MIT-WPU

।। विश्वशान्तिर्ध्रुवं ध्रुवा ।।

Computer Science and Engineering

TY BTech Trimester-VII

Disclaimer:

a. Information included in these slides came from multiple sources. We have tried our best to cite the sources. Please refer to the references to learn about the sources, when applicable.

b. The slides should be used only for preparing notes, academic purposes (e.g. in teaching a class), and should not be used for commercial purposes.

Unit 2: NETWORK LAYER

- Network Layer Design Issues
- Switching Techniques
- Protocol: IPv4 and IPv6 addressing schemes

Functionality of Network Layer

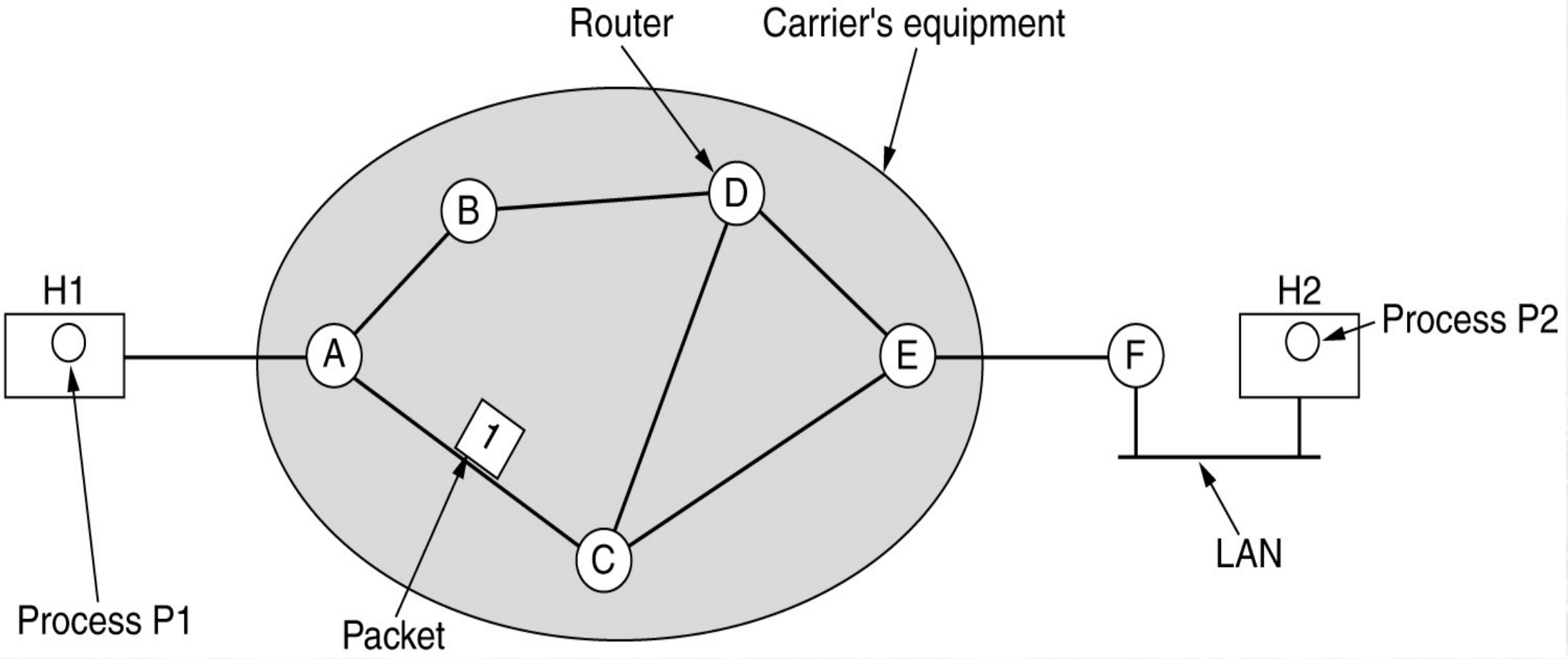
- Implements routing of frames (packets) through the network.
- Defines the most optimum path the packet should take from the source to the destination.
- Defines logical addressing so that any endpoint can be identified.
- Handles congestion in the network.
- Facilitates interconnection between heterogeneous networks (Internetworking).
- The network layer also defines how to fragment a packet into smaller packets to accommodate different media

Network Layer Design Issues

- Store-and-Forward Packet Switching
- Services Provided to the Transport Layer
- Implementation of Connectionless Service
- Implementation of Connection-Oriented Service
- Virtual-Circuit and Datagram Subnets

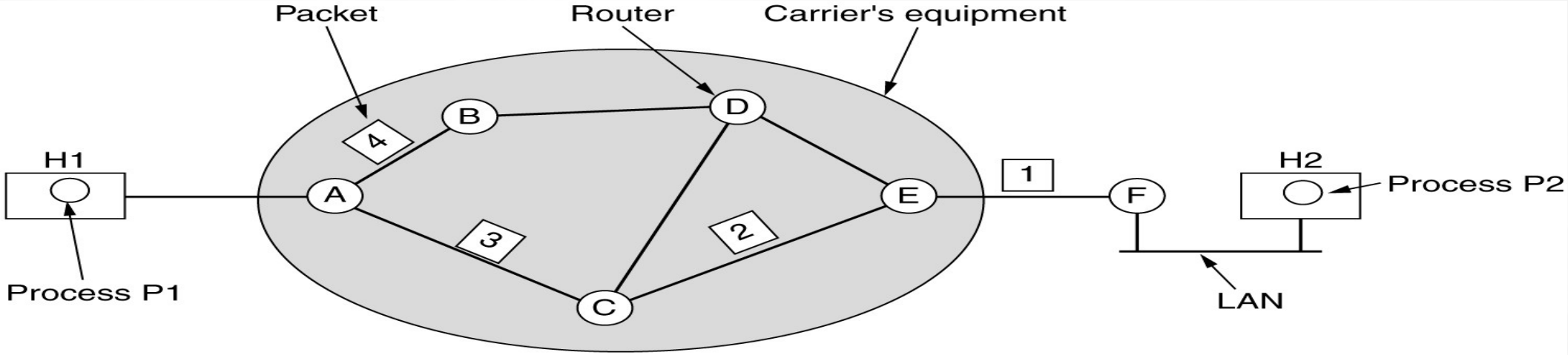
Store-and-Forward Packet Switching

Environment of network layer protocols



Implementation of Connectionless Service

Routing within a diagram subnet



A's table

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

C's table

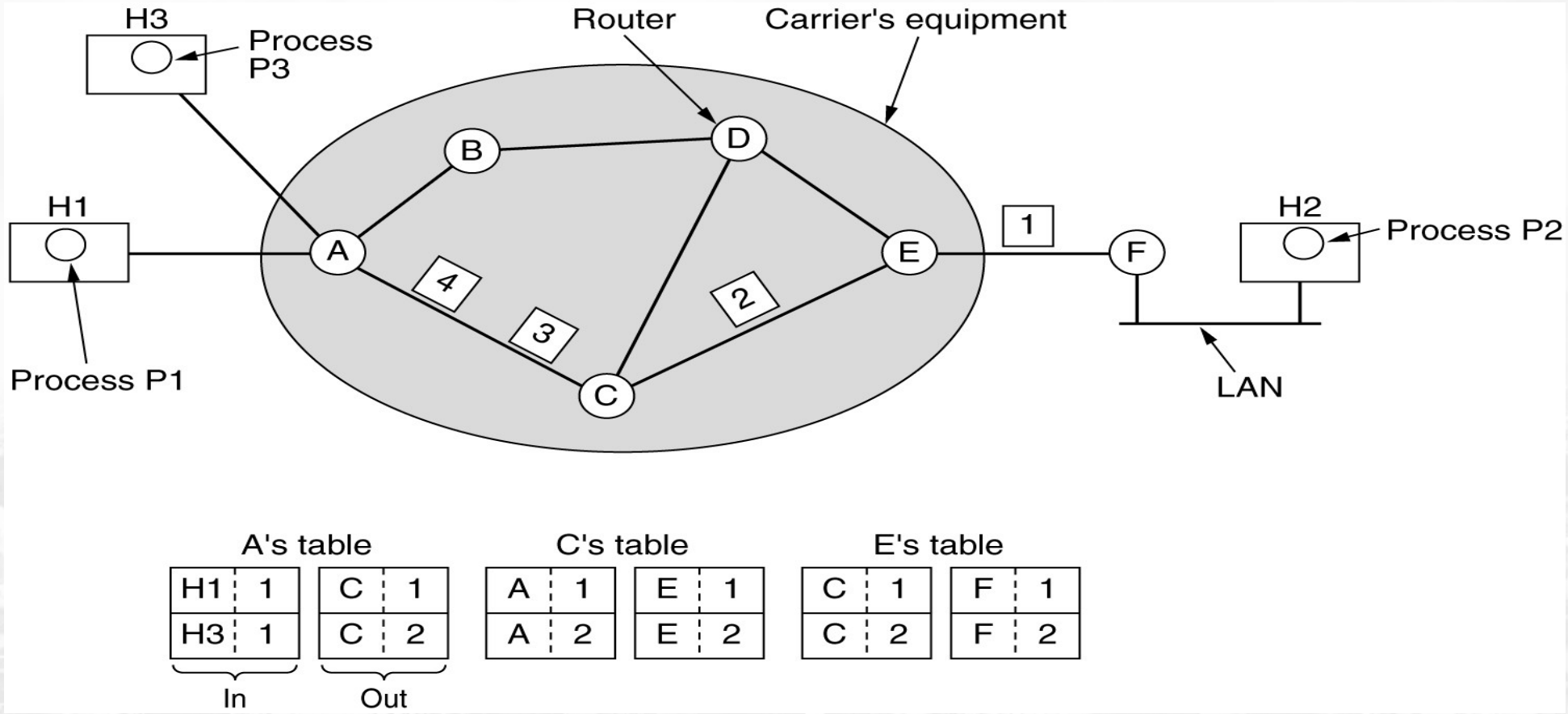
Dest.	Line
A	A
B	A
C	–
D	D
E	E
F	E

E's table

Dest.	Line
A	C
B	D
C	C
D	D
E	–
F	F

Implementation of Connection-Oriented Service

Routing within a virtual-circuit subnet

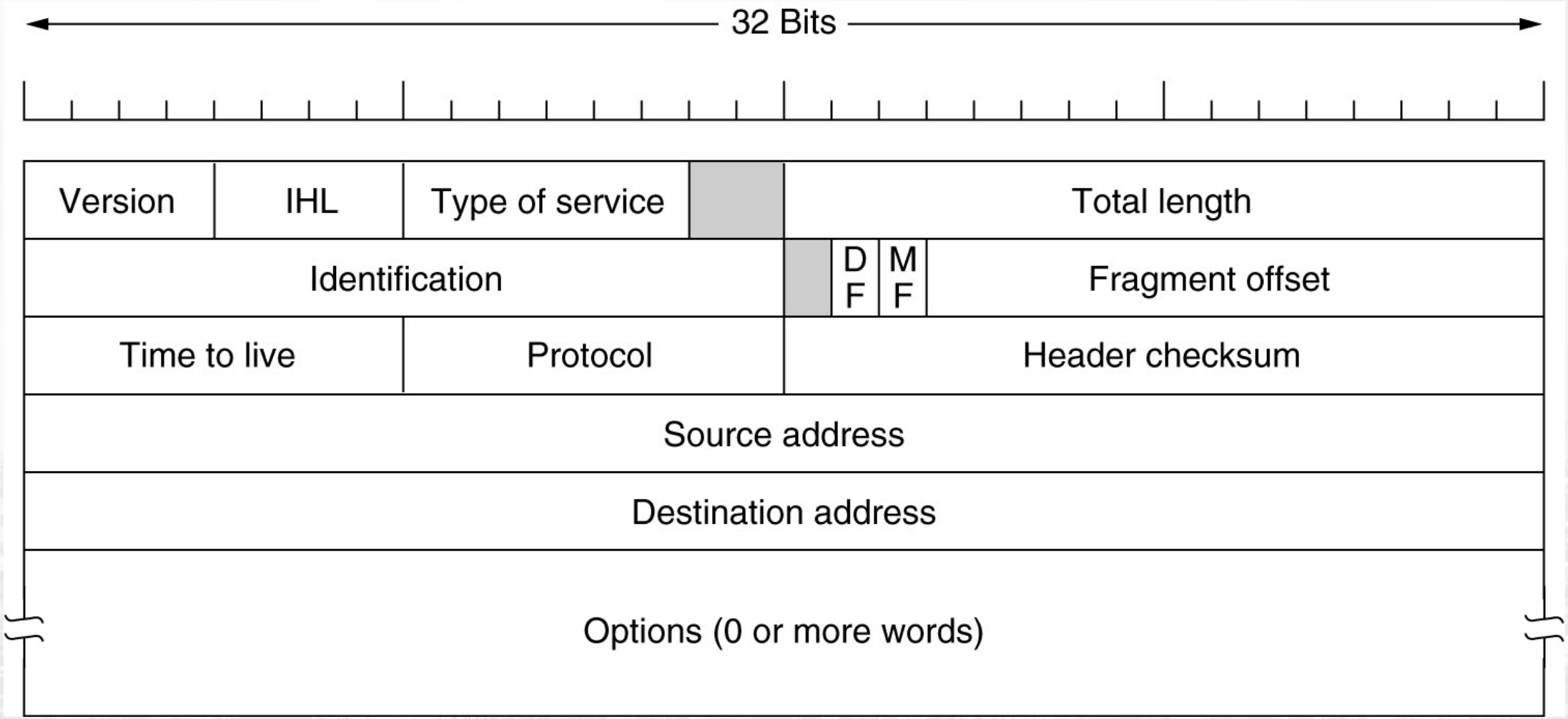


- Virtual Circuit
- Datagram

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

Internet Protocol: IPv4

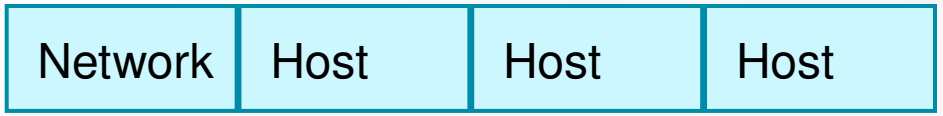


Internet Protocol: IPv4

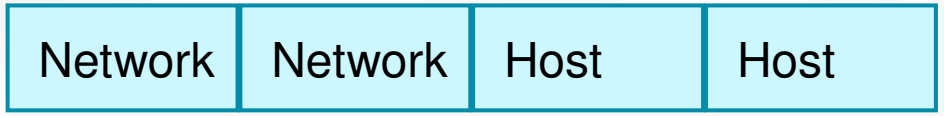
Option	Description
Security	Specifies how secret the datagram is
Strict source routing	Gives the complete path to be followed
Loose source routing	Gives a list of routers not to be missed
Record route	Makes each router append its IP address
Timestamp	Makes each router append its address and timestamp

