計算機ネットワーク

開講クォーター: 1-2Q

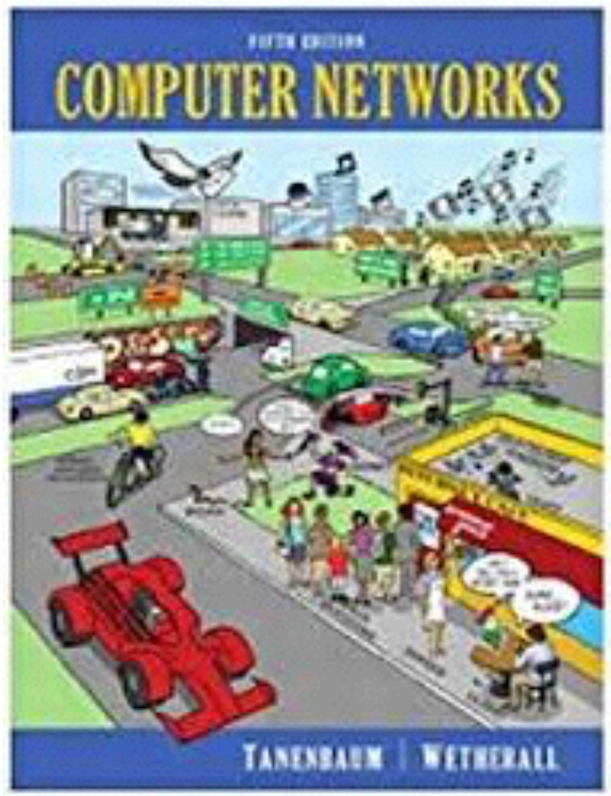
曜日・時限: 火7-8限

講義室: 1Q @ W834, 2Q @ W931

横田理央

rioyokota@gsic.titech.ac.jp

参考書



教科書

講義日程（2Q）

		授業計画		課題
06/14	第９回	ネットワーク層１ ルーティング・輻輳制御	５章	ルーティングの種類を理解し 輻輳制御手法を説明できる
06/21	第１０回	ネットワーク層２ インターネットとサービス品質	５章	インターネットの制御プロトコルを理解し ネットワーク間の接続について説明できる
06/28	第１１回	トランスポート層１ トランスポート・プロトコルの要素	６章	誤り制御とフロー制御を理解し 輻輳制御について説明できる
07/05	第１２回	トランスポート層２ UDP と TCP	６章	TCP の信頼性を理解し TCP のコネクション管理を説明できる
07/12	第１３回	アプリケーション層 DNS, 電子メール, www	７章	DNS, 電子メール, www のしくみを理解し ストリーミング，P2P について説明できる
07/26	第１４回	ネットワークセキュリティ１ 対称鍵暗号，公開鍵暗号	８章	暗号アルゴリズムを理解し SHA-1,2 と RSA について説明できる
08/02	第１５回	ネットワークセキュリティ２ デジタル署名，認証プロトコル	８章	電子メール,Web のセキュリティ の脅威について把握できる

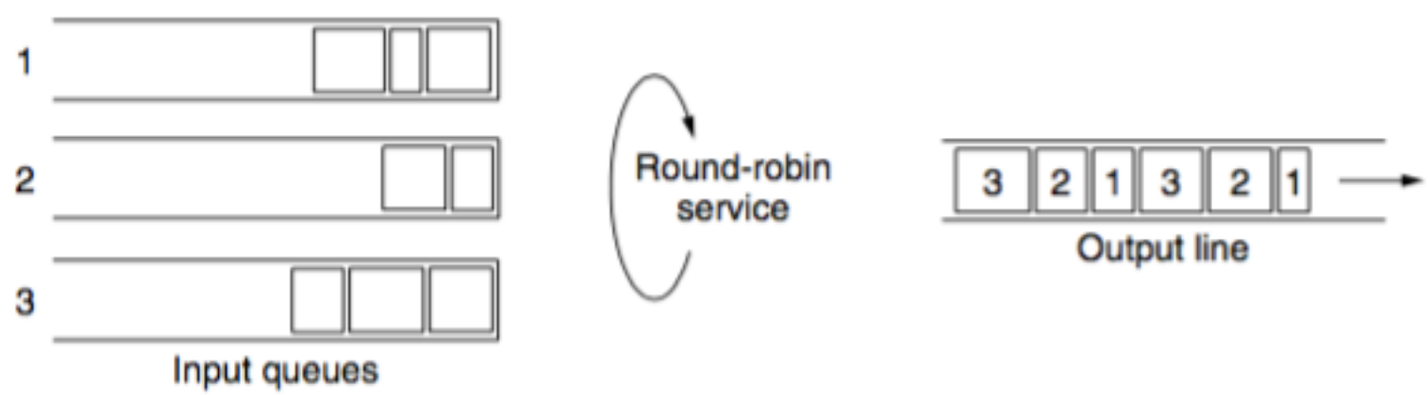
Packet Scheduling

<u>Resources to be reserved</u>

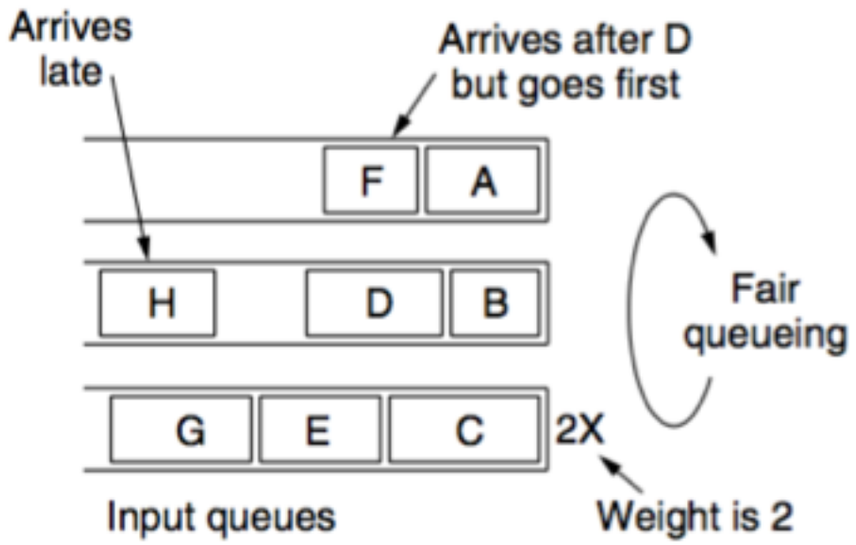
1. Bandwidth
2. Buffer space
3. CPU cycles

<u>Scheduling algorithms</u>

1. FIFO (First-In First-Out)
   - One flow can easily affect the performance of the other flows
2. Fair queueing
   - Gives more bandwidth to hosts that use large packets
3. Byte-by-byte round-robin



Packet Scheduling



(a)

Packet	Arrival time	Length	Finish time	Output order
A	0	8	8	1
B	5	6	11	3
C	5	10	10	2
D	8	9	20	7
E	8	8	14	4
F	10	6	16	5
G	11	10	19	6
H	20	8	28	8

(b)

Scheduling algorithms

4. Weighted fair queueing (WFQ)

Arrival time : A
Finish time : F
Length of packet : L
Weight of flow : W

$$F_i = \max(A_i, F_{i-1}) + L_i / W$$

- Requires that packets be inserted by their finish time into a sorted queue

5. Deficit round-robin

- Can be implemented much more efficiently

Admission Control

<u>QoS routing</u>

New flows may be accommodated by choosing a different route for the flow that has excess capacity

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

<u>Queueing delay</u>

Mean delay of package : T

Mean arrival rate : λ

Mean service rate : μ

CPU utilization : ρ=λ/μ

$$T = \frac{1}{\mu} \times \frac{1}{1 - \lambda/\mu} = \frac{1}{\mu} \times \frac{1}{1 - \rho}$$

