CPE 490: Information Systems Engineering I: Computer Networking

Chap. 5 - The Network Layer

Professor Du

Department of Electrical and Computer Engineering
Stevens Institute of Technology
Email: xdu16@stevens.edu

The Network Layer

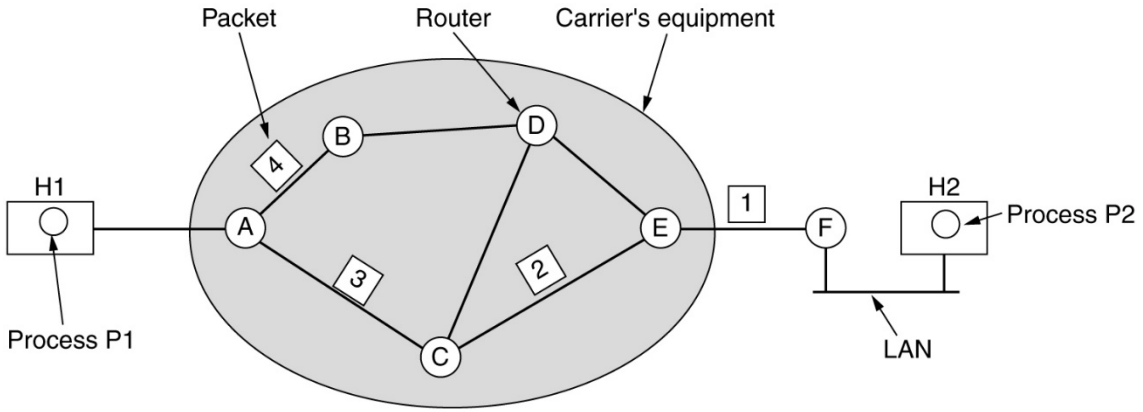
- Services Provided to the Transport Layer
- Implementation of Connectionless Service
- Implementation of Connection-Oriented Service
- Comparison of Virtual-Circuit and Datagram Subnets

Services Provided to the Transport Layer

- The services should be independent of the router technology.
- The transport layer should be shielded from the number, type, and topology of the routers present.
- The network addresses made available to the transport layer should use a uniform numbering plan, even across LANs and WANs.
- Connectionless service
  - ✓ Packets are injected into the subnet individually and routed independently of each other.
  - ✓ Packets – datagrams; subnet – datagram subnet.
  - ✓ The Internet offers connectionless network-layer service
- Connection-oriented service
  - ✓ A path must be set up before the transmission of data packets.
  - ✓ This connection is called a VC (virtual circuit).
  - ✓ ATM offers connection-oriented network-layer service .

Implementation of Connectionless Service

- ✓ The process P1 sends a long message to P2.
- ✓ The network layer of H1 breaks the message into 4 packets and sends to router A using some point-to-point protocol.
- ✓ Each packet is independently routed.
- ✓ Each router has an internal routing table.
- ✓ Each table entry is a pair consisting a destination and the outgoing line.



Routing within a diagram subnet.

A's table

Dest.	initially	later
A	–	–
B	B	B
C	C	C
D	B	B
E	C	B
F	C	B

C's table

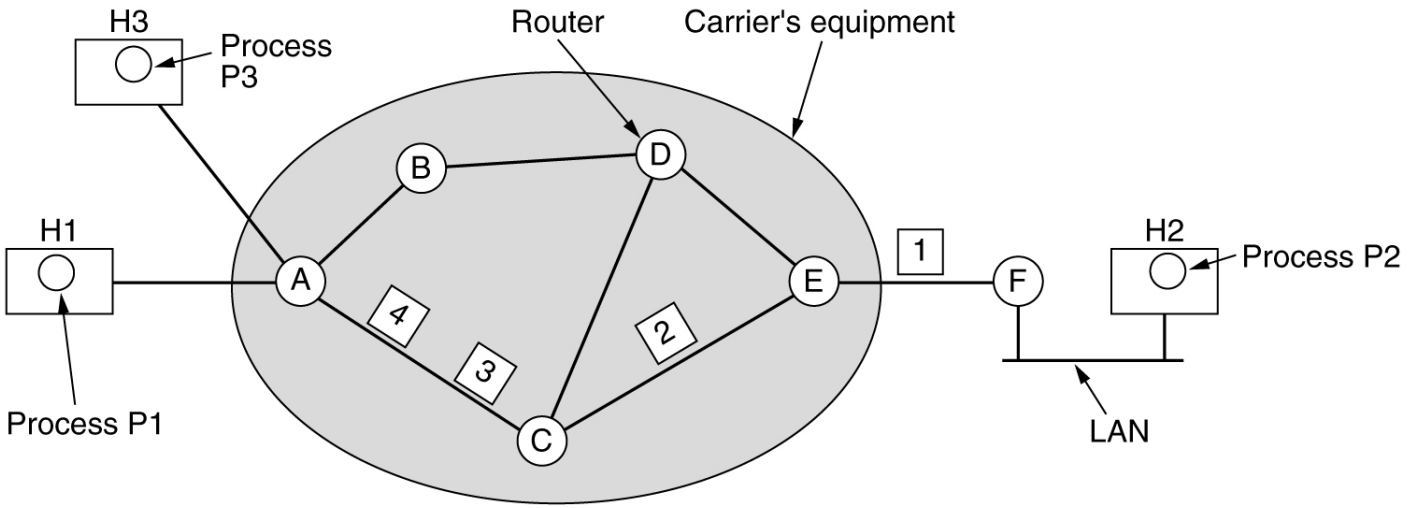
Dest.	Line
A	A
B	A
C	–
D	D
E	E
F	E

E's table

Dest.	Line
A	C
B	D
C	C
D	D
E	–
F	F

Implementation of Connection-Oriented Service

- ✓ When a connection is set up, a route is chosen and stored in routing tables.
- ✓ The same route is used for all packets in the flow.
- ✓ Each packet carries an identifier telling which VC it belongs to.



A's table

In		Out	
H1	1	C	1
H3	1	C	2

C's table

A	1	E	1
A	2	E	2

E's table

C	1	F	1
C	2	F	2

Source Node | Identifier; Next Router | New Identifier

Routing within a virtual-circuit subnet.

Comparison of Virtual-Circuit and Datagram Subnets

Issue	Datagram subnet	Virtual-circuit 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	Routers do not hold state information about connections	Each VC requires router table space per connection
Routing	Each packet is routed independently	Route chosen when VC is set up; all packets follow it
Effect of router failures	None, except for packets lost during the crash	All VCs that passed through the failed router are terminated
Quality of service	Difficult	Easy if enough resources can be allocated in advance for each VC
Congestion control	Difficult	Easy if enough resources can be allocated in advance for each VC

Routing Algorithms

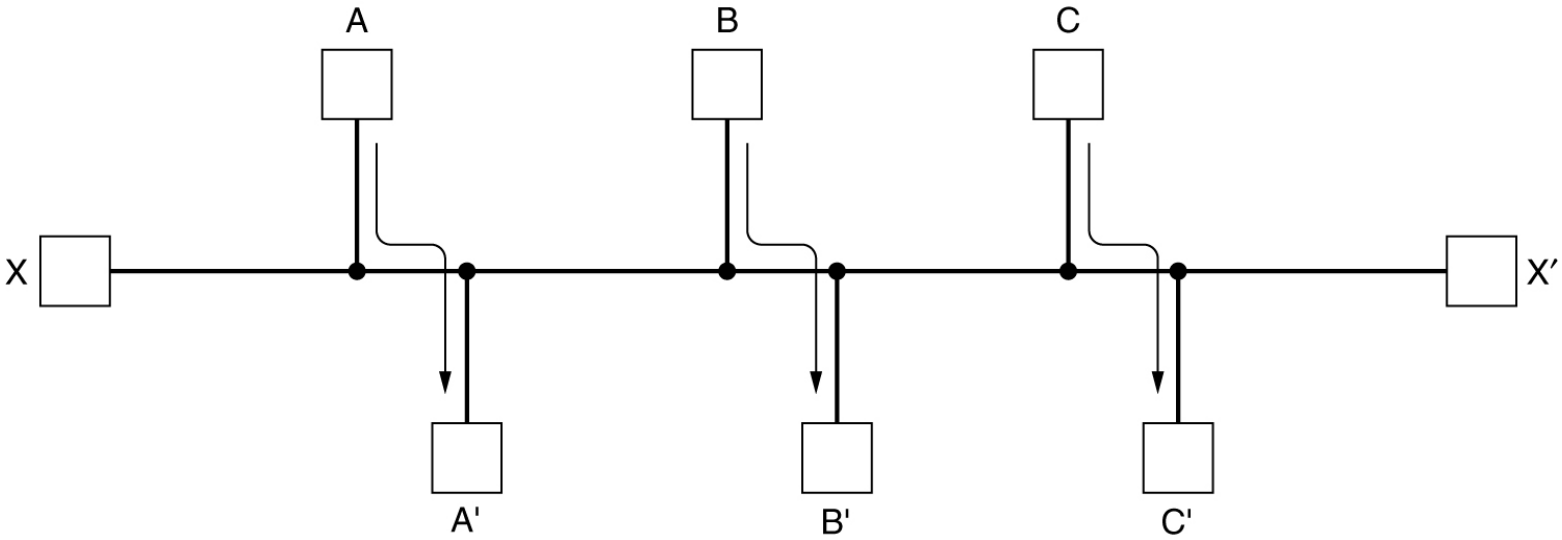
- The Optimality Principle
- Shortest Path Routing
- Flooding
- Distance Vector Routing
- Link State Routing
- Hierarchical Routing
- Broadcast Routing
- Multicast Routing
- Routing for Mobile Hosts
- Routing in Ad Hoc Networks

Routing Algorithms (2)

- The main function of the network layer is routing packets from source to destination.
- The routing algorithm is to decide which output line an incoming packet should be transmitted on.
- A routing algorithm should have the following properties
  - ✓ Correctness and simplicity
  - ✓ Robustness
    - The routing algorithm should be able to cope with changes in the topology and traffic because of hardware and software failure.
  - ✓ Stability
    - The routing algorithm should converge to equilibrium and stay there after some running time.
  - ✓ Fairness
  - ✓ Optimality

Routing Algorithms (3)

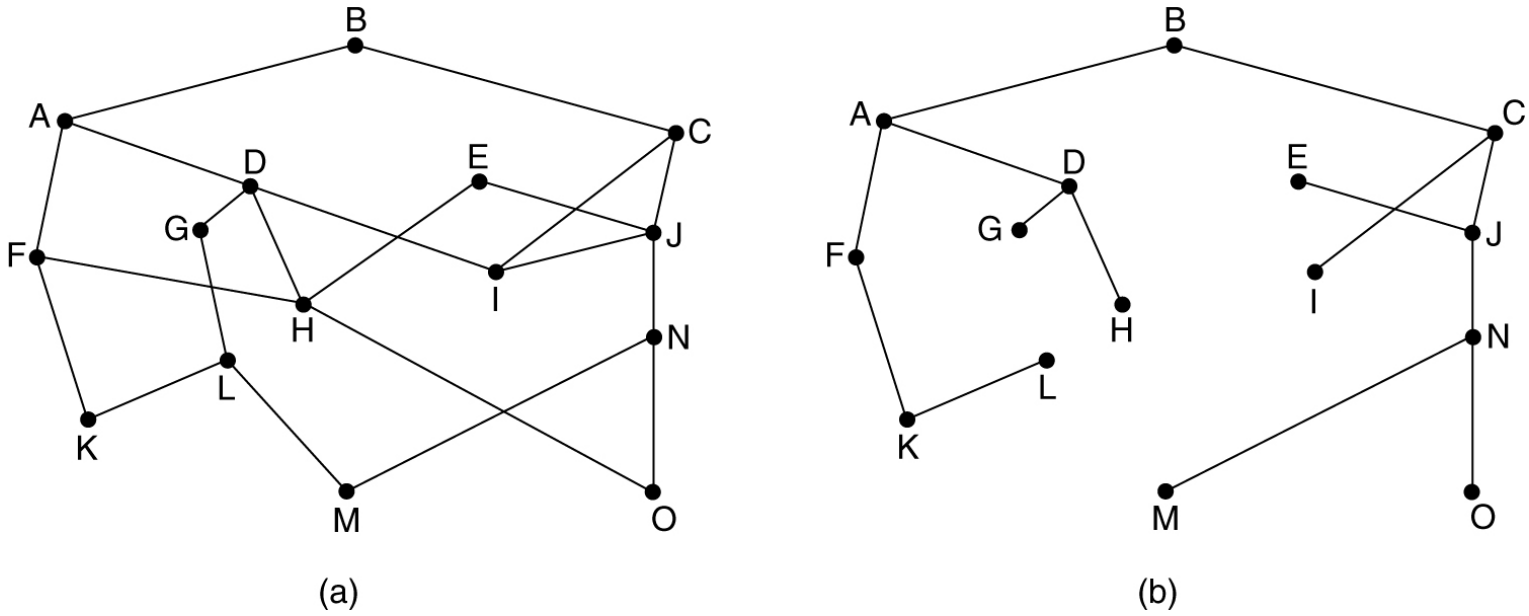
- ✓ Traffic between A and A', B and B', and C and C' saturate the horizontal link.
- ✓ This conflicts with the traffic between X and X'.
- ✓ Routing algorithms can be grouped into two classes:
  - Non-adaptive algorithms – do not change routing decision.
  - Adaptive algorithms – change routing decision if topology or traffic changes.



Conflict between fairness and optimality.

The Optimality Principle

- ✓ The Optimality Principle – if router J is on the optimal path from router I to router K, then the optimal path from J to K also falls along the same route.
- ✓ The set of optimal routes from all sources to a given destination form a tree rooted at the destination – sink tree.



(a) A subnet. (b) A sink tree for router B.

Shortest Path Routing

- ✓ The labels on the arcs could be computed as a function of the distance, bandwidth, average traffic, communication cost, mean queue length, measure delay, and other factors.

The Dijkstra's algorithm

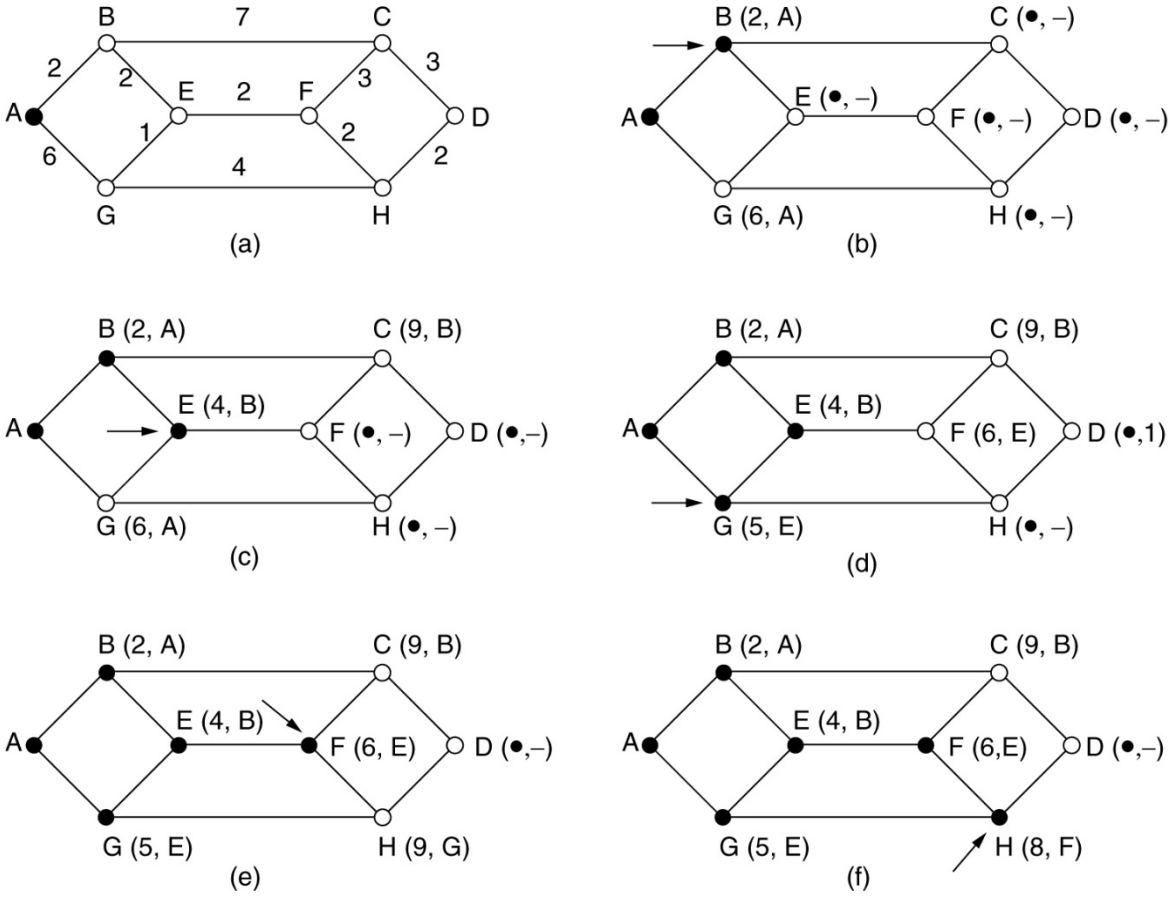
The first 5 steps used in computing the shortest path from A to D. The arrows indicate the working node.

(a) Marking node A as permanent.

(b) Examining each neighbor of node A and relabeling the distance. Making the node with the smallest label the new working node.

(c) Examining each neighbor of node B. Relabeling node E and C with the shortest distance.

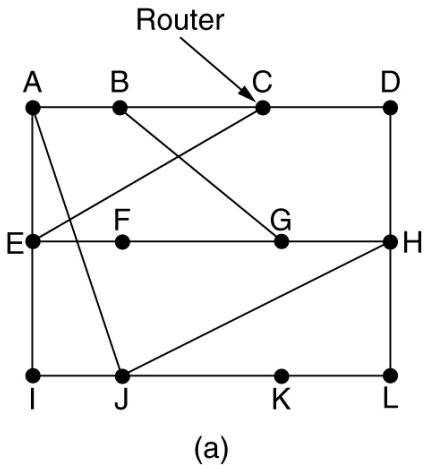
Flooding – Every incoming packet is sent out to every outgoing line except the one it arrived on.



Distance Vector Routing

- ✓ Distance Vector Routing (Bellman-Ford) – A dynamic routing algorithm.
- ✓ Each router maintains a table (vector) giving the best known distance to each other router and which line to use to get there.
- ✓ The tables are updated by exchanging information with neighbors.

- **The first 4 columns show the delay vectors received from the neighbors of J.**
- **Assume each router can estimate the distance to every neighbor.**
- **Now J can compute the updated distance to each router and the new route.**
- **E.g, J → G**
- **J → A → G : 8 + 18 = 26**
- **J → I → G : 31 + 10 = 41**
- **J → H → G : 6 + 12 = 18**
- **J → K → G : 31 + 6 = 37**



(a)

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)

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

Link State Routing

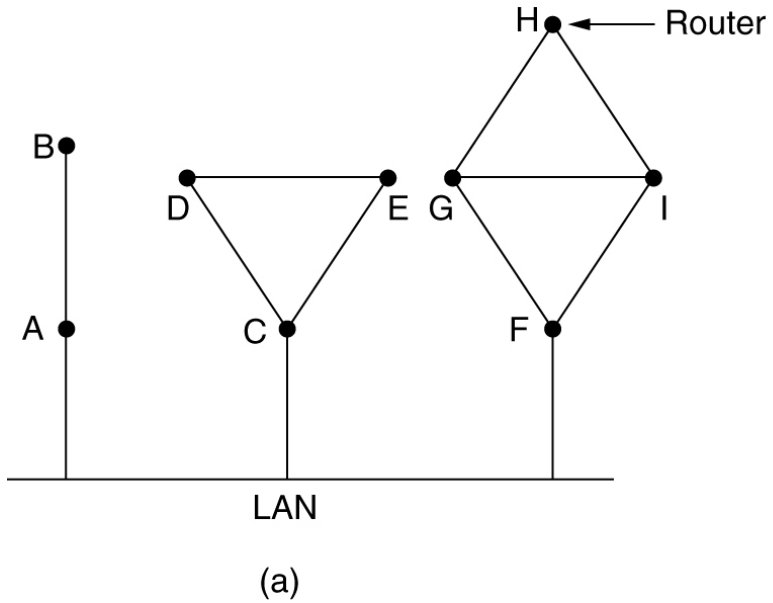
- Distance vector routing was used in the ARPANET until 1979, when it was replaced by link state routing for two reasons:
  - ✓ Line bandwidth was not considered.
  - ✓ The distance vector routing often took too long to converge.
- Link State Routing

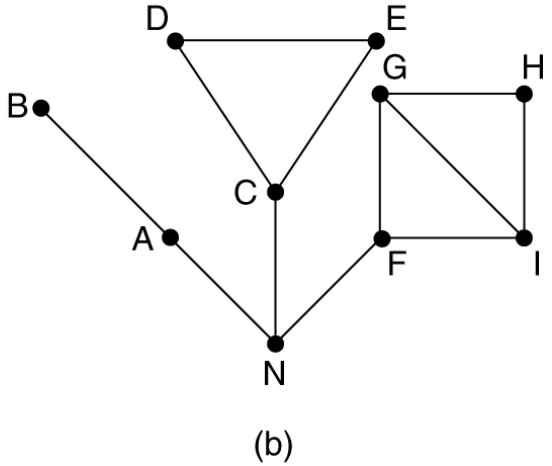
Each router must do the following:

1. Discover its neighbors, learn their network address.
2. Measure the delay or cost to each of its neighbors.
3. Construct a packet telling all it has just learned.
4. Send this packet to all other routers.
5. Compute the shortest path to every other router.