Classes of IP Addresses

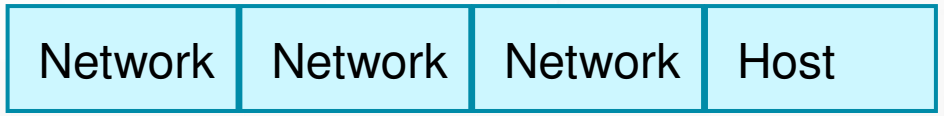
Class A:



Class B:



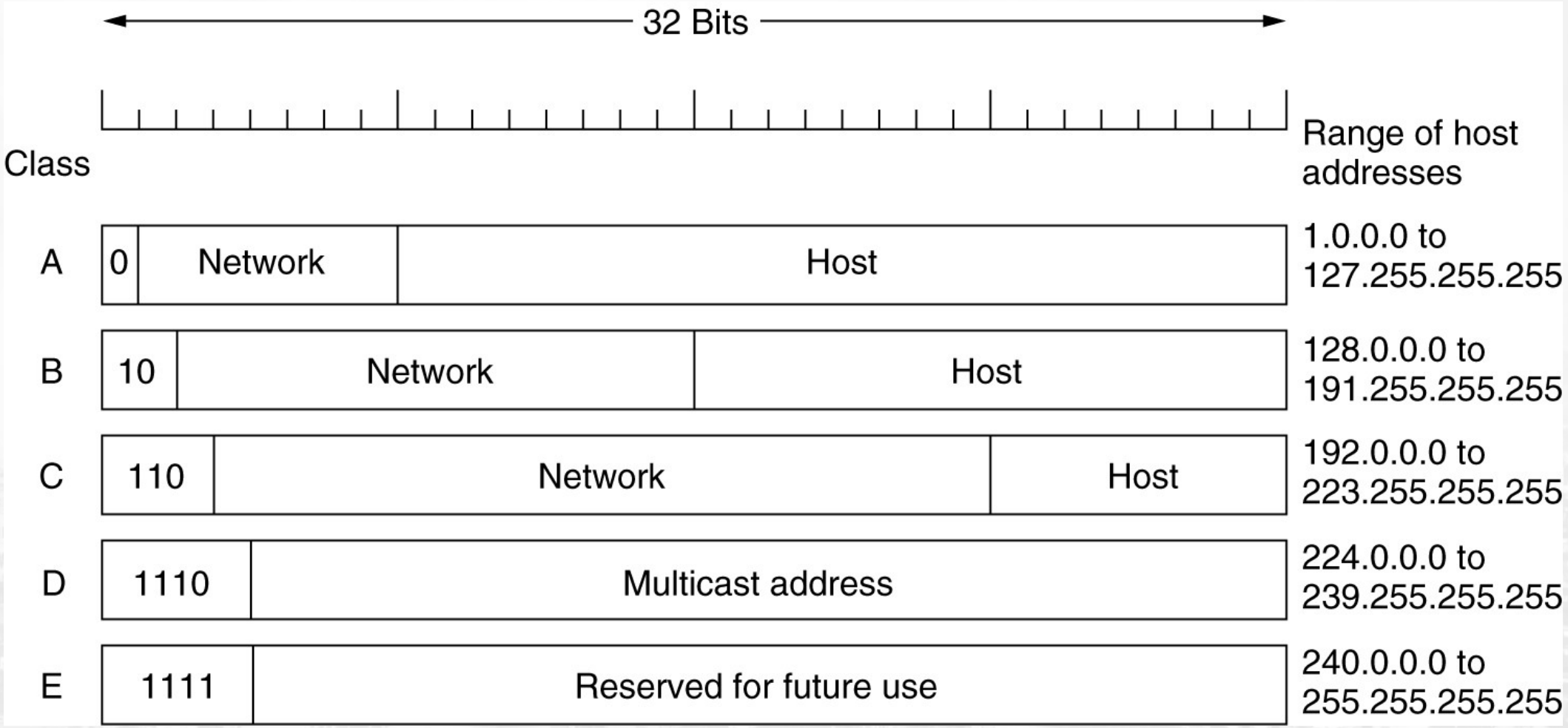
Class C:



Class D: Multicast

Class E: Research

IP Addresses



IP Address Range

IP Address Class	IP Address Range (First Octet decimal value)
Class A	1-126(00000001 to 01111110)*
Class B	128-191(10000000 to 10111111)
Class C	192-223(11000000 to 11011111)
Class D	224-239(11100000 to 11101111)
Class E	240-255(11110000 to 11111111)

***127 (011111111) is a Class A address reserved for loopback testing and cannot be assigned to a network.**

Problem 1

- *Given the network address 17.0.0.0, find the class, the block, and the range of the addresses.*

Solution

- **The class is A because the first byte is between 0 and 126.**
- The block has a netid of 17.
- The addresses range from **17.0.0.1 to 17.255.255.254.**

Problem 2

- *Given the network address 132.21.0.0, find the class, the block, and the range of the addresses.*

Solution

- **The class is B because the first byte is between 128 and 191.**
- The block has a netid of **132.21.**
- The addresses range from **132.21.0.1** to **132.21.255.254.**

Problem 3

- *Given the network address 220.34.76.0, find the class, the block, and the range of the addresses.*

Solution

- **The class is C because the first byte is between 192 and 223.**
- The block has a netid of **220.34.76.**
- The addresses range from **220.34.76.0 to 220.34.76.255.**

Default Subnet Mask

Class	Subnet Mask	Number of Network Bits
A	255.0.0.0	8
B	255.255.0.0	16
C	255.255.255.0	24

Private IP Addresses

Class	Private Address Range
A	10.0.0.0/8 to 10.255.255.255/8
B	172.16.0.0 /12 to 172.31.255.255/12
C	192.168.0.0/16 to 192.168.255.255/16

Subnetting / CIDR / VLSM

- Subnet mask specifies which network the host participates in
  - E.g. 10.0.0.0/16, means that the network is 10.1.0.0, 10.2.0.0, 10.3.0.0, until 10.255.0.0.

Before subnetting

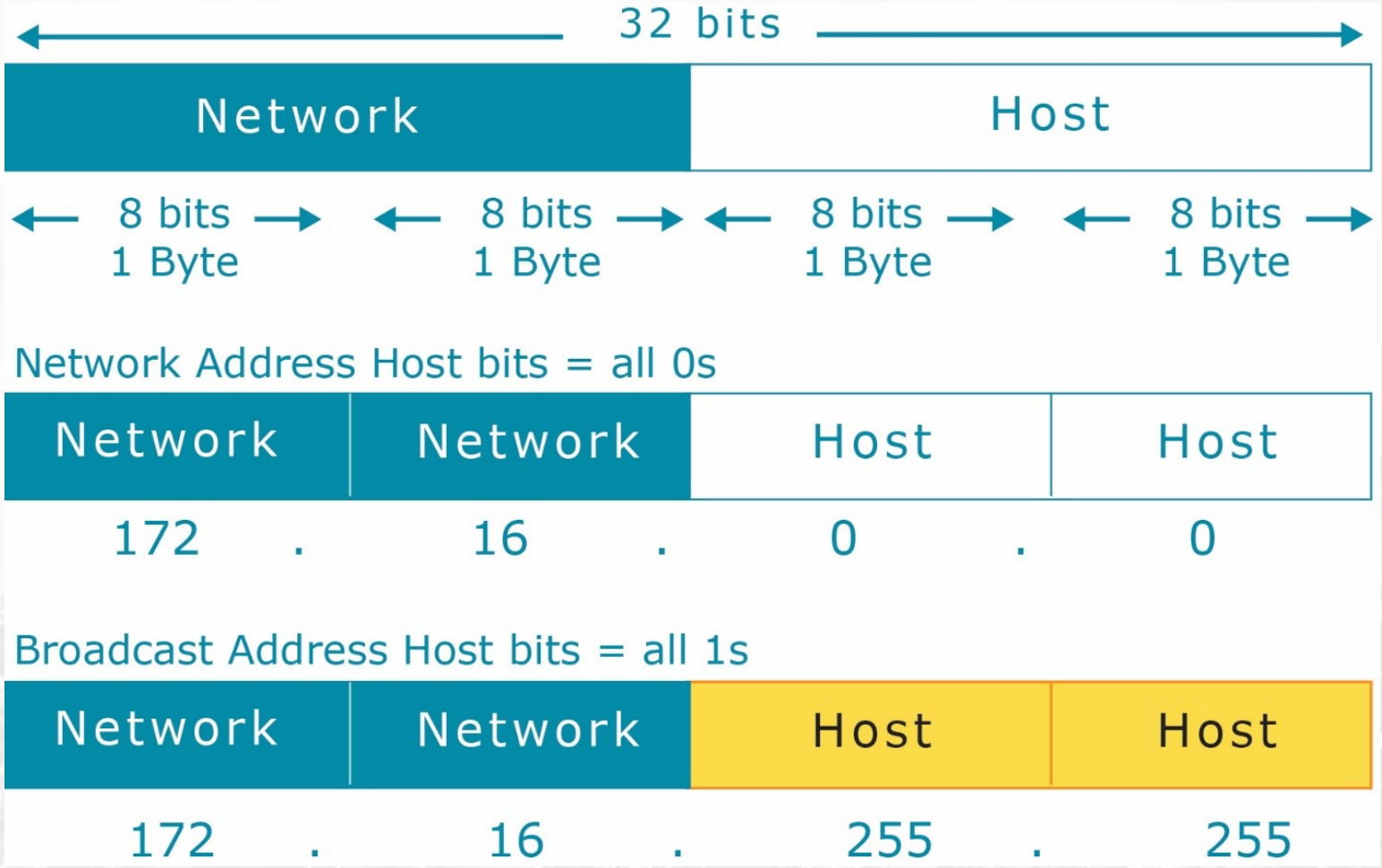
After subnetting

Subnetting / CIDR / VLSM

- To calculate the **number of subnets** available on a network number, use $\mathbf{2^S}$, where S=the number of subnet bits.

- To calculate the **number of hosts available on a network number**, use $\mathbf{2^N–2}$, where N=the number of host bits.

Reserved Address - Network and Broadcast



Subnet Mask Bits

0		0	0	0	0	0	0	0	= 0
1	0	0	0	0	0	0	0	=	128
1		1	0	0	0	0	0	0	= 192
1		1	1	0	0	0	0	0	= 224
1		1	1	1	0	0	0	0	= 240
1		1	1	1	1	0	0	0	= 248
1		1	1	1	1	1	0	0	= 252
1		1	1	1	1	1	1	0	= 254
1		1	1	1	1	1	1	1	= 255

Problem 4

A small organization is given a block with the beginning address and the prefix length 205.16.37.24/29

Find the following

a) Number of subnets and hosts per subnet

b) Network ID and Broadcast ID of each subnet

c) First and Last ID of each subnet

Problem 5

If a company needs 6 subnets with a minimum of 19 PCs per subnet, and the given IP Address is 192.168.1.0, what subnet mask should I use?

Internet Protocol: IPv6

Initial motivation:

- 32-bit address space soon to be completely allocated

Additional motivation:

- header format helps speed processing/forwarding
- header changes to facilitate QoS

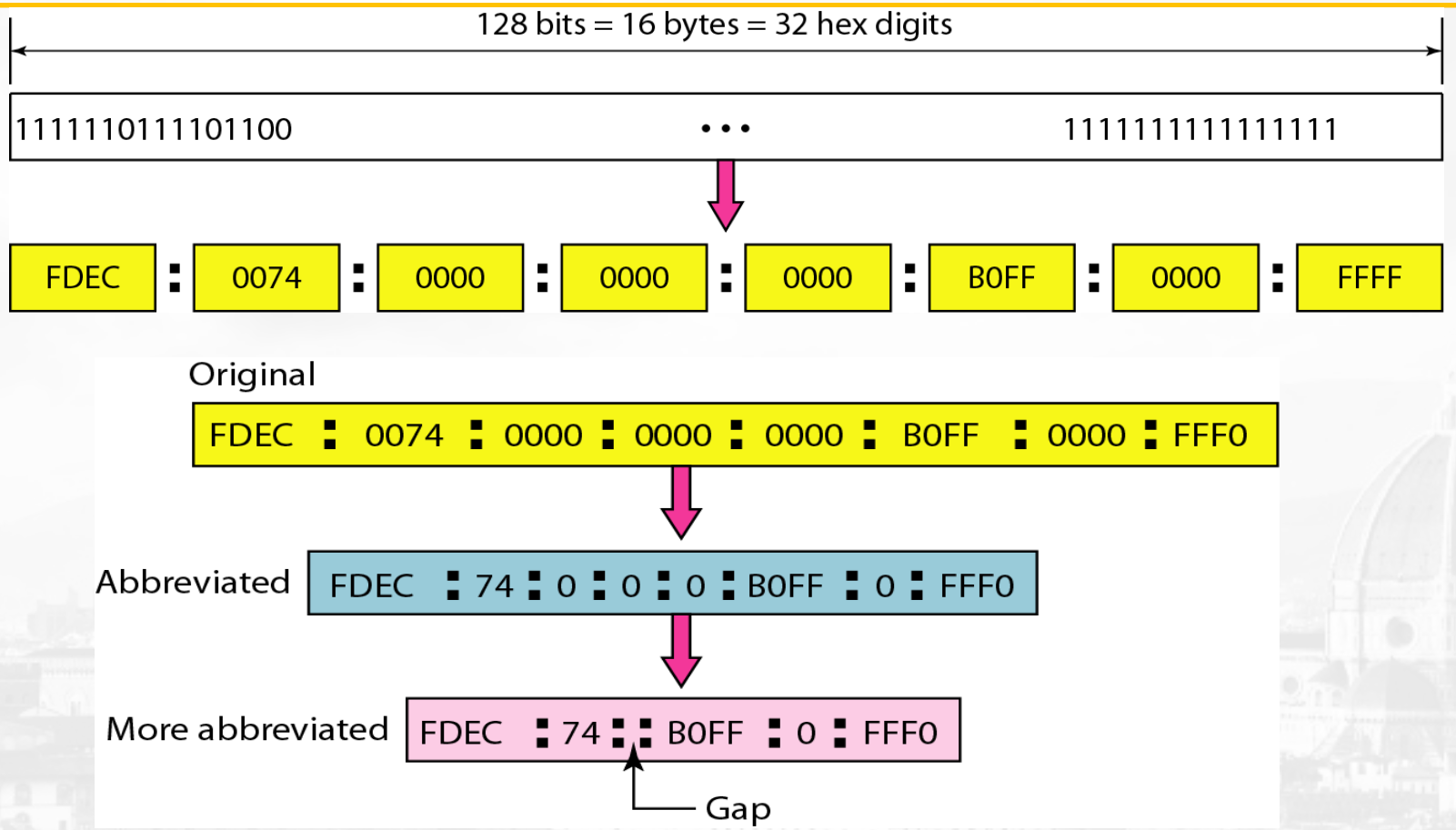
IPv6 datagram format:

- Fixed length 40-byte header
- fragmentation not allowed

IP Version 6 Goals

- Support billions of hosts
- Reduce routing table size
- Simplify protocol
- Better security
- Attention to type of service
- Aid multicasting
- Roaming host without changing address
- Allow future protocol evolution
- Permit coexistence of old, new protocols. . .

