NETWORK LAYER : ROUTING ALGORITHMS

DR. RAVINDRA NATH UIET CSJM
UNIVERSITY KANPUR

FUNCTIONS OF THE NETWORK LAYER

- To transport packets from the source to the destination, possibly through some intermediate nodes.
- This involves:
    - Knowing the topology of the communication network.
    - Choosing routes judiciously to avoid overloading some paths.
    - Resolve problems that may arise if Source and Destination are not on the same network.
- In other words, Network Layer performs:
    - Routing
    - Congestion control
    - Internetworking

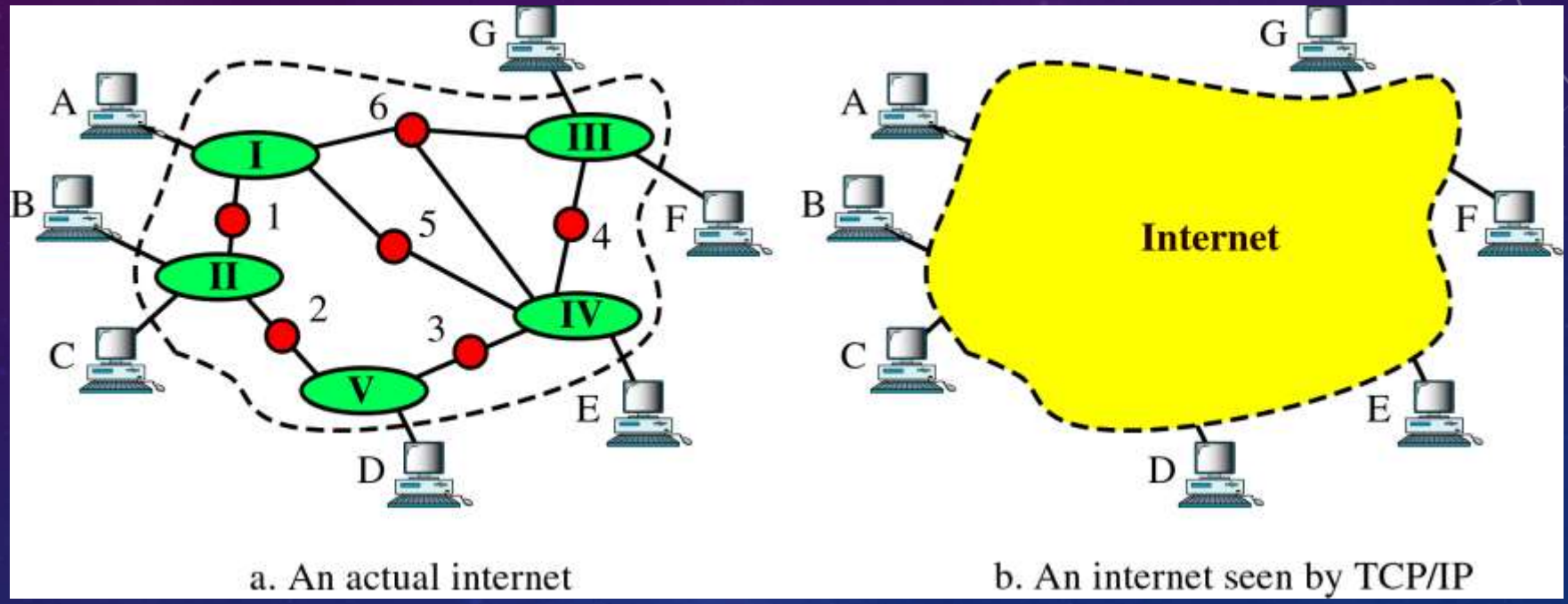
NETWORK LAYER SERVICE CLASSES

Two possible classes:

- Connection-oriented -- *reliable*, in-sequence delivery.
- Connectionless -- *unreliable*, out-of-order delivery.

- Connection -- logical concept of an entity that connects the Source and Destination at its two ends.
- Supporters for both connection-oriented and connectionless service and so OSI framework supports both.
- Issue of *Connection-oriented* and *Connectionless* service also comes up in other layers.

An Internet According to TCP/IP



VIRTUAL CIRCUIT

- Analogous to physical end-to-end telephone connections.
- When connection is setup, the route over which the packet travels is fixed.
- That route is used by all packets delivered on the Virtual Circuit; *Routing decision need not be taken every time.*
- Packets contain just a circuit identifier rather than full destination address; *Packets are thus smaller.*
- *Disadvantage:*
  - If a node along the route fails, or if there is congestion, causes major problems.
  - Some space on the nodes is used up for tables with entries about various Virtual Circuits.
- Useful for **Connection-oriented** service.

DATAGRAMS

- No routes are worked out in advance.
- Each packet is routed independently of its predecessors and is called a *datagram.*
- Successive packets may follow different routes.
- Each packet should contain full source and destination address.
- *Advantage:* Robust, can adapt to failure of intermediate nodes and congestion.
- Disadvantage:
  - Packets are larger and therefore require more bandwidth.
  - Routing decisions to be made every time causes an additional computational overhead.
- Can be used for **both** *Connection-oriented* and *Connectionless* services.

Datagram Vs Virtual Circuit Subnets

Issue	Datagram subnet	VC subnet
Circuit setup	Not needed	Required
Addressing	Each packet contains the full source and destination address	Each packet contains a short VC number
State information	Subnet does not hold state information	Each VC requires subnet table space
Routing	Each packet is routed independently	Route chosen when VC is set up; all packets follow this route
Effect of router failures	None, except for packets lost during the crash	All VCs that passed through the failed router are terminated
Congestion control	Difficult	Easy if enough buffers can be allocated in advance for each VC

Upper layer	Type of subnet	
	Datagram	Virtual circuit
Connectionless	UDP over IP	UDP over IP over ATM
Connection-oriented	TCP over IP	ATM AAL1 over ATM

[redacted] Examples of different combinations of service and subne structure.

ROUTING

- As packets are transported from source nodes to destination nodes, they often require multiple hops to make the journey.
- Routing is the process of deciding what path a packet will take to reach its destination.
- Routing involves the design of:
  - an algorithm to compute routes.
  - data structures to help choose routes.
- A Routing Algorithm:
  - is a part of Network layer software.
  - decides which output link an incoming packet should be transmitted on.

Routing Algorithms

Non Adaptive Algorithms (Static Routing)

The routes are decided or computed in advance, off-line and downloaded to the routers when the network is booted.

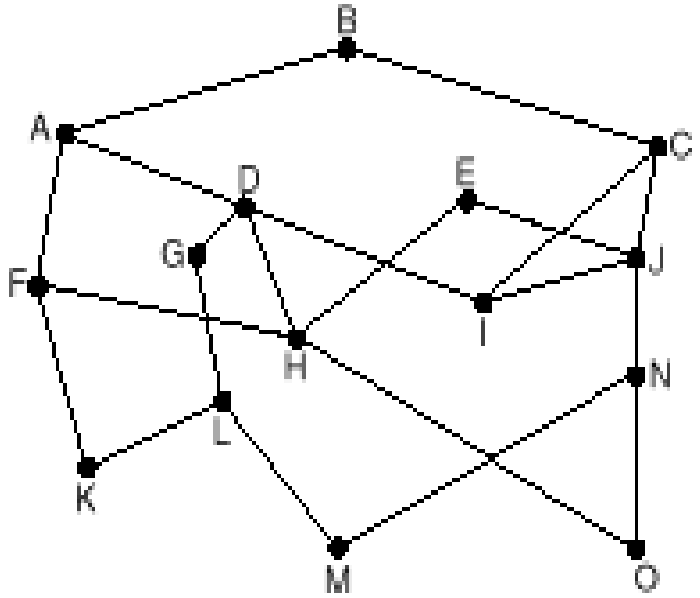
Adaptive Algorithms

Change the routing decisions based on changes in the topology, traffic

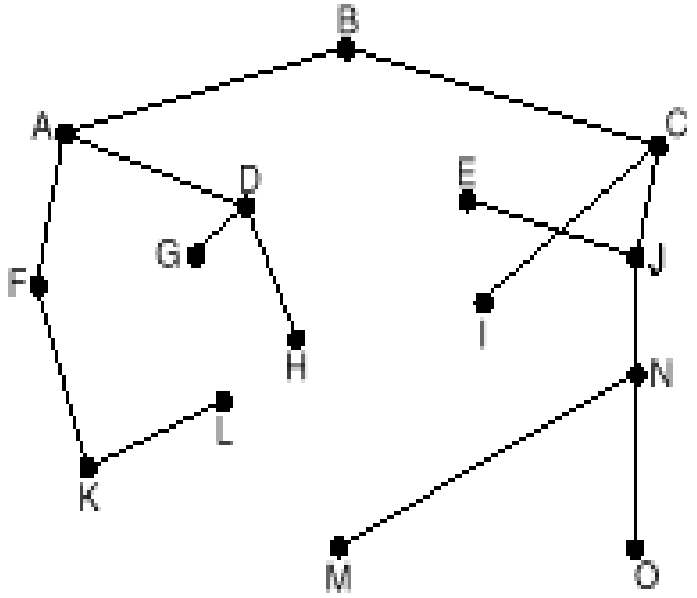
Get the routing information from adjacent routers, or when they change routes (every δT sec, load changes, topology changes)

Metric used for optimization are distance, no. of hops, time etc.,

Sink Tree based on No. of Hops



(a)



(b)

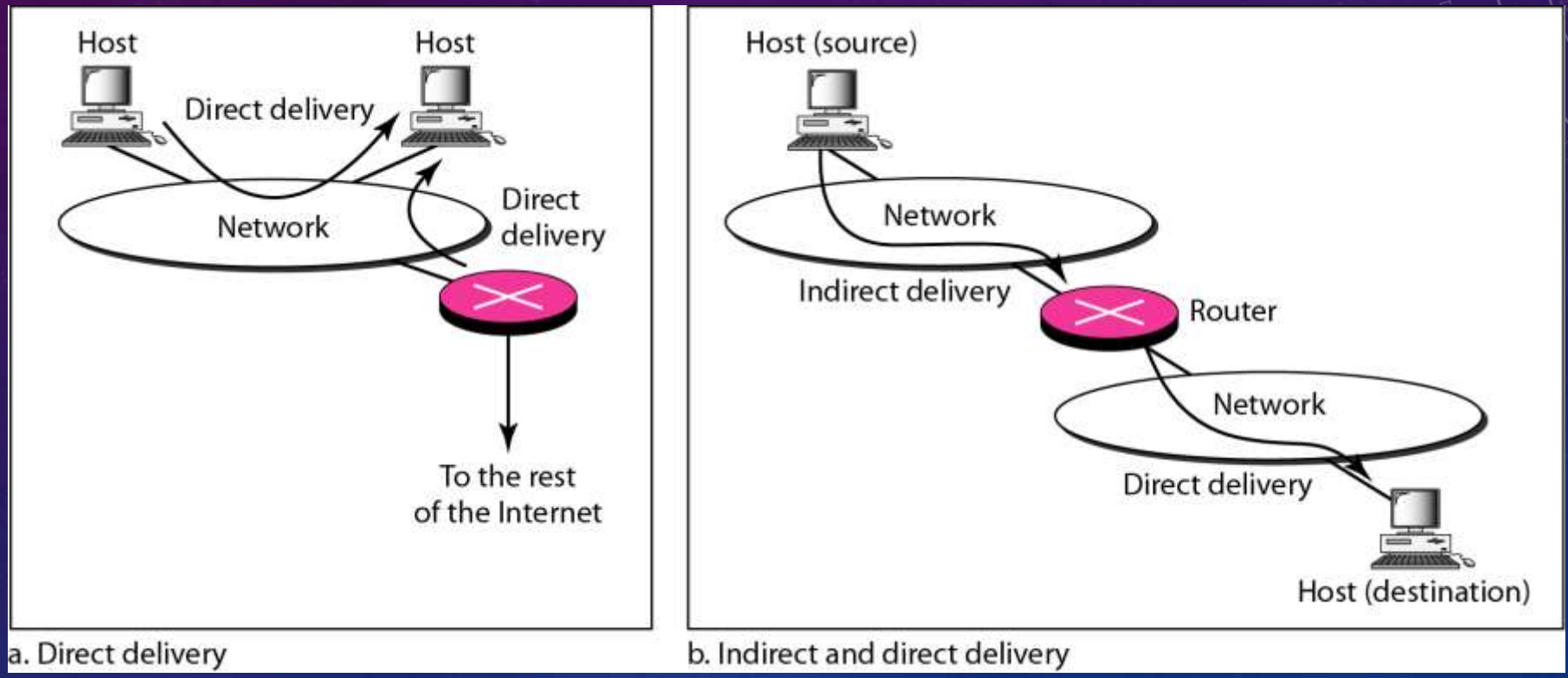
[redacted]. (a) A subnet. (b) A sink tree for router *B*.