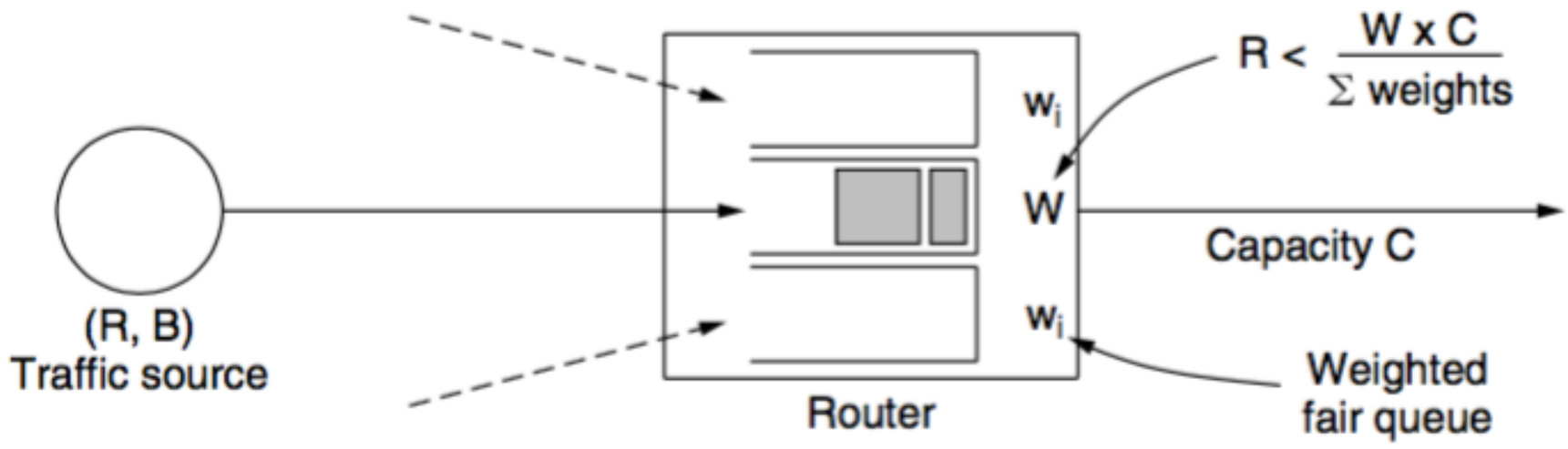
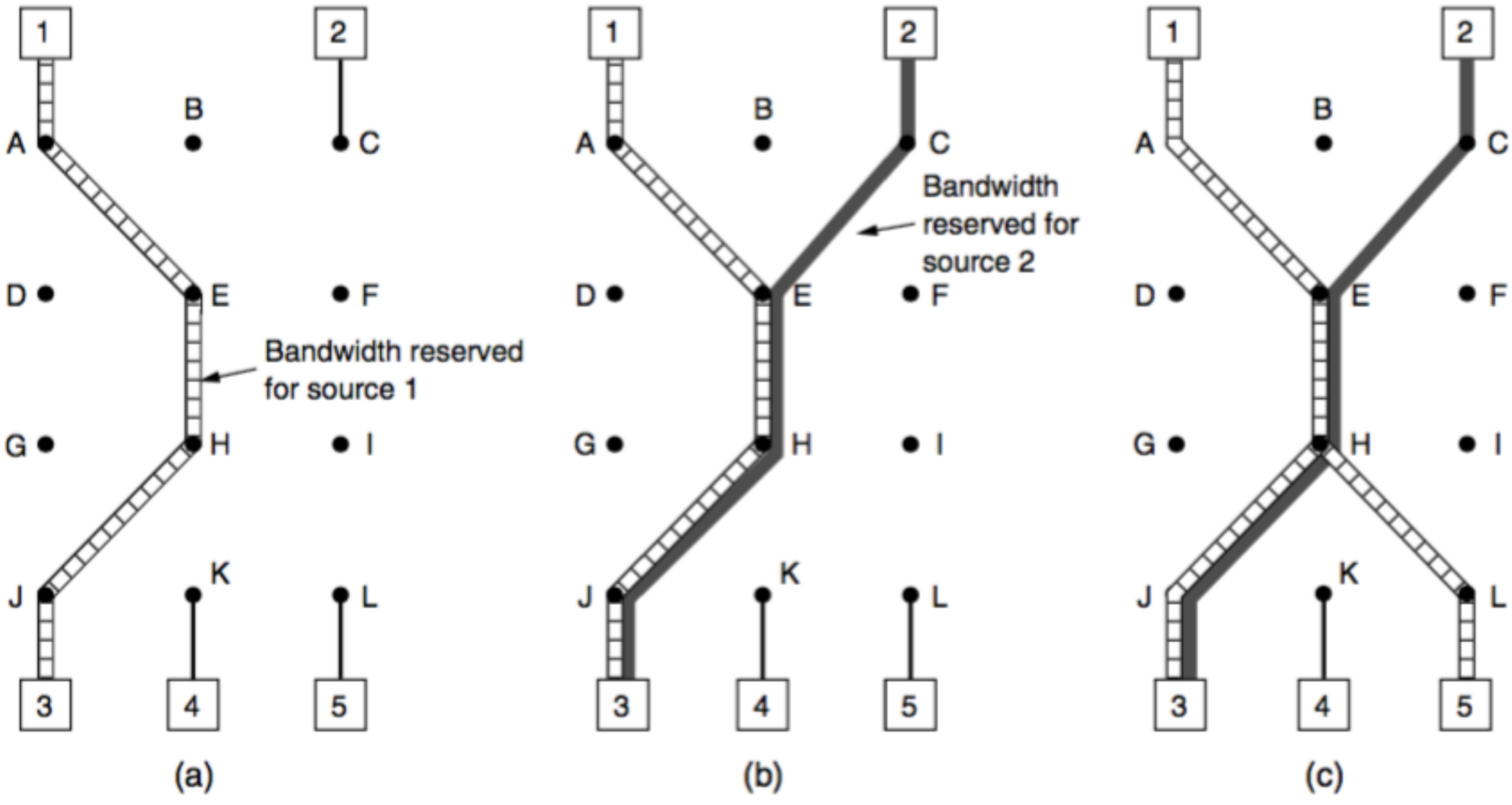


Figure 5-33. Bandwidth and delay guarantees with token buckets and WFQ.

Integrated Services

RSVP (The Resource reSerVation Protocol)

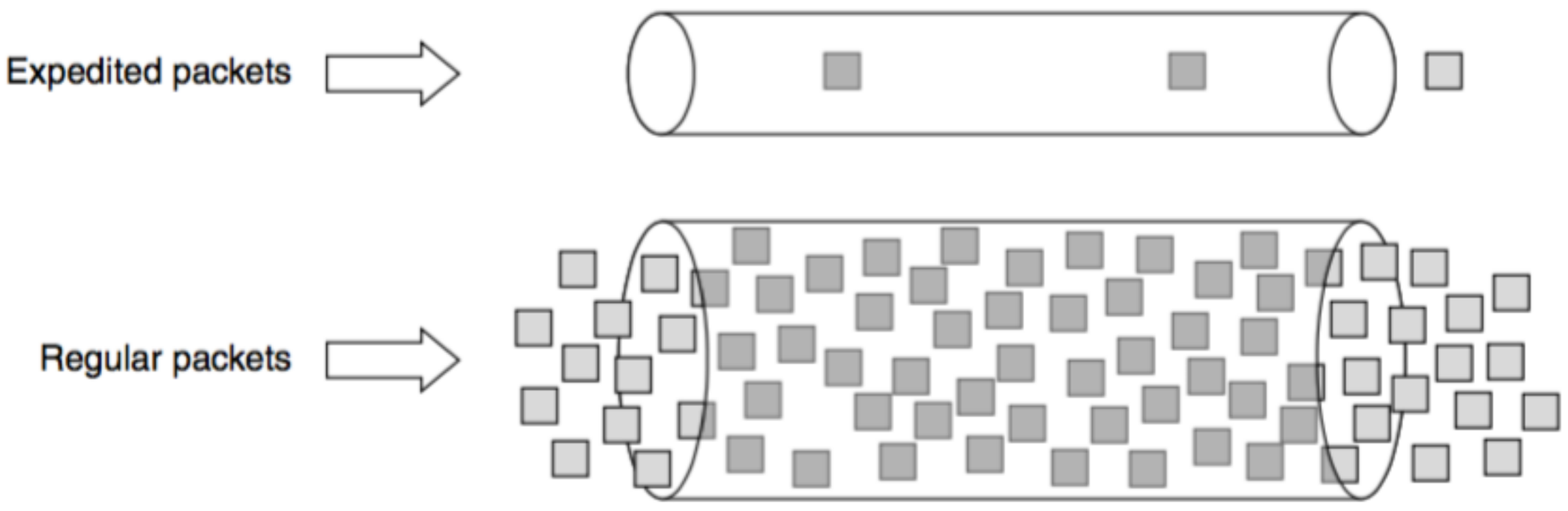
To get better reception and eliminate congestion, any of the receivers in a group can send a reservation message up the tree to the sender. At each hop, the router notes the reservation and reserves the necessary bandwidth.



Differentiated Services

<u>Expedited Forwarding</u>

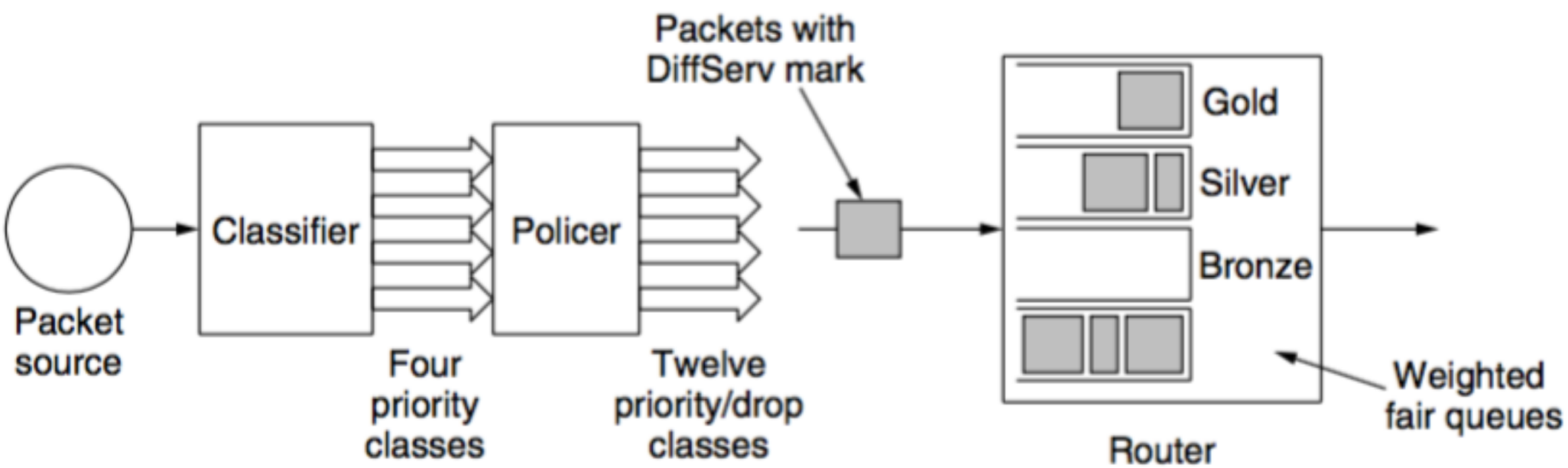
1. The vast majority of the traffic is expected to be regular, but a limited fraction of the packets are expedited.
2. Packets are classified as expedited or regular and marked accordingly on the sending host or in the ingress (first) router.
3. It is becoming common for VoIP packets to be marked for expedited service by hosts.



Differentiated Services

Assured Forwarding

1. Specifies that there shall be four priority classes, each class having its own resources.
2. The next step is to determine the discard class for each packet by passing the packets of each priority class through a traffic policer such as a token bucket.
3. The combination of priority and discard class is then encoded in each packet.
4. Finally, the packets are processed by routers in the network with a packet scheduler that distinguishes the different classes.