Learning about the Neighbors

- ✓ When a router is booted, it first learns who its neighbors are by sending HELLO packet on each line.
- ✓ Each router will send back a reply (with its address) after receiving the HELLO packet.
- ✓ A graph can be constructed based on neighbor info.
- ✓ In the example, an artificial node N is used to represent the LAN.



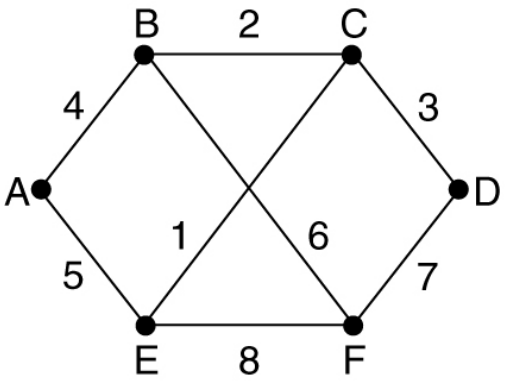


(a) Nine routers and a LAN.

(b) A graph model of (a).

Building Link State Packets

- ✓ The link state routing algorithm requires each router know the delay to each of its neighbor.
  - A special ECHO packet is used.
- ✓ Once the information needed for the exchange has been collected, the next step is for each router to build a packet containing all the data.
- ✓ The packet starts with the identity of the sender, followed by a sequence # and age, and a list of neighbors.
- ✓ For each neighbor, the delay to that neighbor is given.
- ✓ When to build the link state packets?
  - Periodically; When some significant event happens (e.g., router fails).



(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)

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

Distributing the Link State Packets

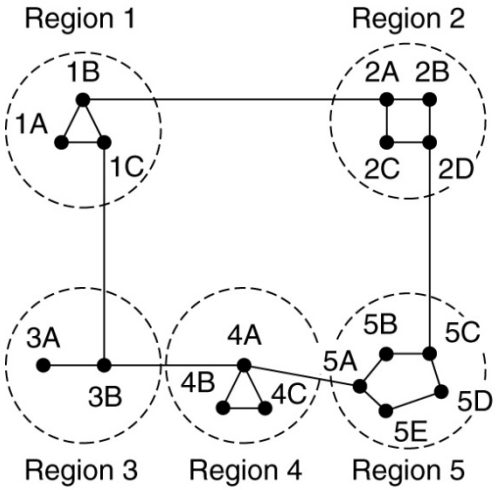
- ✓ Flooding is used to distribute the link state packets.
- ✓ Each packet contains a sequence # that is incremented for each new packet sent. (In addition to seq., the age field is used to solve certain problems – max. hops)
- ✓ Routers keep track of all the (source router, seq.) pairs.
- ✓ When a new link state packet comes in,
  - If the seq. is new, the packet is forwarded on all lines except the incoming line.
  - If it is a duplicate, it is discarded.
  - If the seq. is lower than the highest one seen so far, it is rejected.
- ✓ In the table below, each row is for a link state packet.
- ✓ The send flags mean that the packet must be sent on the line.
- ✓ The Ack flags mean that it must be ack.

- Once a router has a full set of link state packets, it can construct the entire subnet graph and computes the new routes.
- Link state routing protocols: OSPF.

			Send flags			ACK flags			
Source	Seq.	Age	A	C	F	A	C	F	Data
A	21	60	0	1	1	1	0	0	
F	21	60	1	1	0	0	0	1	
E	21	59	0	1	0	1	0	1	
C	20	60	1	0	1	0	1	0	
D	21	59	1	0	0	0	1	1	

Hierarchical Routing

- ✓ As network size grows, the routing tables grow ➔ memory and CPU time increase.
- ✓ Hierarchical Routing: Routers are divided into regions.
  - Each router knows the details about how to route packets to nodes within its region. Gateway router, e.g., 1B.



(a)

Full table for 1A

Dest.	Line	Hops
1A	–	–
1B	1B	1
1C	1C	1
2A	1B	2
2B	1B	3
2C	1B	3
2D	1B	4
3A	1C	3
3B	1C	2
4A	1C	3
4B	1C	4
4C	1C	4
5A	1C	4
5B	1C	5
5C	1B	5
5D	1C	6
5E	1C	5

(b)

Hierarchical table for 1A

Dest.	Line	Hops
1A	–	–
1B	1B	1
1C	1C	1
2	1B	2
3	1C	2
4	1C	3
5	1C	4

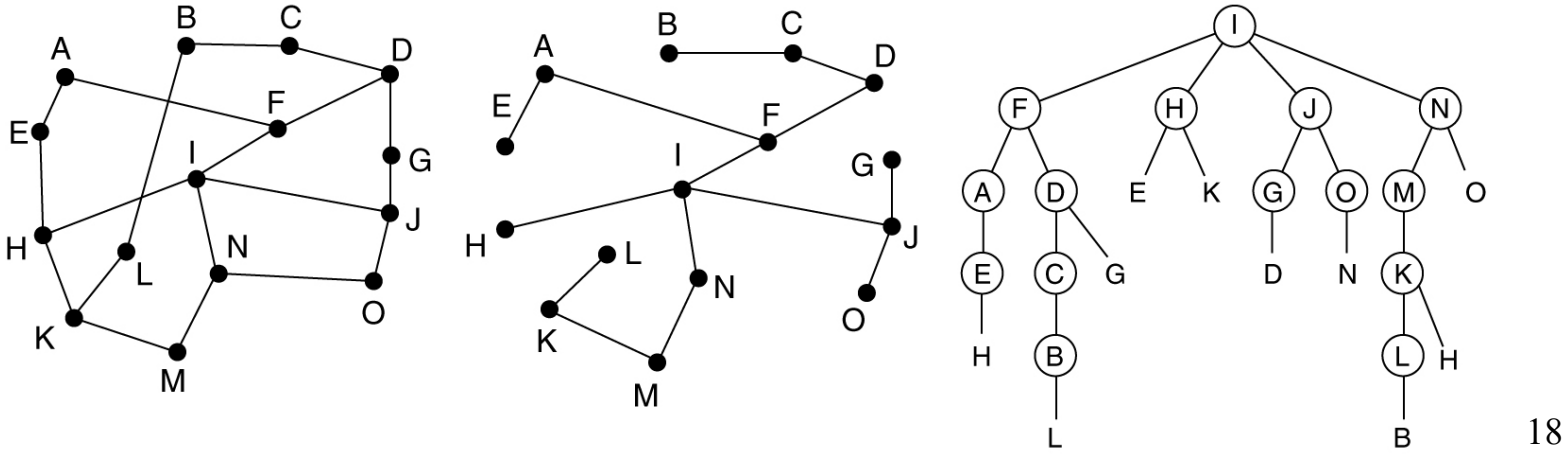
(c)

- Hierarchical Routing reduces the table from 17 to 7 entries.
- The penalty is increased path length. E.g., 1A → 5C (via region 2)

Broadcast Routing

- ✓ Broadcasting - Sending a packet to all destinations simultaneously.
  - Sending a distinct packet to each destination;
  - Flooding;
  - Multi-destination routing: Each packet contains a list (subset) of destinations.
- ✓ Reverse path forwarding – reduce the traffic from flooding.
- ✓ When a broadcast packet arrives at a router, the router checks to see if the packet arrived on the line that is normally used for sending packets to the source of the broadcast.
  - If yes, there is a good chance that the broadcast packet followed the best route from the source and is therefore the first copy to arrive at the router.
    - Then the router forwards copies of the packets to other lines.
  - If no, the packet is discarded.

(a) A subnet. (b) a Sink tree. (c) The tree built by reverse path forwarding.



Multicast Routing

- ✓ Multicasting: Sending a message to a group of nodes.
- ✓ Multicasting requires group management: create, destroy group, allow process to join and leave groups.
- ✓ Routers must know which hosts belong to which groups.
- ✓ To do multicasting, each router computes a spanning tree covering all other routers.
- ✓ A spanning tree is a subset of a graph that includes all the routers but has no loop.

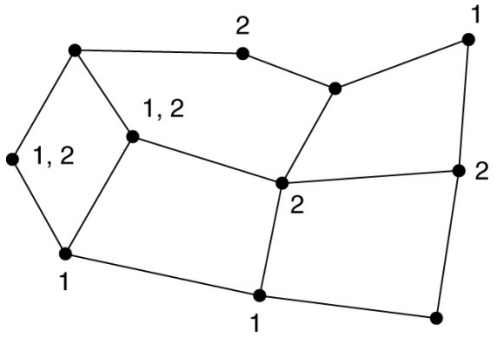
✓Based on group info., the first router (receiving the multicast packet) examines its spanning tree and prunes it – multicast tree.

(a) A network.

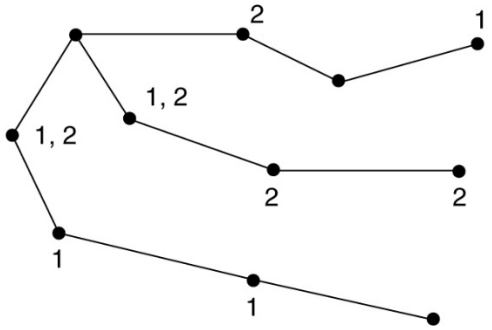
(b) A spanning tree for the leftmost router.

(c) A multicast tree for group 1.

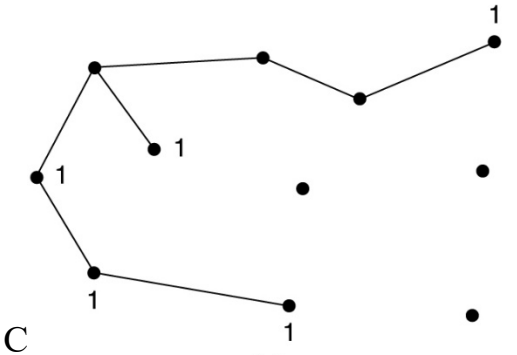
(d) A multicast tree for group 2.



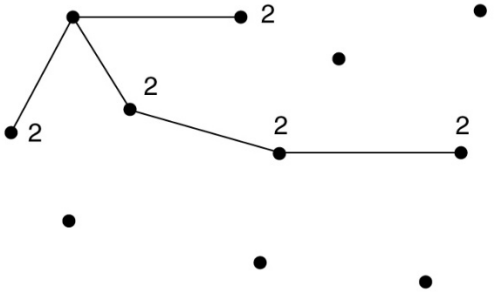
(a)



(b)



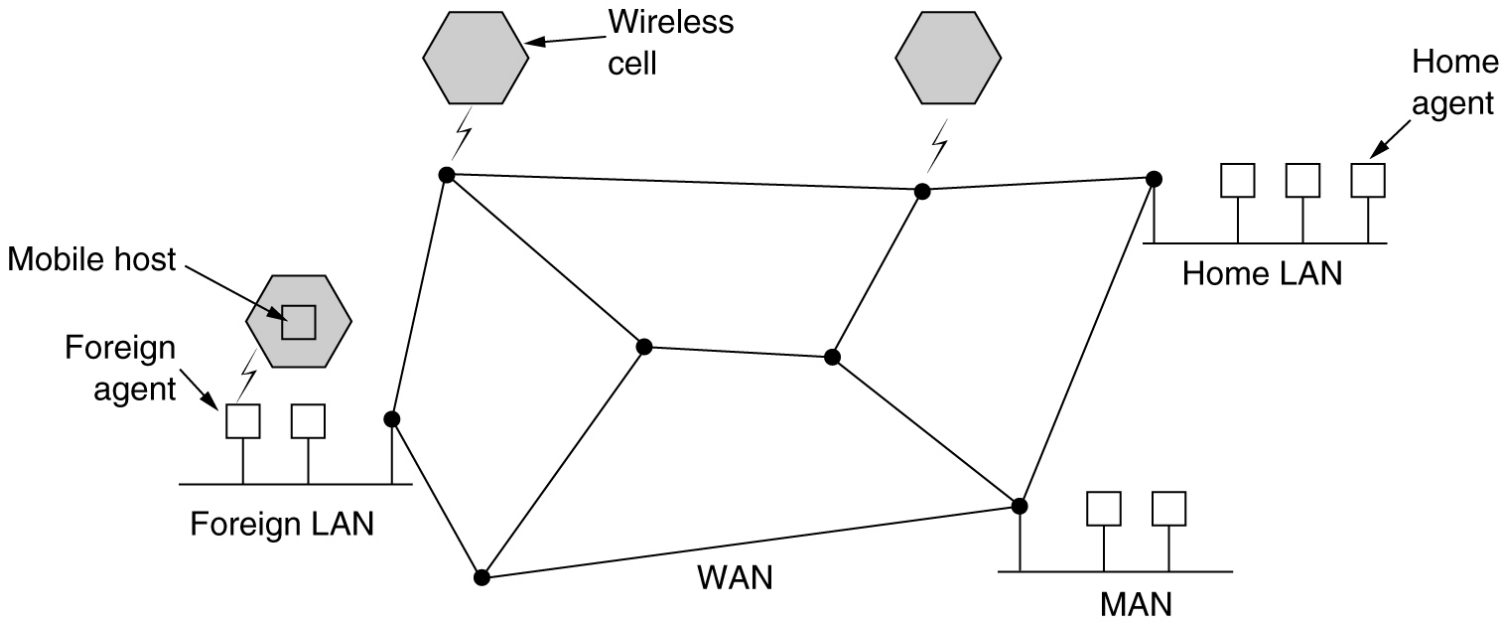
(c)



(d)

Routing for Mobile Hosts

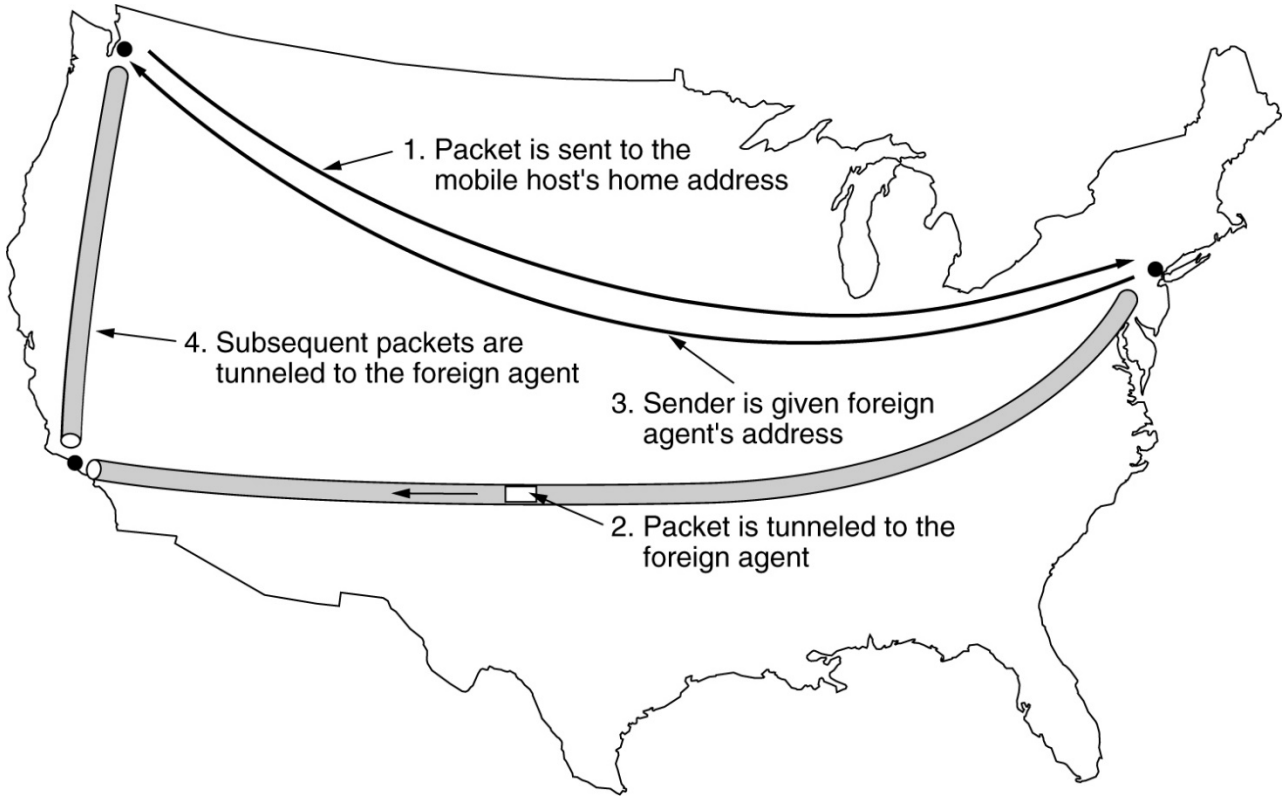
- ✓ All hosts have a permanent home location.
- ✓ The network is divided into small units – areas (e.g., a LAN, wireless cell).
- ✓ Each area has a foreign agent, which keeps track of all visiting mobile hosts.
- ✓ Each area has a home agent, which keeps track of hosts whose home is in the area, but who are currently visiting another area.
- ✓ When a new host enters an area, it must register itself with the foreign agent there.



A WAN to which LANs, MANs, and wireless cells are attached.

Routing for Mobile Hosts (2)

- ✓ When a packet is sent to a mobile host, first it is routed to the host's home LAN.
- ✓ An example: Sender – in Seattle; Receiver – traveling in LA; home in NY.
- ✓ 2. The home agent in NY tunnels the packet to the foreign agent in LA.



Packet routing for mobile users.