ROUTING

- **Direct Routing:**
  - When destination is on the same network.
  - Find the MAC address.
  - Encapsulate the datagram in MAC frame.
  - Send the frame to destination.
- **Indirect Routing:** Find out which is the next host to send the datagram.

The network layer supervises the handling of the packets by the underlying physical networks. We define this handling as the delivery of a packet.

Direct and indirect delivery



a. Direct delivery

b. Indirect and direct delivery

Forwarding

Forwarding means to place the packet in its route to its destination. Forwarding requires a host or a router to have a routing table. When a host has a packet to send or when a router has received a packet to be forwarded, it looks at this table to find the route to the final destination.

ROUTING PROCEDURE

- Try Direct routing.
- Check for host-specific route.
- Check route for the destination network.
- Use the Default route.

Route method versus next-hop method

a. Routing tables based on route

Destination	Route
Host B	R1, R2, host B

Routing table for host A

Destination	Route
Host B	R2, host B

Routing table for R1

Destination	Route
Host B	Host B

Routing table for R2

b. Routing tables based on next hop

Destination	Next hop
Host B	R1

Destination	Next hop
Host B	R2

Destination	Next hop
Host B	---

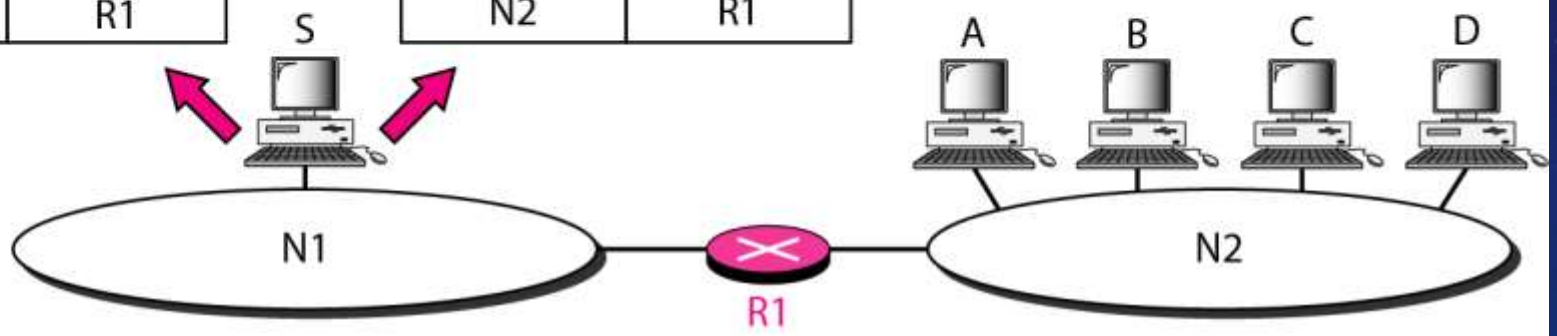
Host-specific versus network-specific method

Routing table for host S based on host-specific method

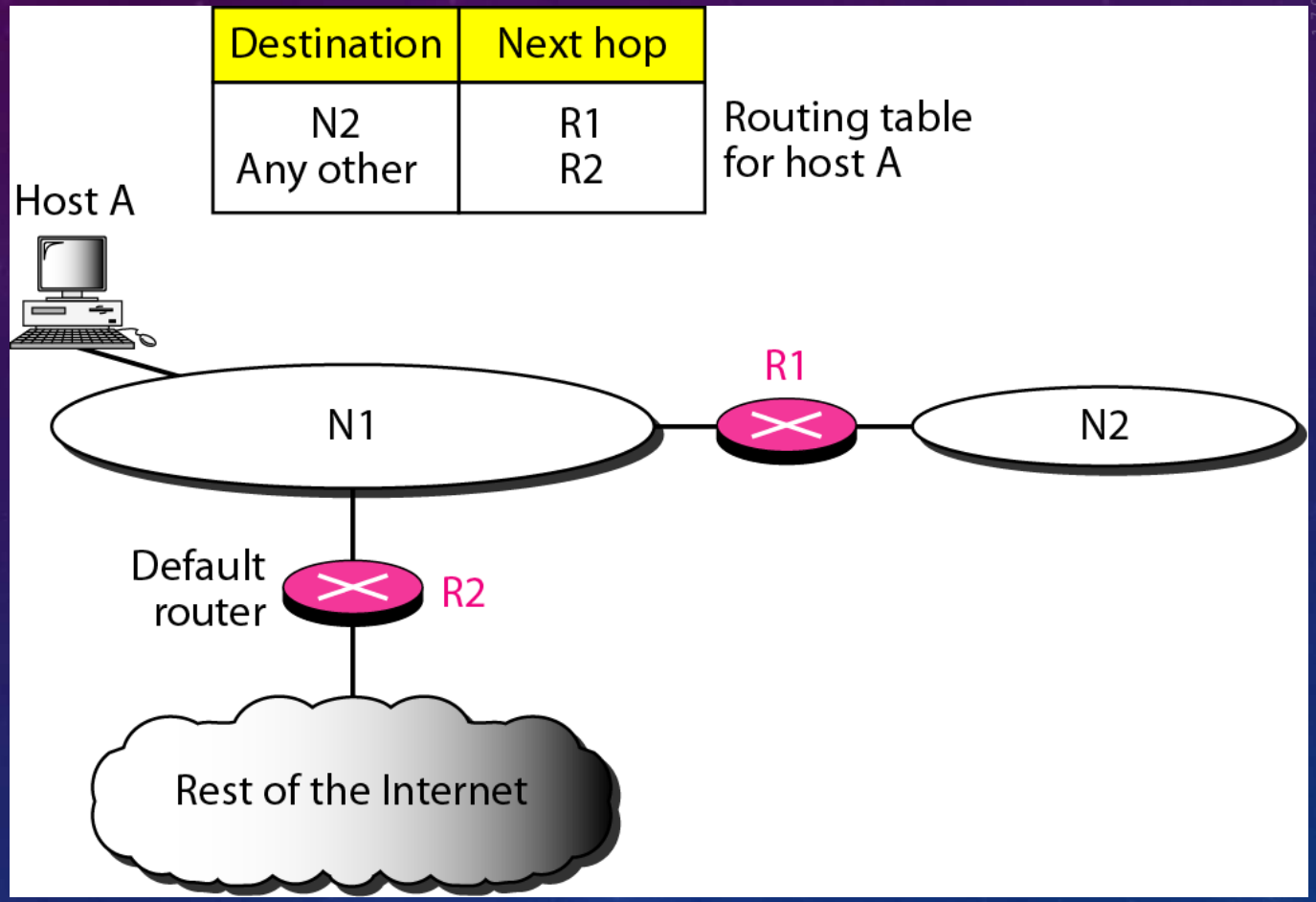
Destination	Next hop
A	R1
B	R1
C	R1
D	R1