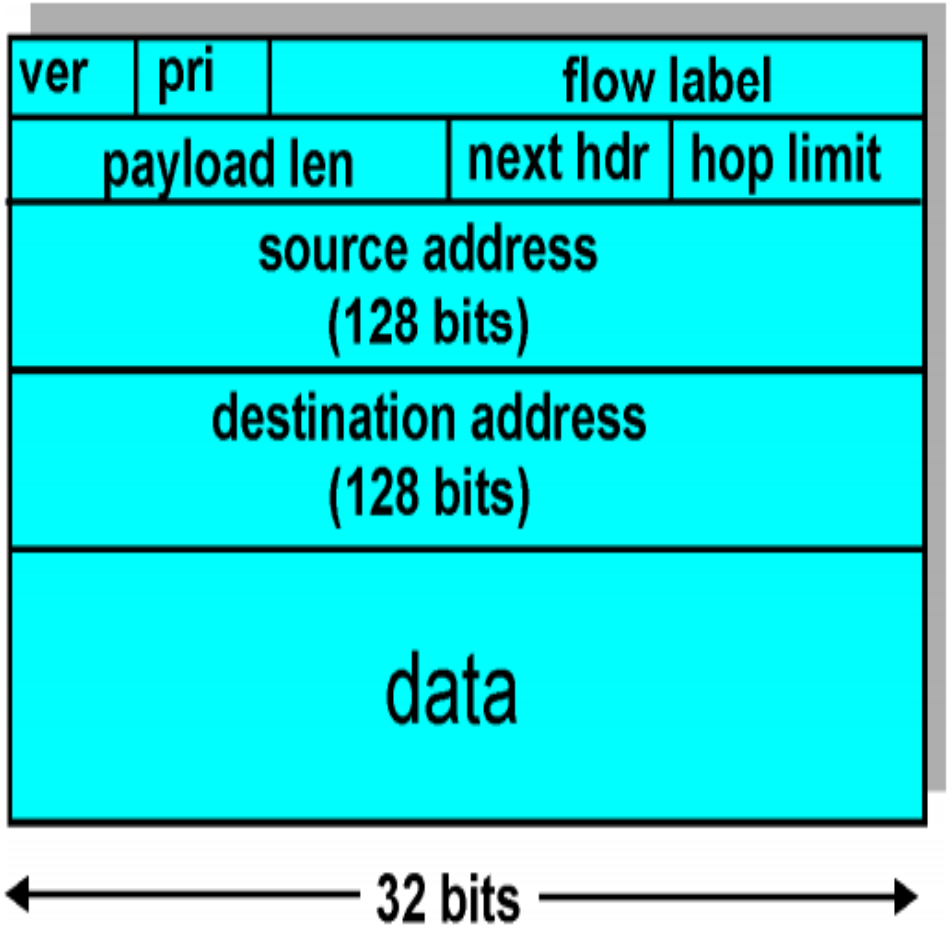
Internet Protocol: IPv6



- Above abbreviation is allowed only once per address.

Internet Protocol: IPv6

- Priority: identify priority among datagrams
- Flow Label: identify datagrams in same ‘flow’
- Next Header: identify upper layer protocol for data



IPv6 Extension Headers

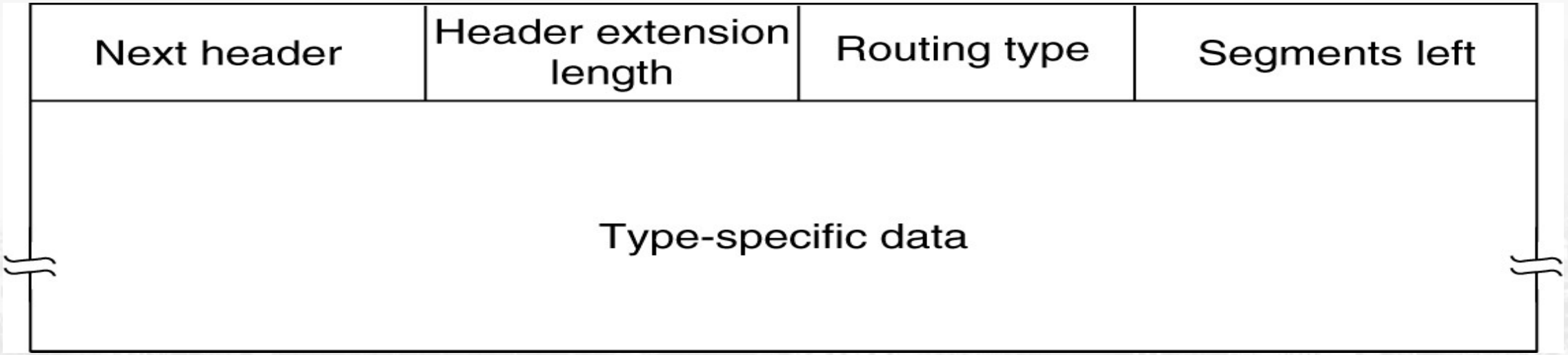
Extension header	Description
Hop-by-hop options	Miscellaneous information for routers
Destination options	Additional information for the destination
Routing	Loose list of routers to visit
Fragmentation	Management of datagram fragments
Authentication	Verification of the sender's identity
Encrypted security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

IPv6 Extension Headers

Hop-by-hop extension header for large datagrams (jumbograms)

Next header	0	194	4
Jumbo payload length			

IPv6 Extension Headers (Routing)

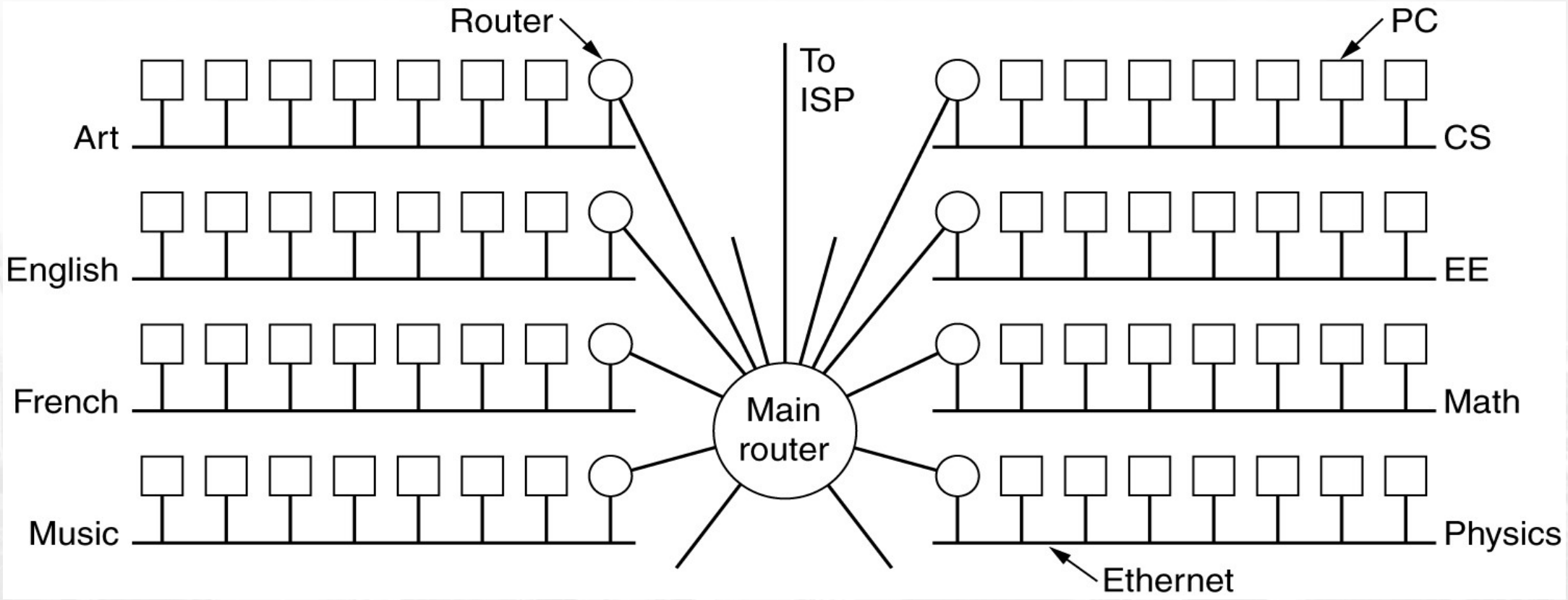


Unit 2: NETWORK LAYER

- Sub netting
- Classless Inter-Domain Routing (CIDR)
- Network Address Translation (NAT)
- Internet Control Message Protocol (ICMP)

Subnets

LAN: Campus network for various departments



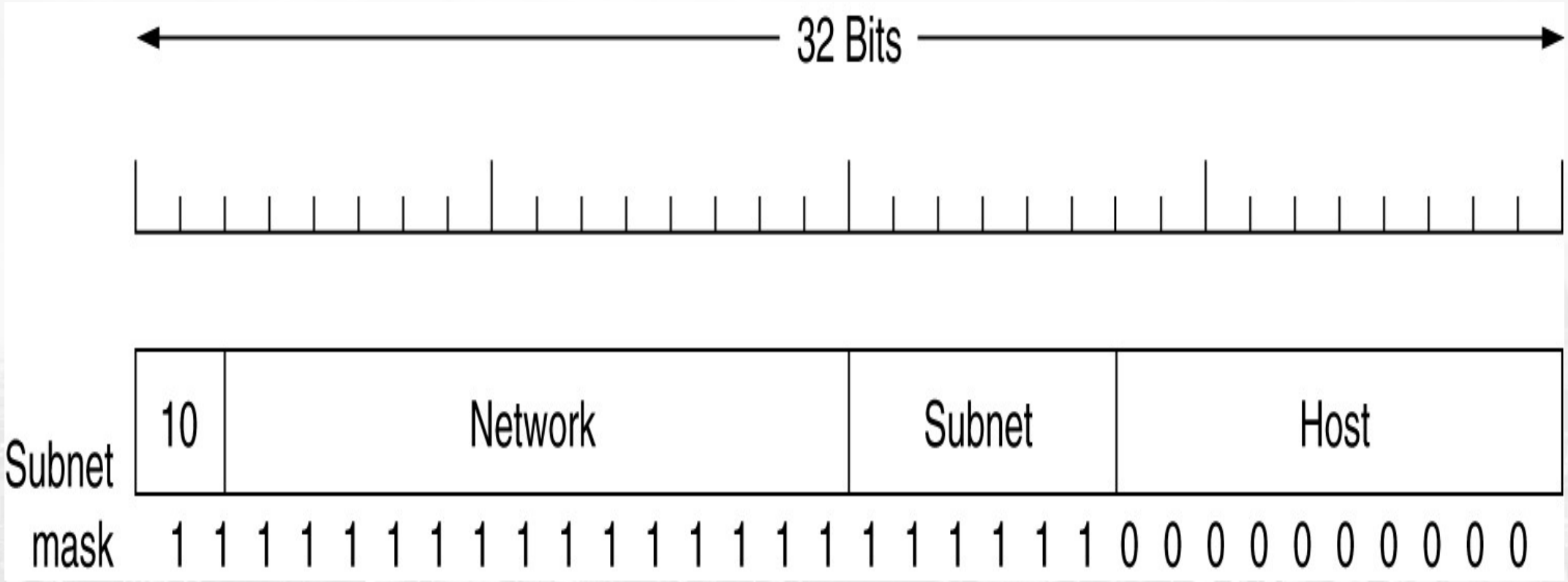
The number of networks and the number of hosts per class can be derived by this formula:

Number of networks	= 2^network_bits
Number of Hosts/Network	= 2^host_bits – 2

- -When calculating hosts' IP addresses, 2 IP addresses are decreased because they cannot be assigned to hosts, i.e. the first IP of a network is network number and the last IP is reserved for Broadcast IP.

Subnets cont..

Class B network: 64 subnets



Classful Addressing (Cntd.)

- A company is granted the site address 201.70.64.0 (class C). The company needs six subnets. Design the subnets.
- *Solution*
- The number of 1s in the default mask is 24 (class C).

- The company needs six subnets. This number 6 is not a power of 2.The next number that is a power of 2 is 8(23).We need 3 more 1s in the sub netmask. The total number of 1s in the subnet mask is 27(24+3).
- The total number of 0s is5(32-27).The mask is
- 11111111 11111111 11111111 **111**00000
- or
- 255.255.255.224
- The number of subnets is 8.
- The number of addresses in each subnet is2^5(5is the number of 0s)or32.

- An organization is granted the block 130.34.12.64/26.The organization needs to have four subnets. What are the subnet addresses and the range of addresses for each subnet?

Solution

- The suffix length is 6.This means the total number of addresses in the block is 64(26).If we create four subnets,each subnet will have 16 addresses.

- Letusfirstfindthesubnetprefix(subnetmask).Weneedfoursubnets,whichmeansweneedtoaddtwomore1stothesiteprefix. Thesubnetprefixisthen/28.
- Subnet1:130.34.12.64/28to130.34.12.79/28.
- Subnet2:130.34.12.80/28to130.34.12.95/28.
- Subnet3:130.34.12.96/28to130.34.12.111/28.
- Subnet4:130.34.12.112/28to130.34.12.127/28.