Routing in Mobile Ad Hoc Networks

Mobile Ad Hoc Networks (MANETs)

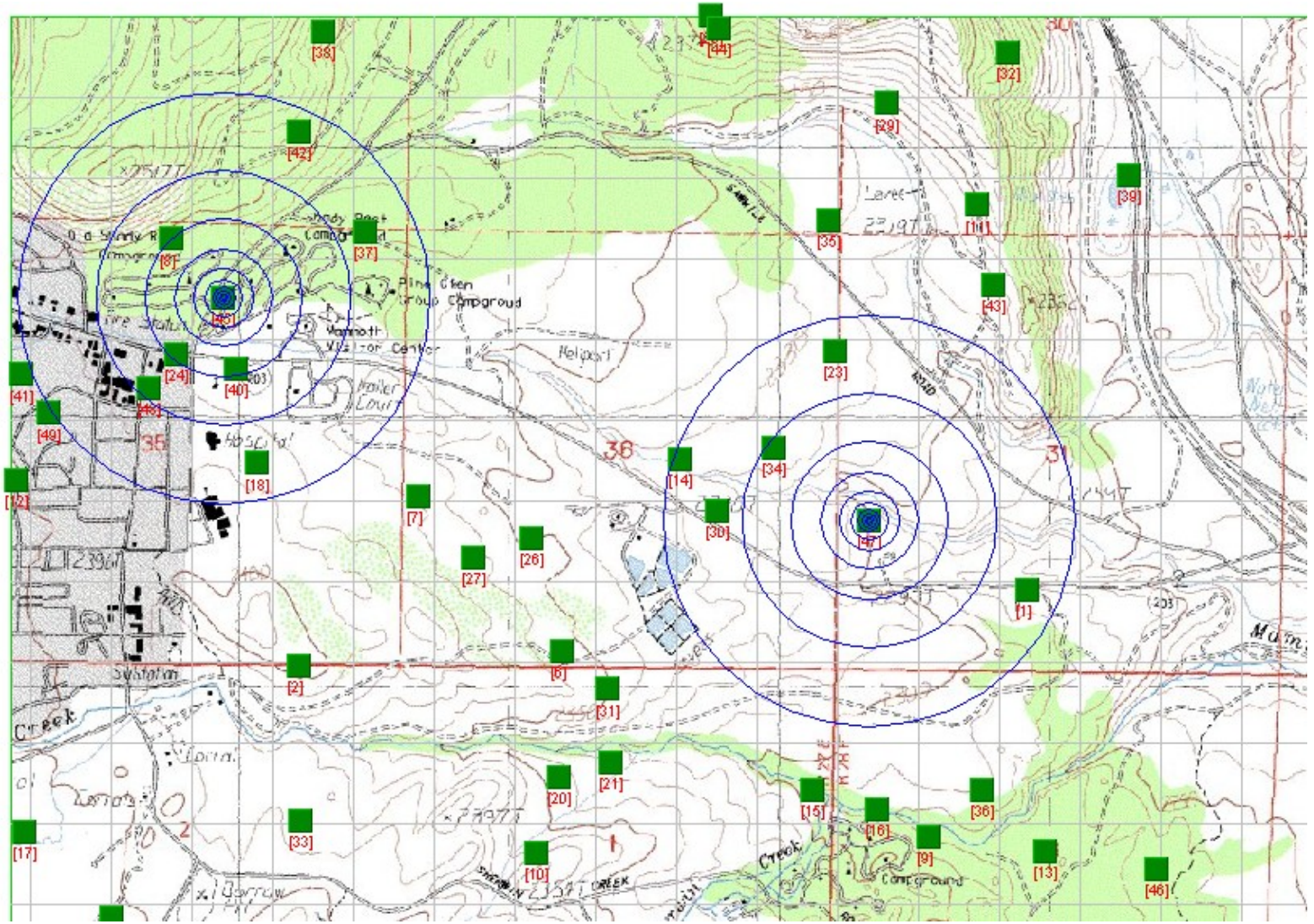
Possibilities when the routers are mobile:

1. Military vehicles on battlefield.
   - No infrastructure.
2. A fleet of ships at sea.
   - All moving all the time
3. Emergency works at earthquake .
   - The infrastructure destroyed.
4. A gathering of people with notebook computers.
   - In an area lacking 802.11.
   - How could they communicate with each other?

Mobile Ad hoc Networks

- Mobile Ad hoc Networks (MANETs)
  - Assume no fixed base station
  - Moving nodes (e.g. mobile computers) form the network
  - Multi-hop connections
  - Link broken when neighbor
    - moves away
    - out of power
  - Nodes serve as host as well as router
  - Topology changes dynamically
  - No fixed infrastructure

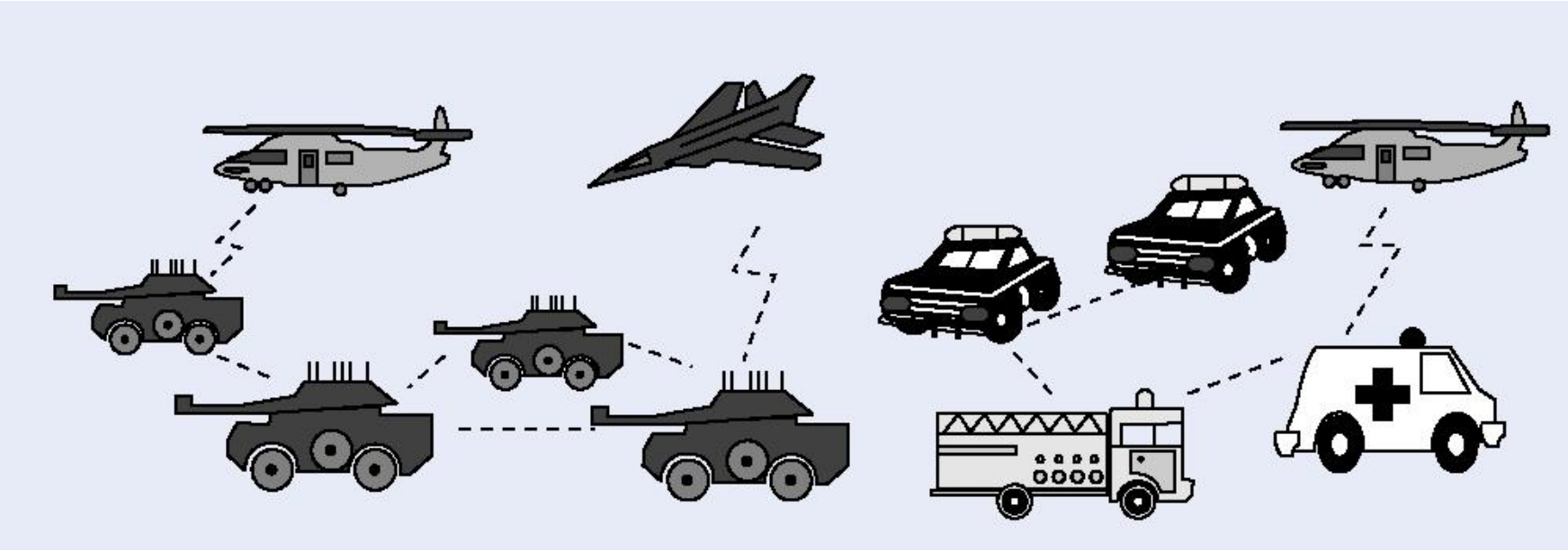
Mobile Ad hoc Networks – An Example



Applications of Mobile Ad hoc Networks

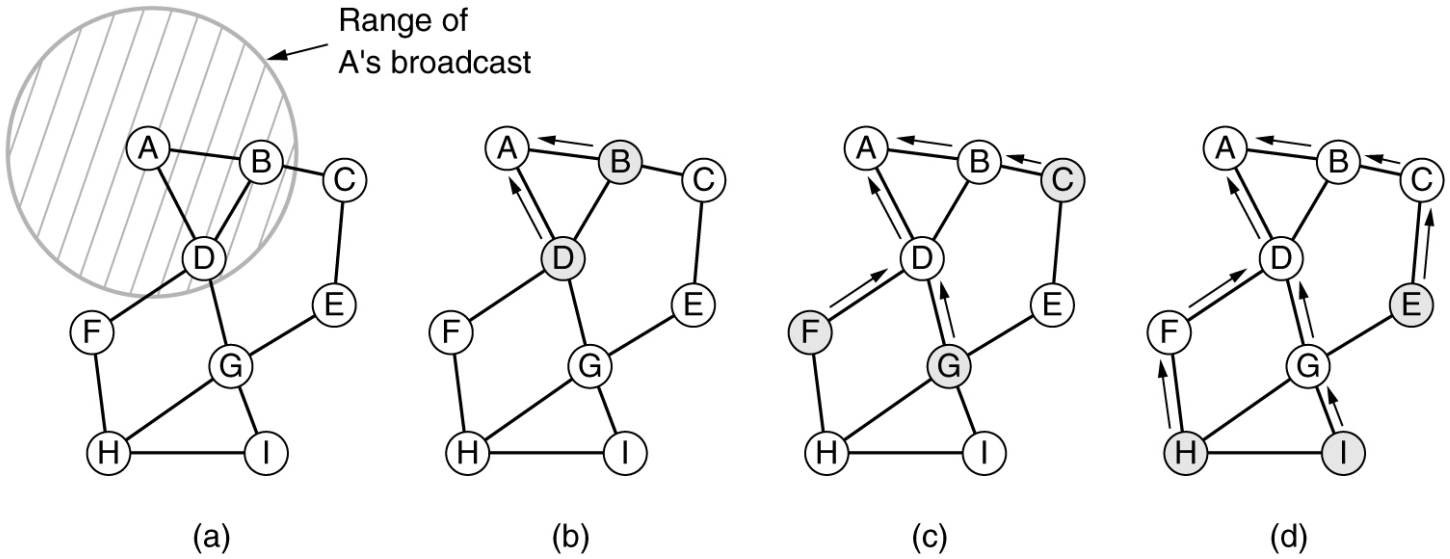
- Next generation of wireless communication systems
  - Rapid deployment of independent mobile users
  - The solution ➔ mobile ad hoc networks
- Ad hoc networks are very attractive for
  - tactical communication in the military
  - and law enforcement
- Applications in civilian life
  - disaster recovery
  - convention centers
  - conferences
  - electronic classrooms

Applications of Mobile Ad hoc Networks



Route Discovery

- ✓ AODV (Ad hoc On-demand Distance Vector) routing algorithm. Two phases:
- ✓ Route discovery – E.g., node A → node I. A floods Route Request (RR) packets.
- ✓ Route maintenance.



(a) Range of A's broadcast.

(b) After B and D have received A's broadcast.

(c) After C, F, and G have received A's broadcast.

(d) After E, H, and I have received A's broadcast.

Shaded nodes are new recipients. Arrows show possible reverse routes.

Route Discovery (2)

- ✓ Request ID – a local counter maintained by each node.
- ✓ Source address + Request ID uniquely identifies a route request session.
- ✓ When node B receives the route request packet, it first checks if this is a duplicate RR packet.
- ✓ Then node B checks if a fresh route to the destination is known by comparing the Dest. Seq. #.
  - If yes, B sends a Route Reply packet to node A.
  - If no, B increases the Hop count by one, and forwards the Route Request packet to other nodes.

Source address	Request ID	Destination address	Source sequence #	Dest. sequence #	Hop count

Format of a ROUTE REQUEST packet.

Route Discovery (3)

- ✓ Either an intermediate node or the destination node I will send a Route Reply (RP) packet to the source node A.
- ✓ When an intermediate node receives the RP packet, it updates its routing table.
- ✓ Lifetime – indicates how long the route may be valid.

Source address	Destination address	Destination sequence #	Hop count	Lifetime

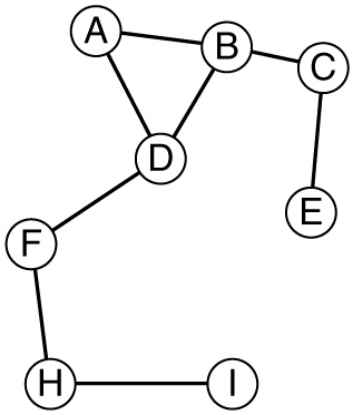
Format of a ROUTE REPLY packet.

Route Maintenance

- ✓ Since nodes can move away or be turned off or fail, the topology changes constantly.
- ✓ Each node keeps track of its active neighbors by periodically sending a Hello message.
- ✓ E.g., if node G goes down, D notifies A, B the event, and removes the entries to node E, G, I.

Dest.	Next hop	Distance	Active neighbors	Other fields
A	A	1	F, G	
B	B	1	F, G	
C	B	2	F	
E	G	2		
F	F	1	A, B	
G	G	1	A, B	
H	F	2	A, B	
I	G	2	A, B	

(a)



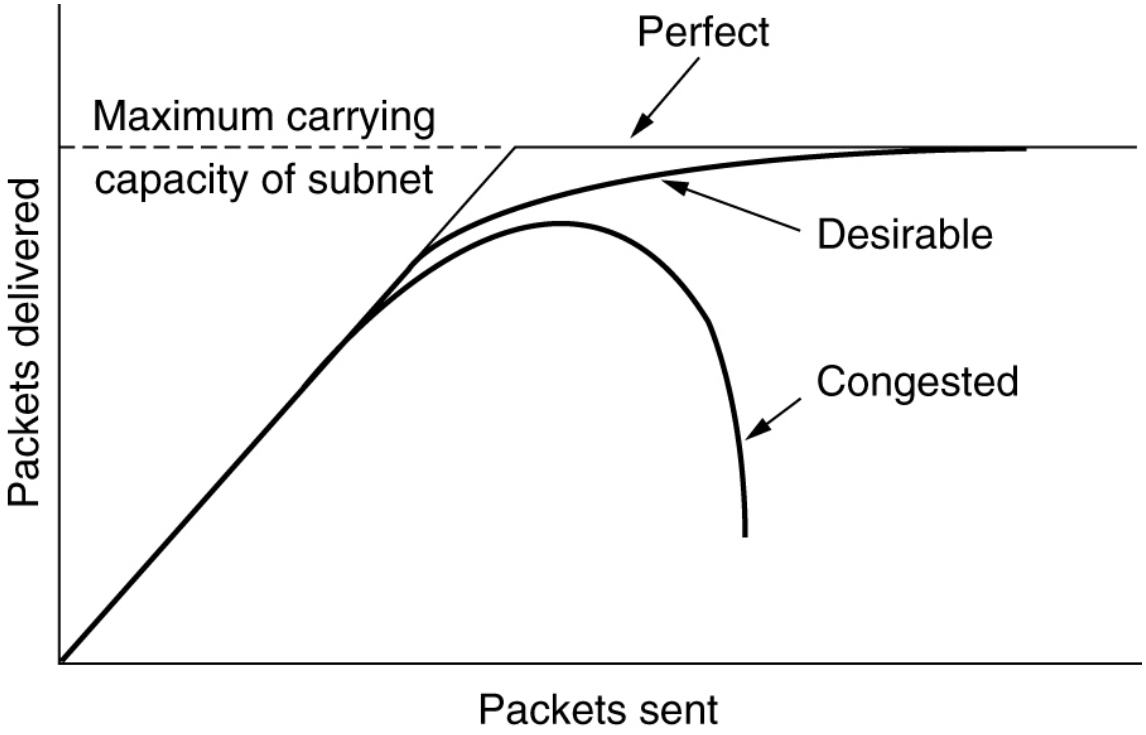
(b)

(a) D's routing table before G goes down. (b) The graph after G has gone down.

5.3 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

Congestion



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

General Principles of Congestion Control

- Open-loop solutions
- Close-loop solutions

1. Monitor the system
   - detect when and where congestion occurs.
   - Metrics include percentage of dropped packets, average queue length, average packet delay, etc.
2. Pass information to where action can be taken.
   - The router sends a packet to the traffic source.
3. Adjust system operation to correct the problem.
   - Reduce traffic volume.

Congestion Prevention Policies

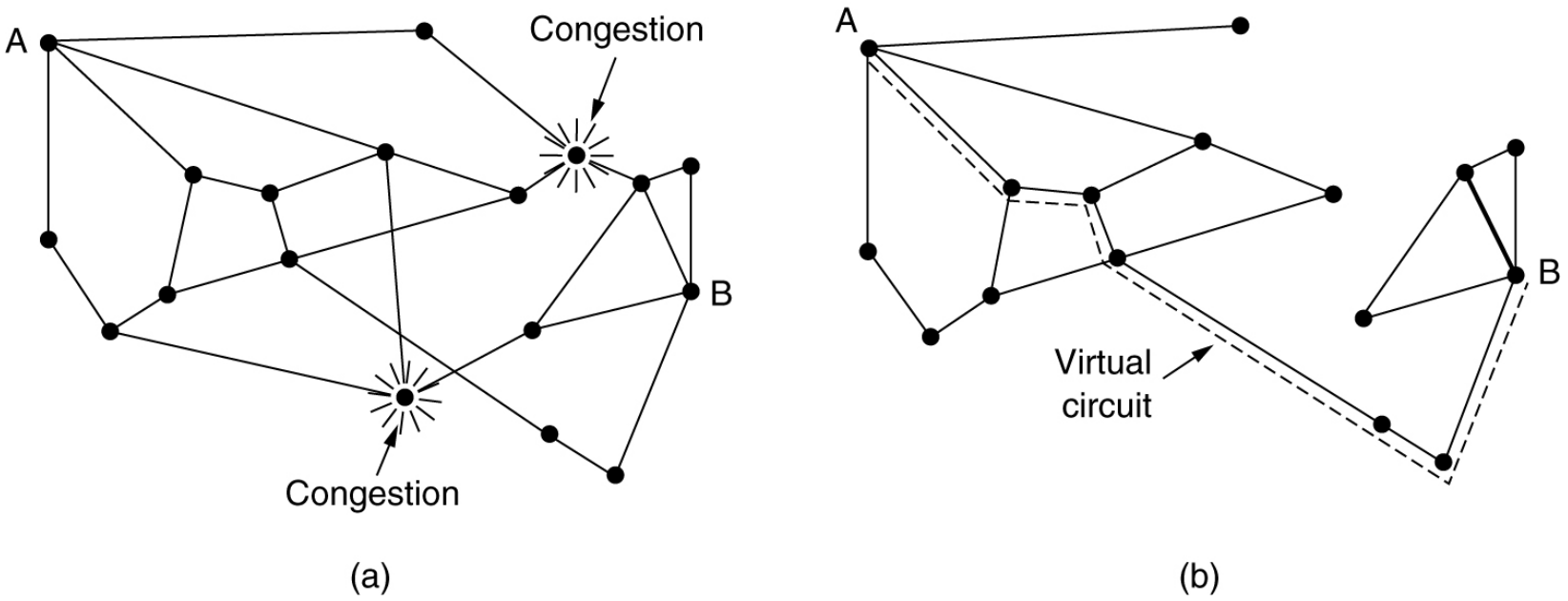
- ✓ Open-loop solutions – Congestion Prevention: The systems are designed to min. congestion in the first place. Appropriate policies are used at various levels.

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.

Congestion Control in Virtual-Circuit Subnets

- ✓ VC - Connection oriented
- ✓ Admission control – once congestion has been signaled, no more VC are set up until the problem has gone away.
  - Preventing congestion from getting worse.
- ✓ Another approach is to allow new VC but carefully route all new VCs around problem areas.



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

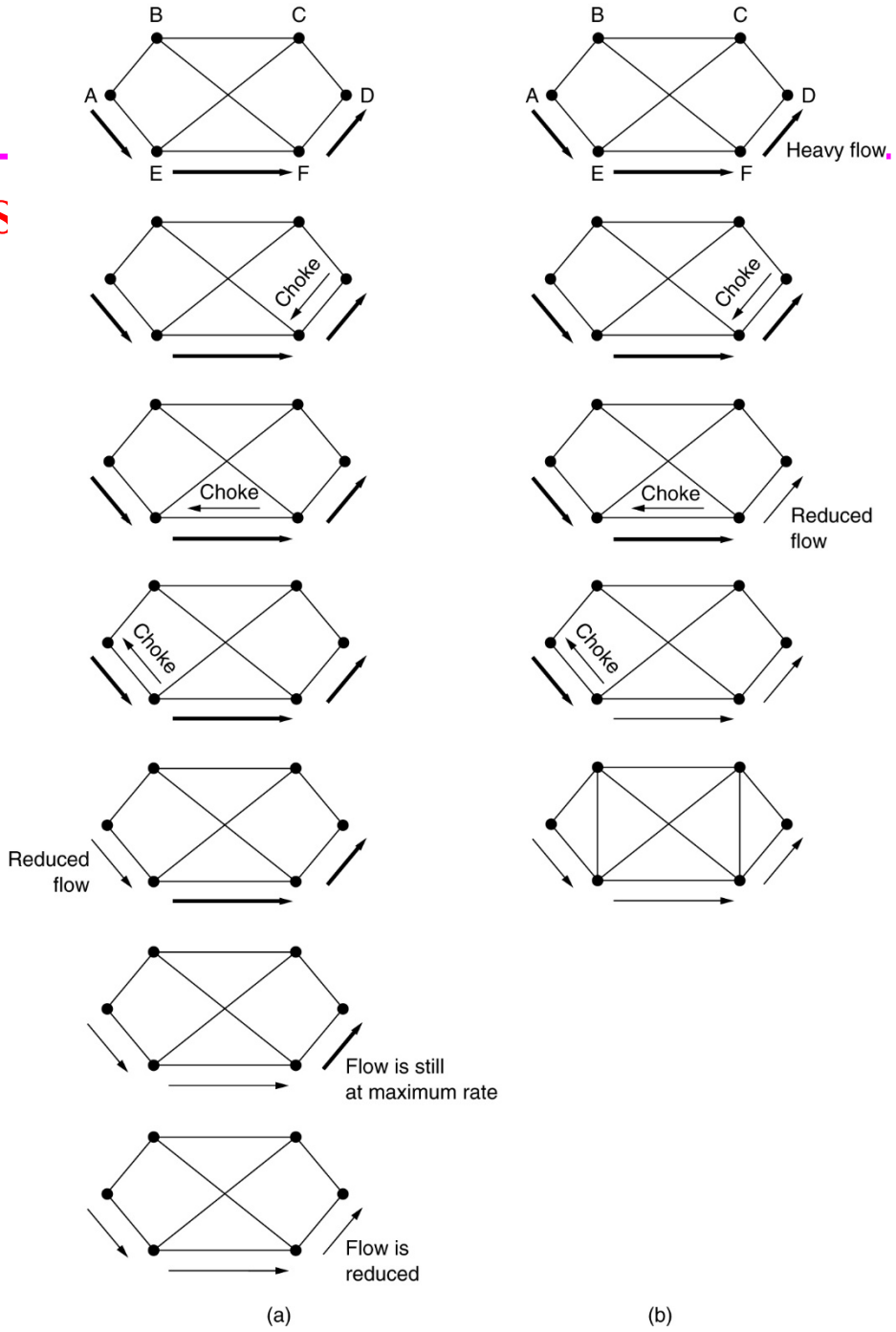
Congestion Control in Datagram Subnets

Hop-by-Hop Choke Packets

- ✓Each router can easily monitor the utilization of its output lines and other resources.
- ✓When the line utilization exceeds a certain threshold, a warning message can be sent to the source – choke packet.
- ✓For long distances, only sending a choke packet to the source does not work well because the reaction is slow.
- ✓The choke packet can take effect at every hop.