Routing table for host S based on network-specific method

Destination	Next hop
N2	R1



Default method

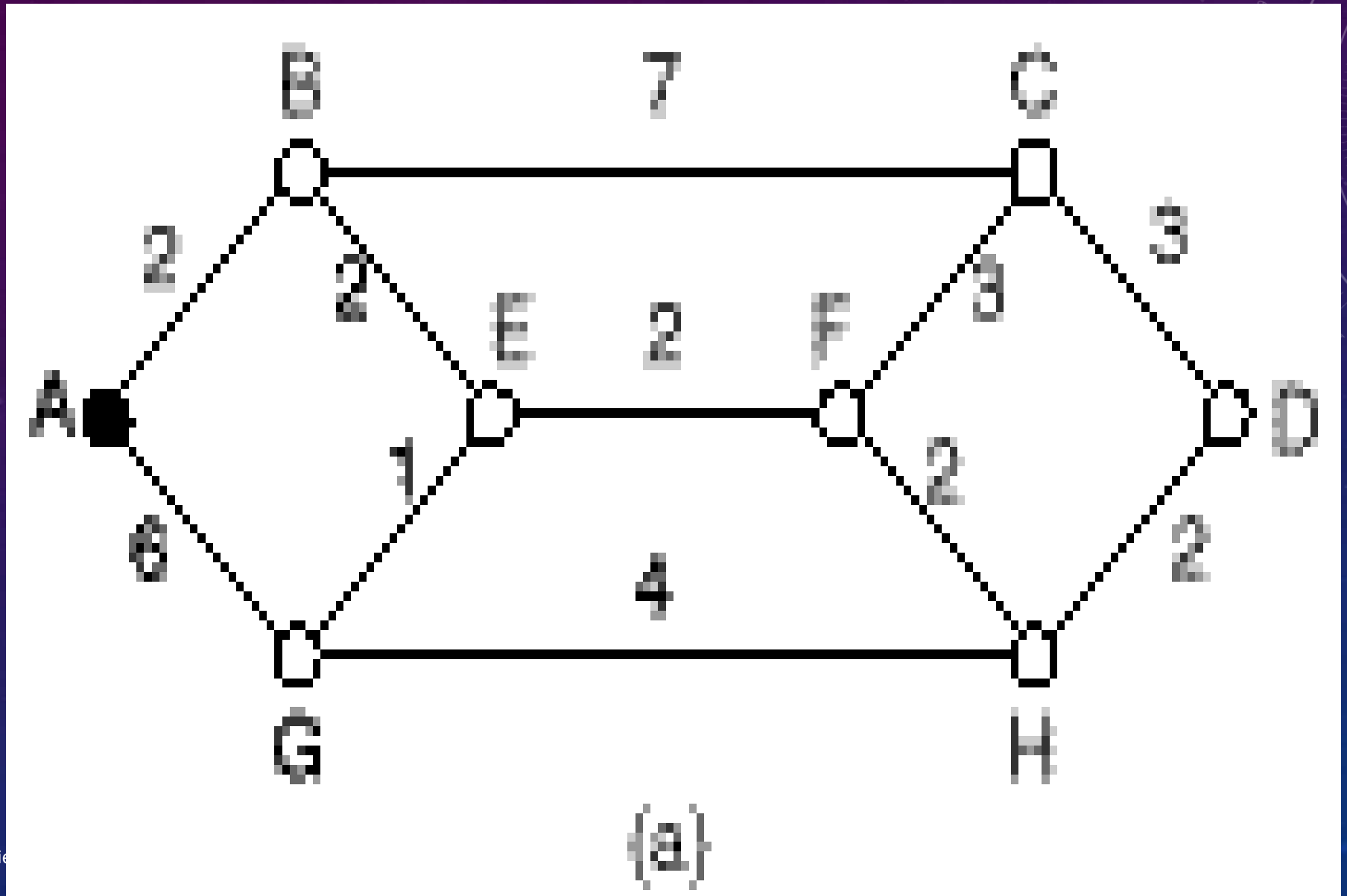


ROUTING TABLE

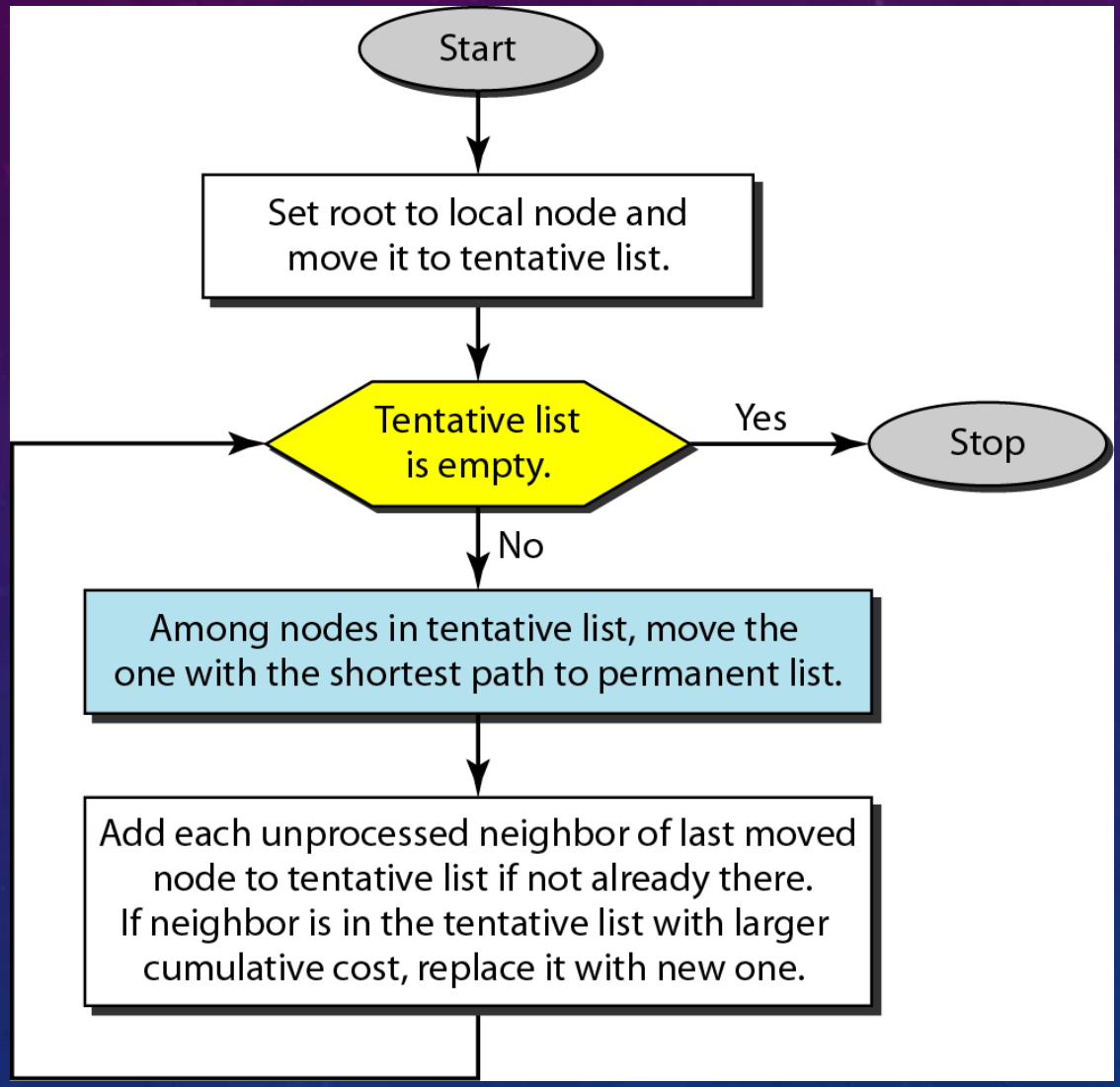
Each node maintains a routing table.

- Table contains pairs (address, next-hop).
- Entries could be network-specific or host-specific.
- Also contains default route entry.
- May contain multiple entries for ToS (type-of-service) routing.
- Table can be created either manually or by a routing protocol, e.g., RIP, or Hello.

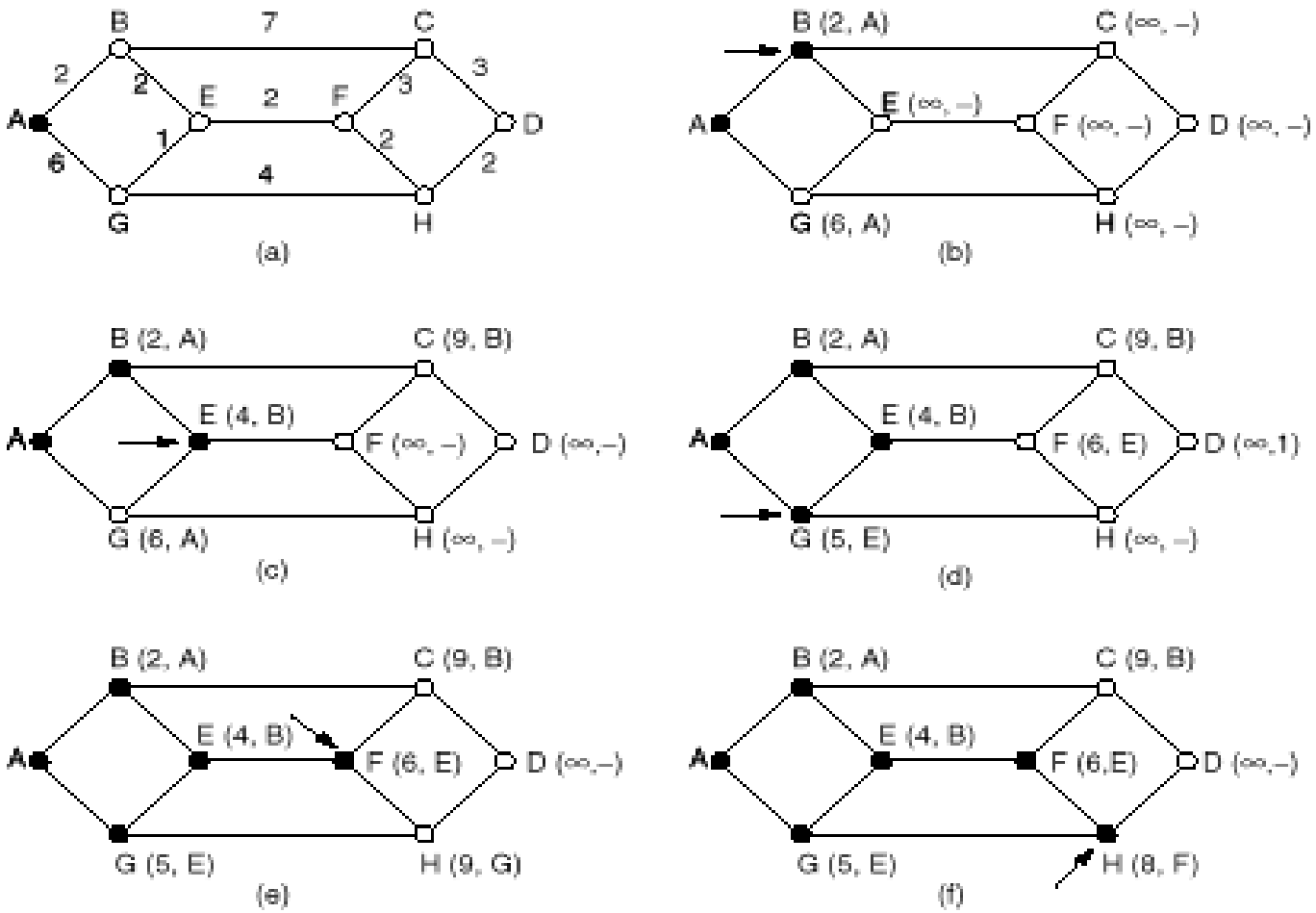
Dijkstra's Shortest Path Routing Algorithm