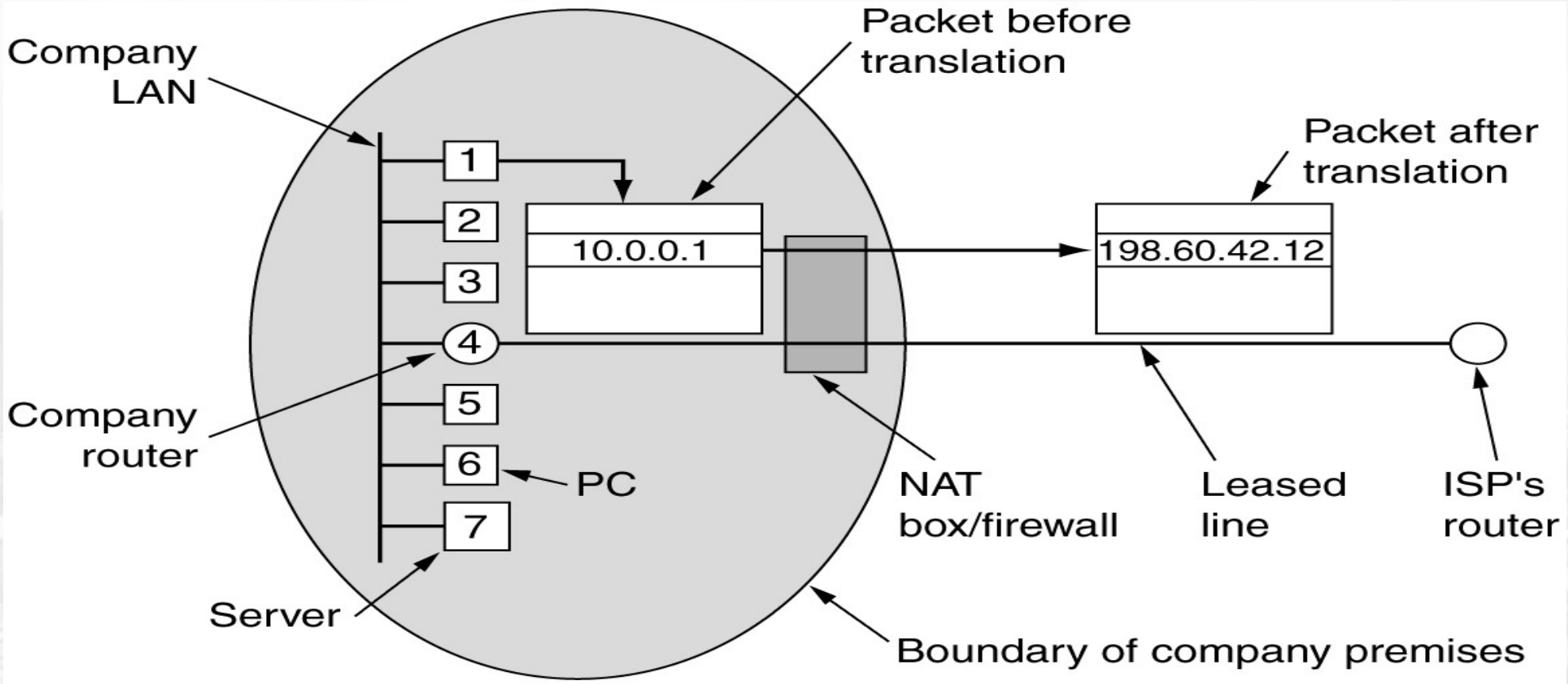
CIDR – Classless Inter Domain Routing

IP address assignments

University	First address	Last address	How many	Written as
Cambridge	194.24.0.0	194.24.7.255	2048	194.24.0.0/21
Edinburgh	194.24.8.0	194.24.11.255	1024	194.24.8.0/22
(Available)	194.24.12.0	194.24.15.255	1024	194.24.12/22
Oxford	194.24.16.0	194.24.31.255	4096	194.24.16.0/20

NAT – Network Address Translation

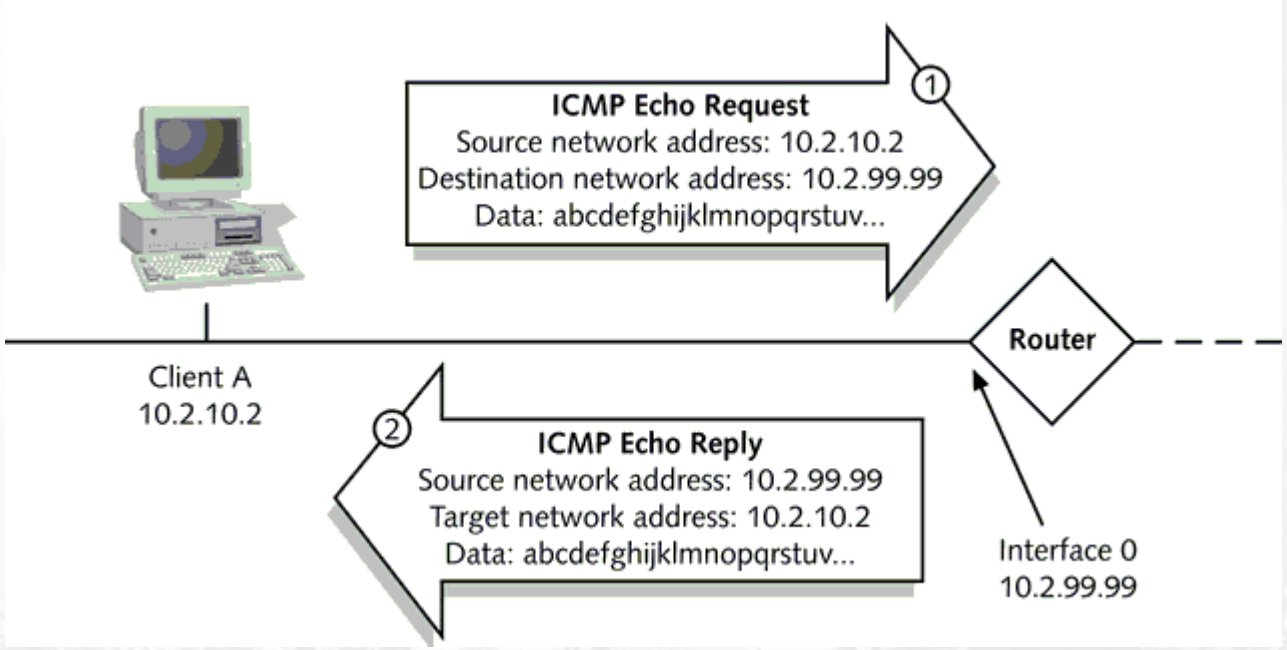
NAT: Placement and operation



Internet Control Message Protocols

- ICMP's most common uses are testing and troubleshooting.

- Two of the most well-known utilities, PING and TRACEROUTE, rely on ICMP to perform *connectivity tests* and *path discovery*.



Internet Control Message Protocols

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 and Echo reply	Check if a machine is alive
Timestamp request/reply	Same as Echo, but with timestamp
Router advertisement/solicitation	Find a nearby router

The principal ICMP message types.

Routing Algorithm

Network Layer responsible for deciding on which output line to transmit an incoming packet.

For virtual circuit subnets:

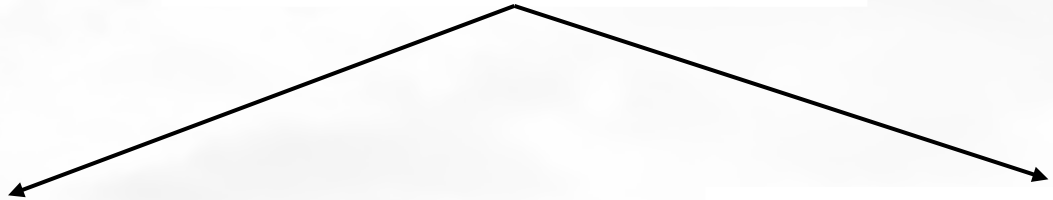
- routing decision is made ONLY at set up

Algorithm properties:

- correctness, simplicity, robustness, stability, fairness, optimality and scalability

Internetwork Routing

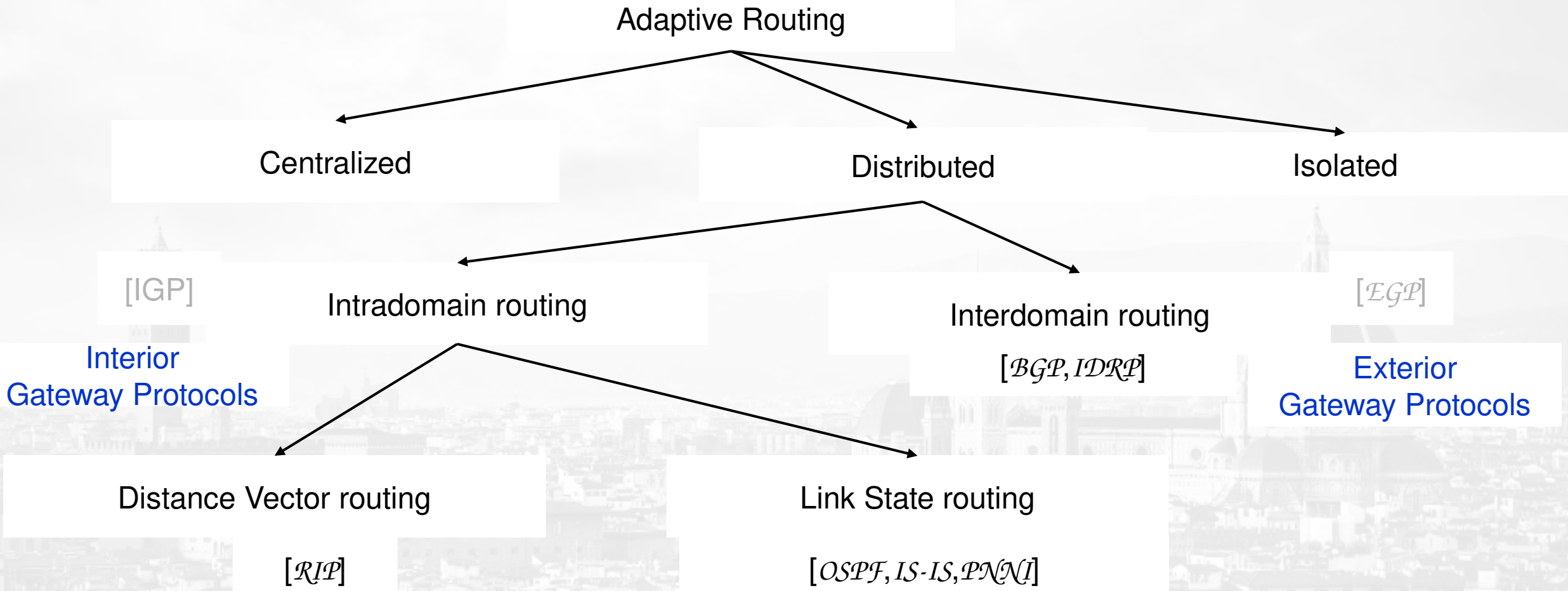
Routing Classification



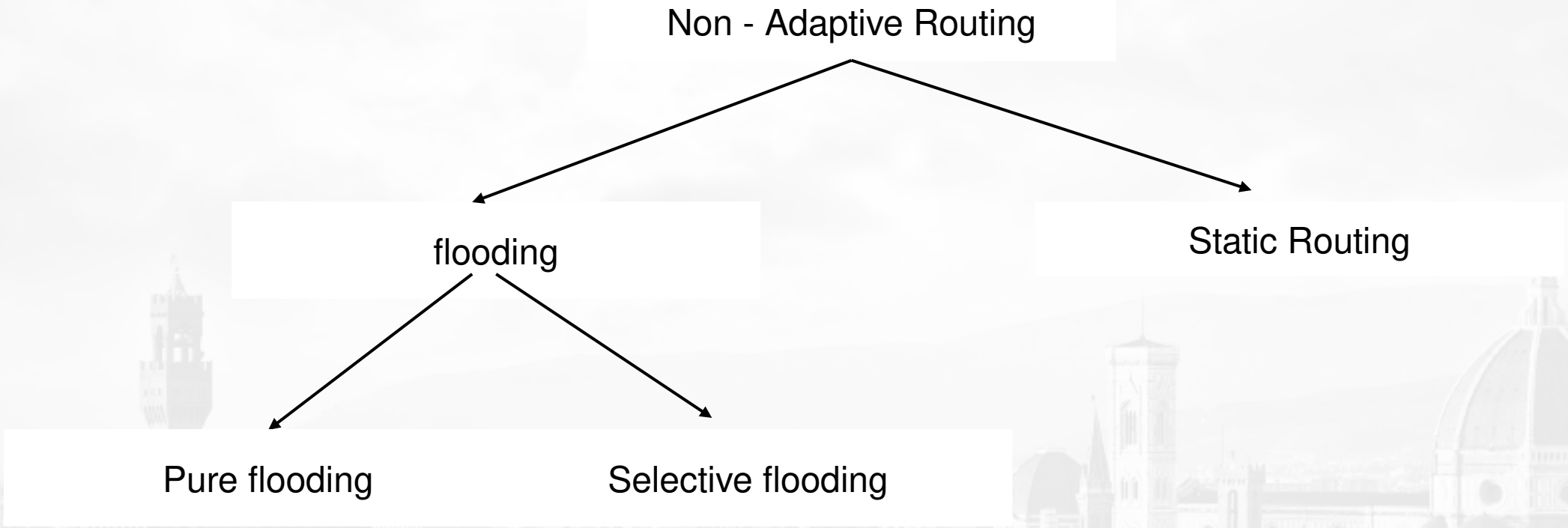
Adaptive Routing
based on current measurements of traffic and/or topology.

Non-Adaptive Routing
routing computed in advance and off-line

Internetwork Routing



Internetwork Routing



Flooding

- *Pure flooding* :: every incoming packet to a node is sent out on *every outgoing line*.
  - Obvious adjustment – do not send out on arriving link (assuming full-duplex links).
  - The routing algorithm can use a hop counter (e.g., TTL) to *dampen the flooding.*
  - *Selective flooding* :: only send on those lines going "approximately" in the right direction.

Shortest Path Routing

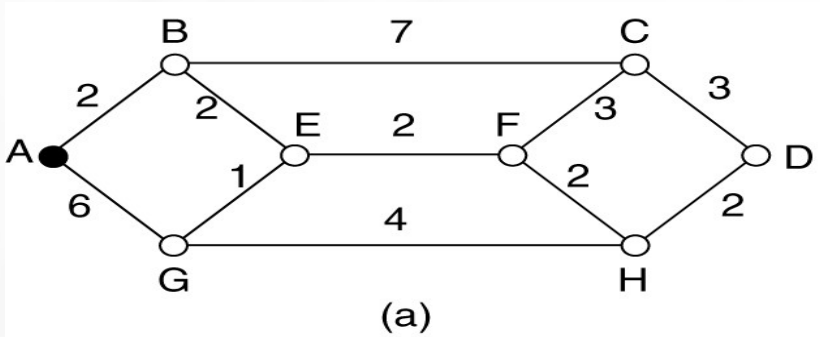
Dijkstra's Algorithm

What does it mean to be the shortest (or optimal) route?