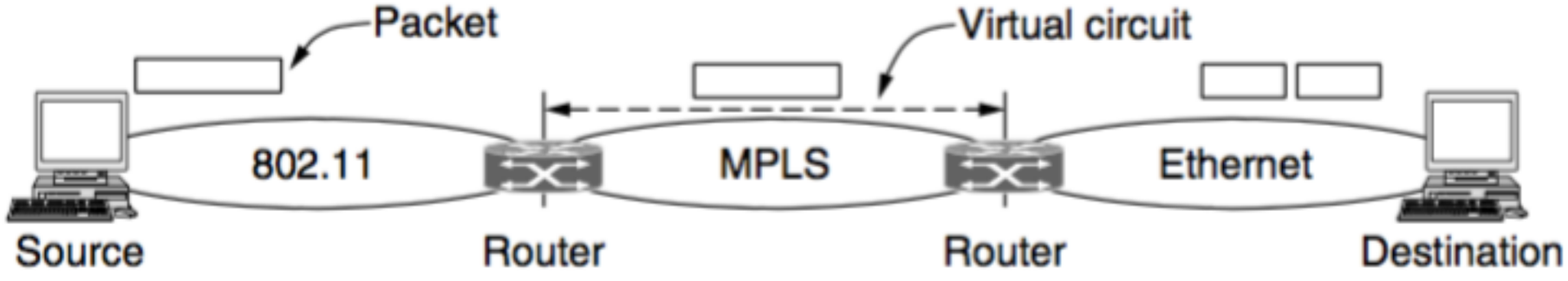


Internetworking

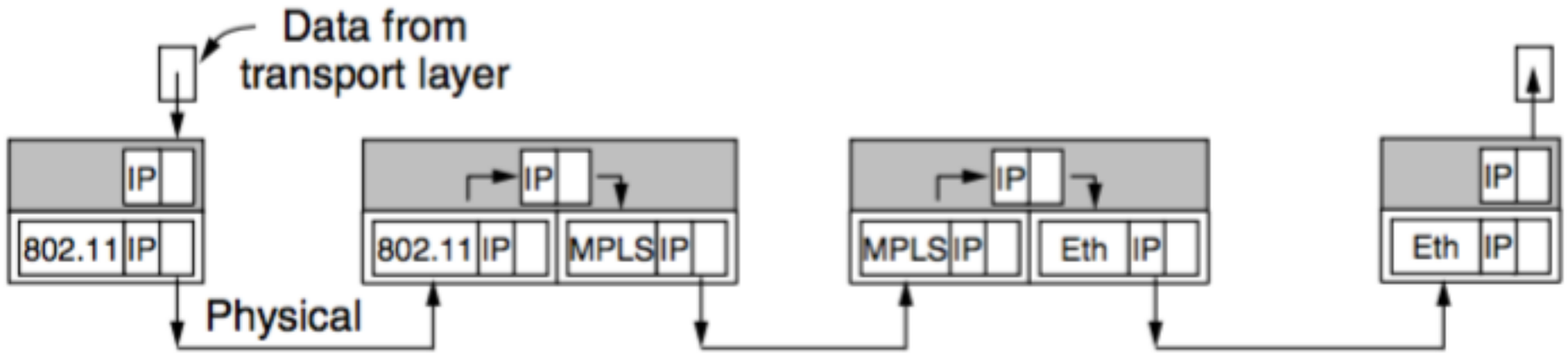
How networks differ

Item	Some Possibilities
Service offered	Connectionless versus connection oriented
Addressing	Different sizes, flat or hierarchical
Broadcasting	Present or absent (also multicast)
Packet size	Every network has its own maximum
Ordering	Ordered and unordered delivery
Quality of service	Present or absent; many different kinds
Reliability	Different levels of loss
Security	Privacy rules, encryption, etc.
Parameters	Different timeouts, flow specifications, etc.
Accounting	By connect time, packet, byte, or not at all

How networks can be connected

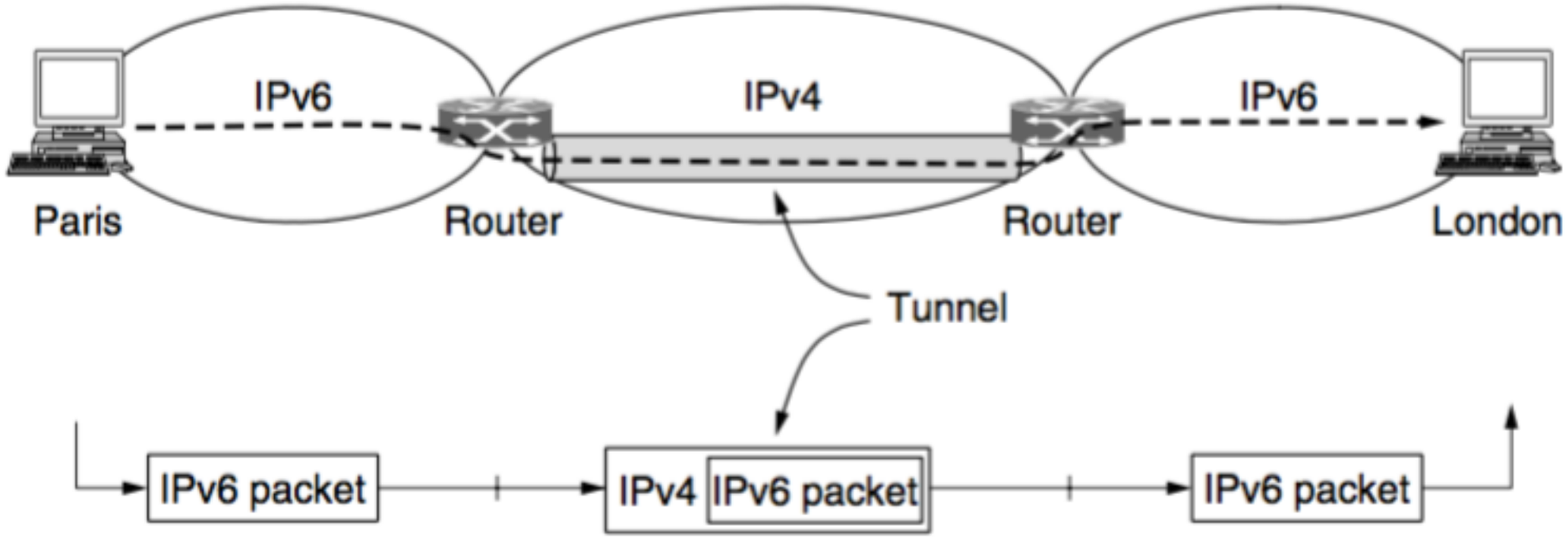


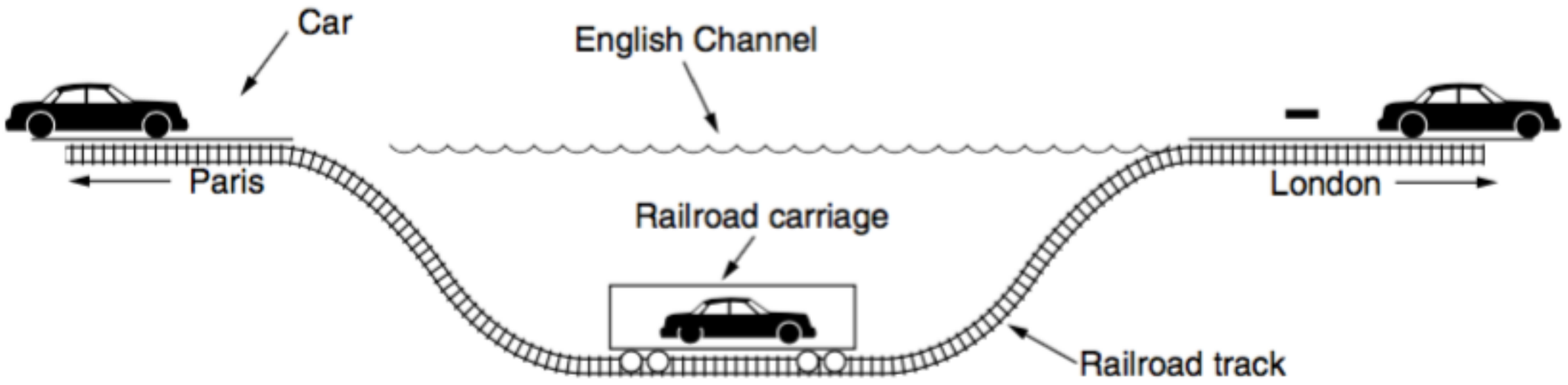
(a)



(b)

Tunneling


IPv6
IPv4
IPv6
Paris
Router
Router
London
Tunnel
IPv6 packet
IPv4
IPv6 packet
IPv6 packet


Car
English Channel
Paris
London
Railroad carriage
Railroad track

Internetwork Routing

Maximum size of packets

1. Hardware (e.g., the size of an Ethernet frame).

2. Operating system (e.g., all buffers are 512 bytes).

3. Protocols (e.g., the number of bits in the packet length field).

4. Compliance with some (inter)national standard.

5. Desire to reduce error-induced retransmissions to some level.

6. Desire to prevent one packet from occupying the channel too long.

Ethernet : 1500 bytes
802.11 : 2272 bytes
IP : 65,515 bytes

Packet Fragmentation

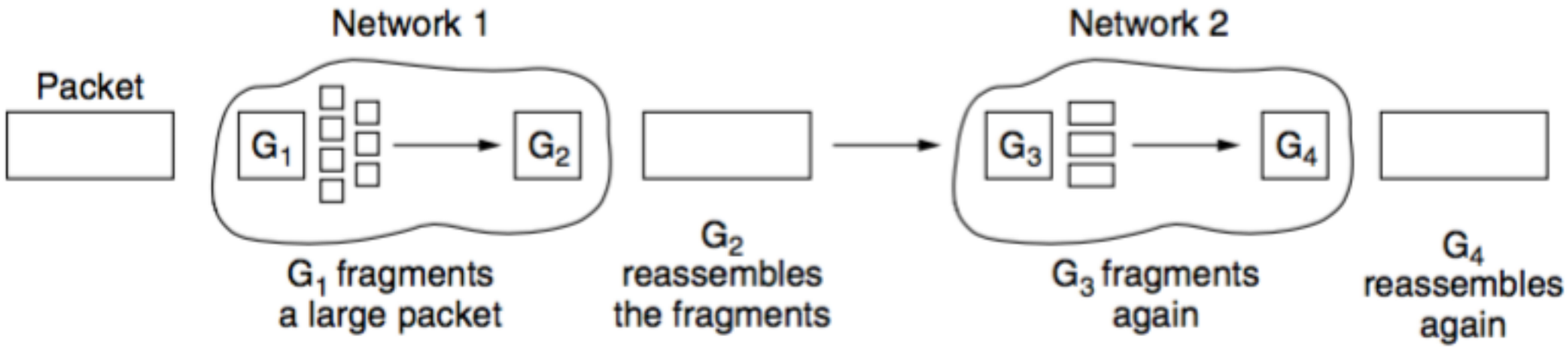
Transparent fragmentation

Make fragmentation transparent to any subsequent networks through which the packet must pass