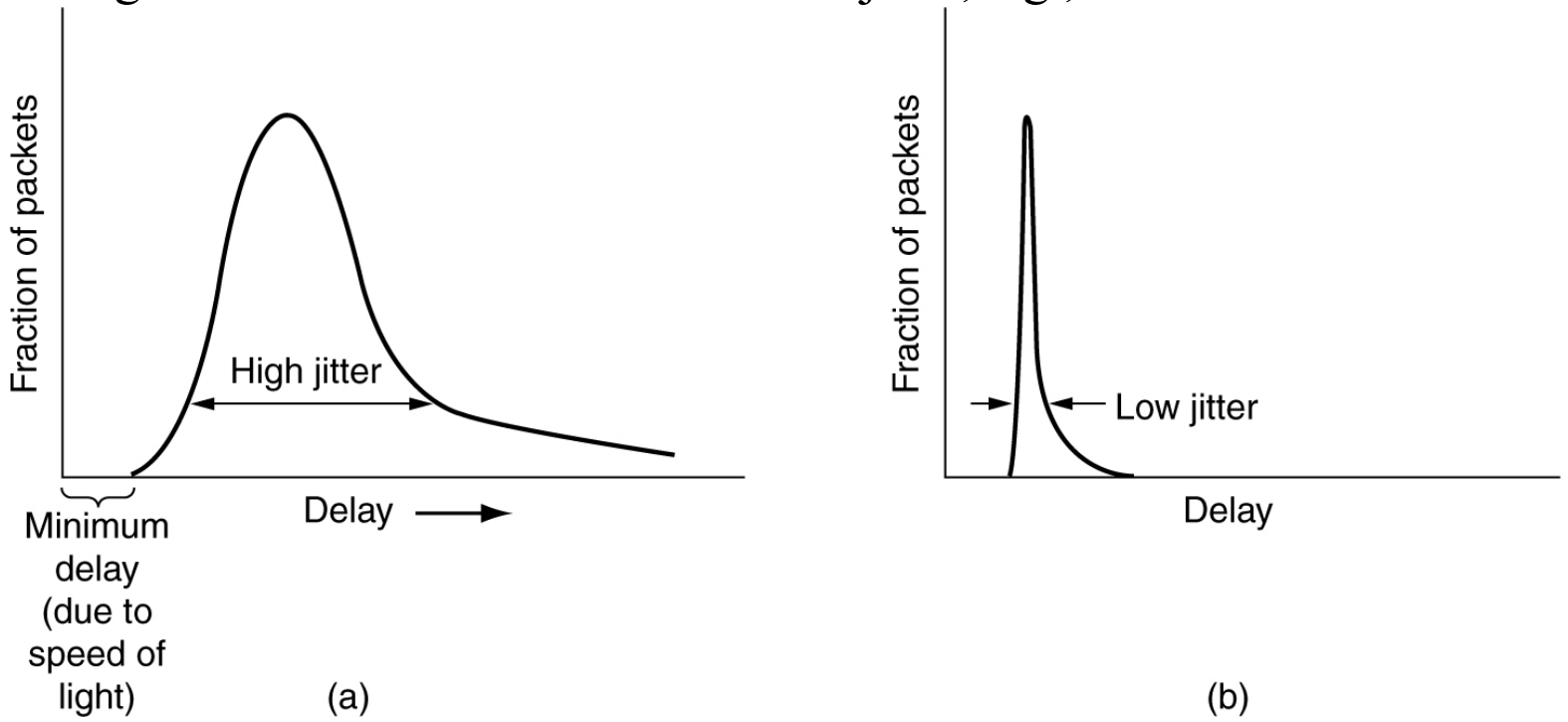
(a) A choke packet that affects only the source.

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



Jitter Control

- ✓ Jitter – The variation (i.e., the standard deviation) in the packet arrival time.
- ✓ Audio and video streams require low jitter.
- ✓ High jitter – Some packets take 20 msec and others take 30 msec.
- ✓ Each router can check to see if a packet is behind or ahead of its schedule, then the router can arrange packet position in the outgoing queue.
- ✓ Buffering at the receiver can also eliminate jitter, e.g., online video.



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

5.4 Quality of Service (QoS)

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

Requirements

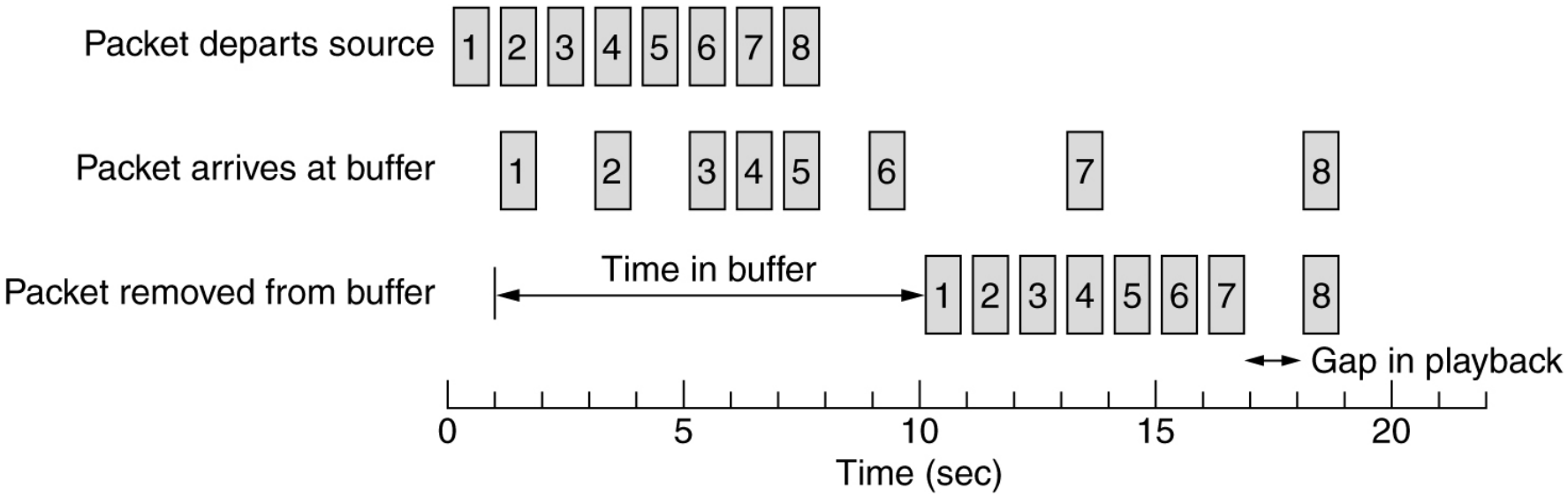
Application	Reliability	Delay	Jitter	Bandwidth
E-mail	High	Low	Low	Low
File transfer	High	Low	Low	Medium
Web access	High	Medium	Low	Medium
Remote login	High	Medium	Medium	Low
Audio on demand	Low	Low	High	Medium
Video on demand	Low	Low	High	High
Telephony	Low	High	High	Low
Videoconferencing	Low	High	High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

How stringent the quality-of-service requirements are.

Techniques for Achieving Good Quality of Service

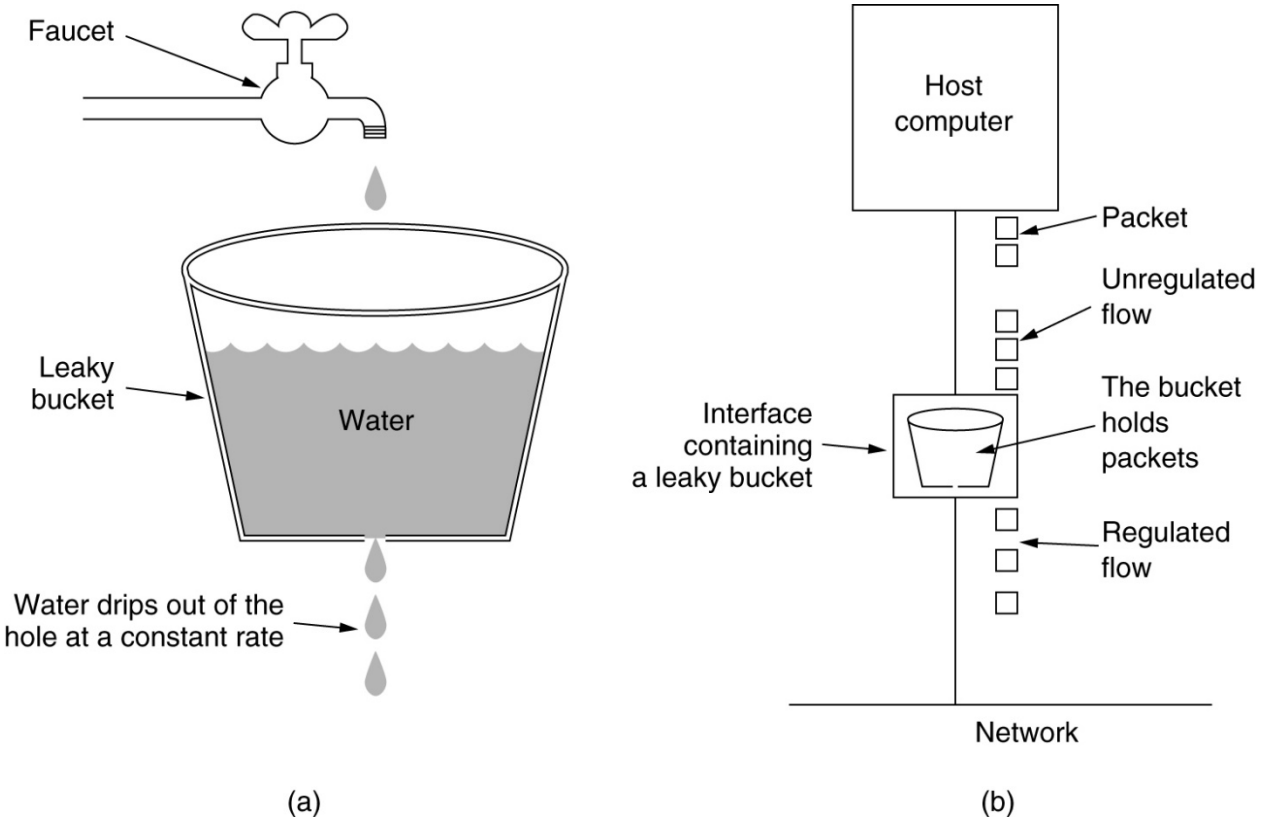
- Over-provisioning
  - ✓ Providing much router capacity, buffer space and bandwidth.
  - ✓ The problem - expensive.
- Buffering
  - ✓ Flows can be buffered on the receiving side before being delivered.
  - ✓ Buffering does not affect the reliability and bandwidth, and increases the delay, but reduces the jitter.
- Traffic Shaping
  - ✓ makes the server (sender) transmit at a uniform rate.
  - ✓ smoothes out the traffic on the server side.
  - ✓ Regulate the average rate of data transmission.
  - ✓ The Leaky Bucket Algorithm
    - Rigid output pattern
  - ✓ The Token Bucket Algorithm
    - Output rate may change depends on incoming traffic bursts.

Buffering



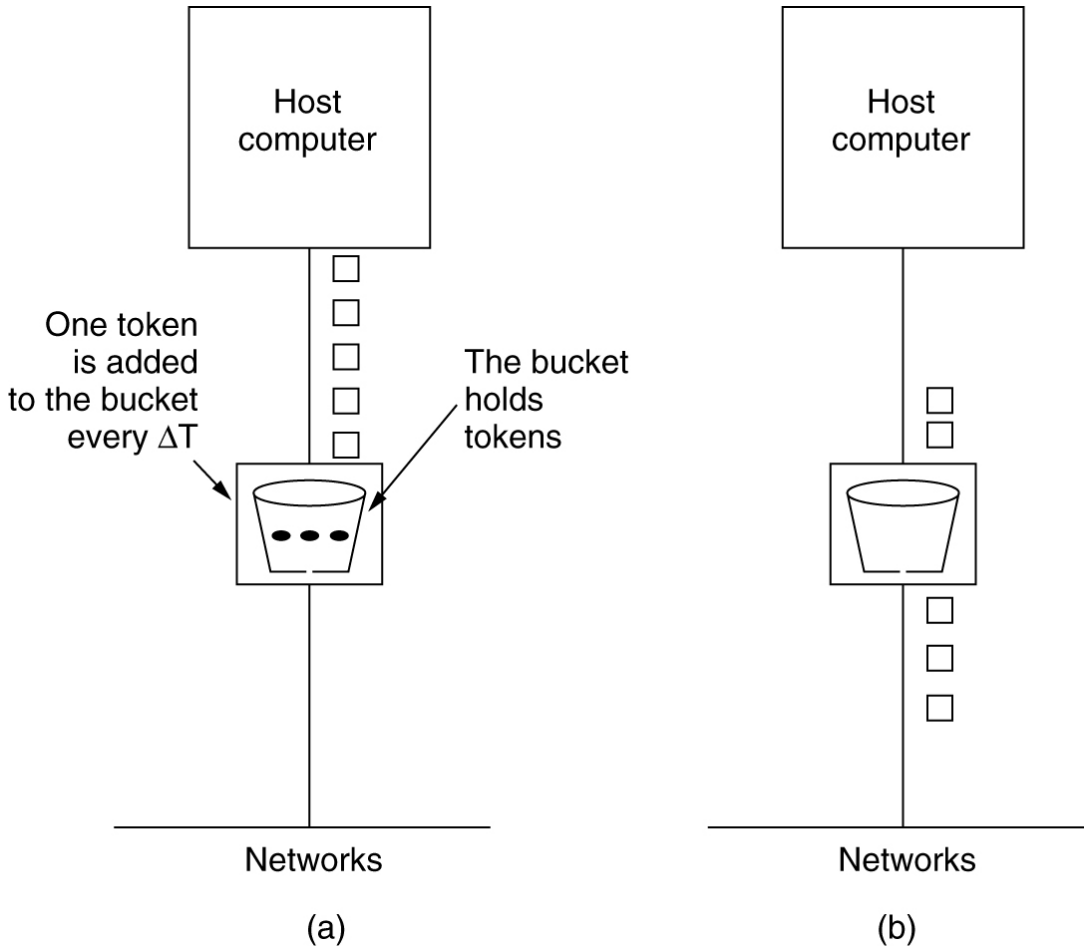
Smoothing the output stream by buffering packets.

The Leaky Bucket Algorithm



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

The Token Bucket Algorithm



(a) Before. (b) After.

Admission Control

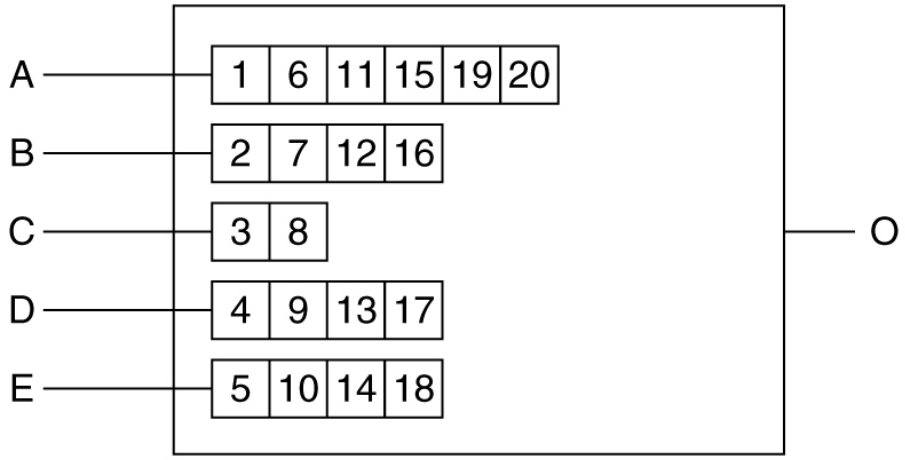
- ✓ Admission Control – When a flow is offered to a router, it has to decide whether to admit or reject the flow, based on
  - its capacity and current commitments.
- ✓ A flow is specified by a set of parameters – flow specification

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

An example of flow specification.

Packet Scheduling

- ✓ If a router is handling multiple flows, it needs to avoid letting one flow occupying the outgoing line.
- ✓ Queuing algorithms are used to solve the issue.
- ✓ Fair queuing algorithm – round robin
- ✓ Improved algorithm – the packets are sorted based on their finishing time.
- ✓ Weighted fair queuing – assign weights to different traffics.



(a)

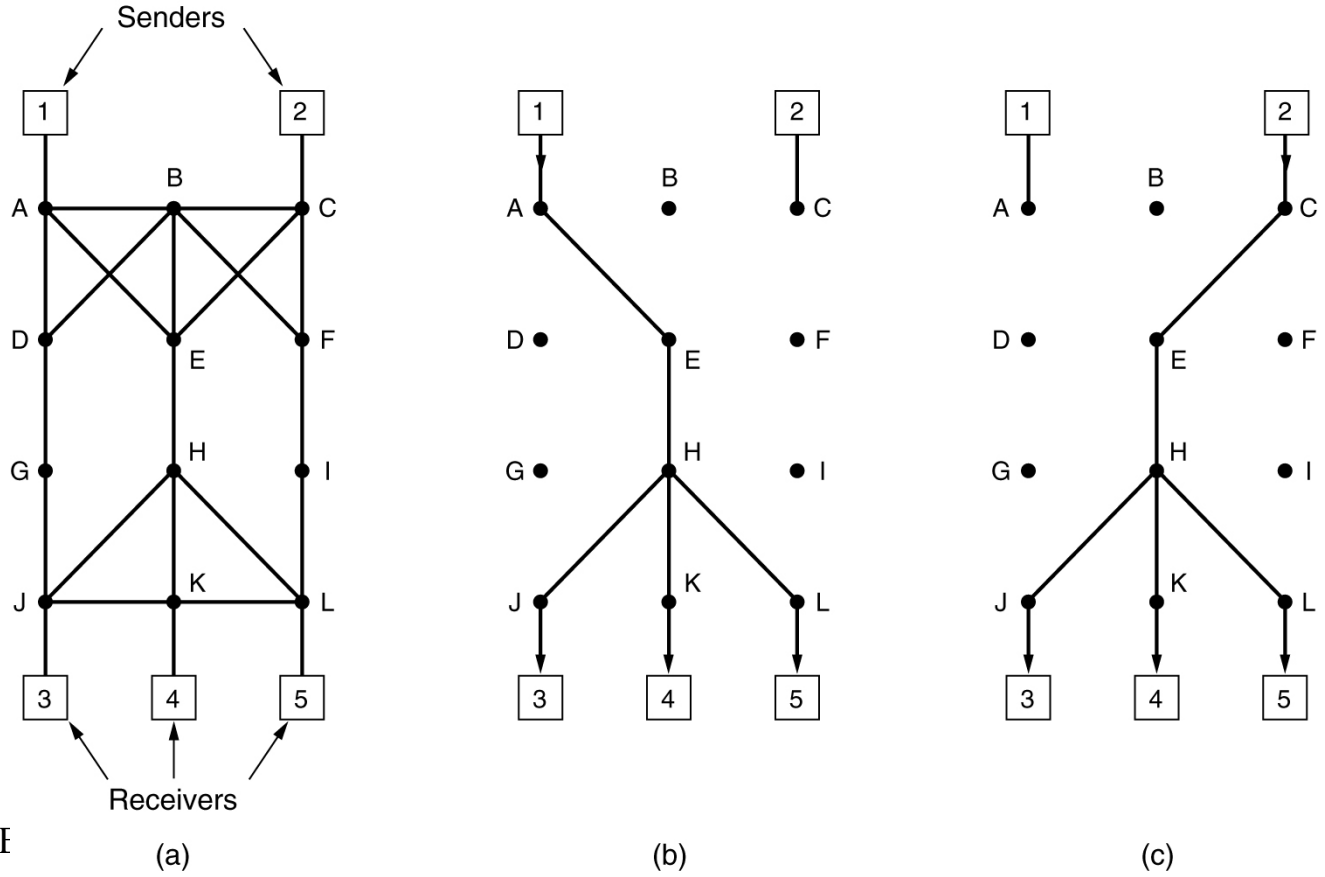
Packet	Finishing time
C	8
B	16
D	17
E	18
A	20

(b)

(a) A router with five packets queued for line O. (b) Finishing times for the five packets.