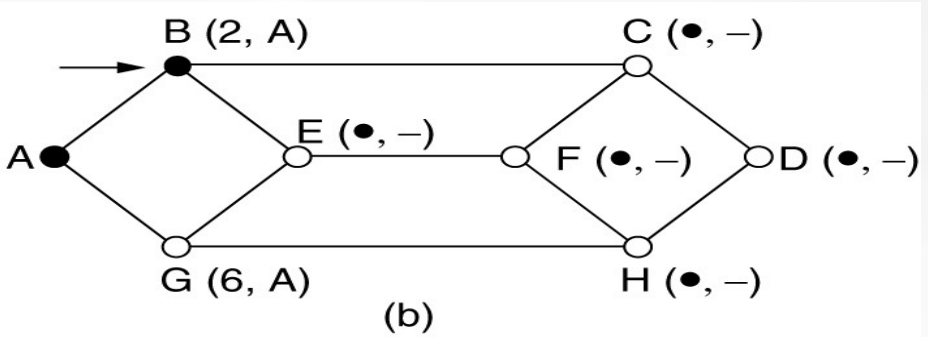
Choices:

a. **Minimize the number of hops along the path.**
b. **Minimize mean packet delay.**
c. **Maximize the network throughput.**

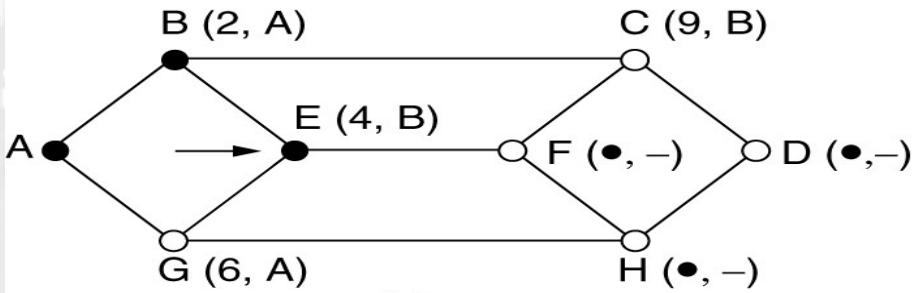
Dijkstra's Algorithm Shortest Path Routing



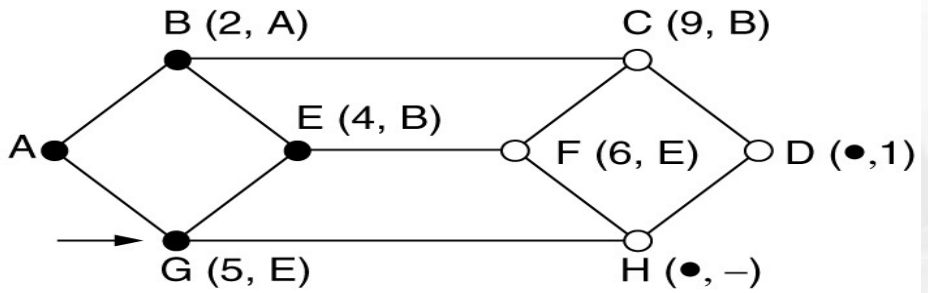
(a)



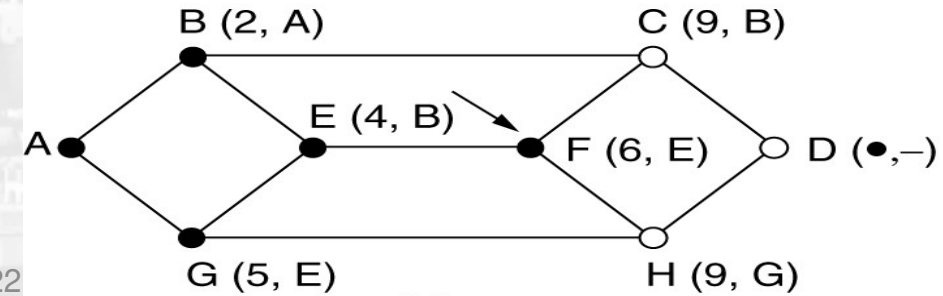
(b)



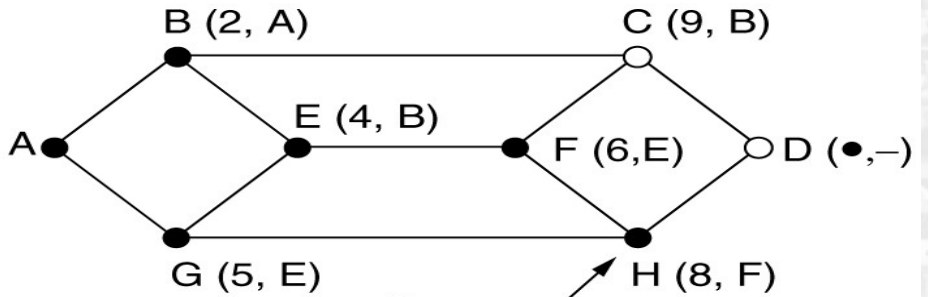
(c)



(d)

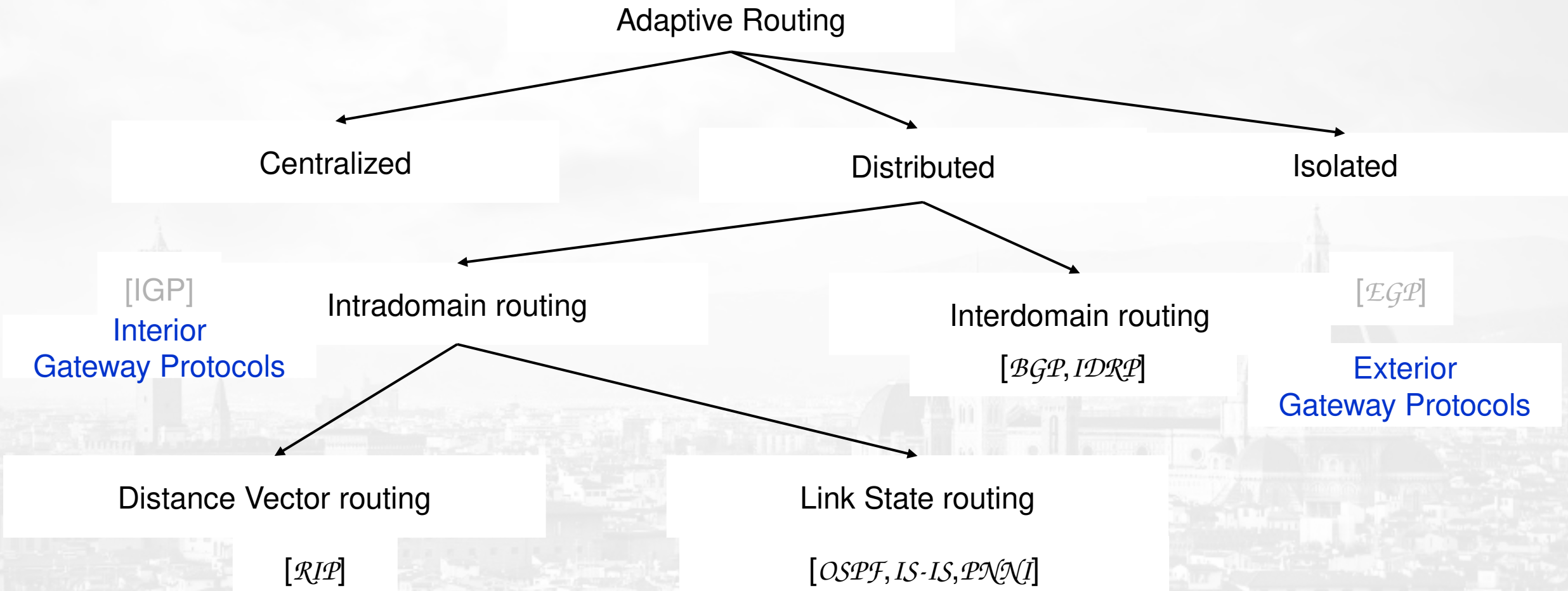


(e)



(f)

Internetwork Routing



Adaptive Routing

Basic functions:

1. Measurement of pertinent network data.
2. Forwarding of information to where the routing computation will be done.
3. Compute the routing tables.
4. Convert the routing table information into a *routing decision* and then *dispatch* the data packet.

Distance Vector Routing

Information kept by DV router

1. each router has an ID
2. associated with each link connected to a router, there is a link cost (static or dynamic) **the metric issue!**

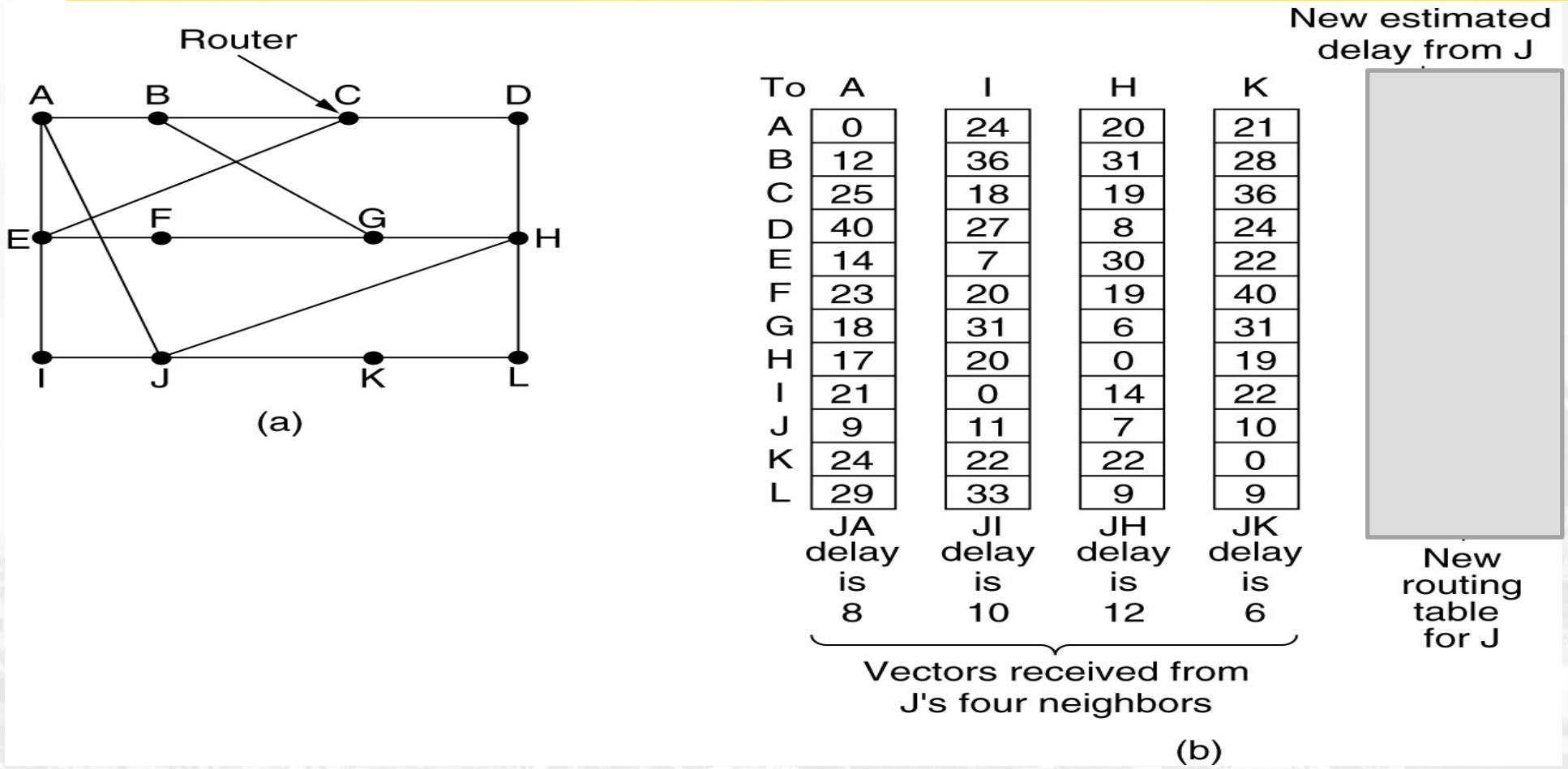
- Distance Vector Table Initialization
- Distance to itself = 0
- Distance to ALL other routers = infinity number

Distance Vector Algorithm

1. Router transmits its distance vector to each of its neighbors.
2. Each router receives and saves the most recently received *distance vector* from each of its neighbors.
3. A router **recalculates** its distance vector when:
   a. It receives a *distance vector* from a neighbor containing different information than before.
   b. It discovers that a link to a neighbor has gone down (i.e., a topology change).

- The DV calculation is based on minimizing the cost to each destination.