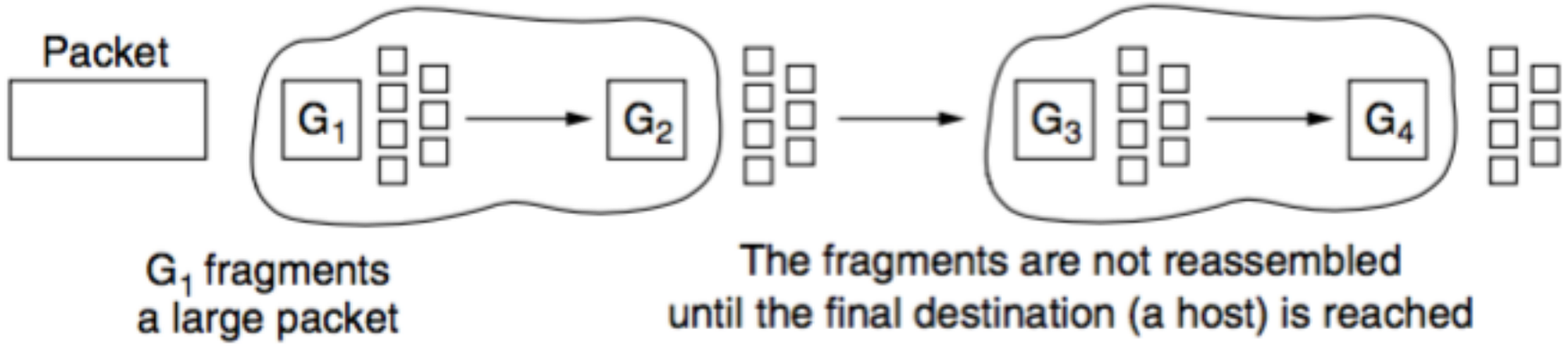
Nontransparent fragmentation

Refrain from recombining fragments at any intermediate routers.

Requires routers to do less work.

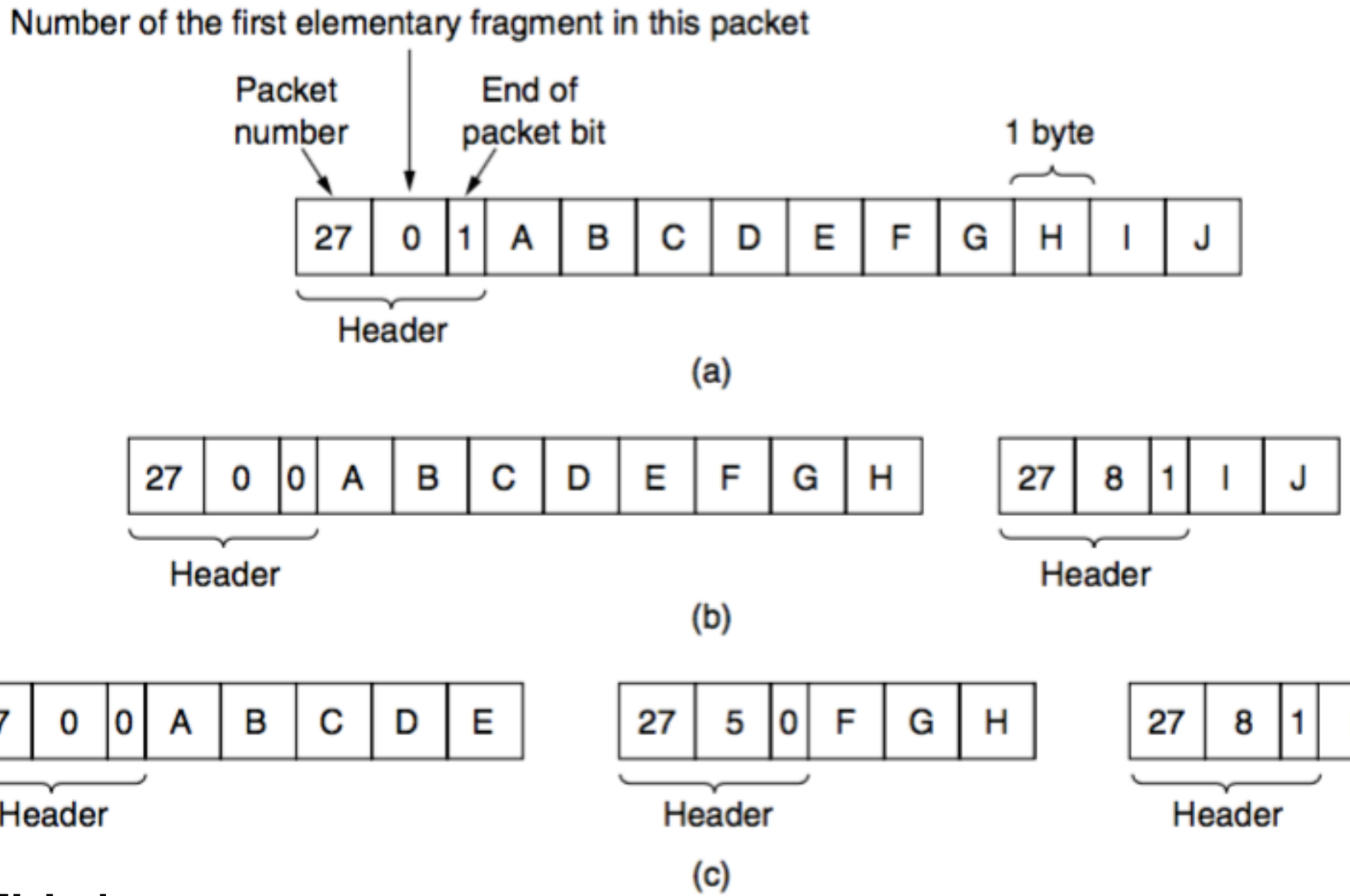


(a)

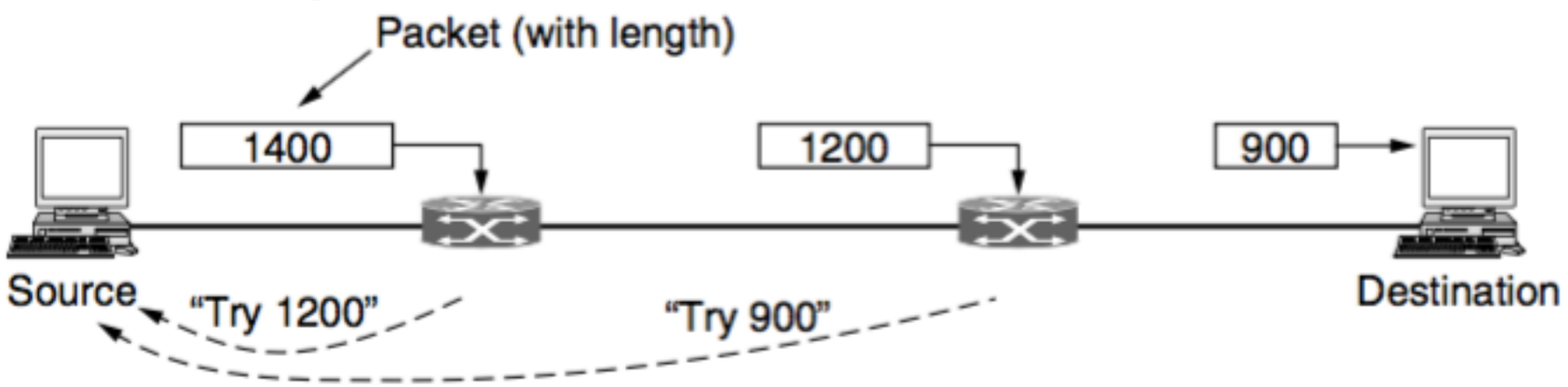


(b)