RSVP-The ReSerVation Protocol

- ✓ Integrated Services – addressing both unicast and multicast multimedia applications
- ✓ RSVP – is used for making reservation, and allows multiple senders to transmit to multiple groups of receivers, optimizes bandwidth use while eliminating congestion.

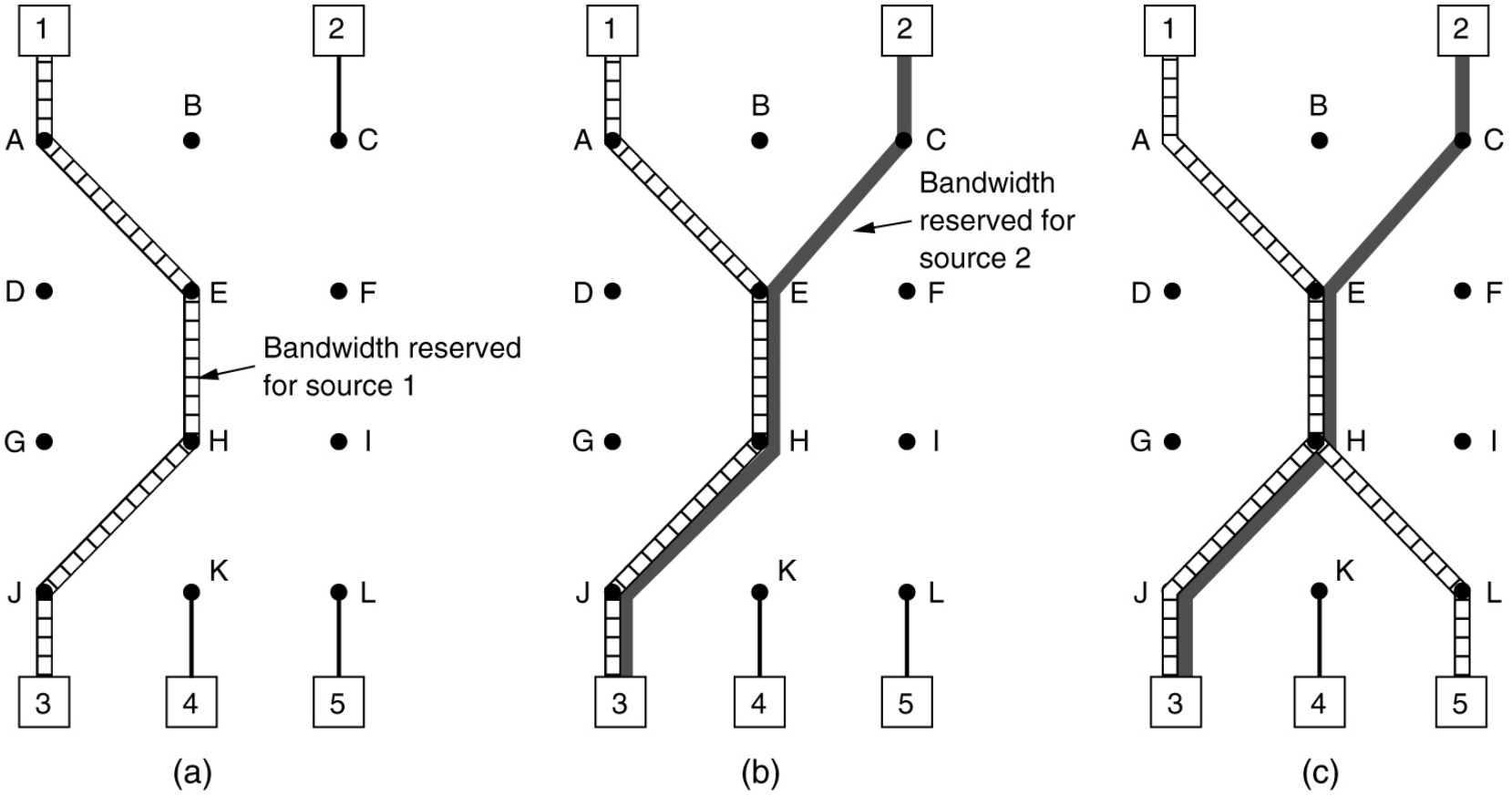


(a) A network

(b) The multicast spanning tree for host 1.

(c) The multicast spanning tree for host 2.

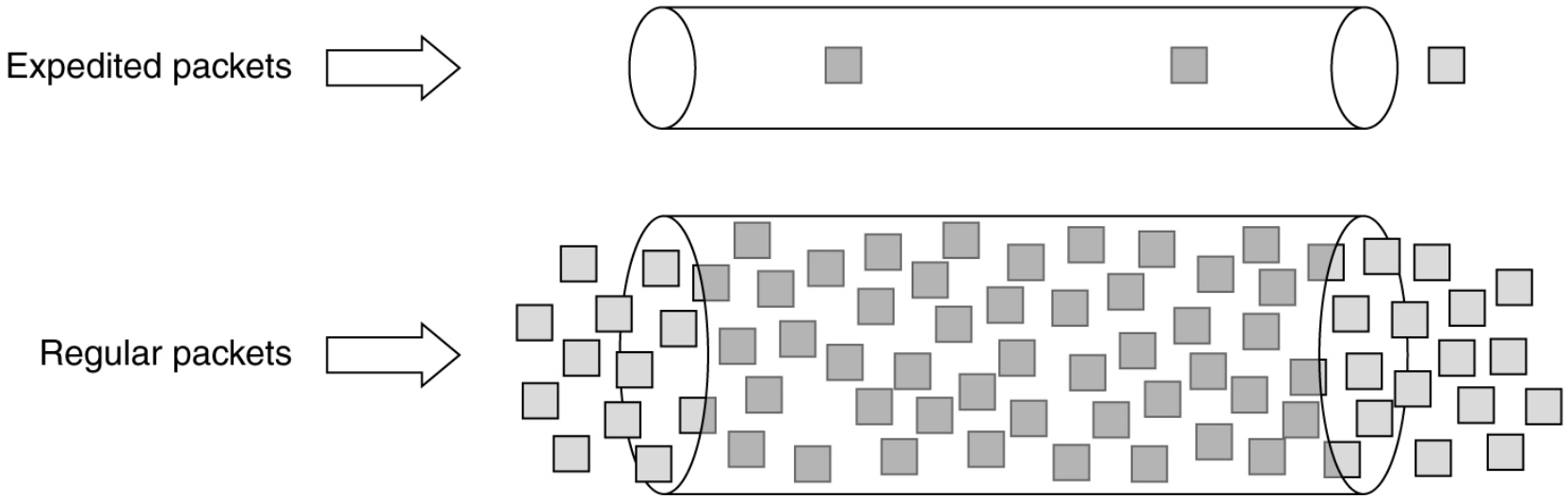
RSVP-The ReSerVation Protocol (2)



(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.

Expedited Forwarding

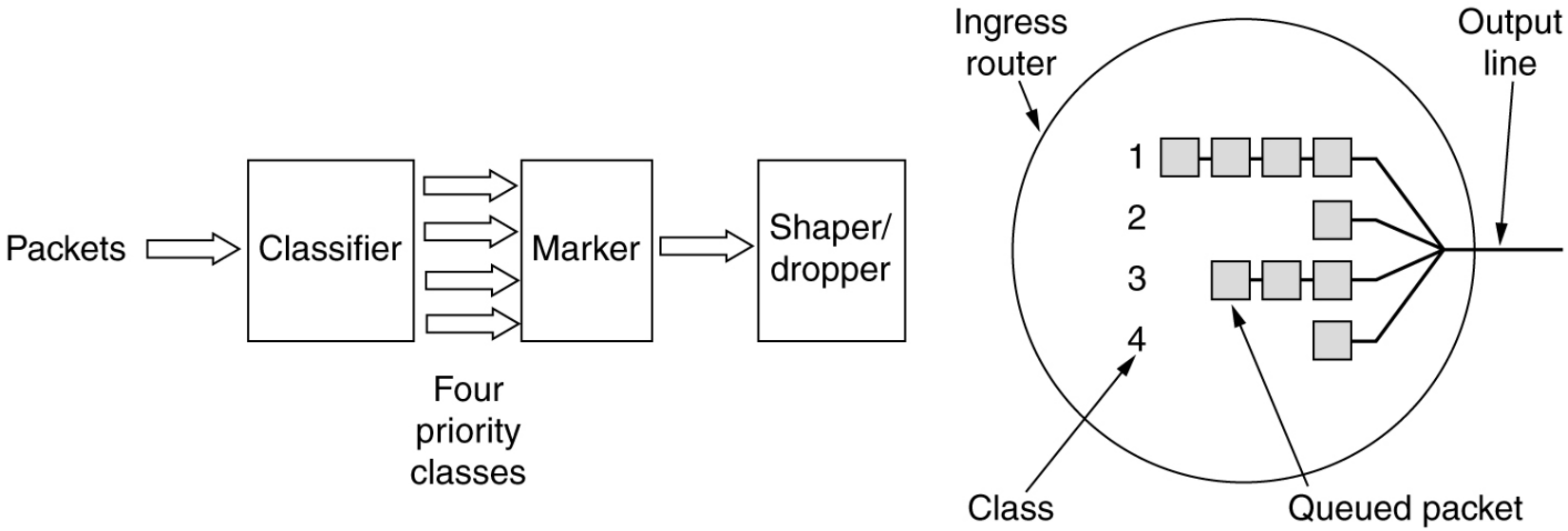
- ✓ Differentiated Services – flows are assigned with different class of service.
- ✓ Regular class and expedited class (higher priority).



Expedited packets experience a traffic-free network.

Assured Forwarding

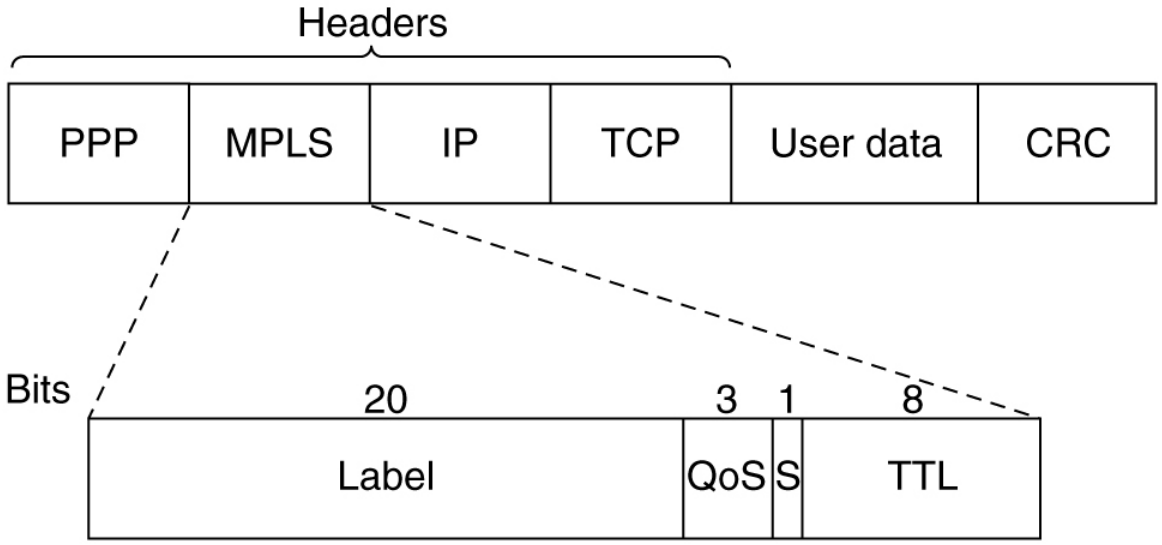
- ✓ Assured Forwarding– four priority classes.



A possible implementation of the data flow for assured forwarding.

Label Switching and MPLS

- ✓ MPLS – Multi-Protocol Label Switching.
- ✓ Routing packet based on the label.
  - Label – the label index
  - QoS – Class of service
  - S – stacking multiple labels in hierarchical networks
  - TTL – Time to Live.

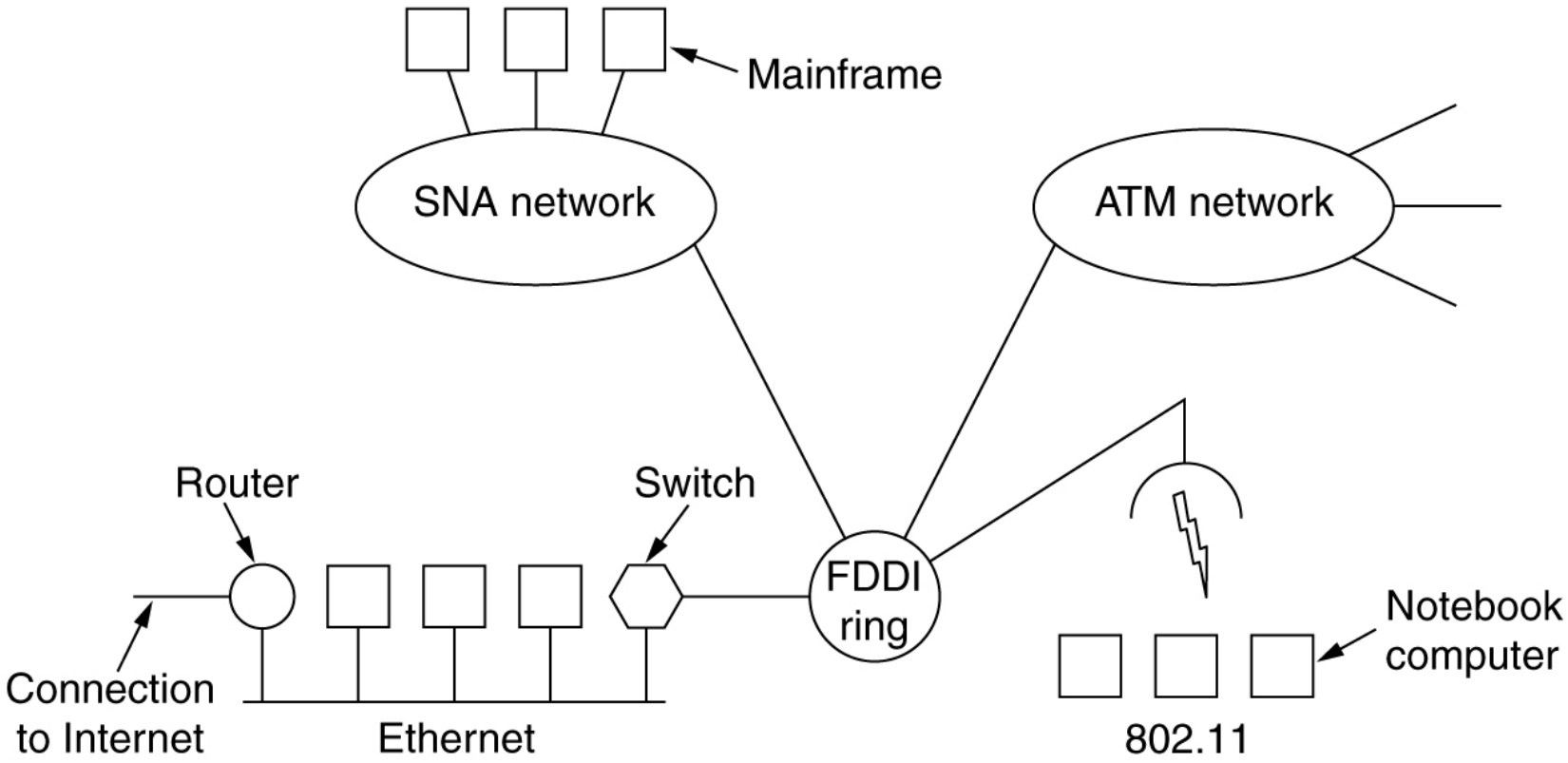


Transmitting a TCP segment using IP, MPLS, and PPP.

Internetworking

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

Connecting Networks



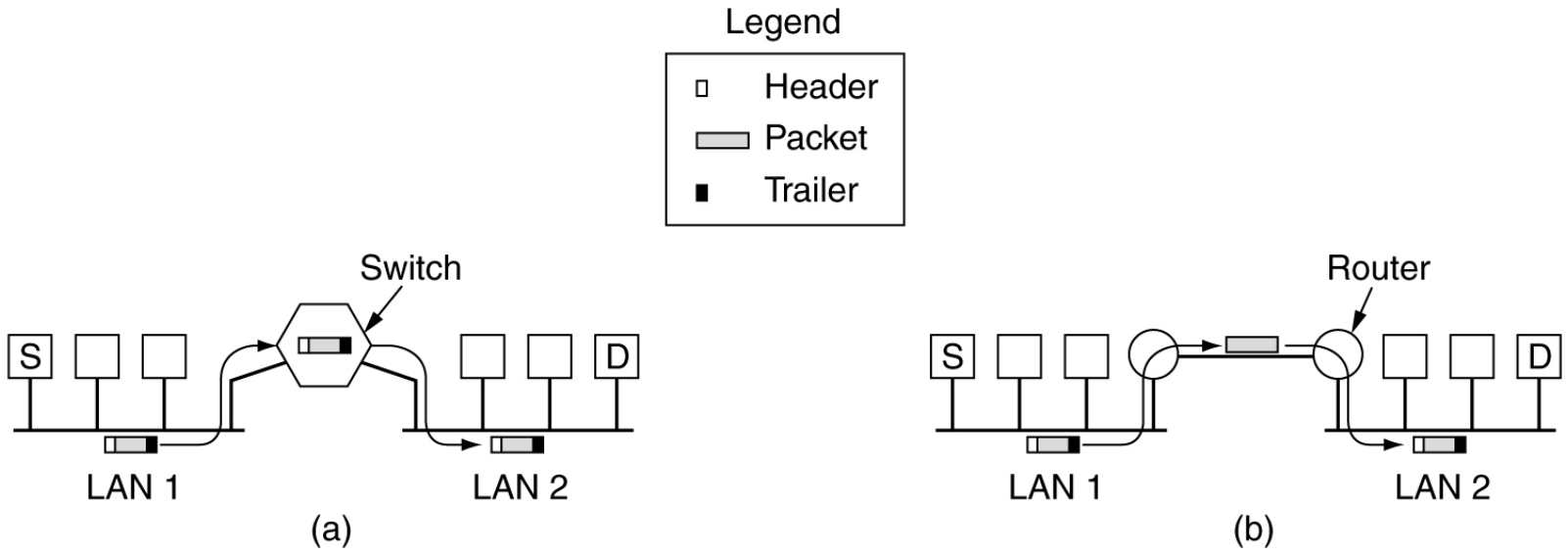
A collection of interconnected networks.

How Networks Differ

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

Some of the many ways networks can differ.