Dijkstra algorithm

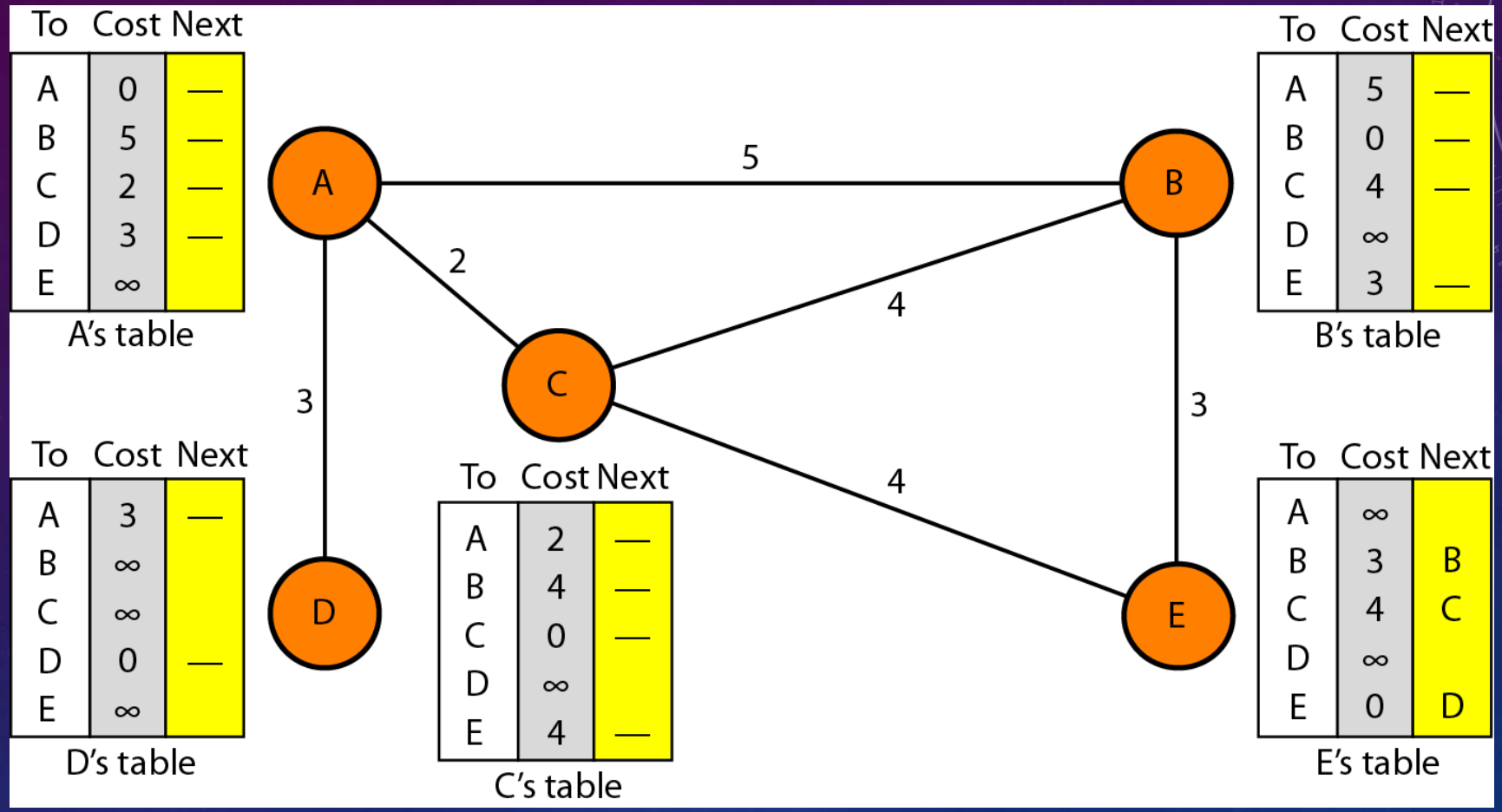


Dijkstra's Shortest Path Routing Algorithm



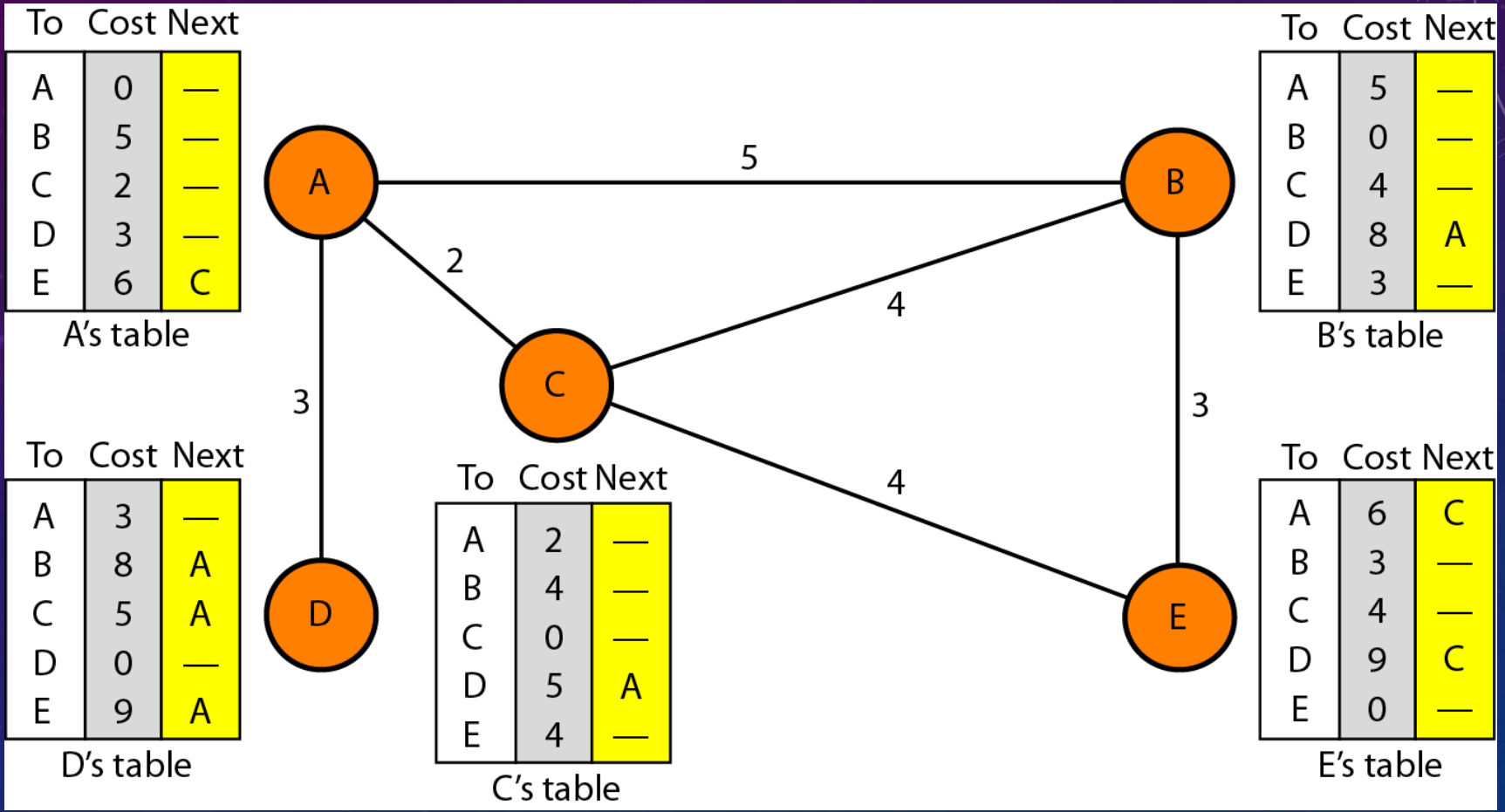
[redacted] The first five steps used in computing the shortest path from *A* to *D*. The arrows indicate the working node.

Initialization of tables in distance vector routing

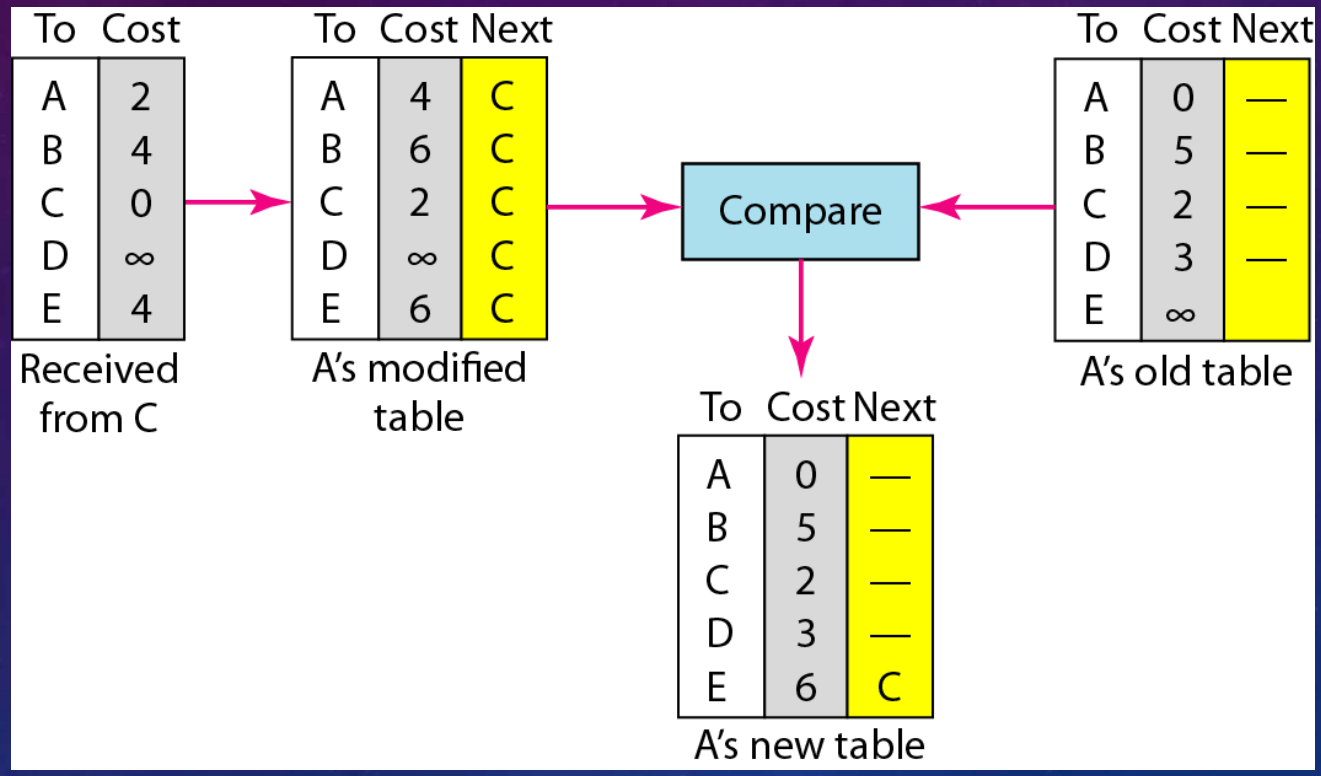


In distance vector routing, each node shares its routing table with its immediate neighbors periodically and when there is a change.

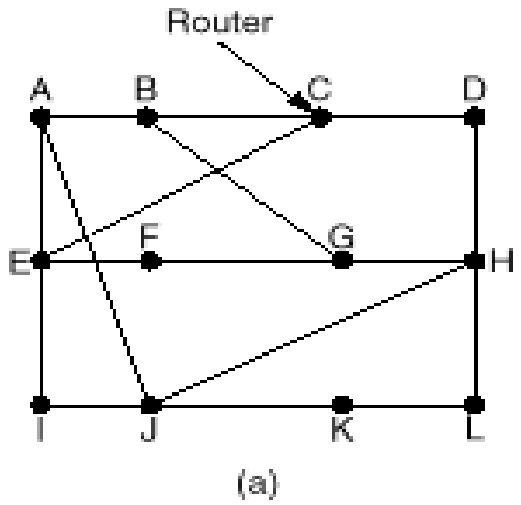
Distance vector routing



Updating in distance vector routing



DISTANCE VECTOR ROUTING



To	A	I	H	K	New estimated delay from J	Line
A	0	24	20	21	8	A
B	12	36	31	28	20	A
C	25	18	19	36	28	I
D	40	27	8	24	20	H
E	14	7	30	22	17	I
F	23	20	19	40	30	I
G	18	31	6	31	18	H
H	17	20	0	19	12	H
I	21	0	14	22	10	I
J	9	11	7	10	0	—
K	24	22	22	0	6	K
L	29	33	9	9	15	K

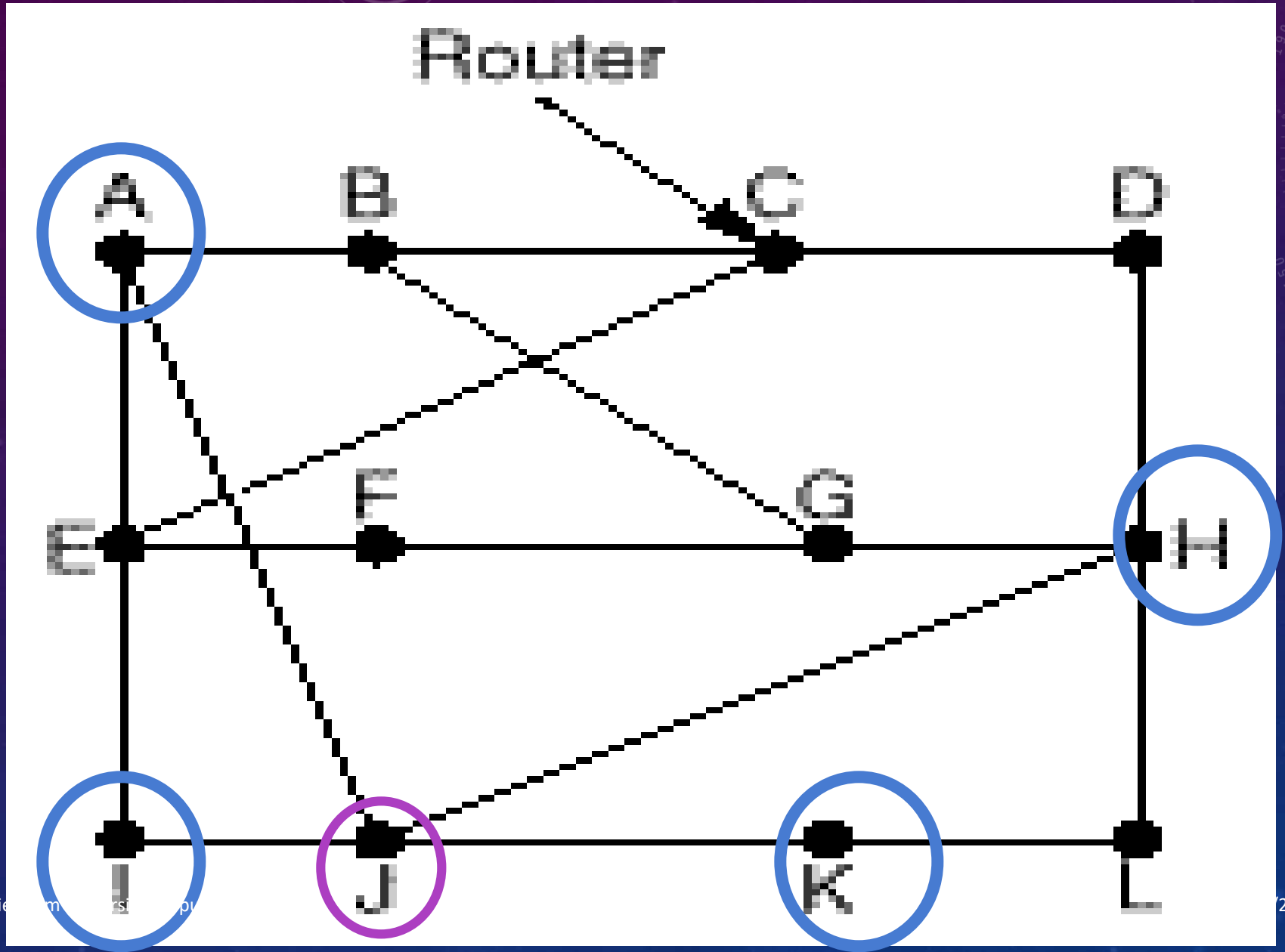
JA delay is 8 | JI delay is 10 | JH delay is 12 | JK delay is 6