Packet Fragmentation



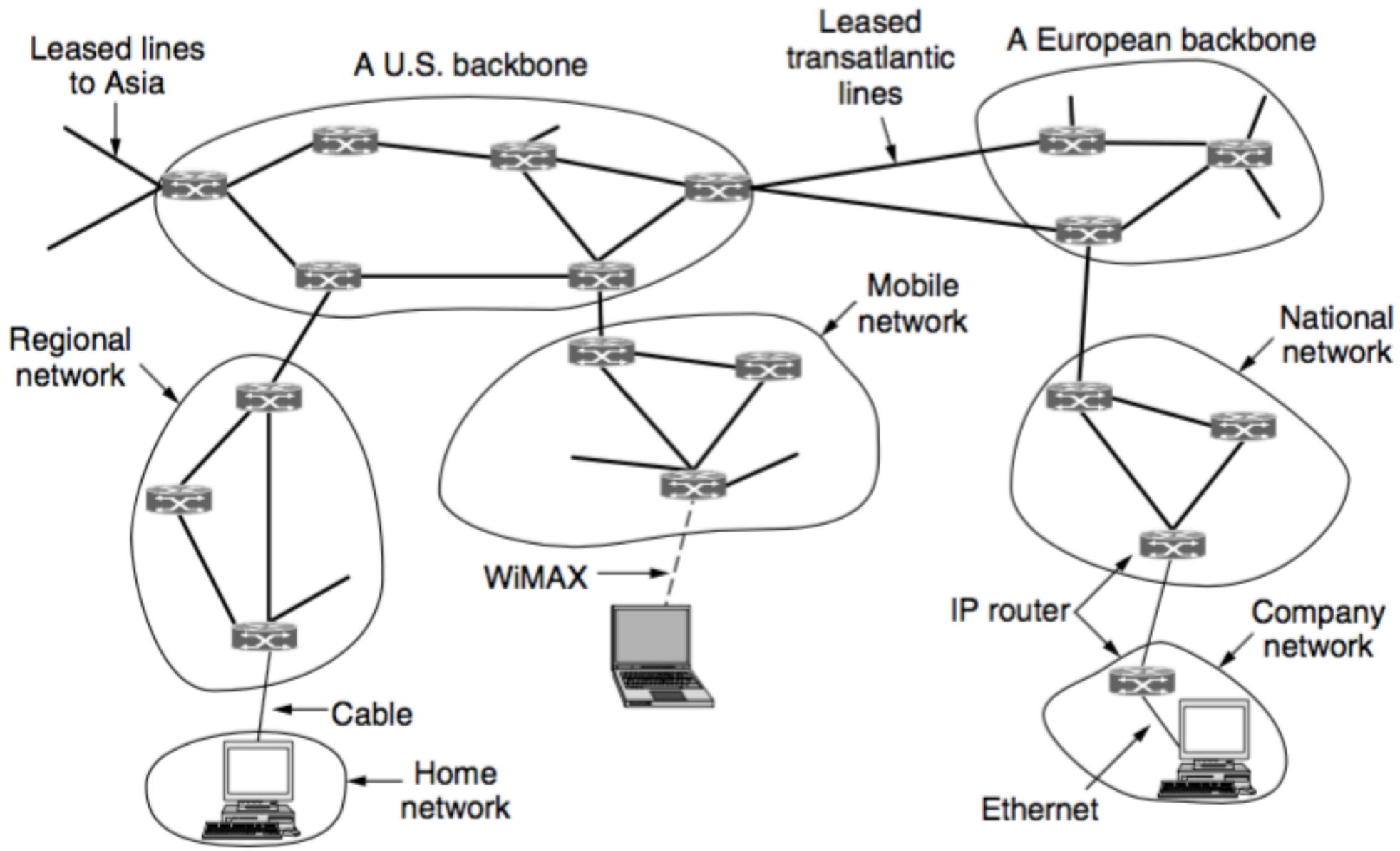
Path MTU discovery



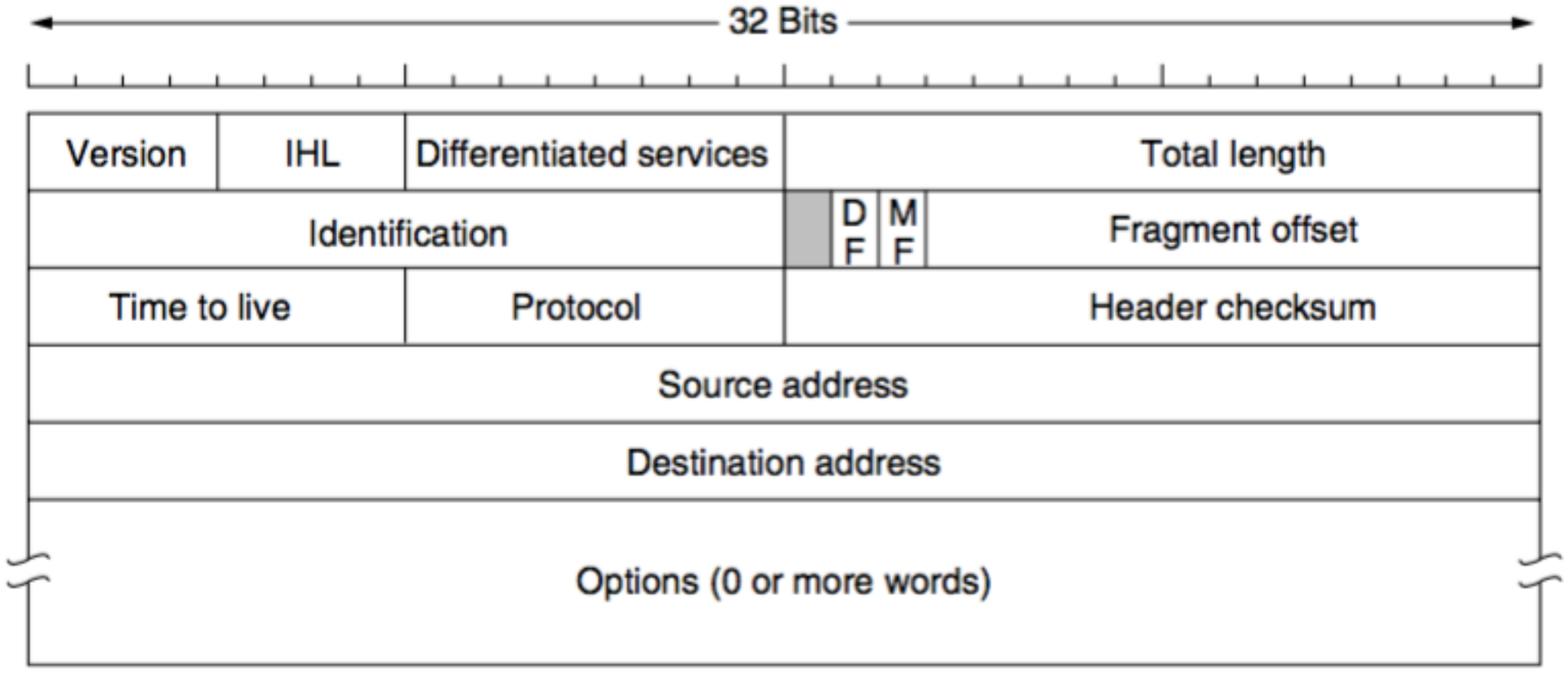
The Network Layer in the Internet

IP (Internet Protocol)

The network layer protocol that holds together the Internet

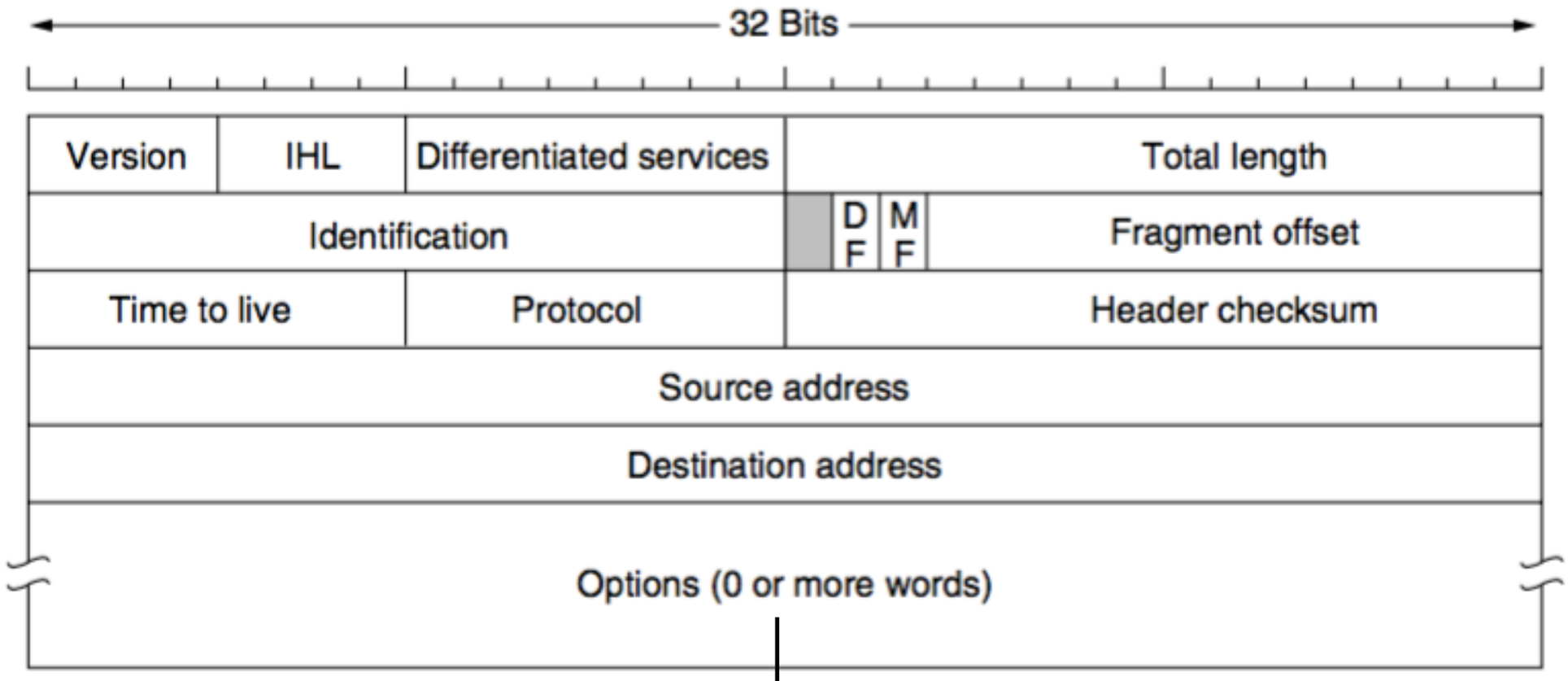


The IP Version 4 Protocol



Version: IPv4 or IPv6
IHL: Tells how long the header is (min value 5, max value 15)
Differentiated services: Service class, congestion notification information
Total length: Everything in the datagram (max value 65,535)
Identification: Which packet the fragment belongs to
DF: Don't fragment (used to discover the path MTU)
MF: More fragments
Fragment offset: Where in the current packet this fragment belongs
Time to live: Counter used to limit packet lifetimes (traceroute exploits this)
Protocol: TCP, UDP, etc.
Header checksum: Assumed to be zero upon arrival
Options: Include information not present in the original design