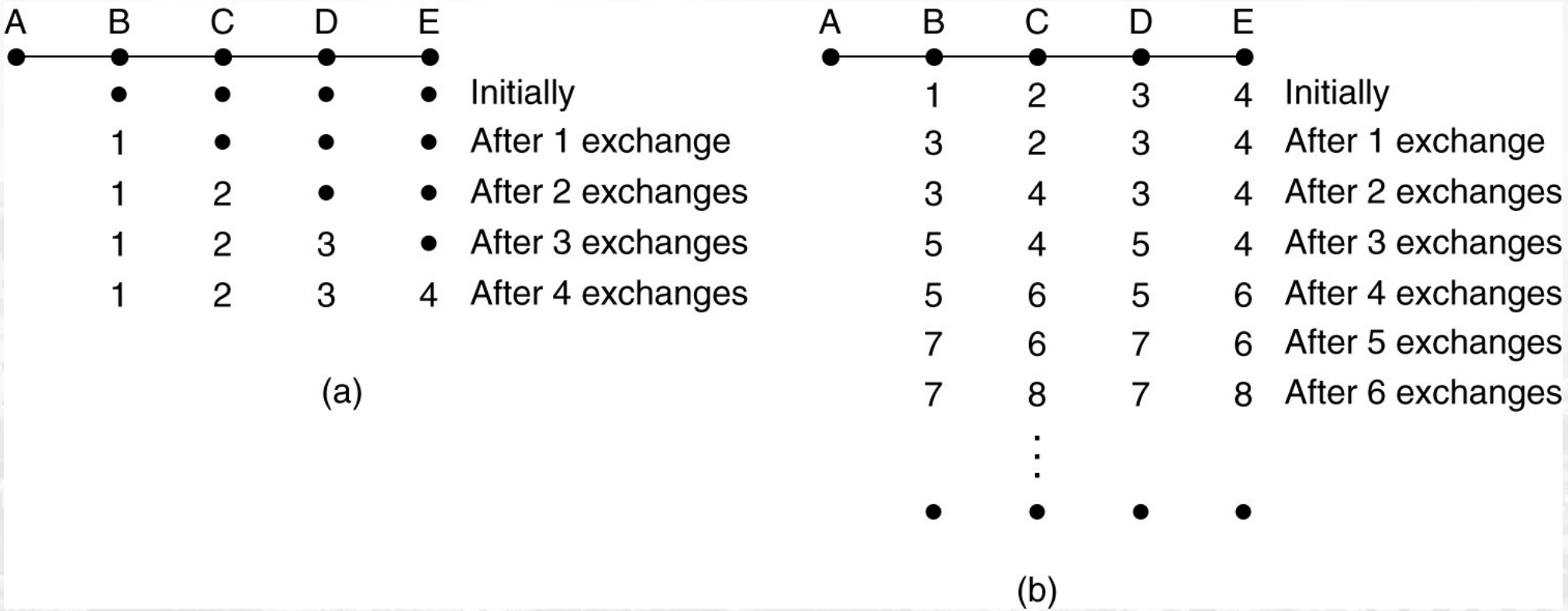
Distance Vector Routing



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

The count-to-infinity problem

- Count to ∞

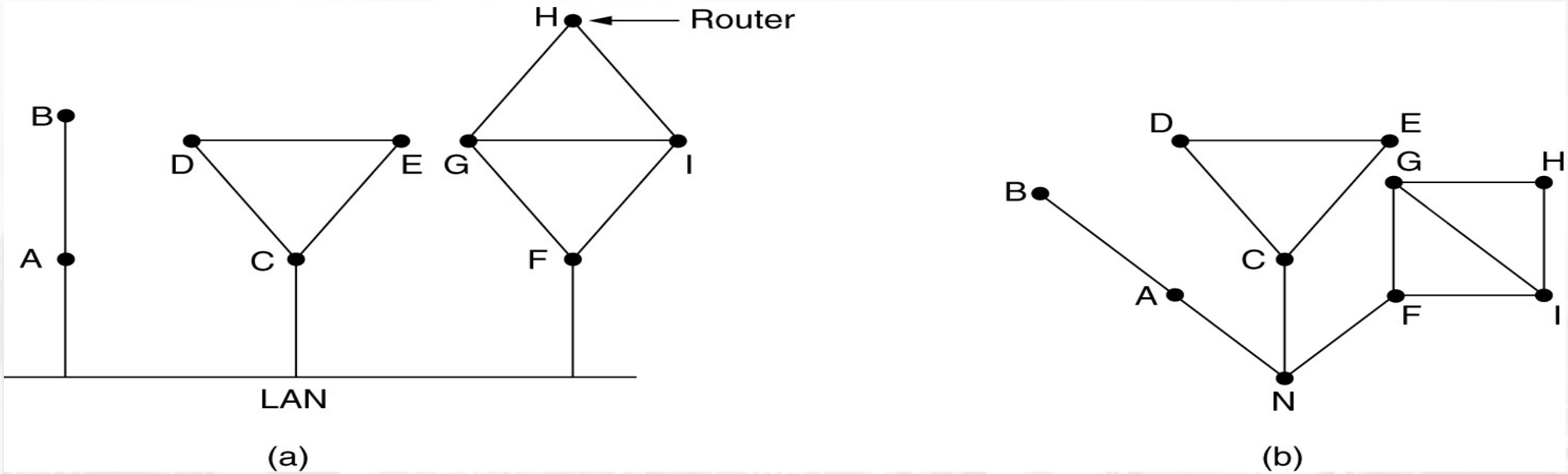


Link State Algorithm

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.

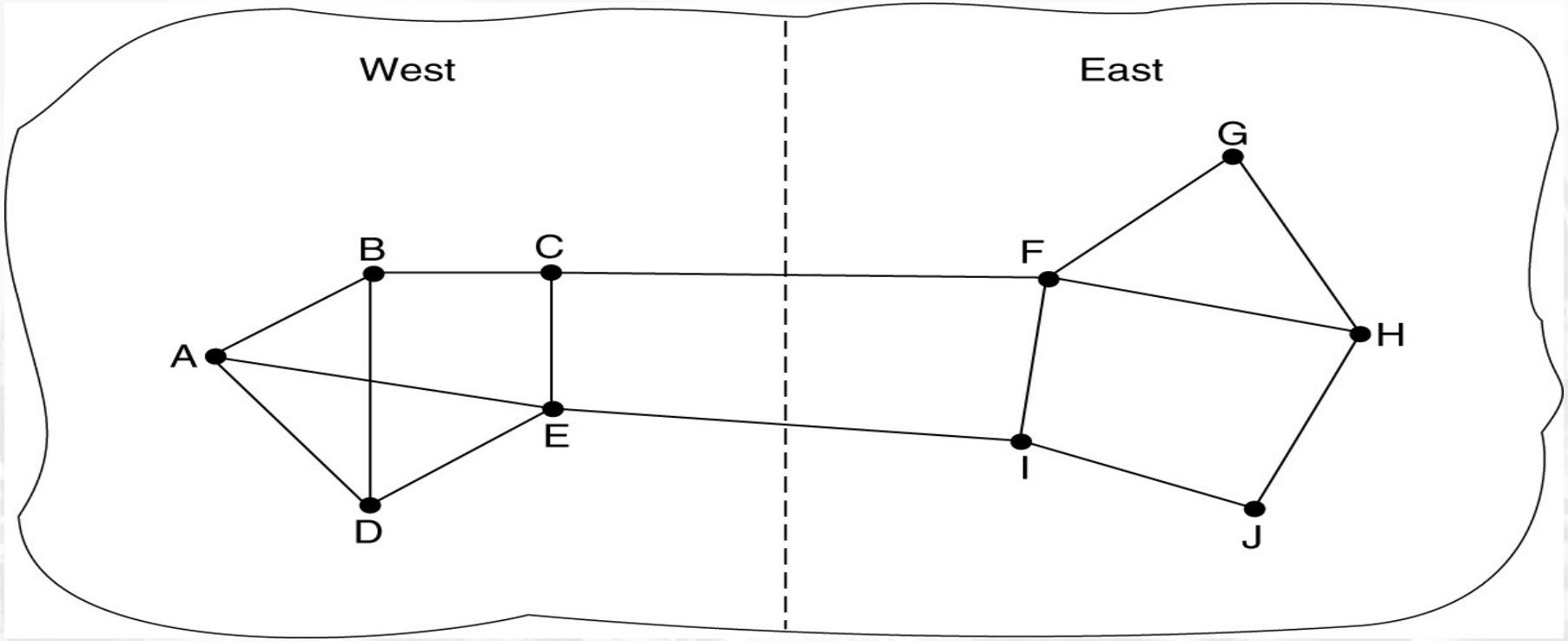
Learning about the Neighbors



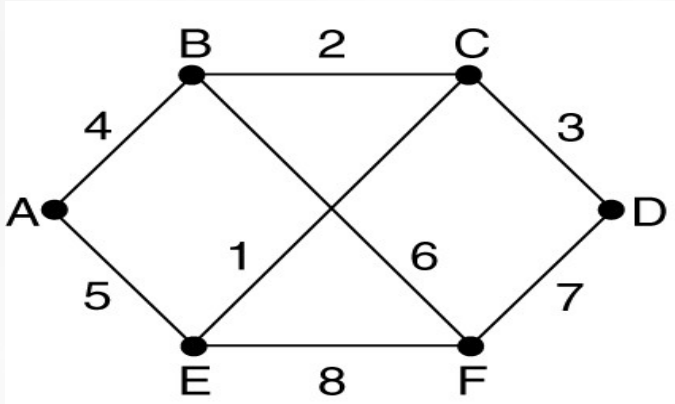
(a) Nine routers and a LAN. (b) A graph model of (a).

Measuring Line Cost

A subnet in which the East and West parts are connected by two lines.



Building Link State Packets



(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

The packet buffer for router B in the previous slide

Source	Seq.	Age	Send flags A	Send flags C	Send flags F	ACK flags A	ACK flags C	ACK flags 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	

Routing Information Protocol (RIP)

- A simple intra domain protocol
- Straightforward implementation of Distance Vector Routing
- Each router advertises its distance vector every 30 seconds (or whenever its routing table changes) to all of its neighbors
- RIP always uses 1 as link metric
- Maximum hop count is 15, with “16” equal to “∞”
- Routes are timeout (set to 16) after 3 minutes if they are not updated

RIPv2

- RIPv2 is an extension of RIPv1:
  - Subnet masks are carried in the route information
  - Authentication of routing messages
  - Route information carries next-hop address
  - Exploits IP multicasting

- Extensions of RIPv2 are carried in unused fields of RIPv1 messages

RIP Messages

- This is the operation of RIP in **`routed`**. Dedicated port for RIP is UDP port 520.

- Two types of messages:
  - **Request messages**
    - used to ask neighboring nodes for an update
  - **Response messages**
    - contains an update

Routing with RIP

- **Initialization:** Send a **request packet** (command = 1, address family=0..0) on all interfaces:
    - RIPv1 uses broadcast if possible,
    - RIPv2 uses multicast address 224.0.0.9, if possible

  requesting routing tables from neighboring routers
- **Request received**: Routers that receive above request send their entire routing table
- **Response received**: Update the routing table

- Typically, there is a routing daemon (routed) that is an **application layer process** that provides access to routing tables.

Routing with Rip Cont.

- **Regular routing updates**: Every 30 seconds, send all or part of the routing tables to every neighbor in an response message
- **Triggered Updates:** Whenever the metric for a route change, send entire routing table.
- If a router does not hear from its neighbor once every 180 seconds, the neighbor is deemed unreachable.

Security

- Issue: Sending bogus routing updates to a router
- RIPv1: No protection
- RIPv2: Simple authentication scheme

RIP Problems

- RIP takes a long time to stabilize
  - Even for a small network, it takes several minutes until the routing tables have settled after a change
- The maximum path in RIP is 15 hops

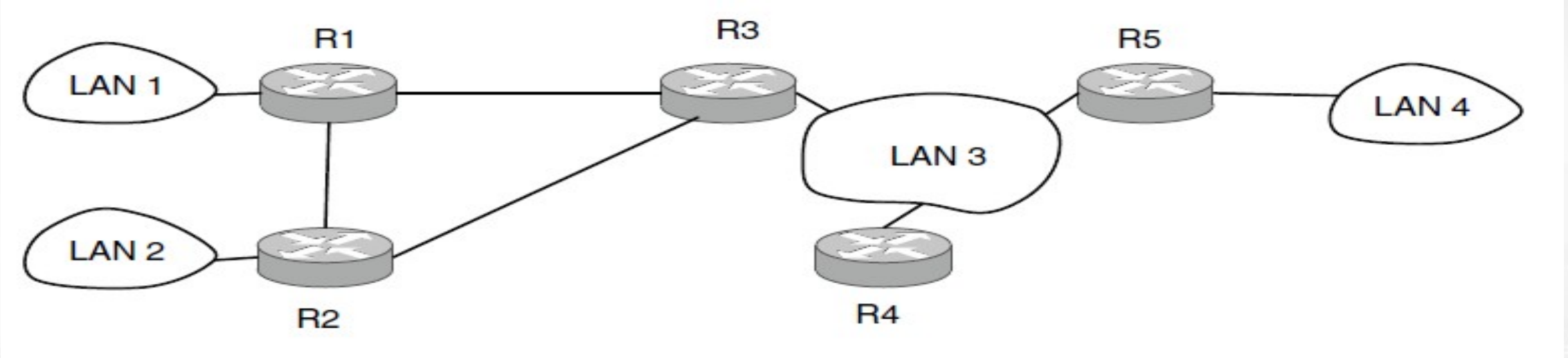
Open Shortest Path First(OSPF)

- Provides for authentication of routing messages.
  - 8-byte password designed to avoid misconfiguration.
- Provides additional hierarchy
  - Domains are partitioned into *areas.*
  - This reduces the amount of information transmitted in packet.
- Provides load-balancing via multiple routes.