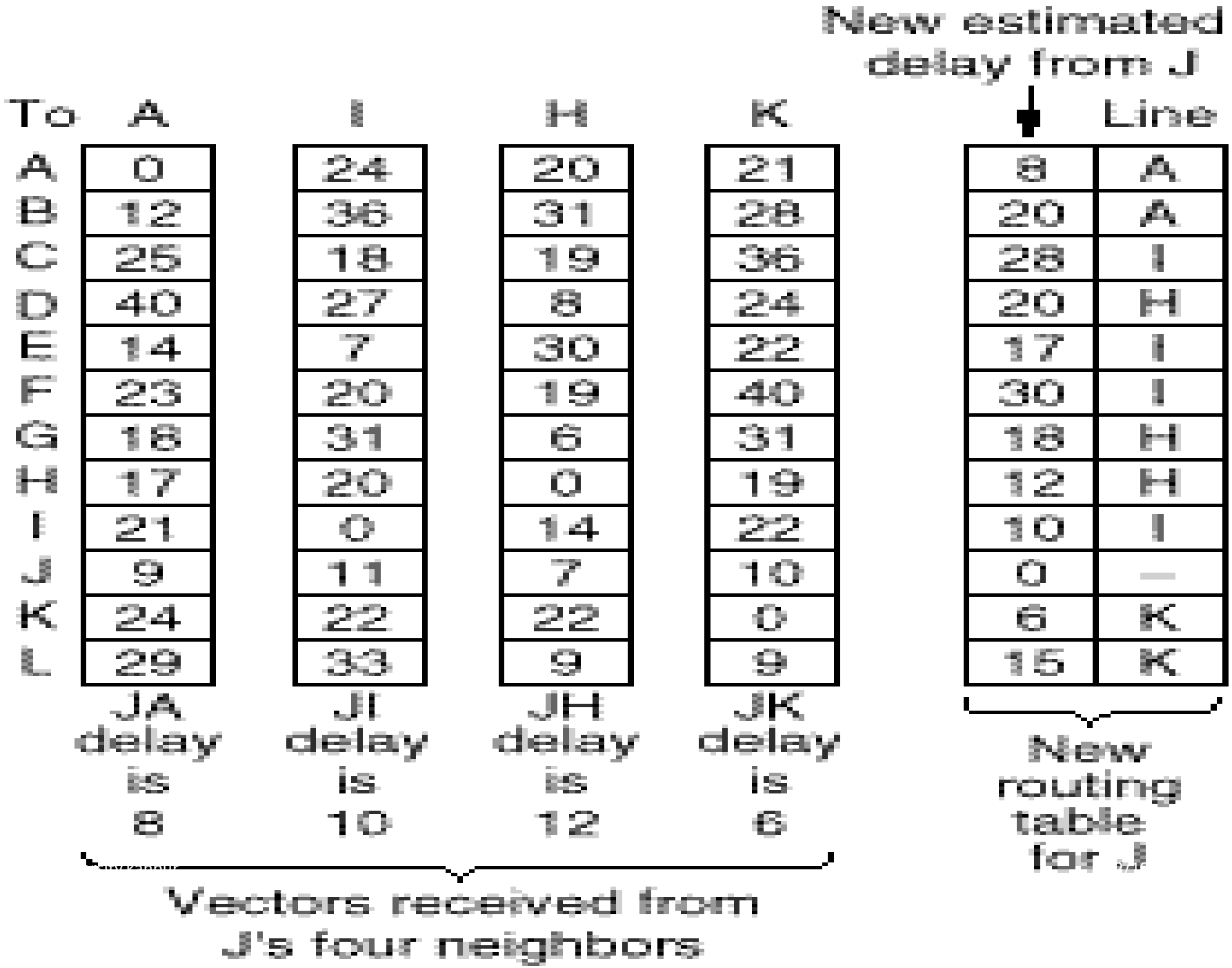
Vectors received from J's four neighbors

New routing table for J

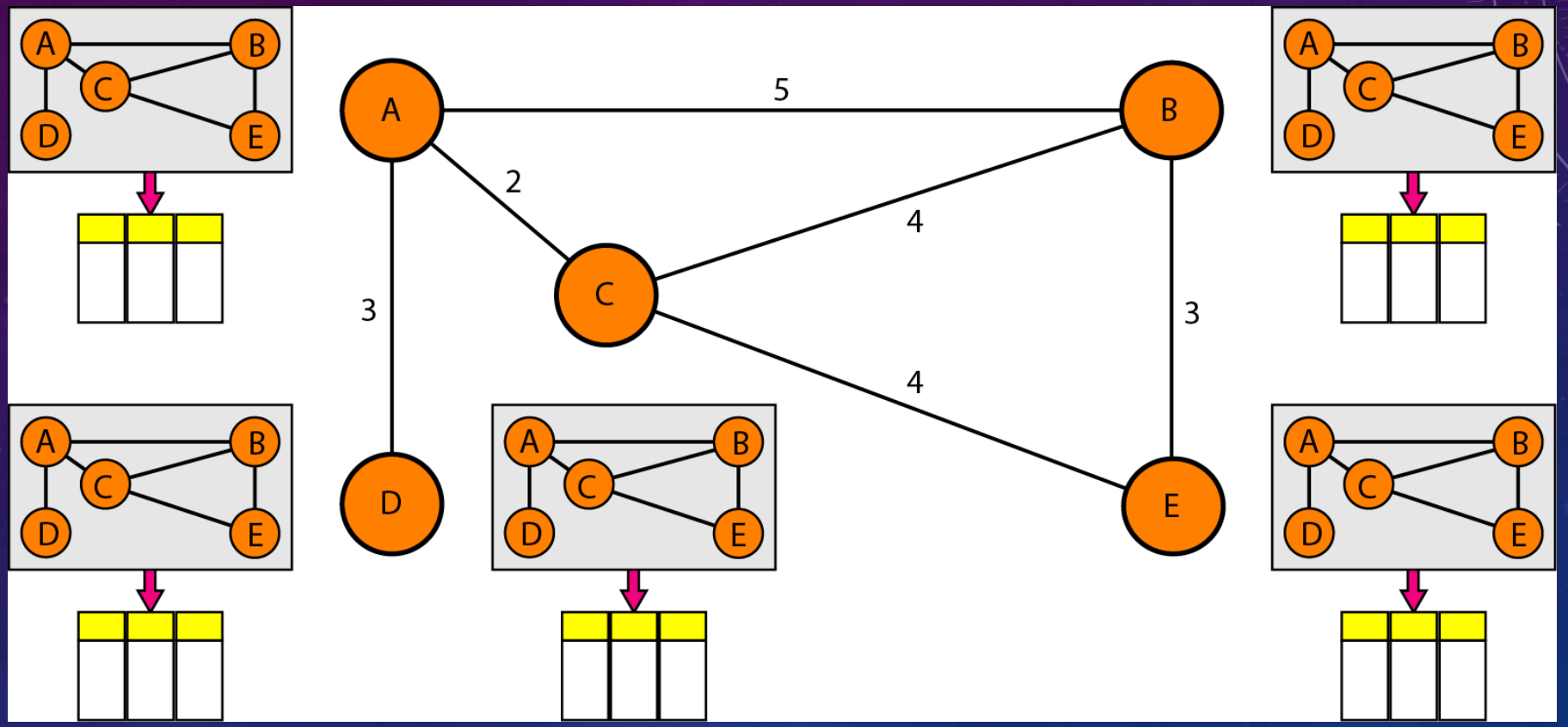
(b)

[redacted] (a) A subnet. (b) Input from *A*, *I*, *H*, *K*, and the new routing table for *J*.

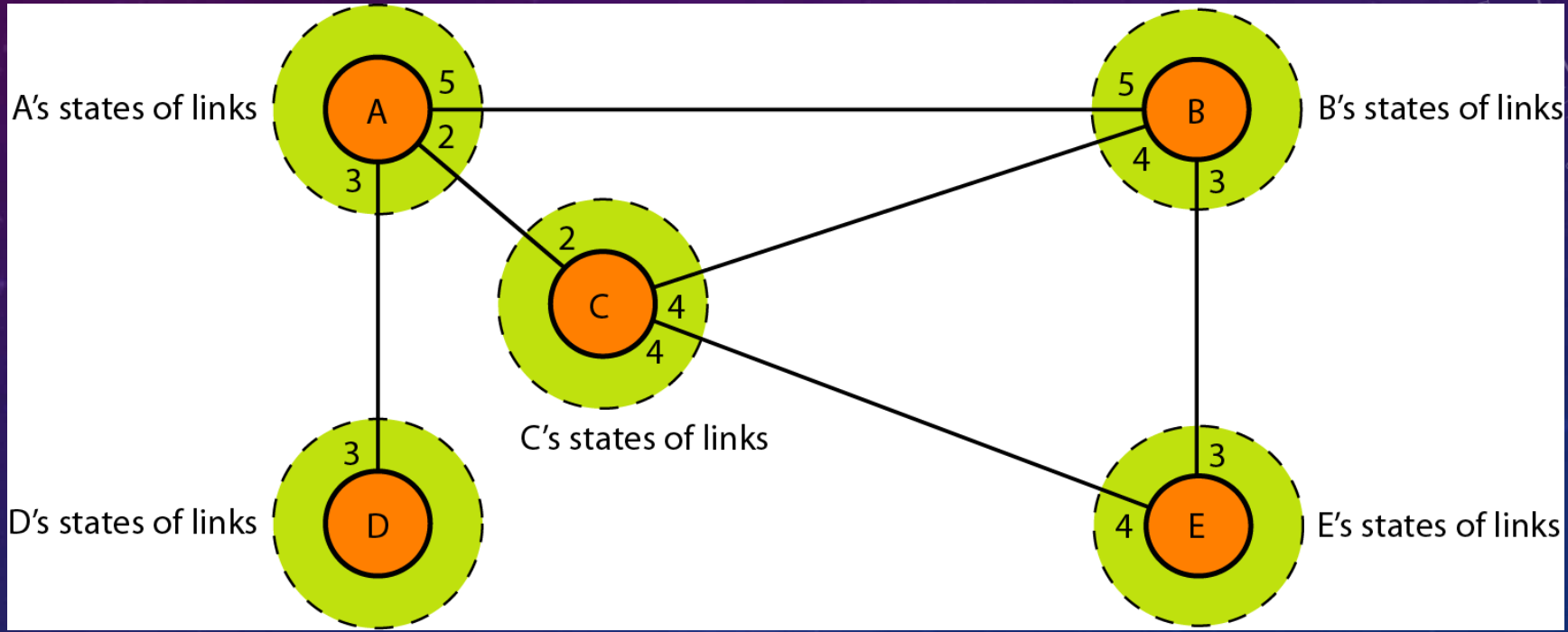

Router
A
B
C
D
E
F
G
H
I
J
K
L


New estimated delay from J
To
A
I
H
K
Line
A 0 24 20 21 8 A
B 12 36 31 28 20 A
C 25 18 19 36 28 I
D 40 27 8 24 20 H
E 14 7 30 22 17 I
F 23 20 19 40 30 I
G 18 31 6 31 18 H
H 17 20 0 19 12 H
I 21 0 14 22 10 I
J 9 11 7 10 0 —
K 24 22 22 0 6 K
L 29 33 9 9 15 K
JA delay is 8
JI delay is 10
JH delay is 12
JK delay is 6
New routing table for J
Vectors received from J's four neighbors