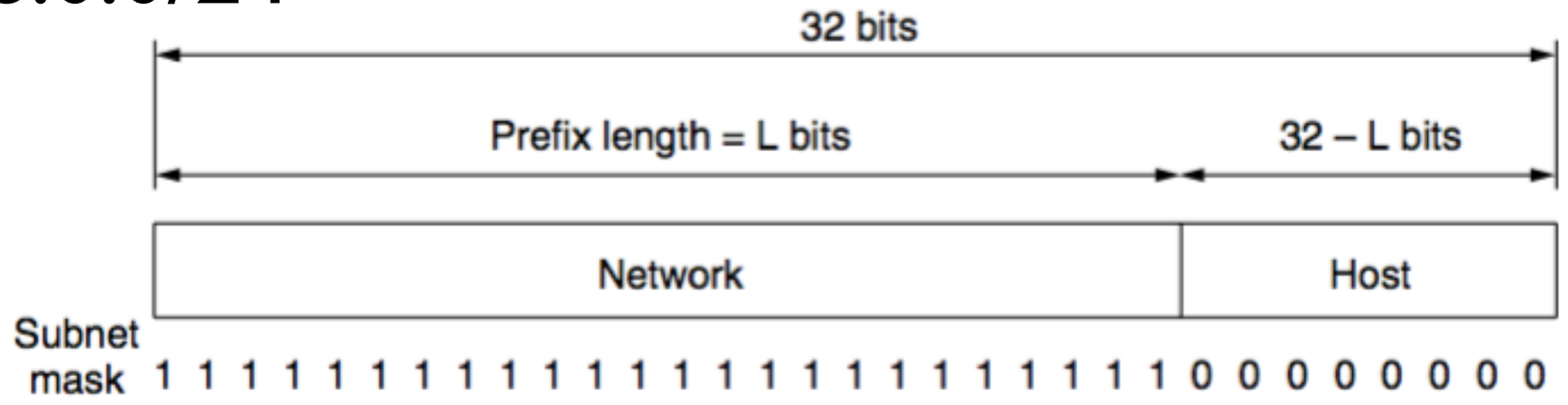
The IP Version 4 Protocol Options



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

IP Addresses

128.208.0.0/24



255.255.255.0

The network portion is in the top bits (prefix) and a host portion in the bottom bits

The network portion has the same value for all hosts on a single network

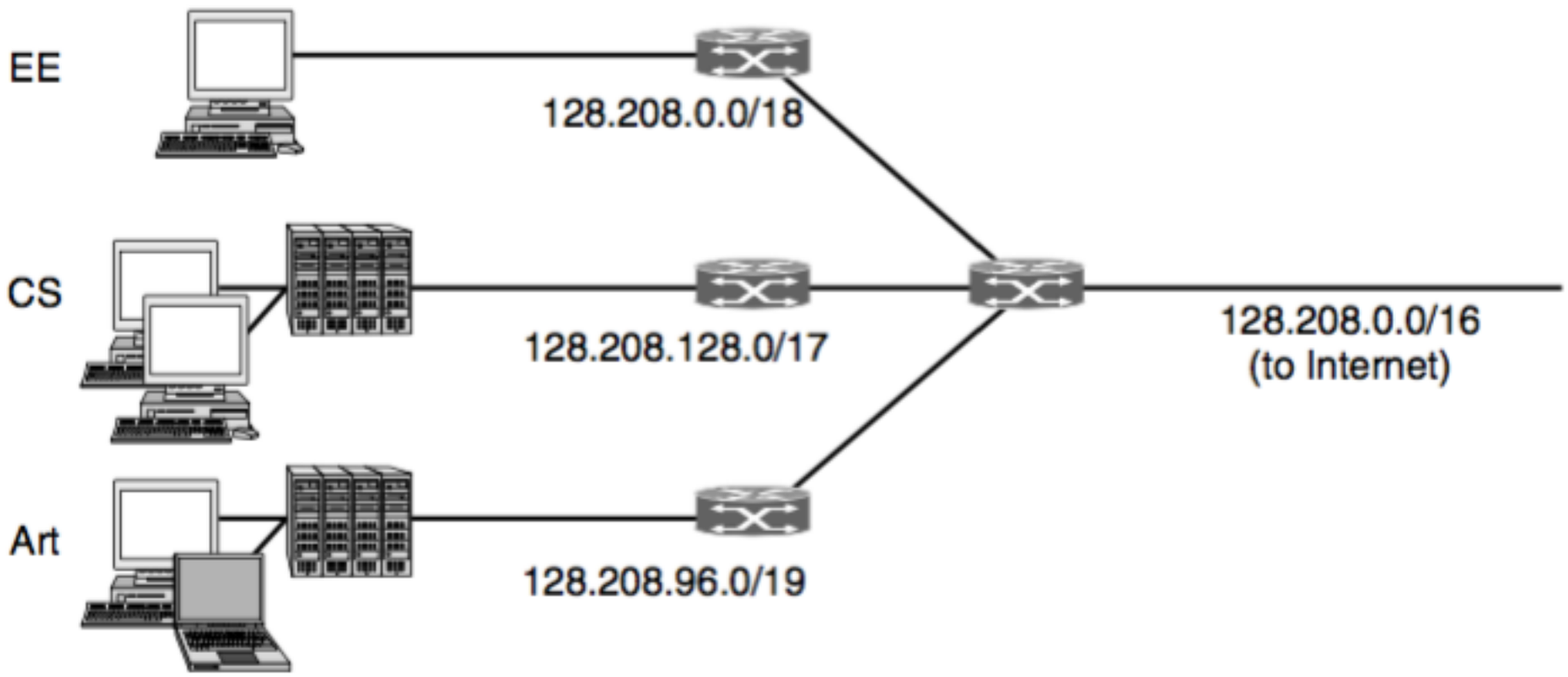
By using a hierarchy, routers need to keep routes for only around 300,000 prefixes

Subnets

Network numbers are managed by a nonprofit corporation called ICANN (Internet Corporation for Assigned Names and Numbers)

Computer Science:	10000000	11010000	1|xxxxxxx	xxxxxxxx
Electrical Eng.:	10000000	11010000	00|xxxxxx	xxxxxxxx
Art:	10000000	11010000	011|xxxxx	xxxxxxxx

Here, the vertical bar (|) shows the boundary between the subnet number and the host portion.



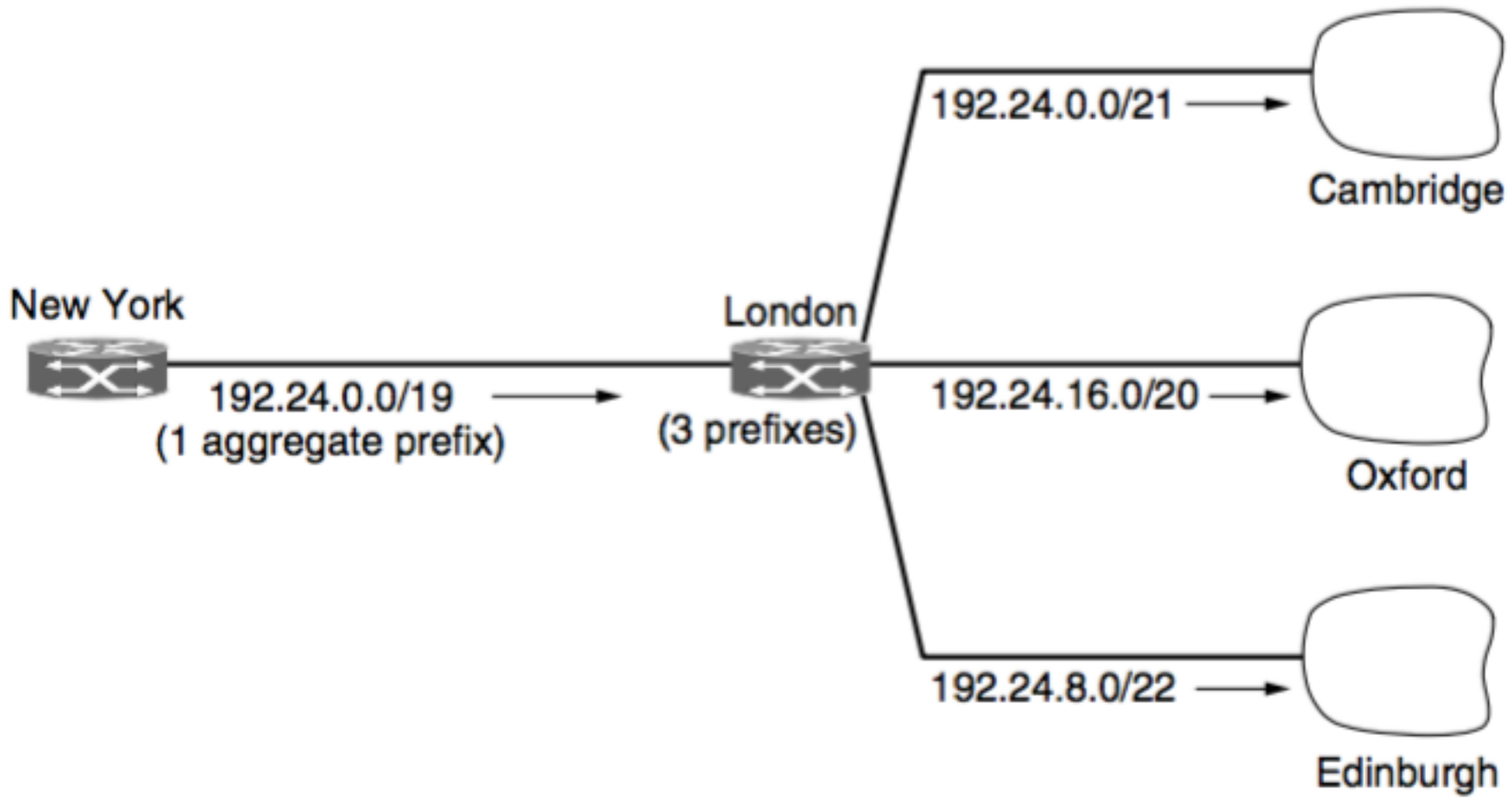
CIDR—Classless InterDomain Routing

Routers in ISPs and backbones in the middle of the Internet must know which way to go to get to every network