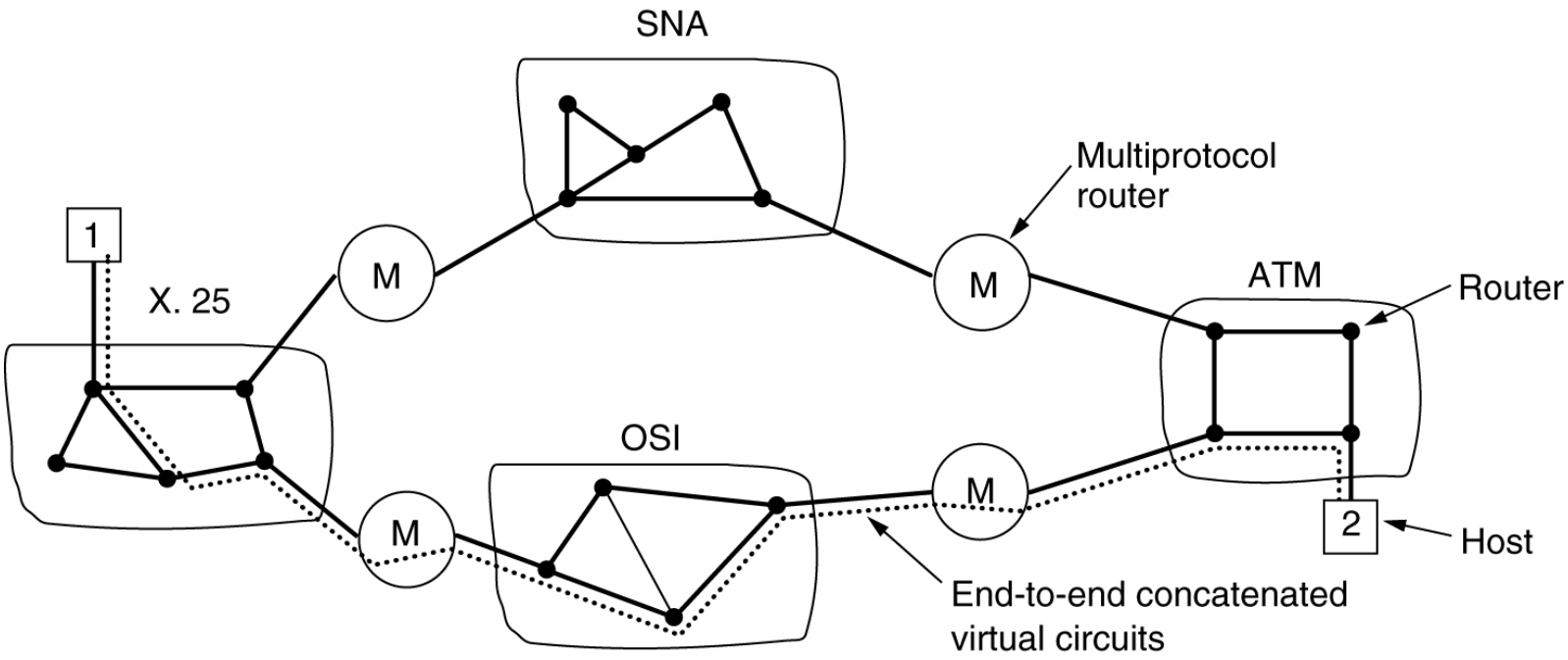
How Networks Can Be Connected



(a) Two Ethernets connected by a switch.

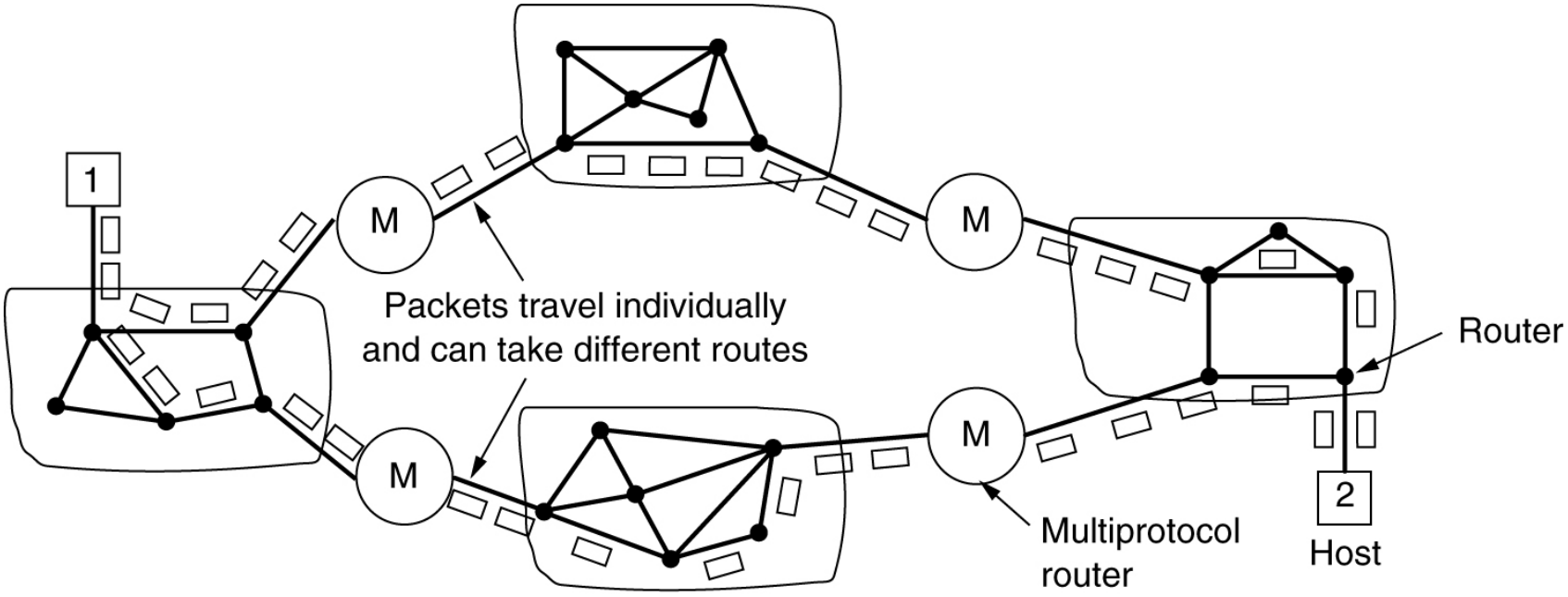
(b) Two Ethernets connected by routers.

Concatenated Virtual Circuits



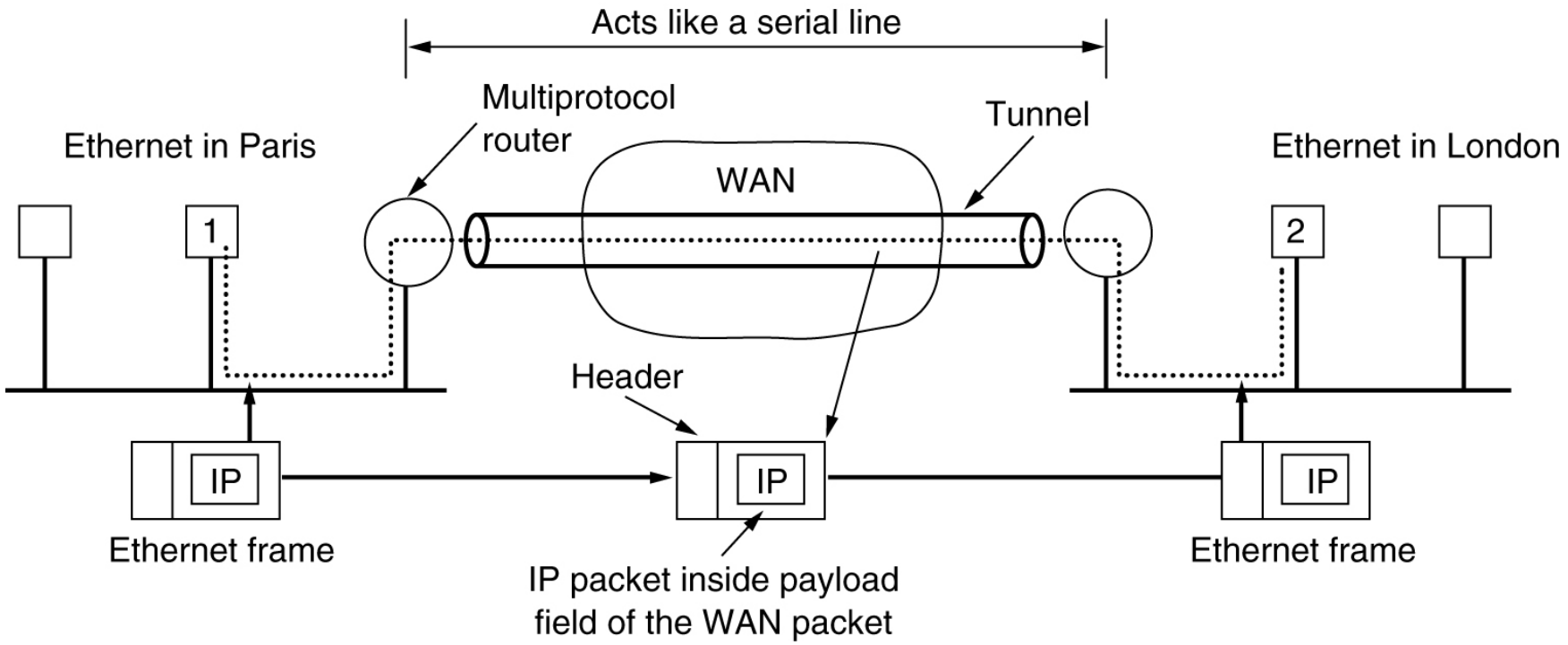
Internetworking using concatenated virtual circuits.

Connectionless Internetworking



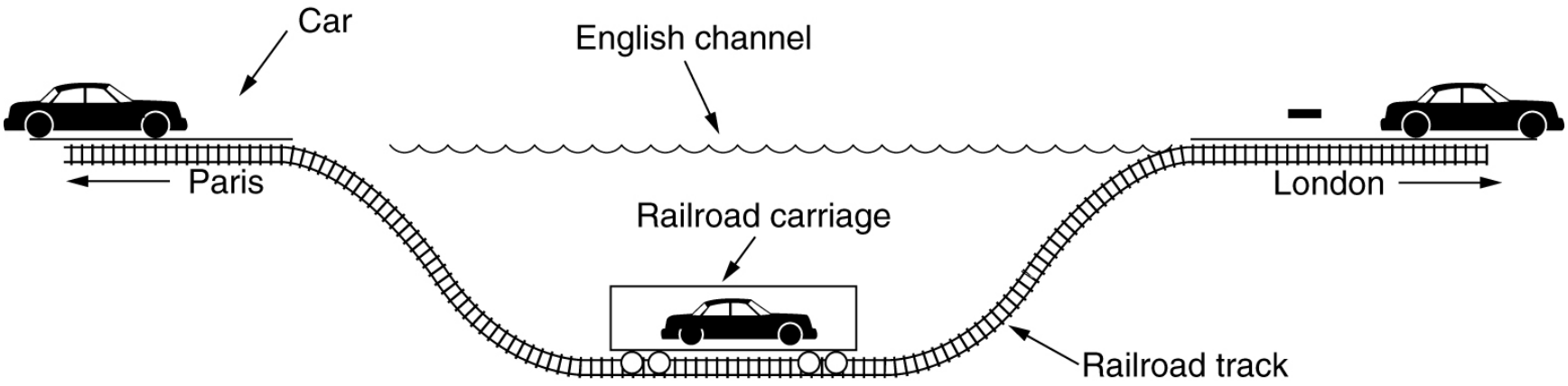
A connectionless internet.

Tunneling



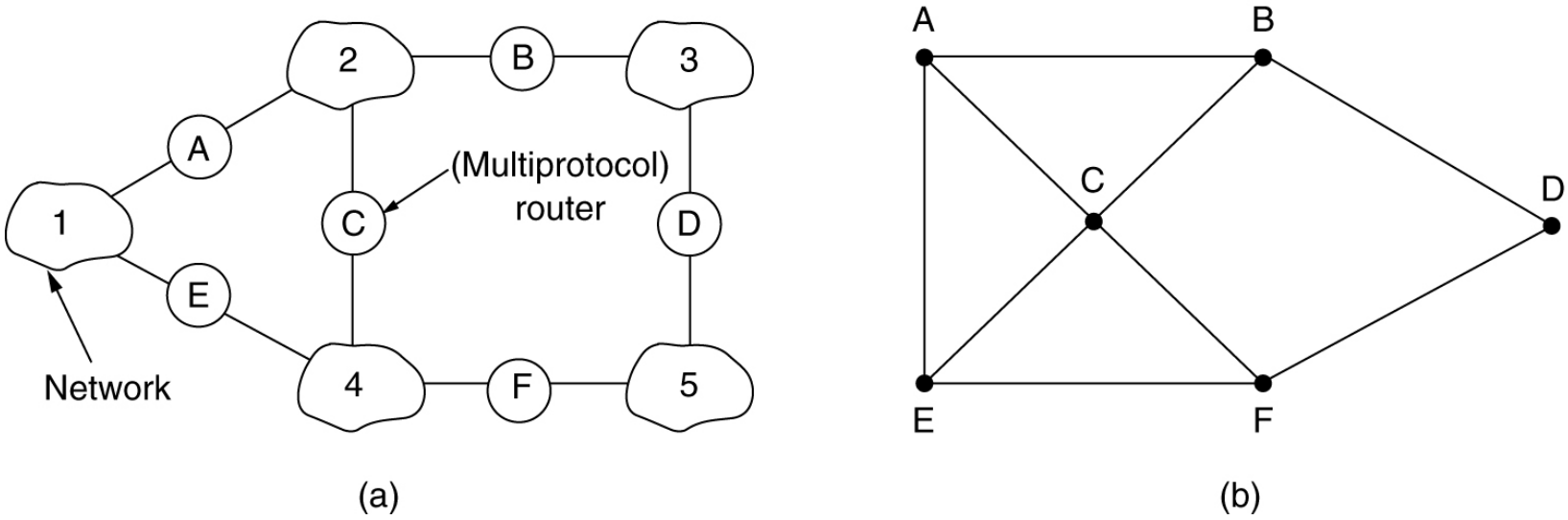
Tunneling a packet from Paris to London.

Tunneling (2)



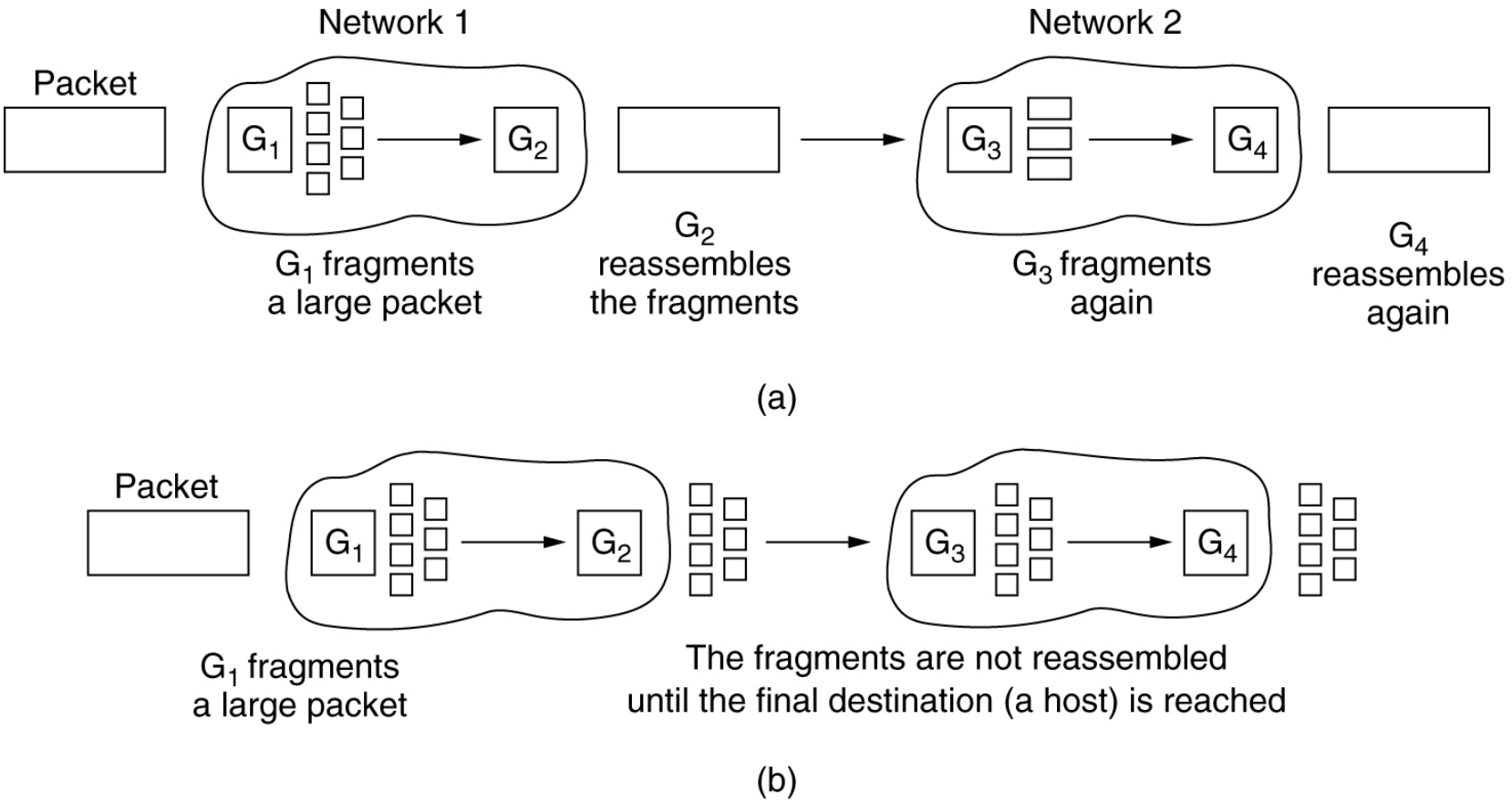
Tunneling a car from France to England.

Internetwork Routing



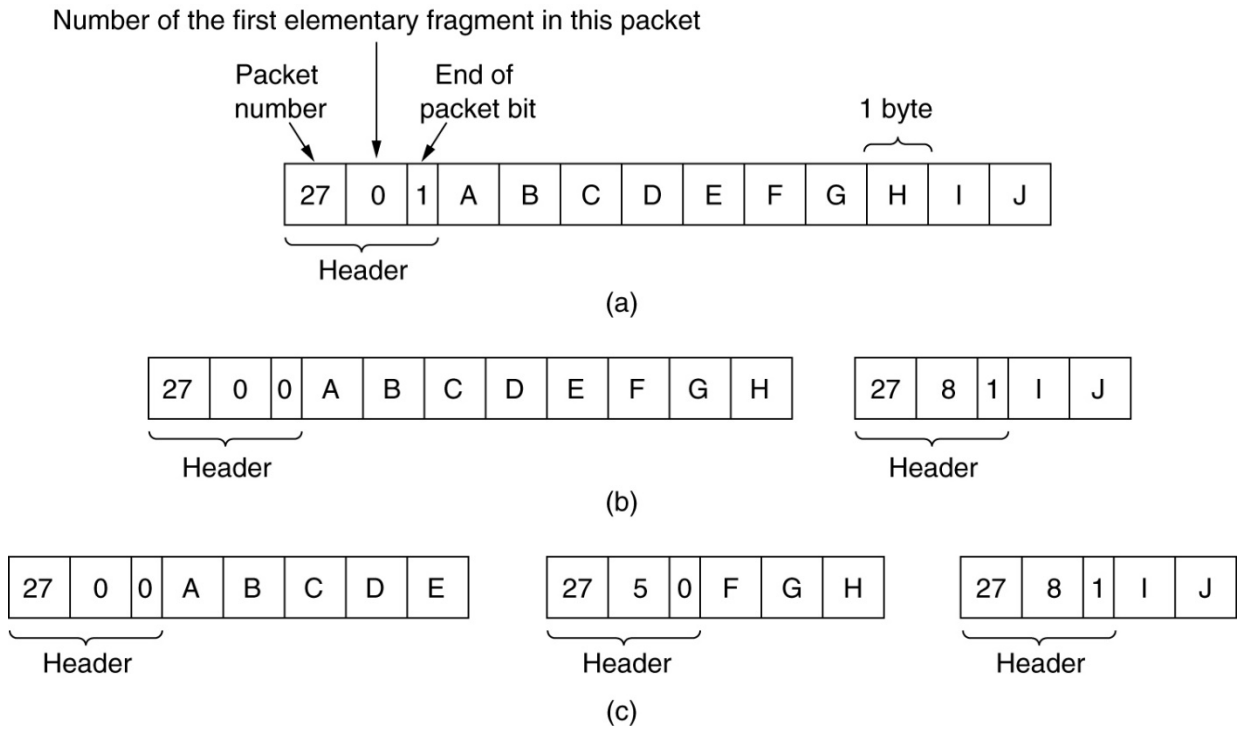
(a) An internetwork. (b) A graph of the internetwork.