Open Shortest Path First(OSPF)

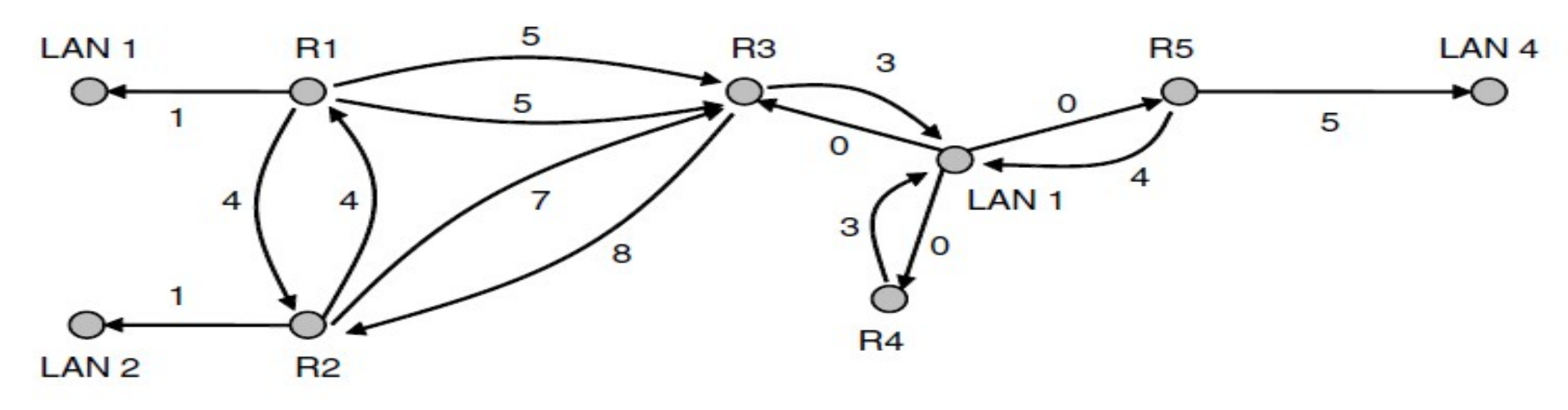
- OSPF runs *on top of* IP, i.e., an OSPF packet is transmitted with IP data packet header.
- Uses Level 1 and Level 2 routers
- Has: backbone routers, area border routers, and AS boundary routers

OSPF—An Interior Gateway Routing Protocol (1)



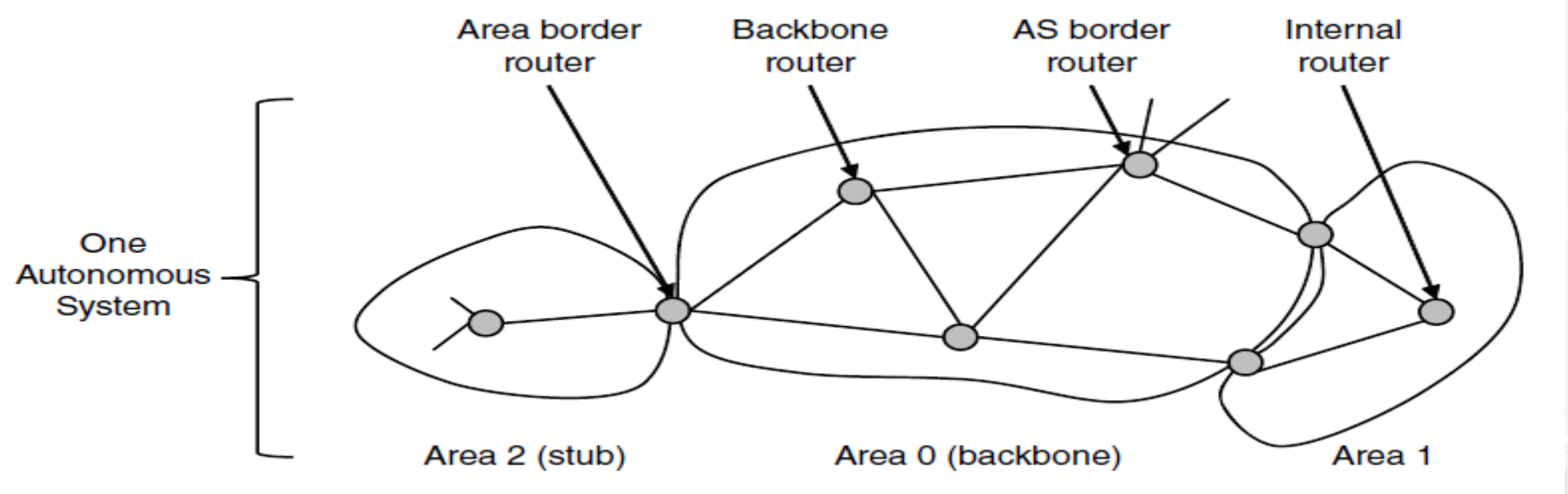
An autonomous system

OSPF—An Interior Gateway Routing Protocol (2)



A graph representation of the previous slide.

OSPF—An Interior Gateway Routing Protocol (3)



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

OSPF Terminology

Internal router :: a level 1 router.

Backbone router :: a level 2 router.

Area border router (ABR) :: a backbone router that attaches to more than one area.

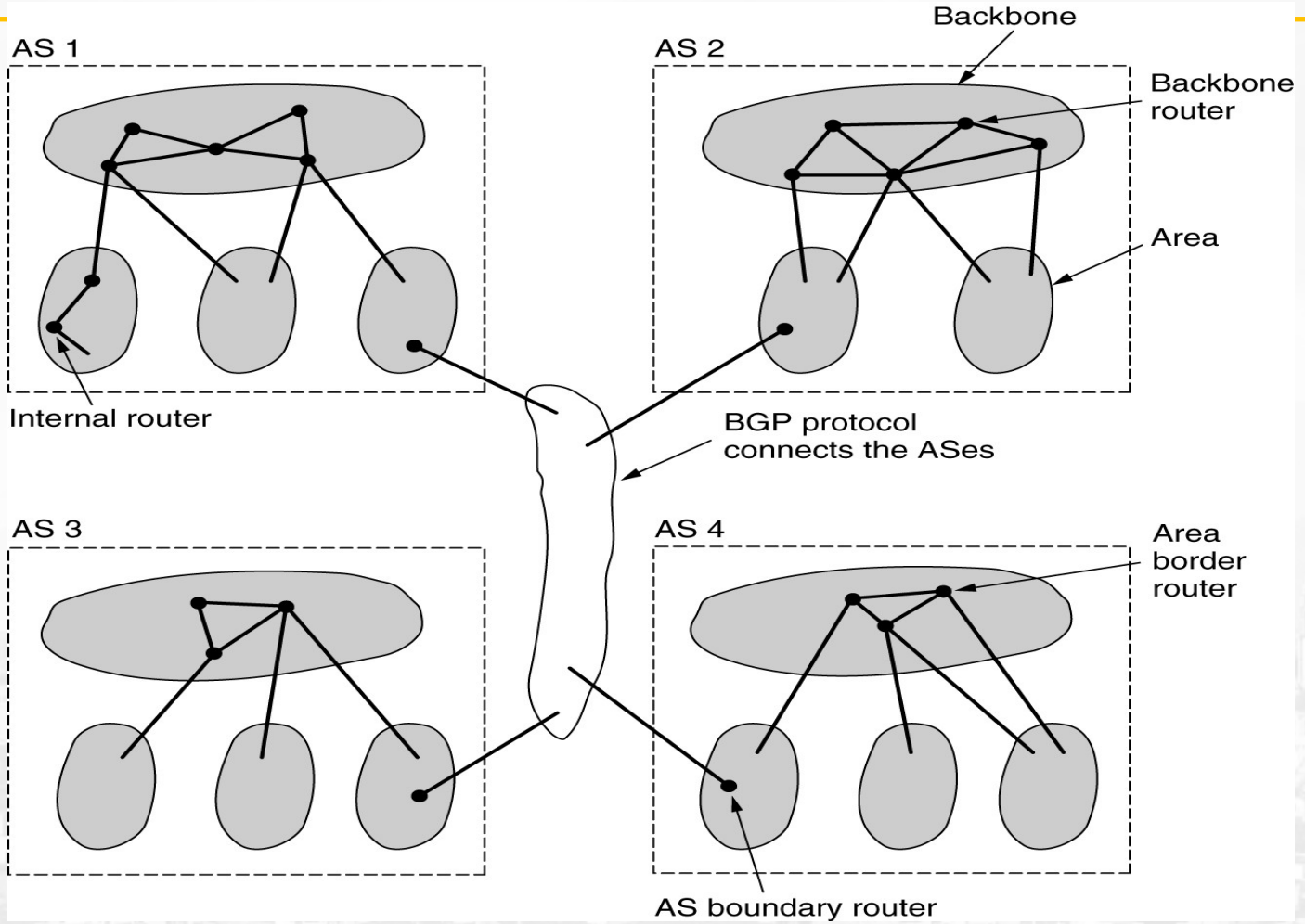
AS border router :: (an interdomain router), namely, a router that attaches to routers from other ASs across AS boundaries.

OSPF—An Interior Gateway Routing Protocol (4)

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

OSPF

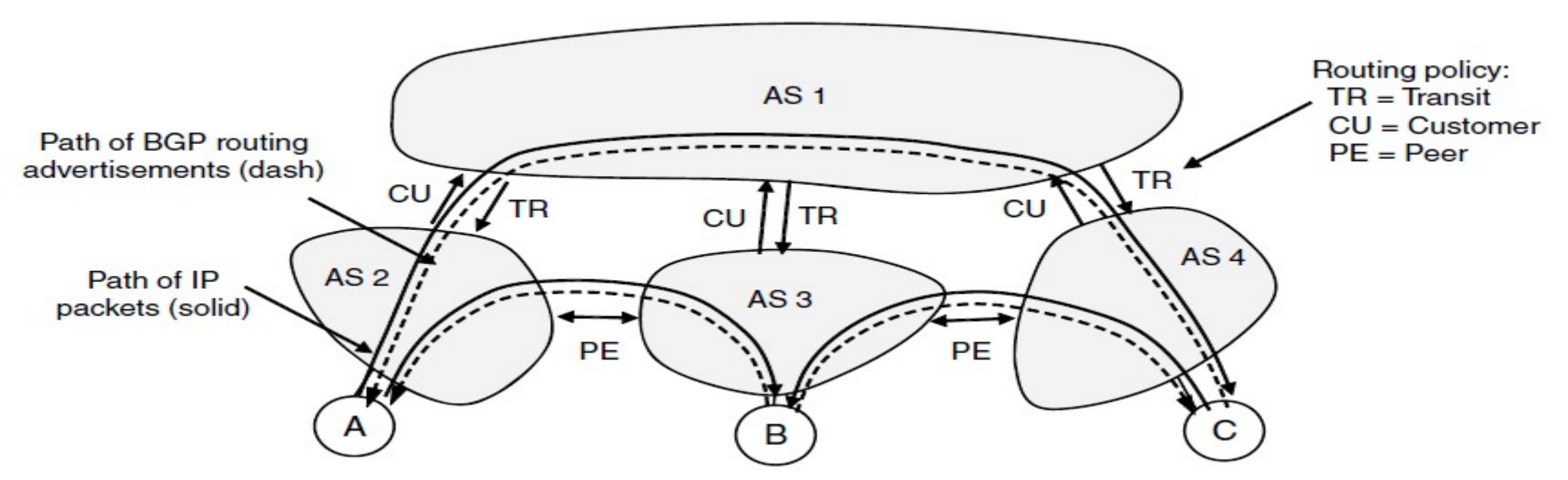


The relation between ASes, backbones, and areas in OSPF.

Border Gateway Protocol (BGP)

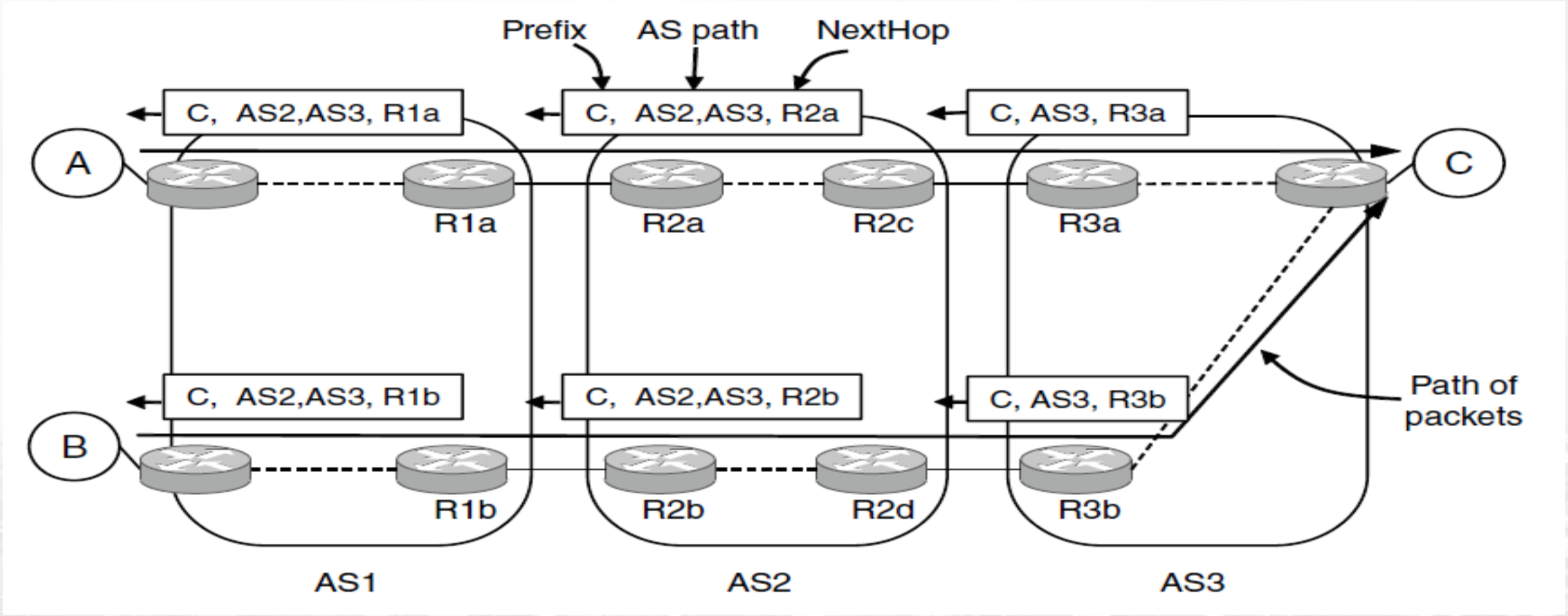
- Current version is BGP-4.
- BGP assumes the Internet is an arbitrary interconnected set of AS's.
- In *interdomain* routing the goal is to find ANY path to the intended destination that is loop-free. The protocols are more concerned with **reachability** than optimality.