Route aggregation (supernet)

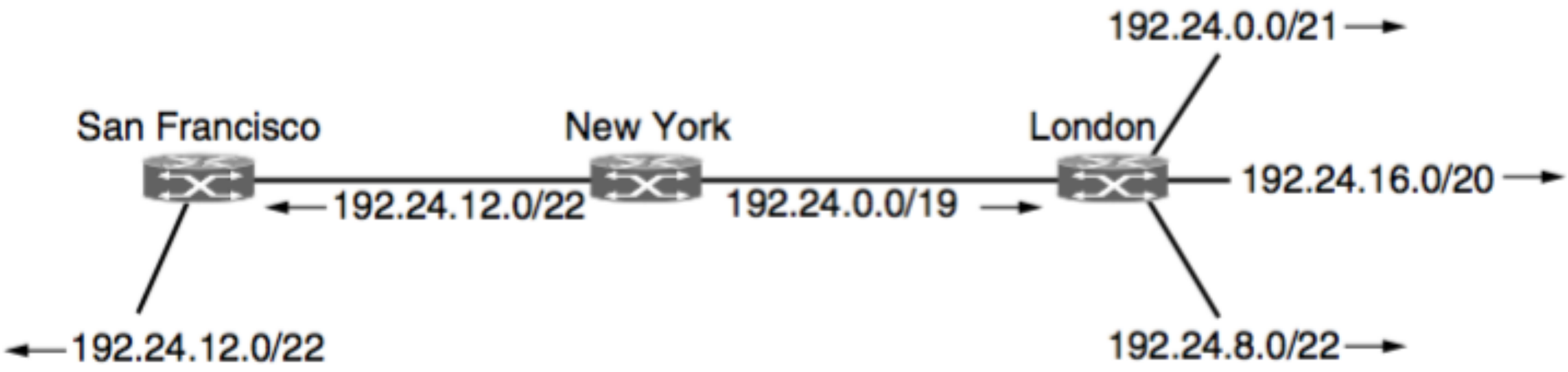
Combine multiple small prefixes into a single large prefix

University	First address	Last address	How many	Prefix
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	194.24.12.0/22
Oxford	194.24.16.0	194.24.31.255	4096	194.24.16.0/20

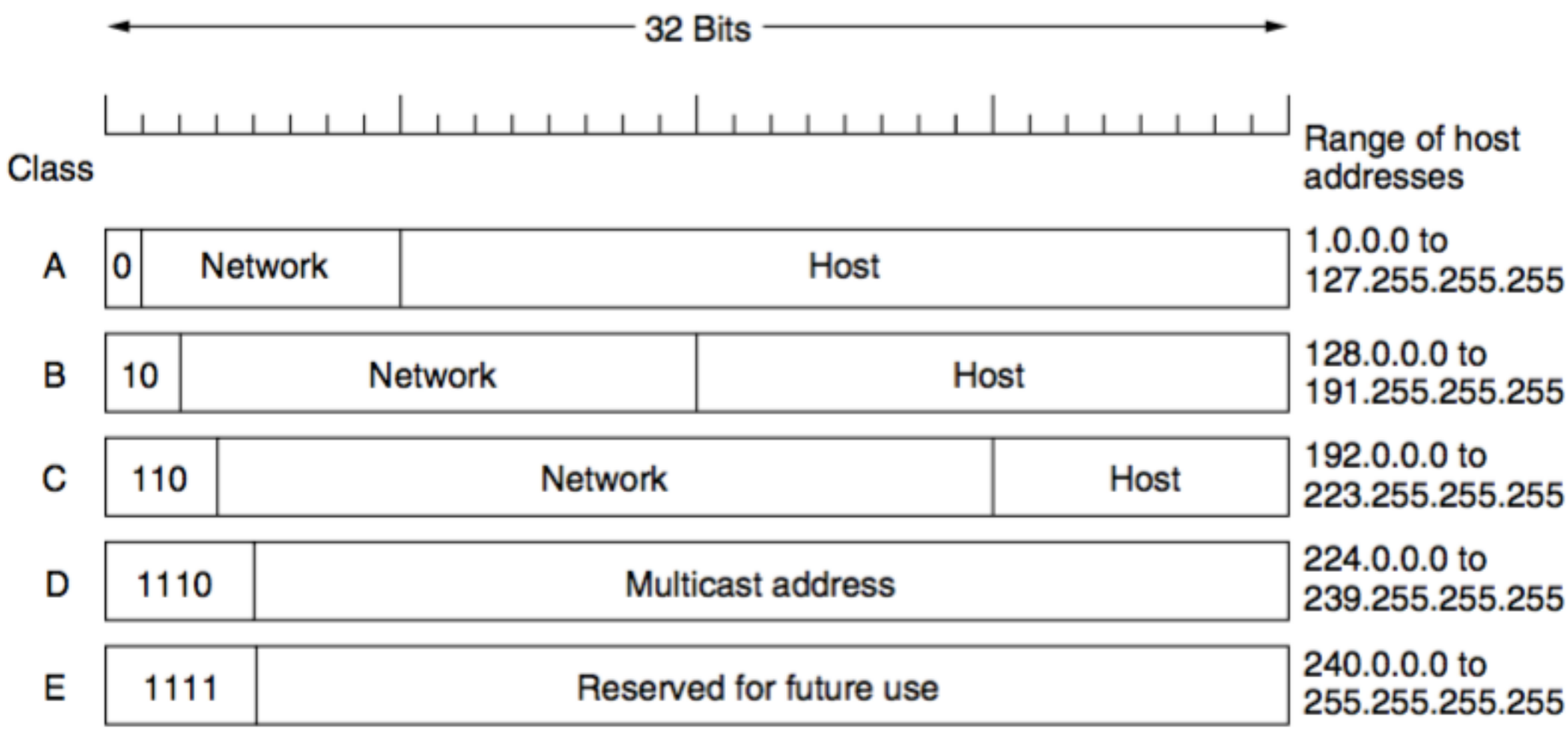


CIDR—Classless InterDomain Routing

1. When a packet comes in, the routing table is scanned to determine if the destination lies within the prefix.
2. It is possible that multiple entries with different prefix lengths will match, in which case the entry with the longest matching prefix is used.
3. If there is a match for a /20 mask and a /24 mask, the /24 entry is used to look up the outgoing line for the packet.



Classful Addressing



Before 1993

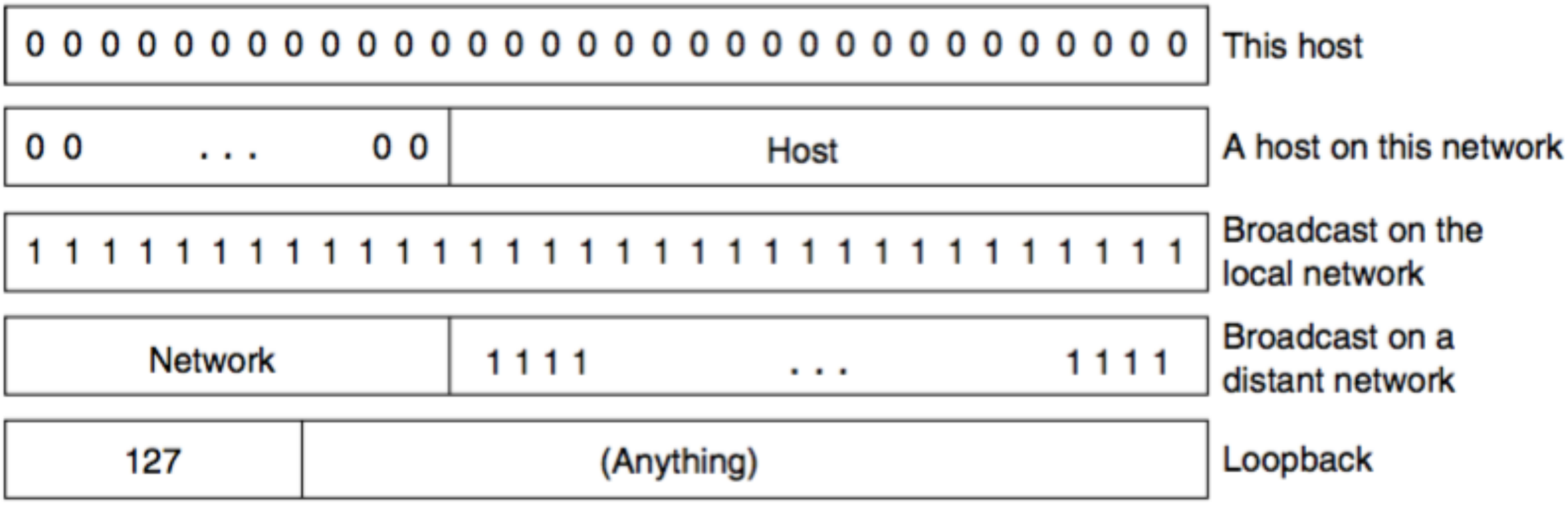
Unlike CIDR the sizes of the address blocks are fixed.

Today, the bits that indicate whether an IP address belongs to class A, B, or C network are no longer used.