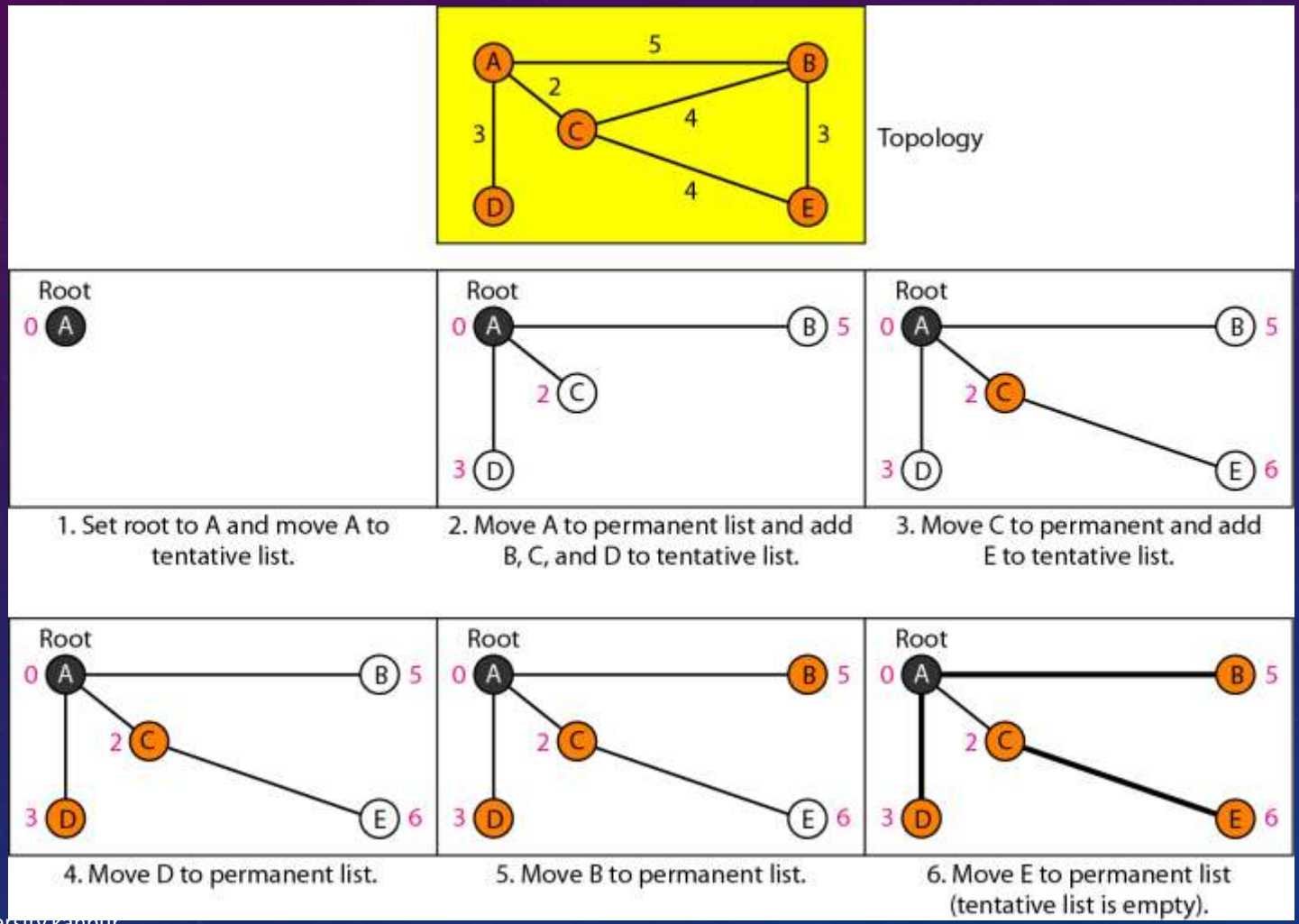
Concept of link state routing



Link state knowledge



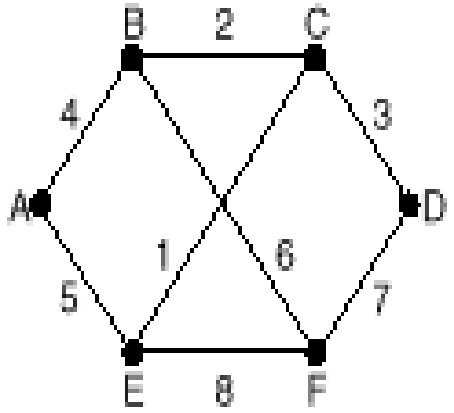
Example of formation of shortest path tree



Routing table for node A

Node	*Cost*	*Next Router*
A	0	—
B	5	—
C	2	—
D	3	—
E	6	C

LINK STATE ROUTING



(a)

Link State Packets

A	B	C	D	E	F
Seq.	Seq.	Seq.	Seq.	Seq.	Seq.
Age	Age	Age	Age	Age	Age
B 4	A 4	B 2	C 3	A 5	B 6
E 5	C 2	D 3	F 7	C 1	D 7
	F 6	E 1		F 8	E 8

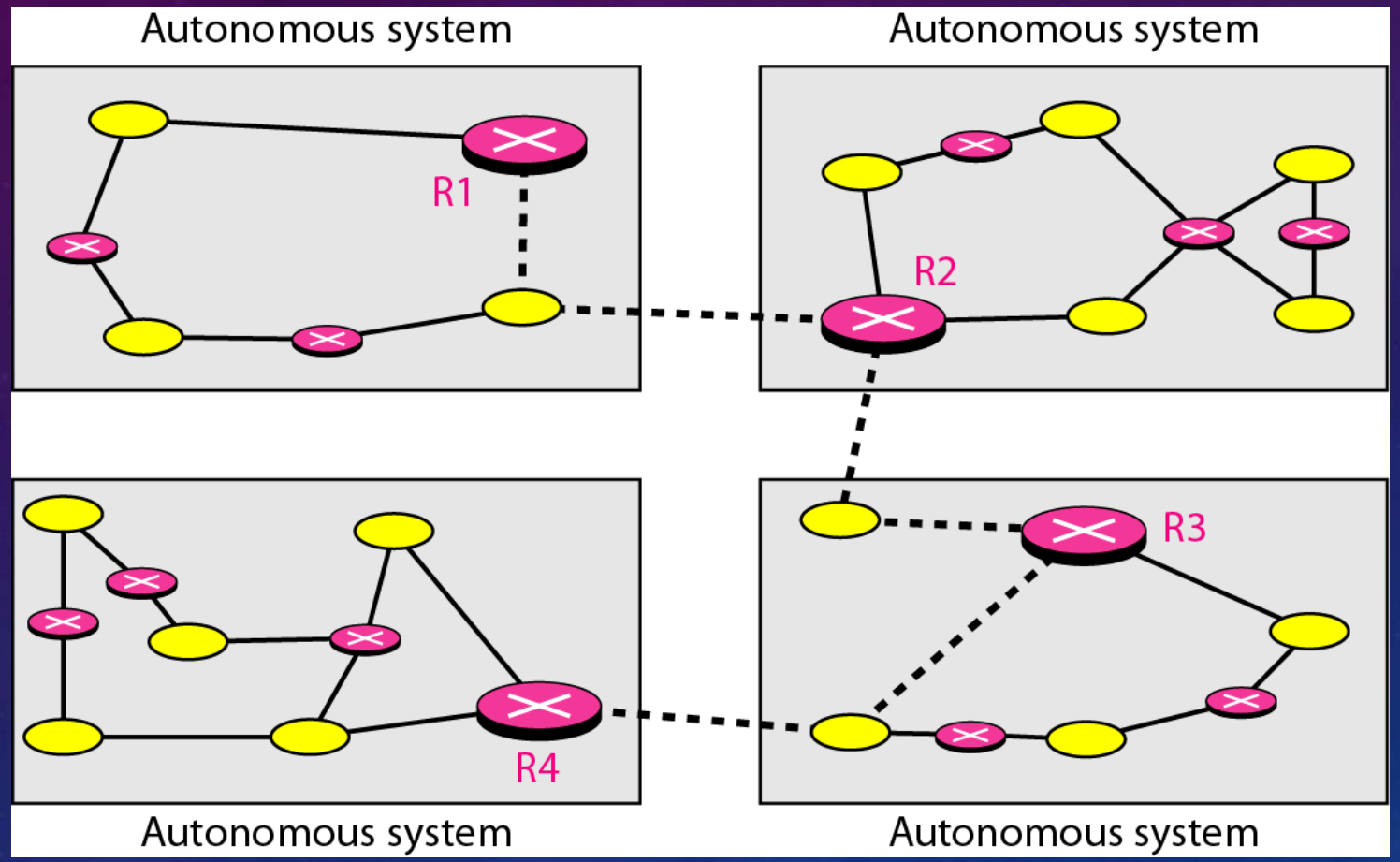
(b)

[redacted] (a) A subnet. (b) The link state packets for this subnet.

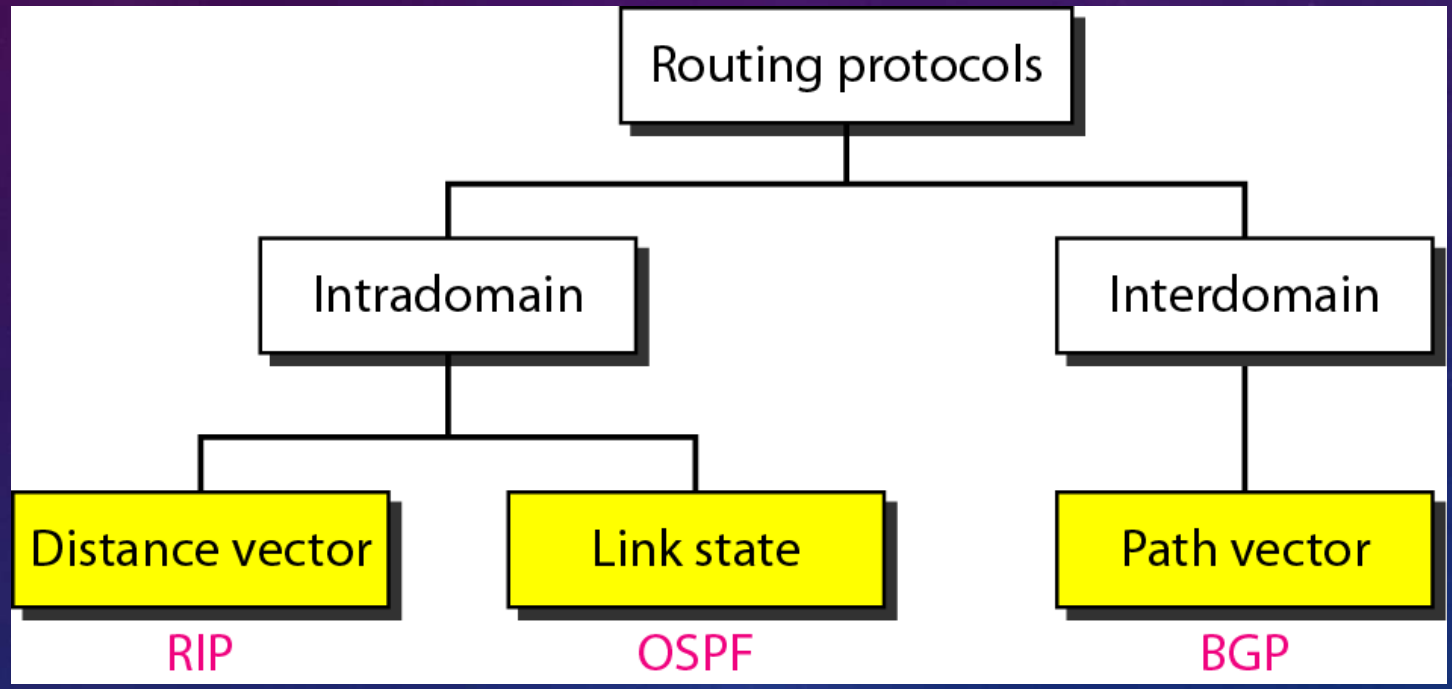
DYNAMIC ROUTING

- Routers talk to adjacent routers, using a *routing protocol.*
- The process responsible is called a routing daemon.
- Updates the kernel's *routing tables.*
- Internet is a collection of *Autonomous Systems* (AS).
- *Intra* Domain Routing Protocol - for use within an AS.
- *Inter* Domain Routing Protocol - for use between ASs.

Autonomous systems

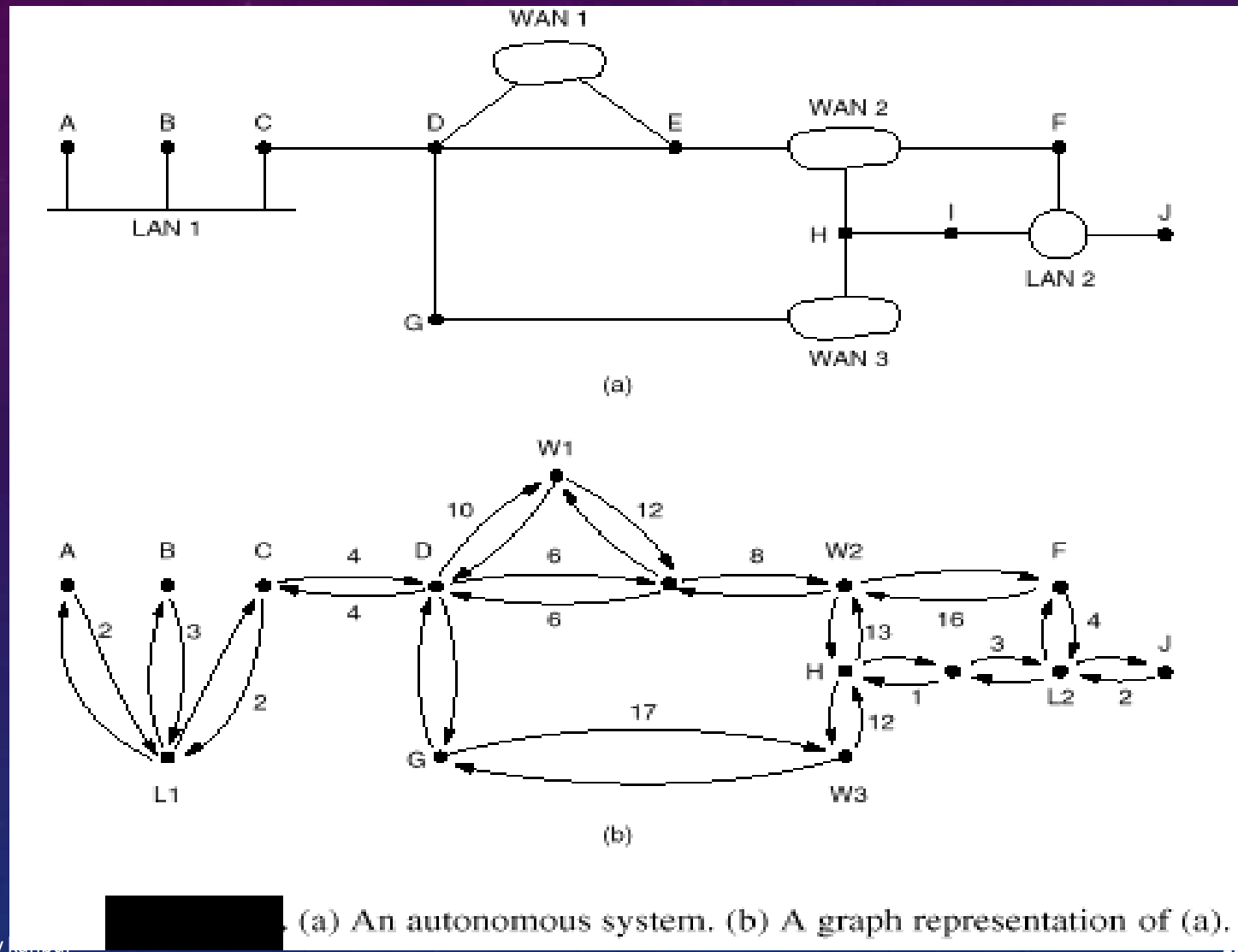


Popular routing protocols



ROUTING PROTOCOLS

- Intra-domain routing protocols
  - Routing Information Protocol (RIP)
  - HELLO
  - Open Shortest Path First (OSPF)
- Inter-domain routing protocols
  - Border Gateway Protocol (BGP)



[redacted]. (a) An autonomous system. (b) A graph representation of (a).