BGP—The Exterior Gateway Routing Protocol (2)



Routing policies between four Autonomous Systems

BGP—The Exterior Gateway Routing Protocol (3)

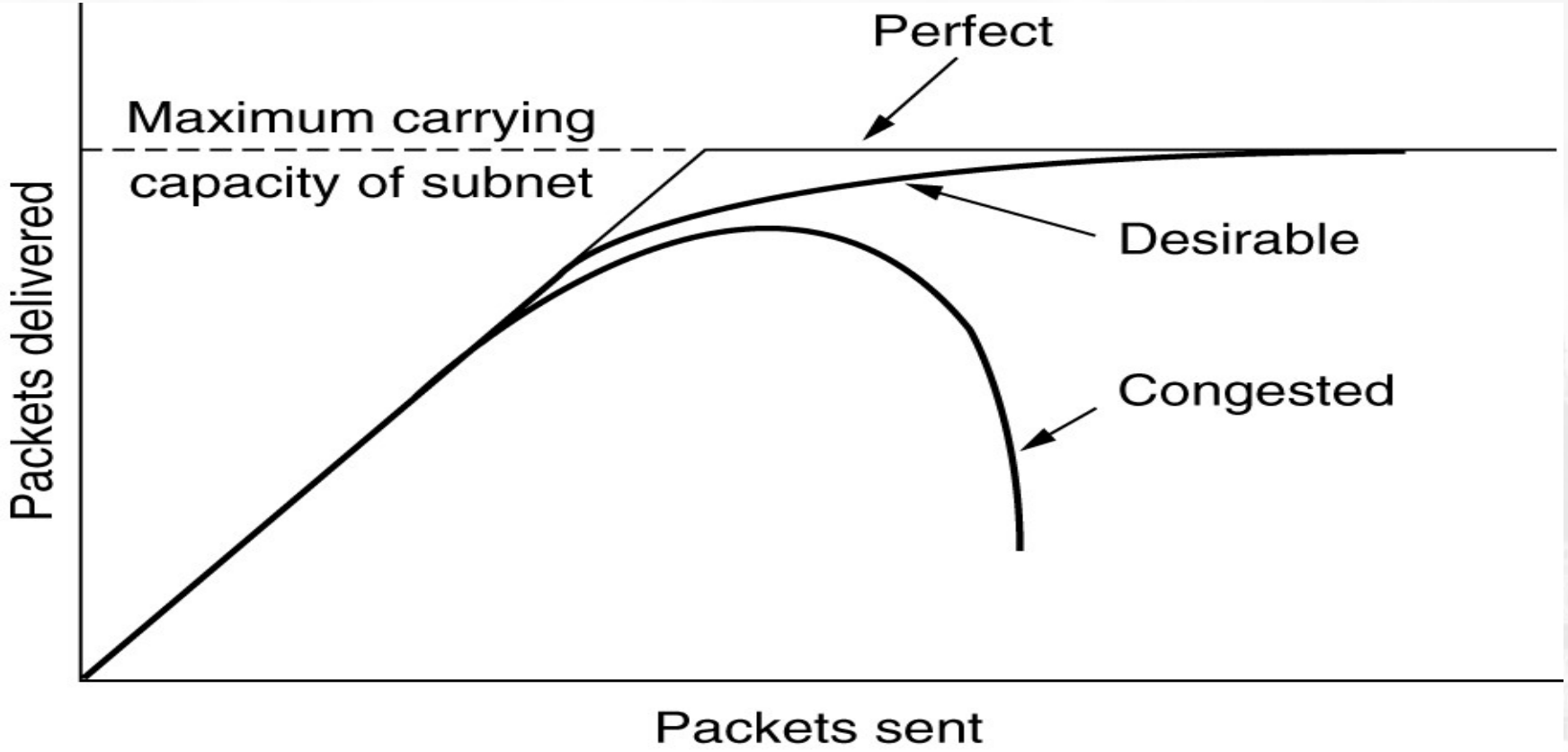


Propagation of BGP route advertisements

Congestion Control

- Too many packets present in the network
  - packet delay and loss
- Congestion occurs within the network
  - Affects the network layer
  - it must ultimately determine what to do with the excess packets.
- The network and transport layers share the responsibility for handling congestion
- Congestion at the network layer is related to two issues
  - throughput
  - delay

Congestion



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

Congestion Control Algorithms

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

General Principles of Congestion Control

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

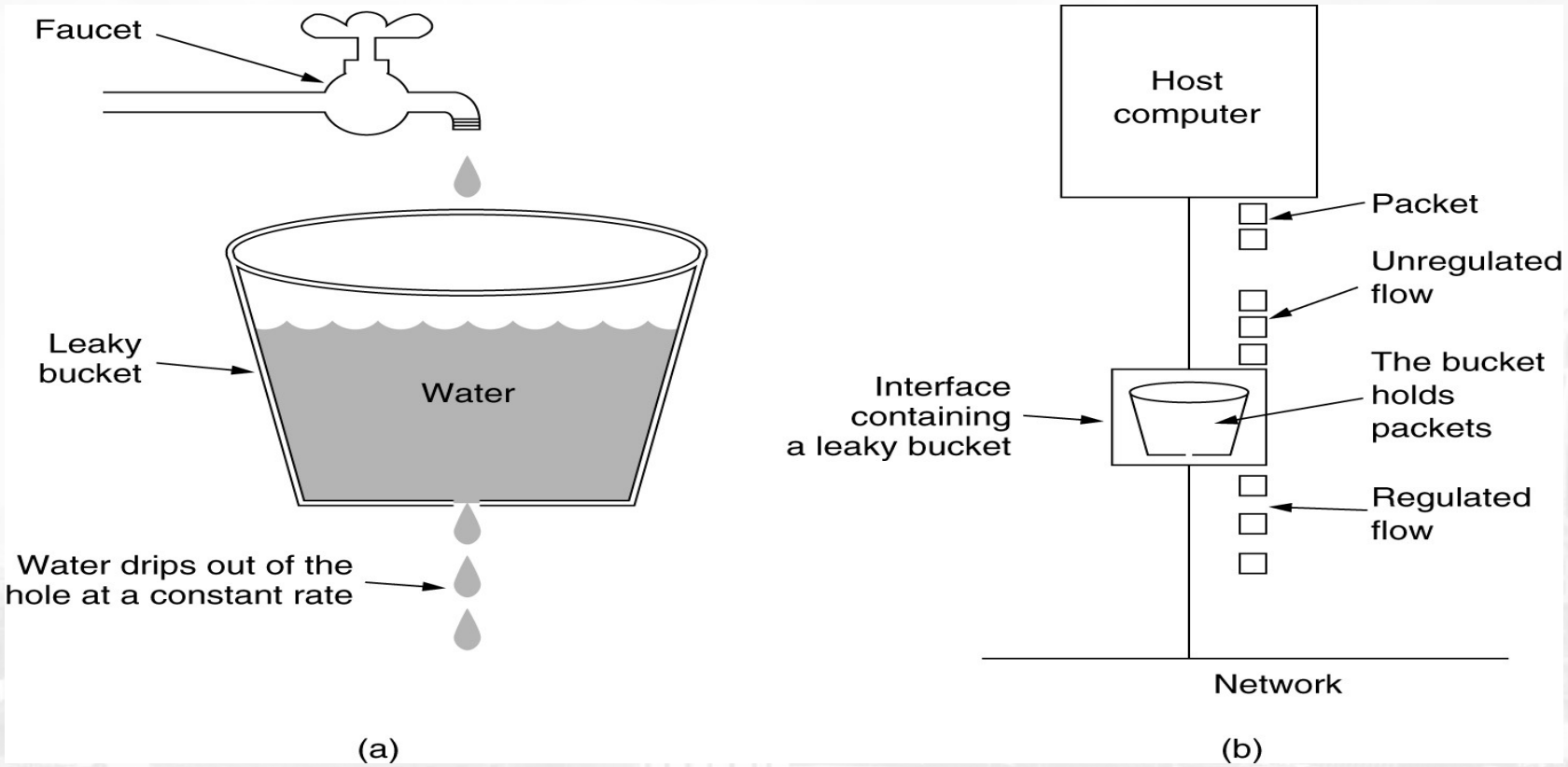
Congestion Prevention Policies

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

Quality of Service

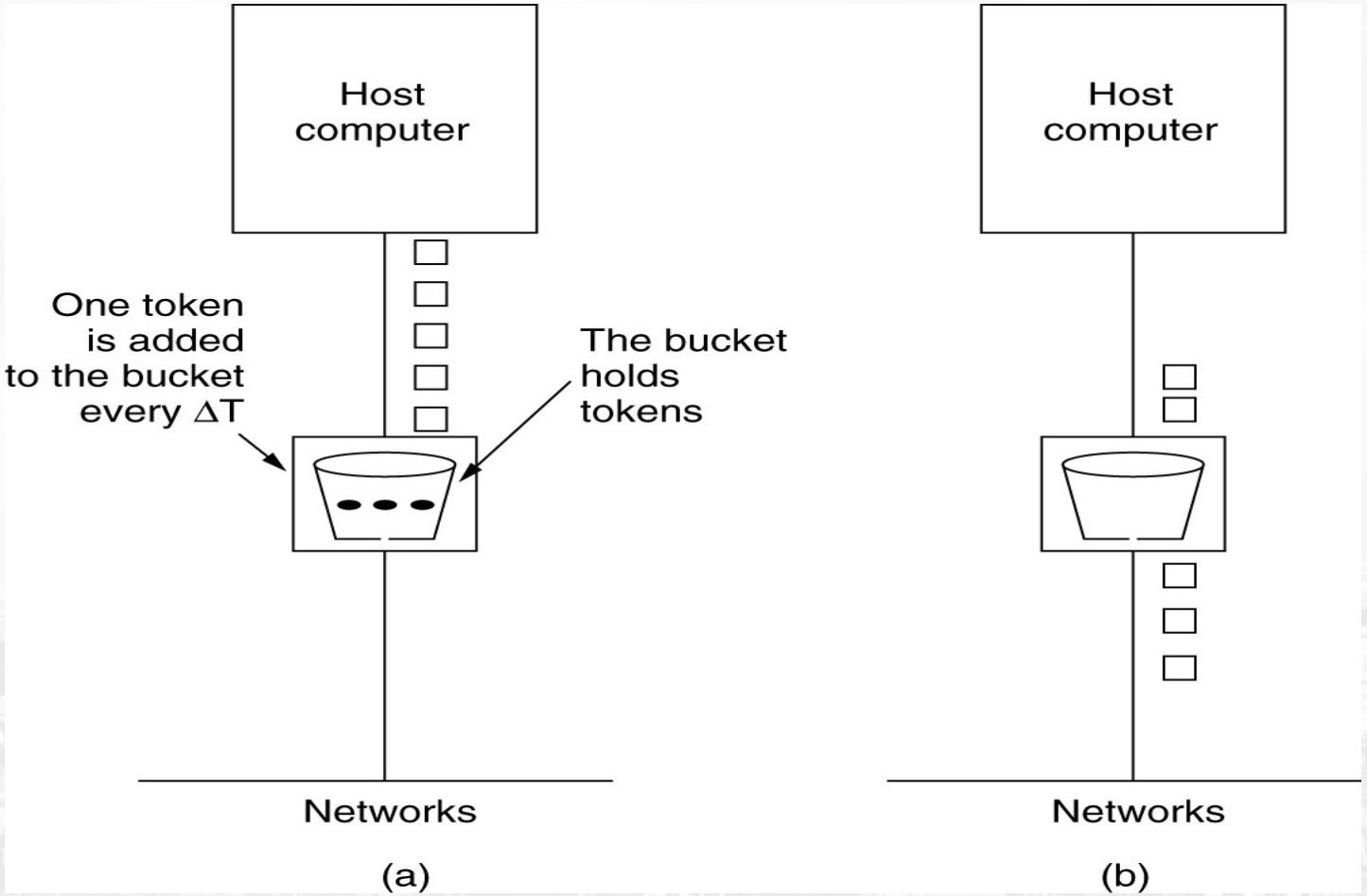
- Overprovisioning
- Buffering
- Traffic Shaping
- The Leaky Bucket Algorithm
- The Token Bucket Algorithm
- Fragmentation

The Leaky Bucket Algorithm



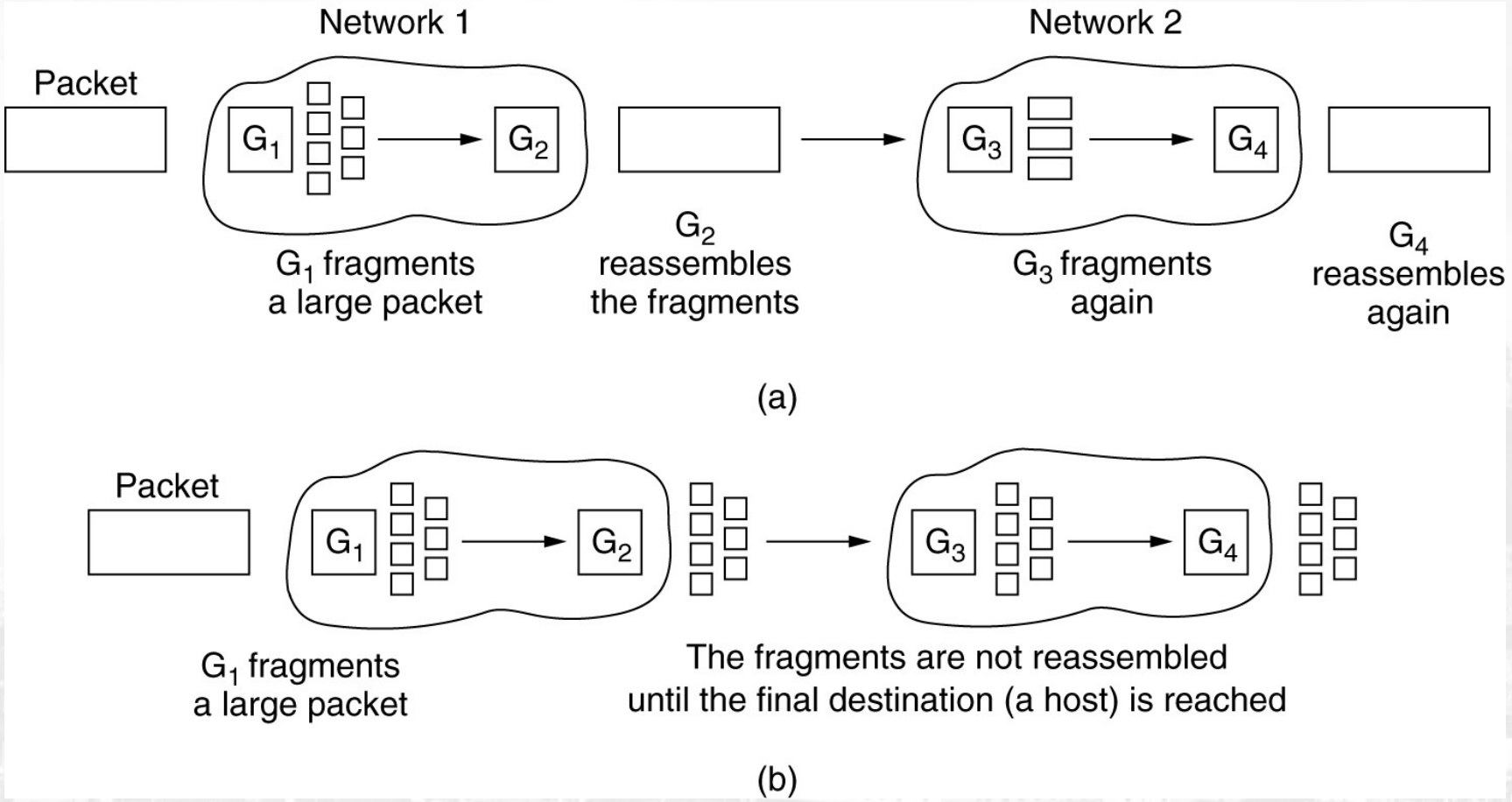
(a) A leaky bucket with water. (b) a leaky bucket with packets.

The Token Bucket Algorithm



(a) Before. (b) After.

Fragmentation



(a) Transparent fragmentation. (b) Nontransparent fragmentation.

Fragmentation