Fragmentation



(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.

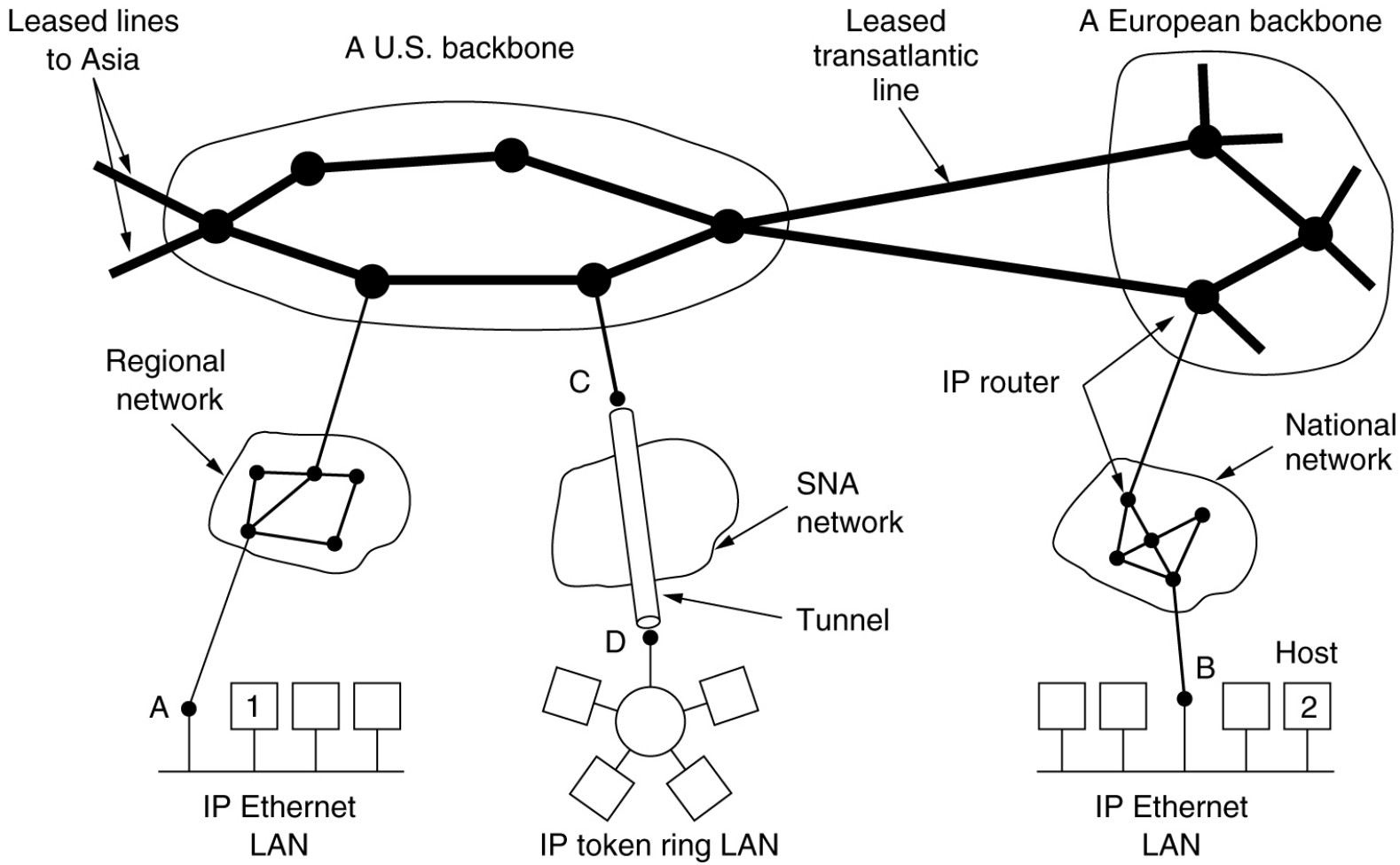
The Network Layer in the Internet

- The IP Protocol
- IP Addresses
- Internet Control Protocols
- OSPF – The Interior Gateway Routing Protocol
- BGP – The Exterior Gateway Routing Protocol
- Internet Multicasting
- Mobile IP
- IPv6

Design Principles for Internet

1. Make sure it works.
2. Keep it simple.
3. Make clear choices.
4. Exploit modularity.
5. Expect heterogeneity.
6. Avoid static options and parameters.
7. Look for a good design; it need not be perfect.
8. Be strict when sending and tolerant when receiving.
9. Think about scalability.
10. Consider performance and cost.

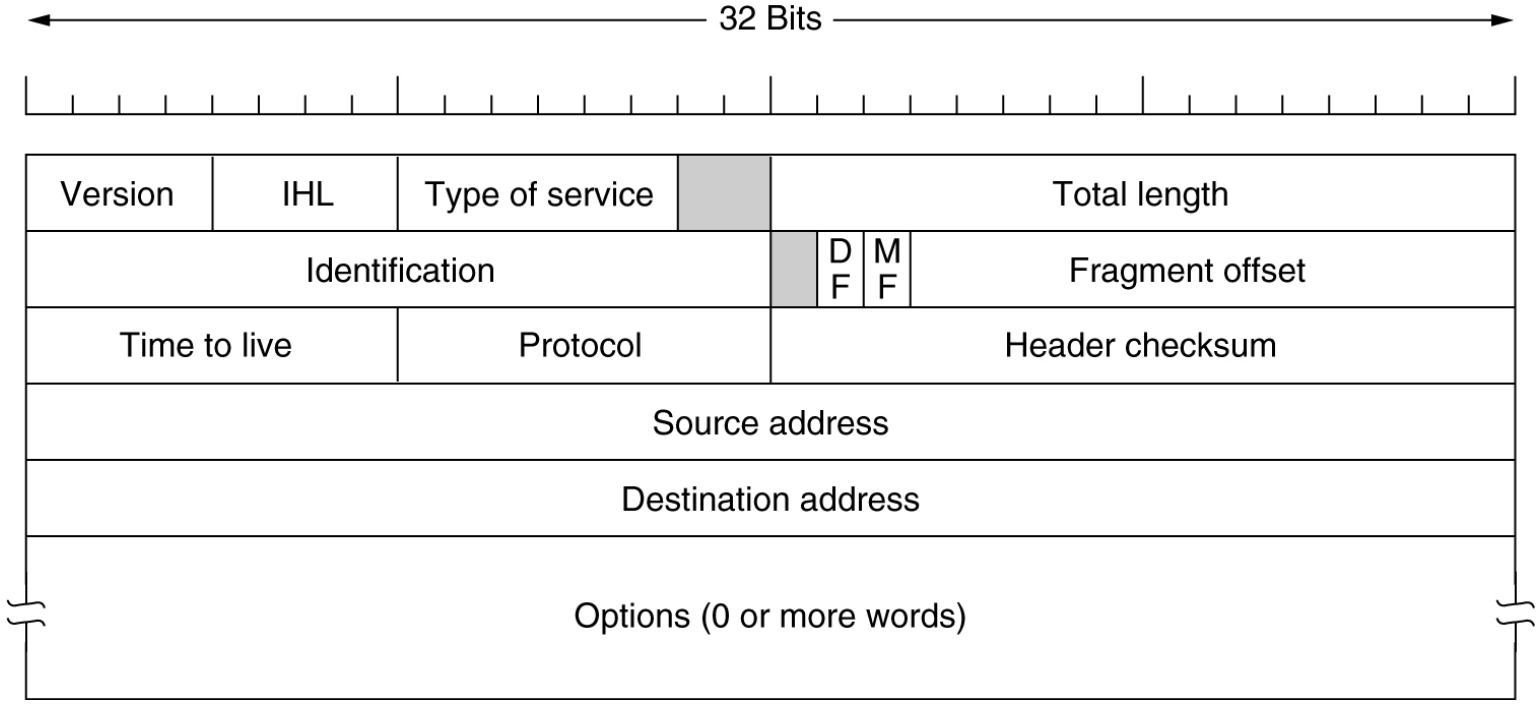
Collection of Subnetworks



The Internet is an interconnected collection of many networks.

The IP Protocol

- ✓ IHL – IP Header Length.
- ✓ Total length – includes both header and data
- ✓ DF – Don't Fragment. To order the router not to fragment it.
- ✓ MF – More Fragment
- ✓ Protocol – tell which transport protocol



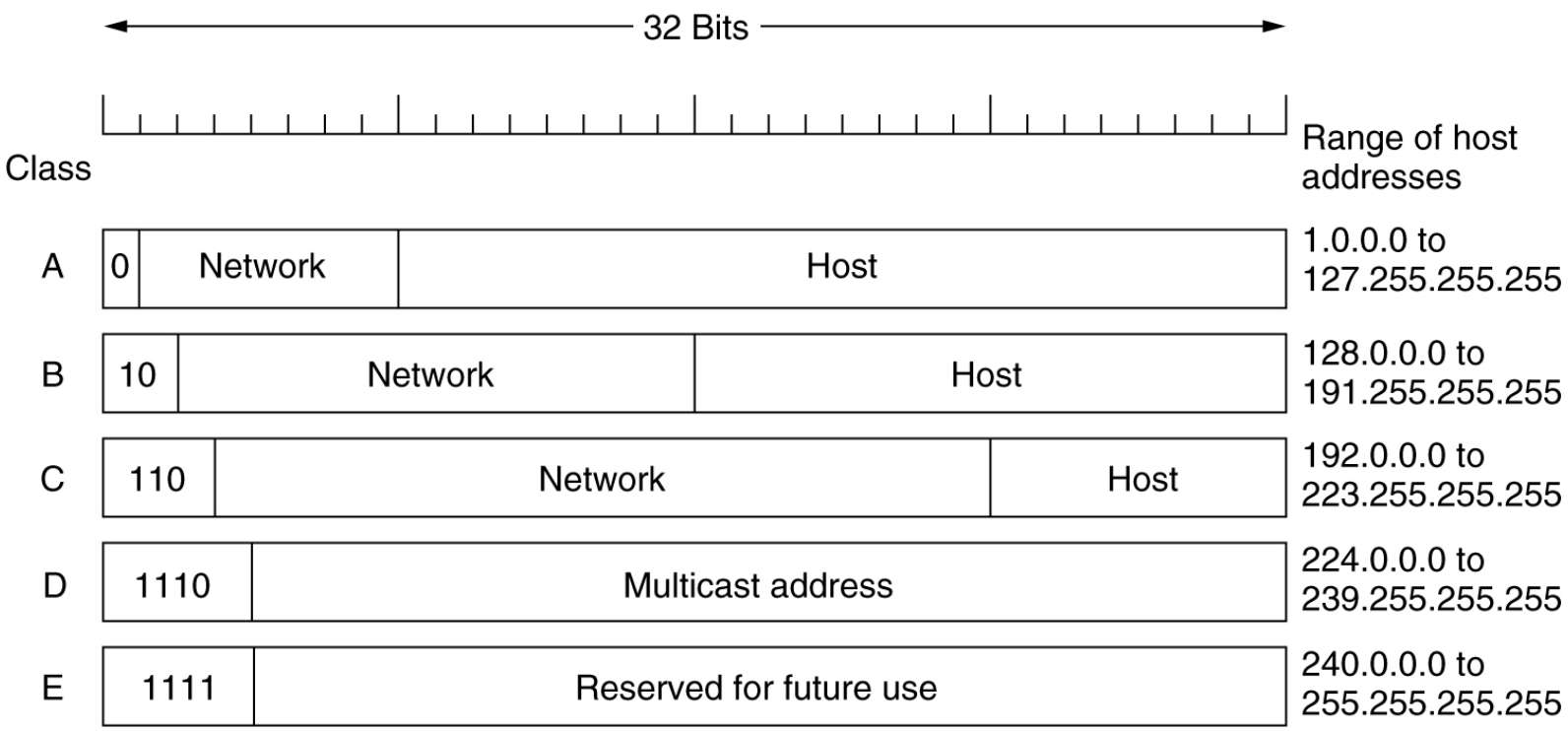
The IPv4 (Internet Protocol) header.

The IP Protocol (2)

Option	Description
Security	Specifies how secret the datagram is
Strict source routing	Gives the complete path to be followed
Loose source routing	Gives a list of routers not to be missed
Record route	Makes each router append its IP address
Timestamp	Makes each router append its address and timestamp

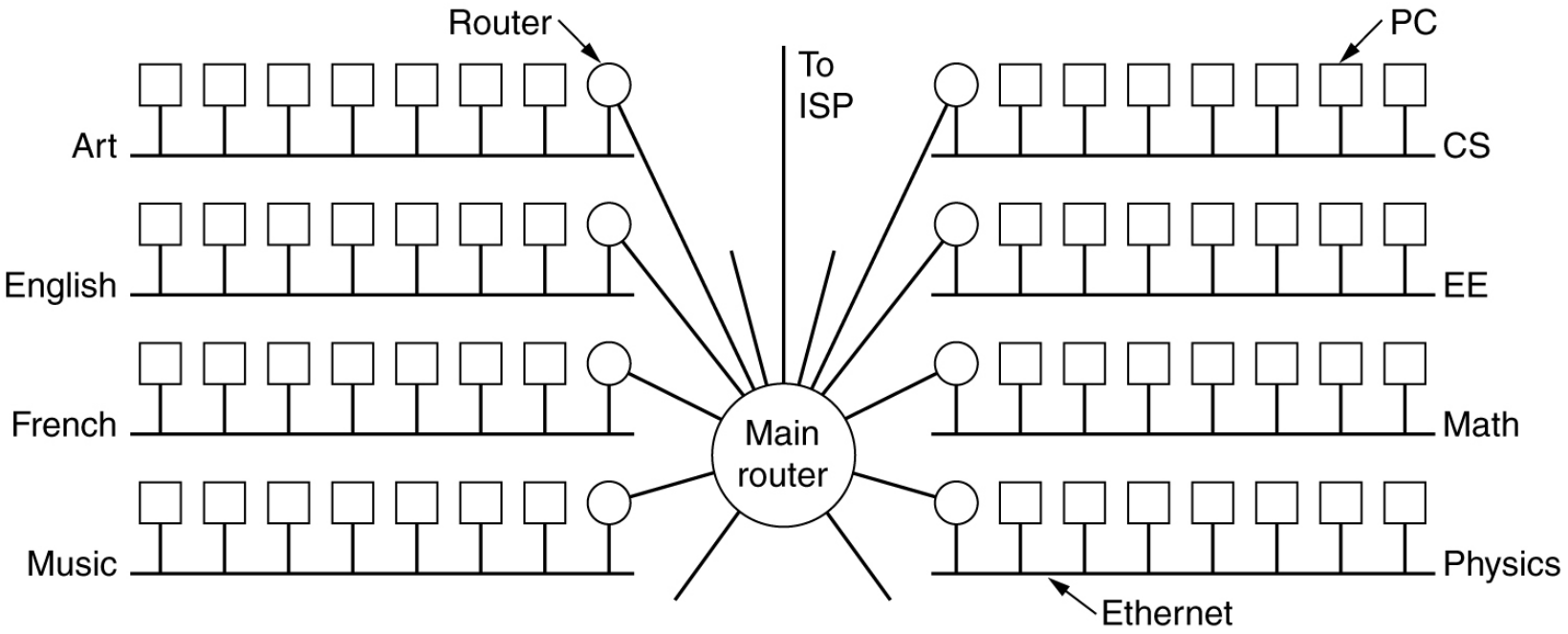
Some of the IP options.

IP Addresses



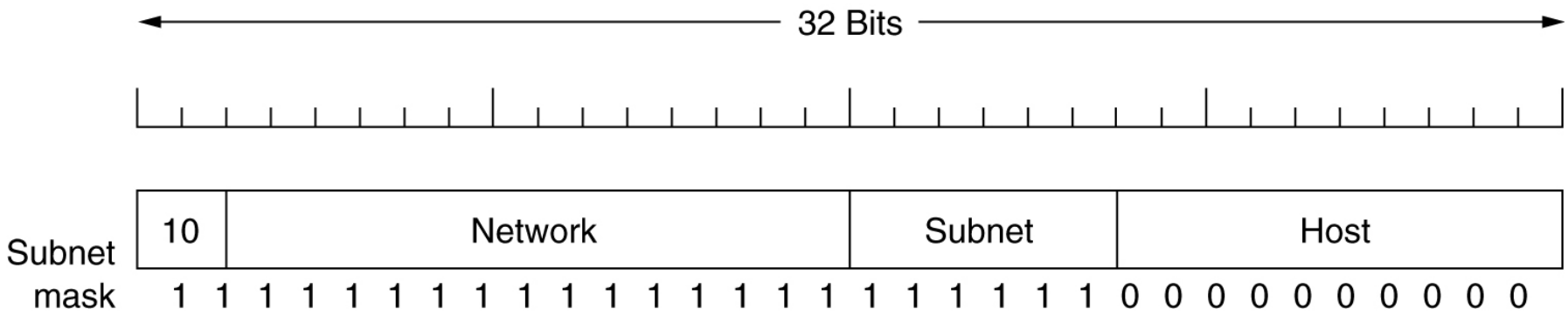
IP address formats.

Subnets



A campus network consisting of LANs for various departments.

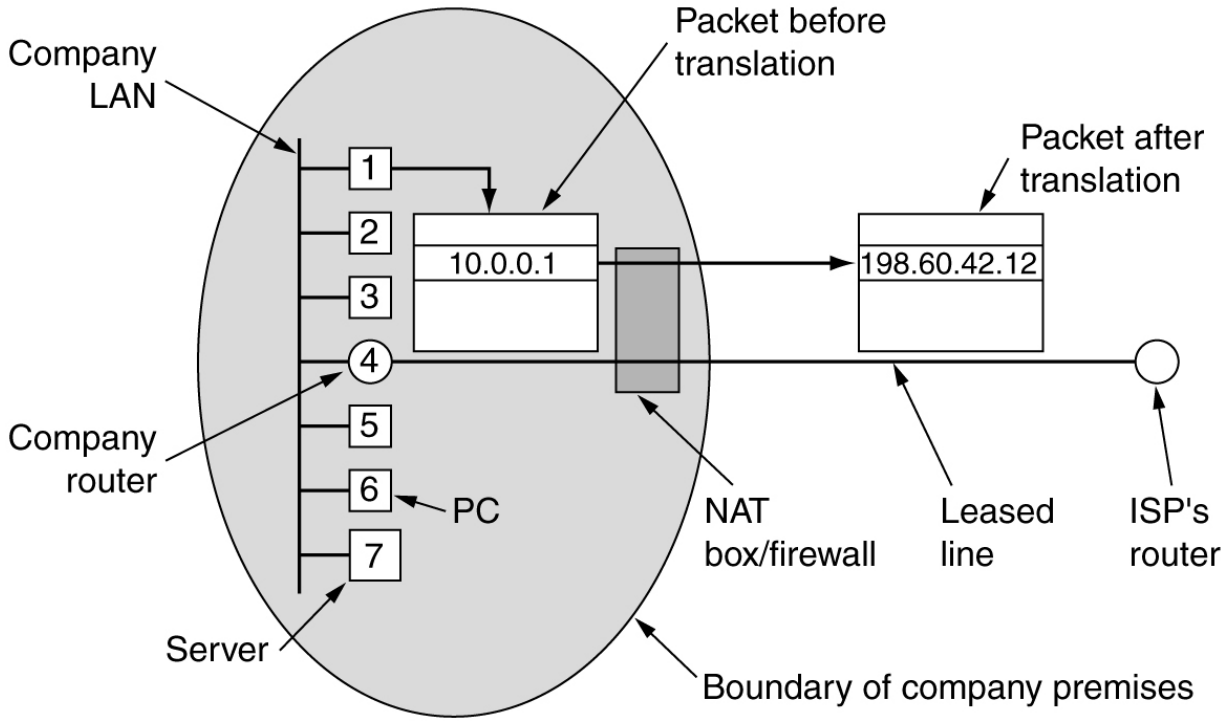
Subnets (2)



A class B network subnetted into 64 subnets.

NAT – Network Address Translation

- ✓ IP addresses are scarce.
- ✓ A LAN uses one IP address.
- ✓ Each computer uses an internal IP address, which is converted into the real IP address by NAT.
- ✓ For incoming traffic, the port number is used to identify the computer.



Placement and operation of a NAT box.