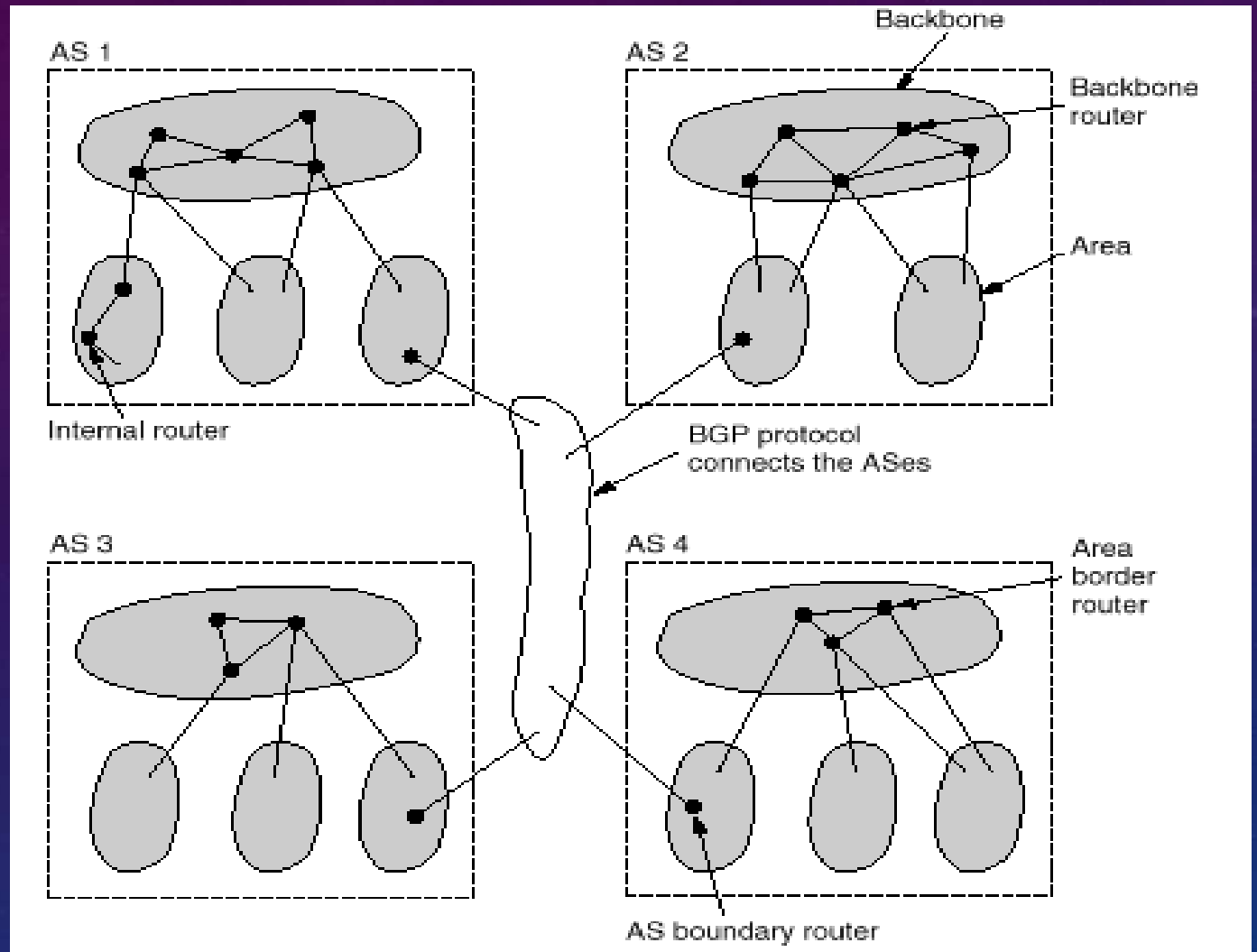
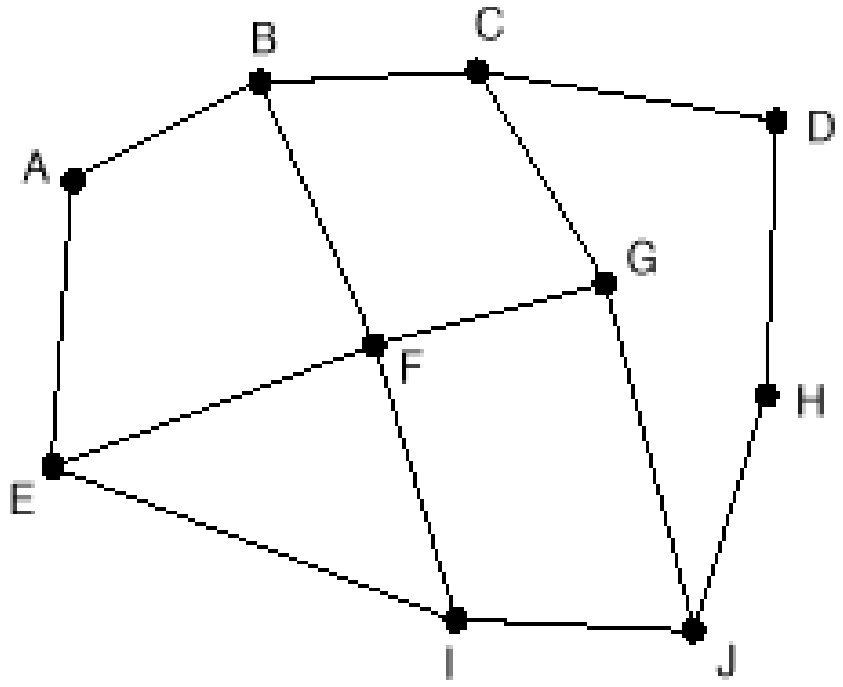


Fig. 5-53. The relation between ASes, backbones, and areas in OSPF.

Message type	Description
Hello	Used to discover who the neighbors are
Link state update	Provides the sender's costs to its neighbors
Link state ack	Acknowledges link state update
Database description	Announces which updates the sender has
Link state request	Requests information from the partner

The five types of OSPF messages.



(a)

Information F receives from its neighbors about D

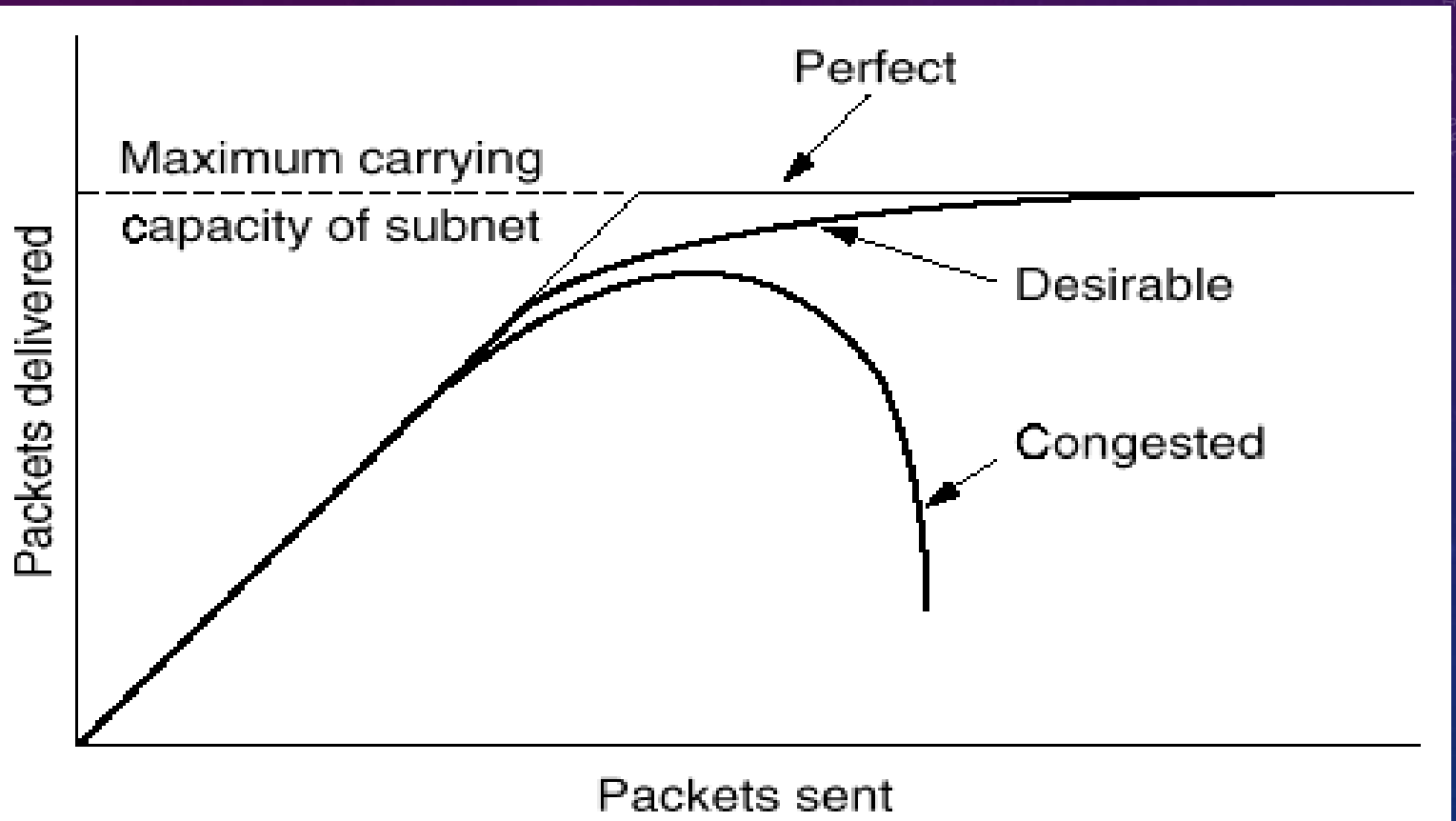
From B: "I use BCD"
From G: "I use GCD"
From I: "I use IFGCD"
From E: "I use EFGCD"

(b)

[redacted] (a) A set of BGP routers. (b) Information sent to *F*.

