a size 5 gateway.