Internet Control Message Protocol

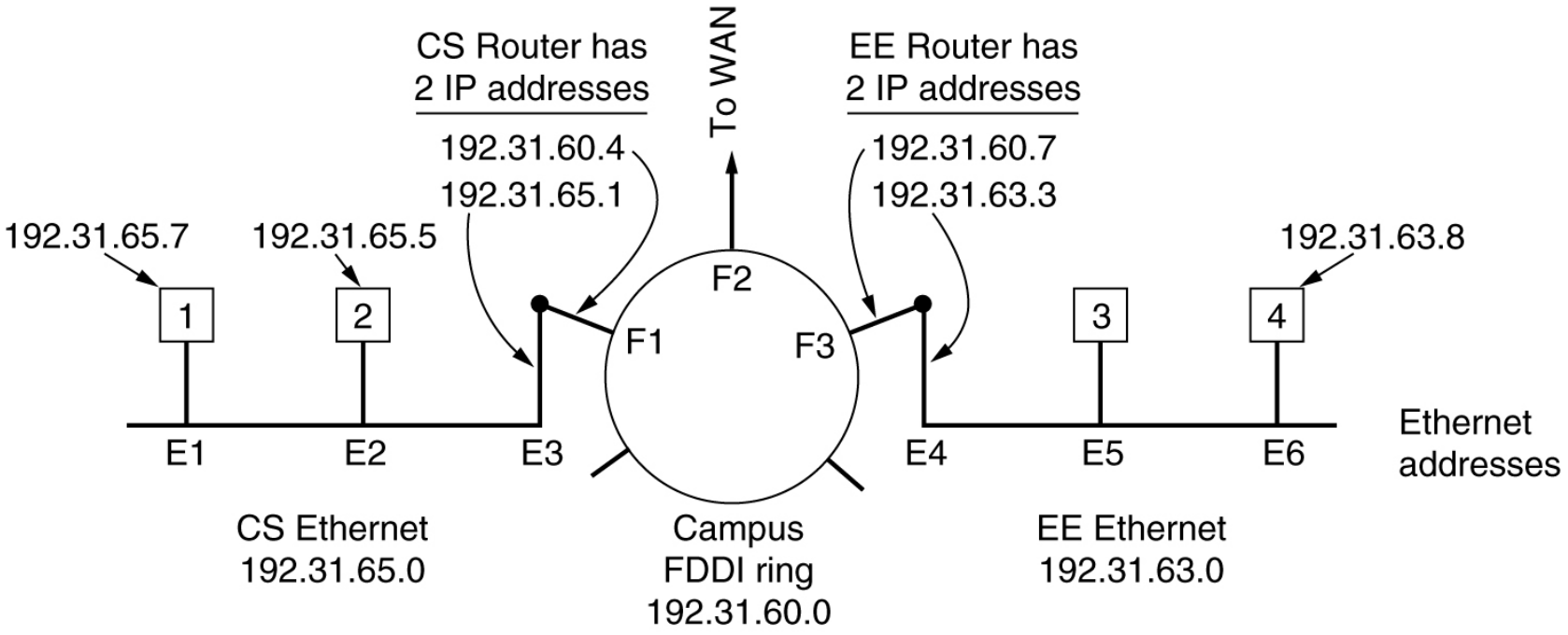
- ✓ ICMP is used to report unusual events in the Internet.
- ✓ Each ICMP message type is encapsulated in an IP packet.

Message type	Description
Destination unreachable	Packet could not be delivered
Time exceeded	Time to live field hit 0
Parameter problem	Invalid header field
Source quench	Choke packet
Redirect	Teach a router about geography
Echo request	Ask a machine if it is alive
Echo reply	Yes, I am alive
Timestamp request	Same as Echo request, but with timestamp
Timestamp reply	Same as Echo reply, but with timestamp

The principal ICMP message types.

ARP– The Address Resolution Protocol

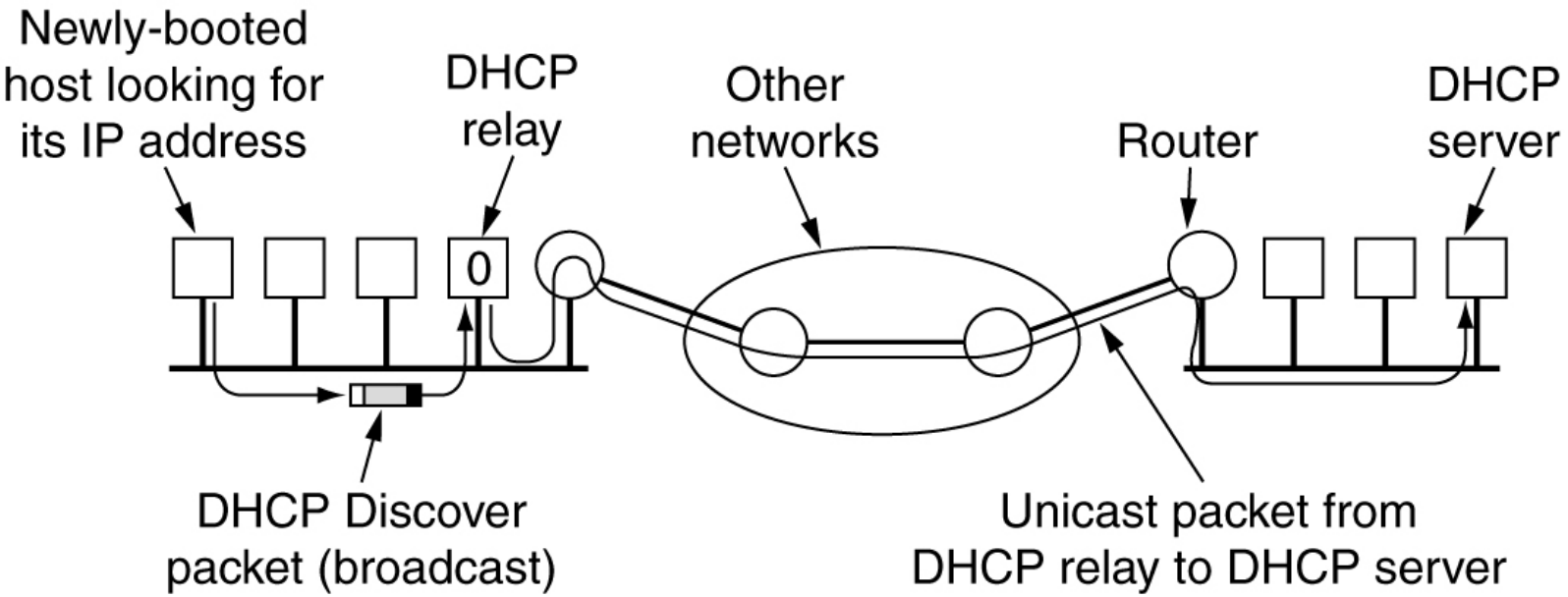
- ✓ The data link layer hardware does not understand IP address.
- ✓ LANs use data link layer address – e.g., a 48-bit Ethernet address (MAC address).
- ✓ How do IP addresses get mapped onto data link layer addresses?
- ✓ Configuration profile can be used.
- ✓ ARP asks the Ethernet: Who owns this IP address? The owner replies.



Three interconnected /24 networks: two Ethernets and an FDDI ring.

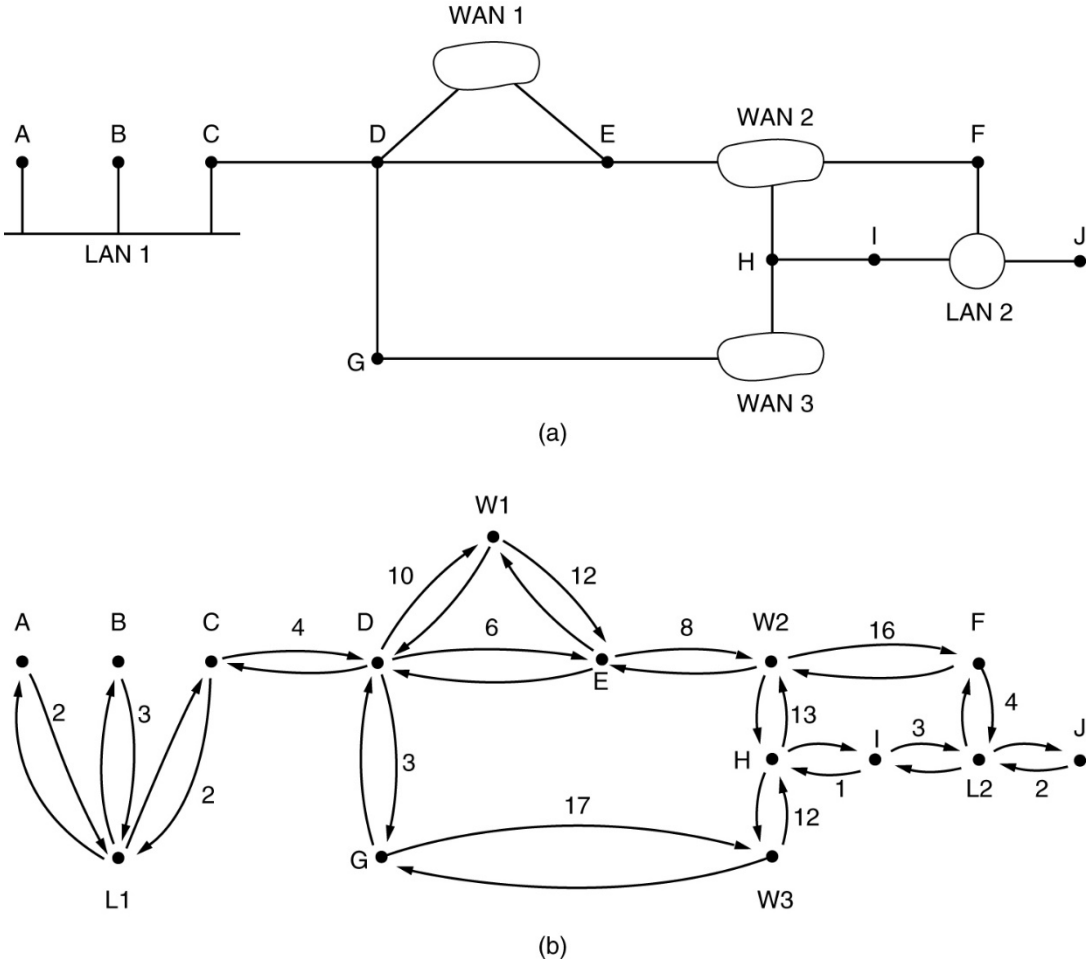
Dynamic Host Configuration Protocol

- ✓ DHCP allows both manual IP address assignment and automatic assignment.
- ✓ DHCP is based on a server to assign IP addresses to hosts asking for one.



Operation of DHCP.

Open Shortest Path Forwarding (OSPF) Routing

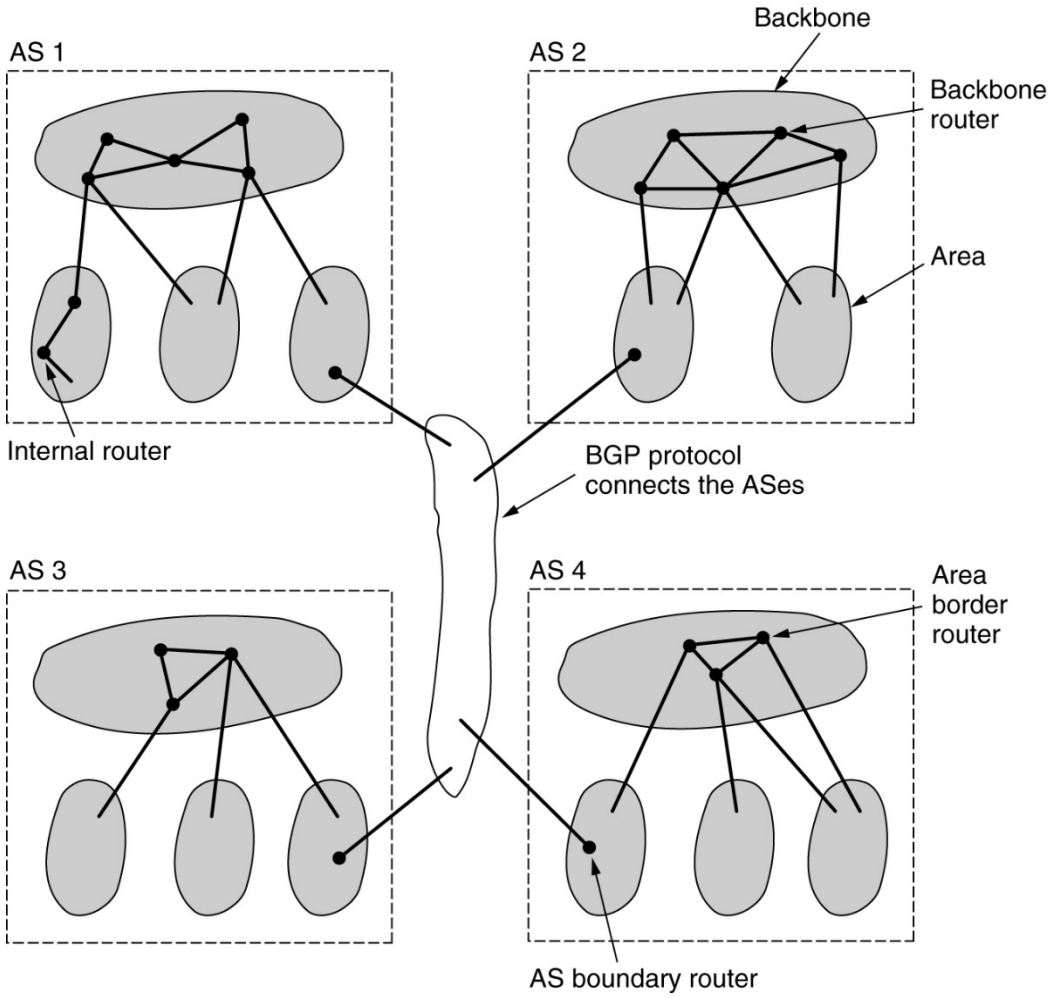


(a) An Autonomous System (AS) – A network under one administration.
(b) A graph representation of (a).

OSPF (2)

- ✓OSPF is a link state routing protocol.
- ✓An AS is divided into areas.
- ✓Four types of routers:

1. Internal routers are wholly within one area.
2. Area border routers connect two or more areas.
3. Backbone routers are on backbone.
4. AS boundary routers talk to routers in other AS.



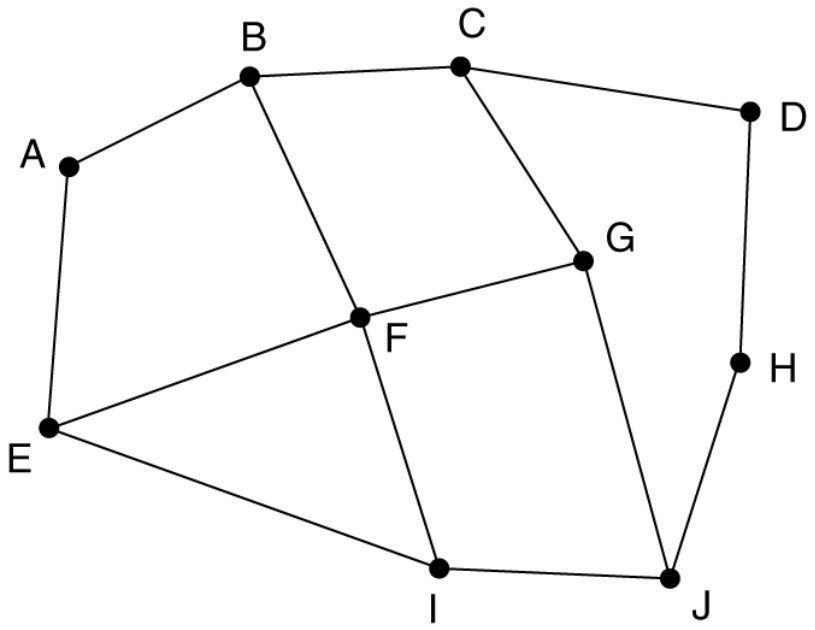
The relation between ASes, backbones, and areas in OSPF.

OSPF (3)

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.

BGP – The Exterior Gateway Routing Protocol



(a)

Information F receives from its neighbors about D

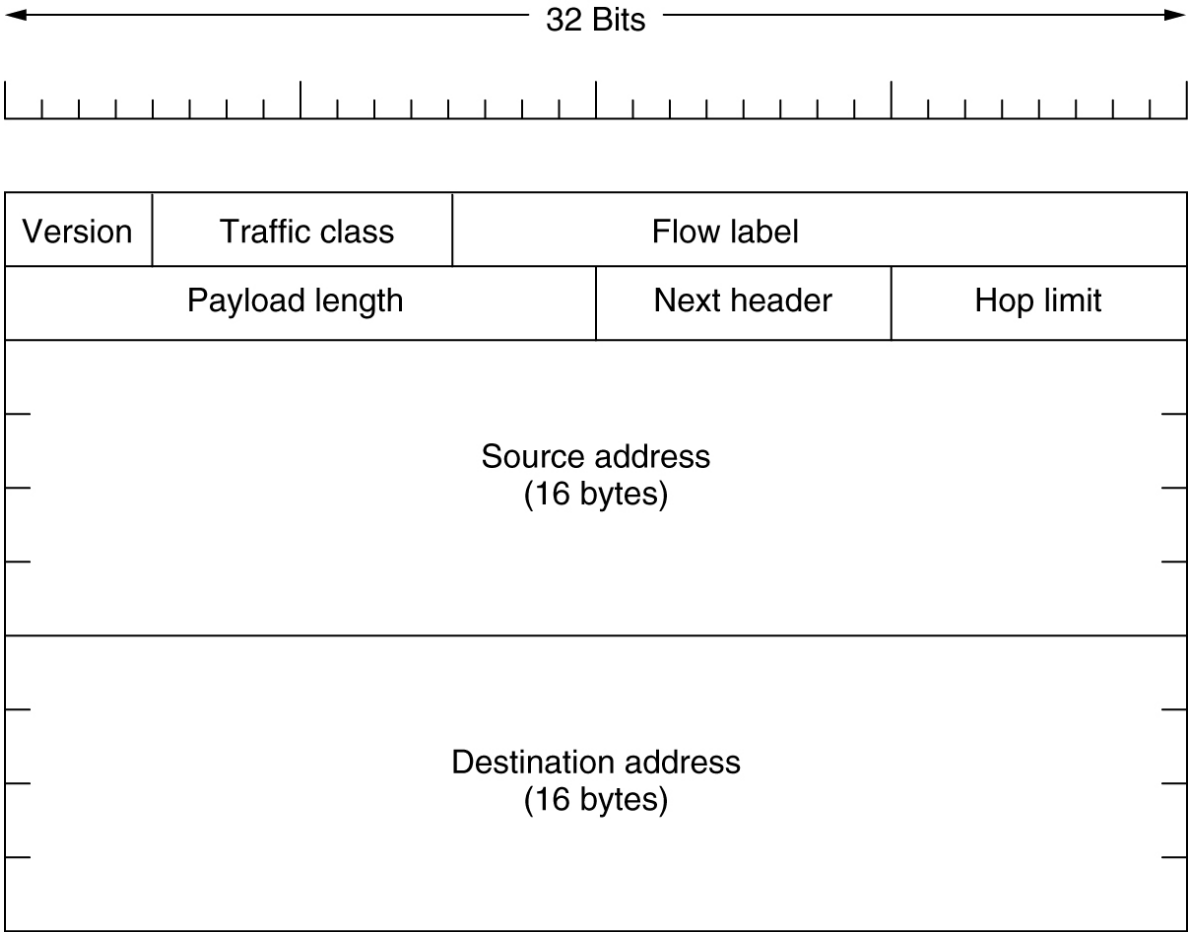
From B: "I use BCD"
From G: "I use GCD"
From I: "I use IFGCD"
From E: "I use EFGCD"

(b)

(a) A set of BGP (Border Gateway Protocol) routers. (b) Information sent to F.

The Main IPv6 Header

- ✓ Next header – tells which one of the six extension header is used.



The IPv6 fixed header (required).

Extension Headers

Extension header	Description
Hop-by-hop options	Miscellaneous information for routers
Destination options	Additional information for the destination
Routing	Loose list of routers to visit
Fragmentation	Management of datagram fragments
Authentication	Verification of the sender's identity
Encrypted security payload	Information about the encrypted contents

IPv6 extension headers.