CONGESTION CONTROL

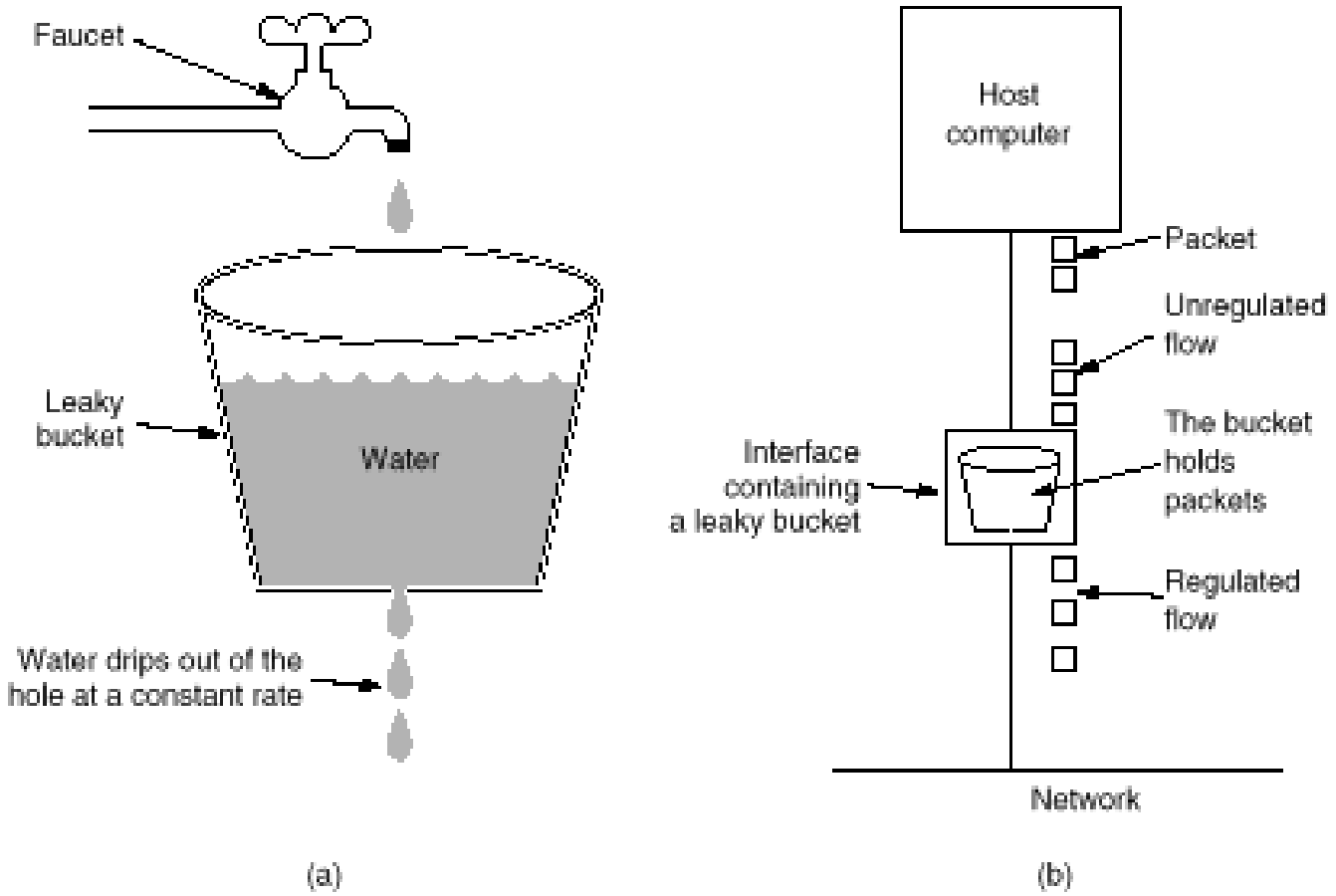
- When too many packets are present in the subnet, performance degrades. This situation is called *congestion.*
- Congestion can be brought about by several factors:
  - when nodes do not have enough processing capability.
  - when the rate of incoming traffic exceeds the rate of outgoing traffic.
- Following strategies can be used for congestion control:
  - Allow nodes to discard packets if they cannot be processed quickly.
  - Restrict the total number of packets in the network.
  - Use flow control to avoid congestion.
  - Choke the input when the network is overloaded.
  - Allocate the resources in advance.



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

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

Policies that affect congestion.

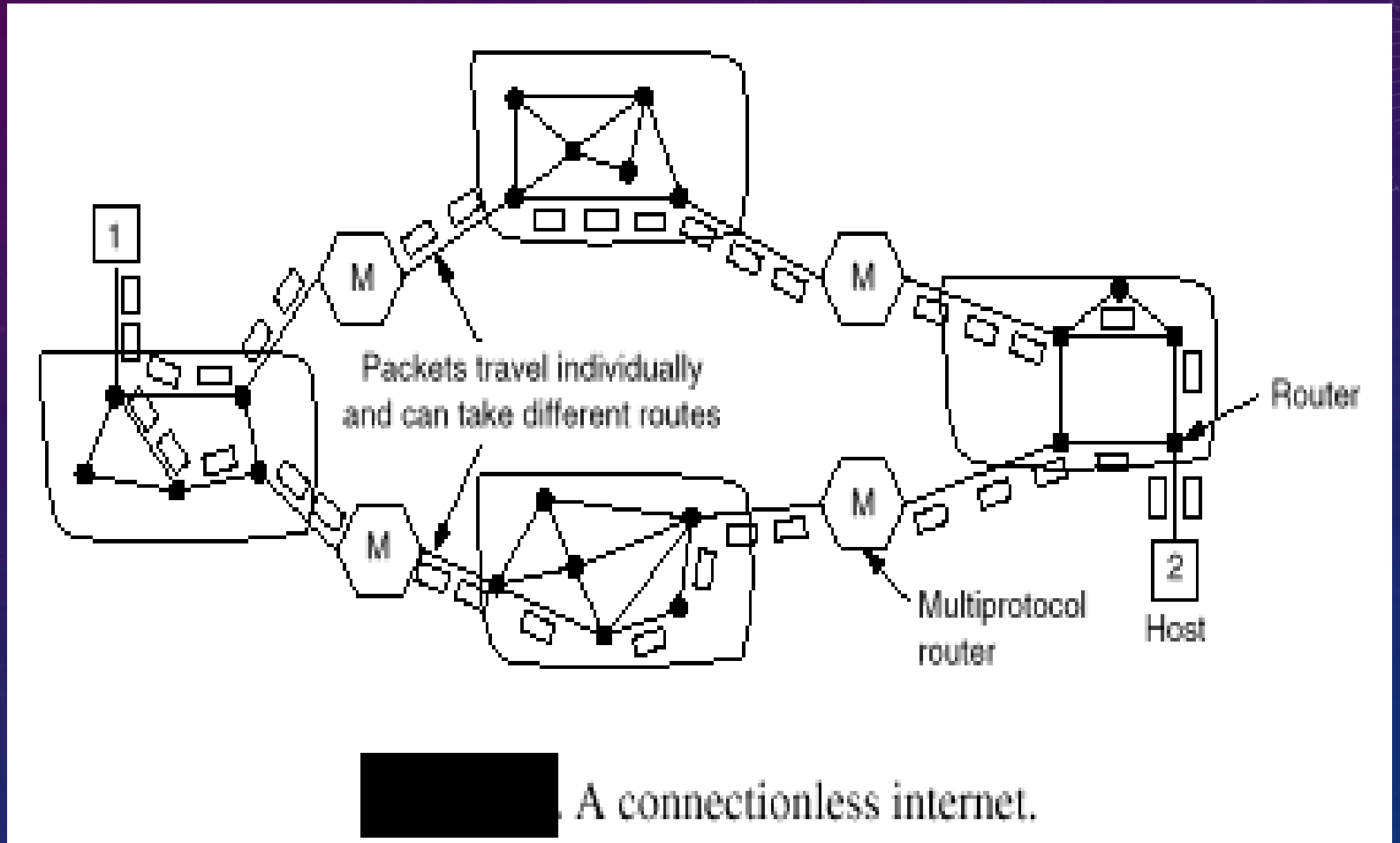


[redacted](a) A leaky bucket with water. (b) A leaky bucket with packets.

INTERNETWORKING

Another primary function of the Network Layer.

- Network Layer has to deal with the issues that arise when Source and Destination are on different networks.
- Some of the issues are:
  - Routing across networks -- more complex routing decisions.
  - Different protocols used in different networks --requires conversion between the protocols.
  - One can also use encapsulation technique.



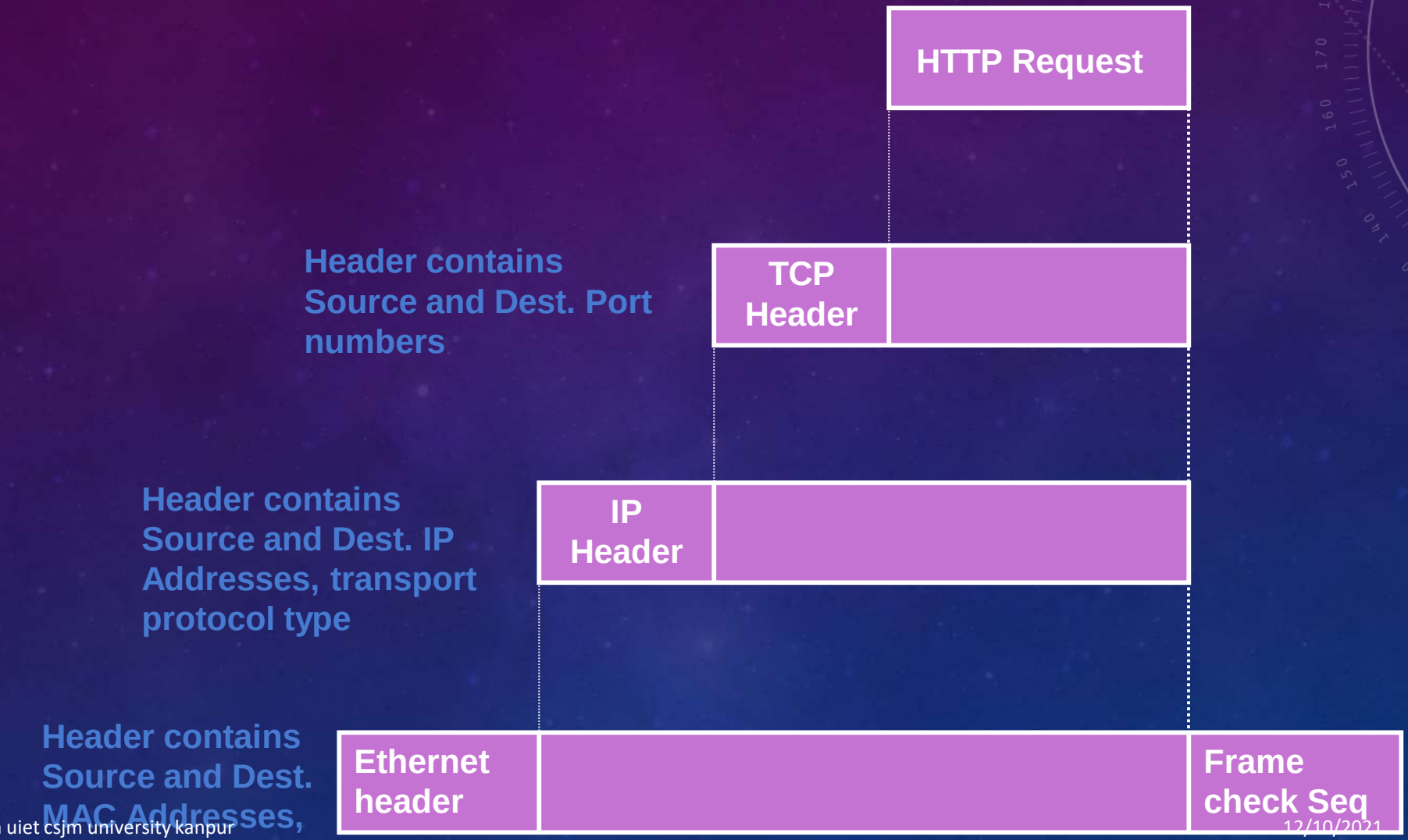
[redacted] A connectionless internet.

ENCAPSULATION

- When a packet of one protocol is sent as data portion of another protocol, it is called encapsulation.
- In a layered network architecture, each protocol encapsulates packet from upper layer protocol.
- Can also be used for internetworking. For example, to transmit an IP packet across an X.25 network:
  - At the border router of IP and X.25, create an X.25 packet with source address as that of this border router.
  - Set the destination address to that of multi-protocolrouter on the other side, which connects X.25 network

    to the IP network.
  - Include the IP packet as data portion of X.25 packet.
  - Transmit the packet.

Encapsulation



Item	Some Possibilities
Service offered	Connection-oriented versus connectionless
Protocols	IP, IPX, CLNP, AppleTalk, DECnet, etc.
Addressing	Flat (802) versus hierarchical (IP)
Multicasting	Present or absent (also broadcasting)
Packet size	Every network has its own maximum
Quality of service	May be 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, 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

Fig. 5-35. Some of the many ways networks can differ.