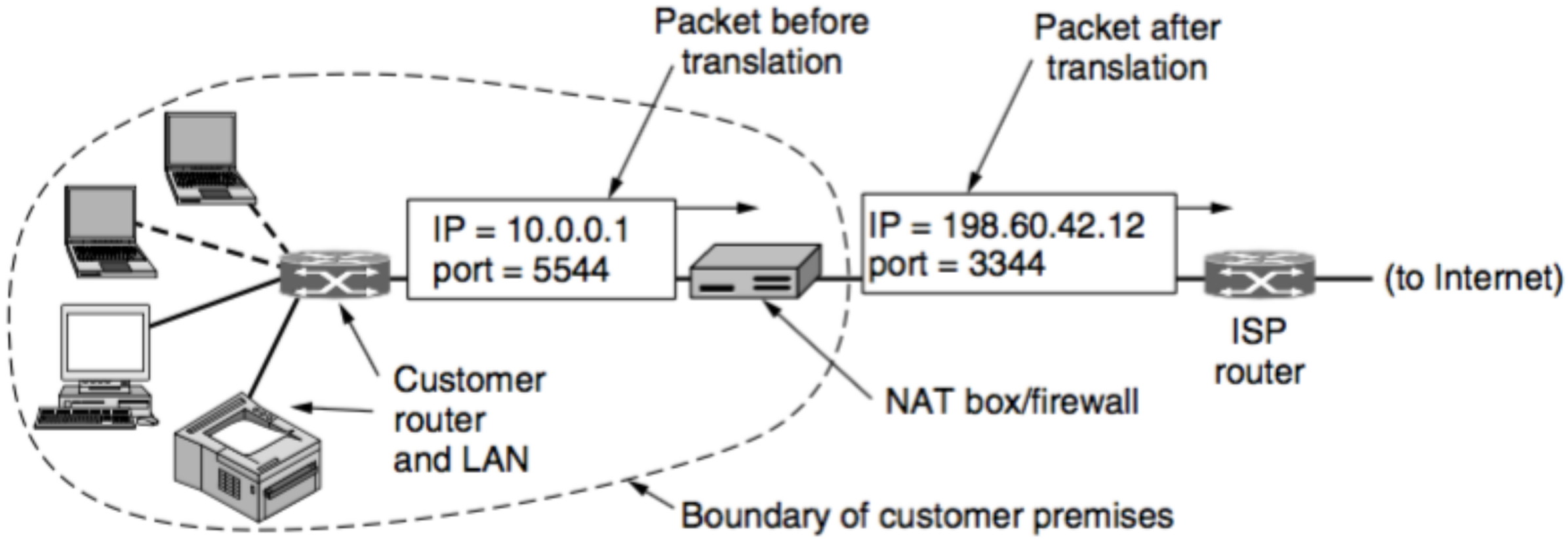
Class D addresses continue to be used in the Internet for multicast.

Special Addressing

0.0.0.0: This network, this host
255.255.255.255: All hosts on the network (broadcast)
127.xx.xx.xx: Reserved for loopback testing



NAT—Network Address Translation



Whenever an outgoing packet enters the NAT box, the 10.x.y.z source address is replaced by the customer's true IP address.

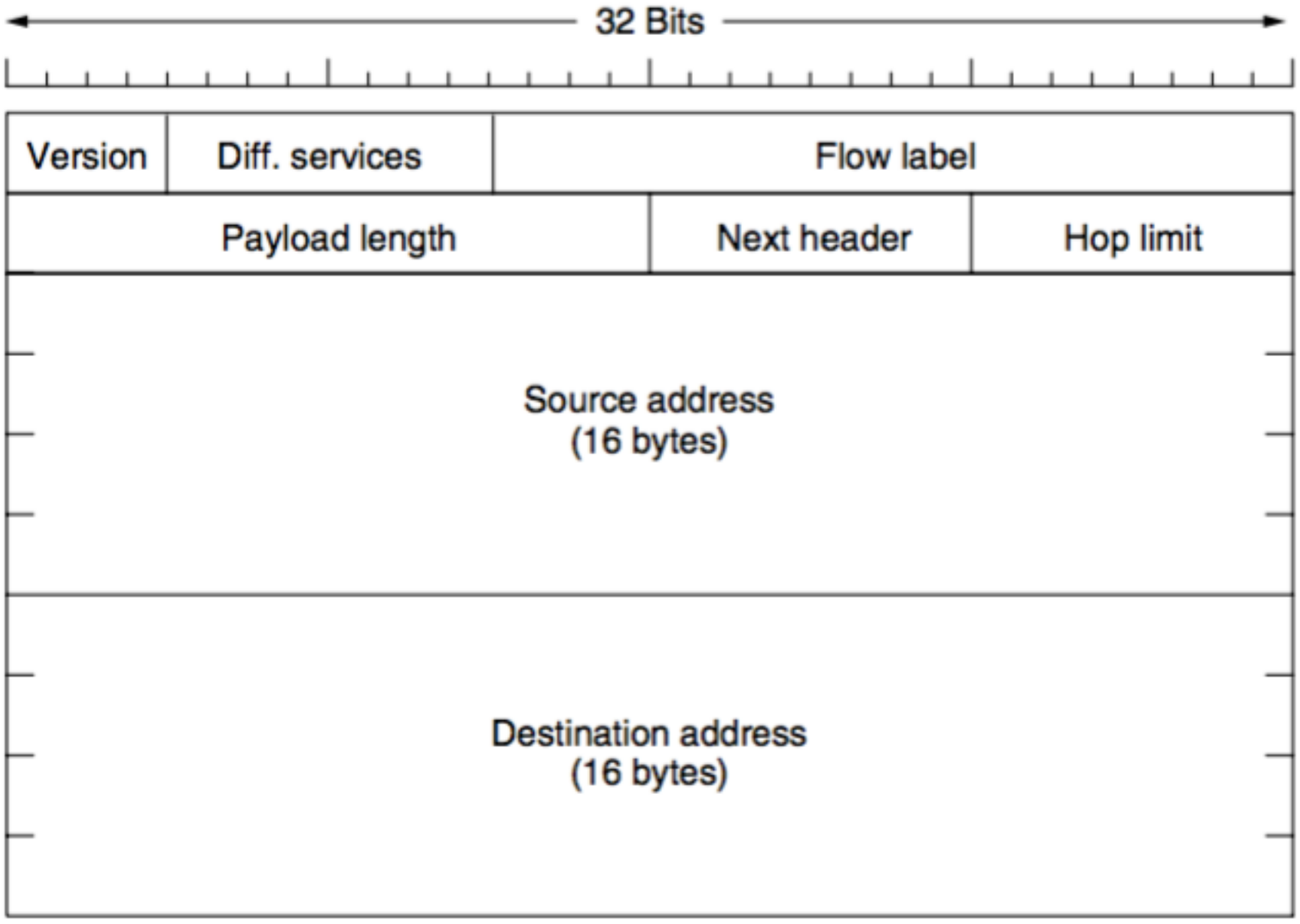
When a packet arrives at the NAT box from the ISP, the Source port in the TCP header is extracted and used as an index into the NAT box's mapping table.

IP Version 6

IPv4: 32-bit
IPv6: 128-bit

1. Support billions of hosts, even with inefficient address allocation.
2. Reduce the size of the routing tables.
3. Simplify the protocol, to allow routers to process packets faster.
4. Provide better security (authentication and privacy).
5. Pay more attention to the type of service, particularly for real-time data.
6. Aid multicasting by allowing scopes to be specified.
7. Make it possible for a host to roam without changing its address.
8. Allow the protocol to evolve in the future.
9. Permit the old and new protocols to coexist for years.

The Main IPv6 Header



Version: IPv4 or IPv6
Differentiated services: Service class, congestion notification information
Flow label: Mark groups of packets that have the same requirements
Payload length: Everything in the datagram excluding the header (max value 65,535)
Next header: Which extension headers follow this one
Hop limit: Used to keep packets from living forever

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

Hop-by-hop extension header

	Type	Length	Value
Next header	0	194	4
Jumbo payload length			

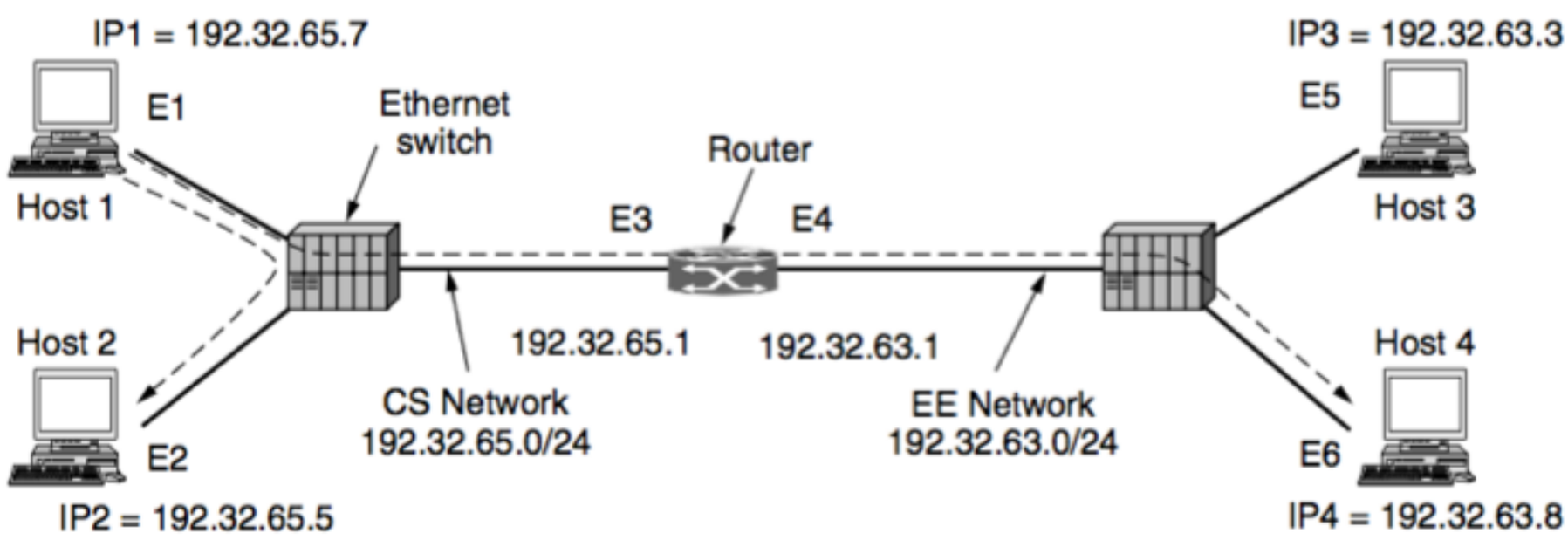
Routing extension header

Next header	Header extension length	Routing type	Segments left
Type-specific data			

IMCP—The Internet Control Message Protocol

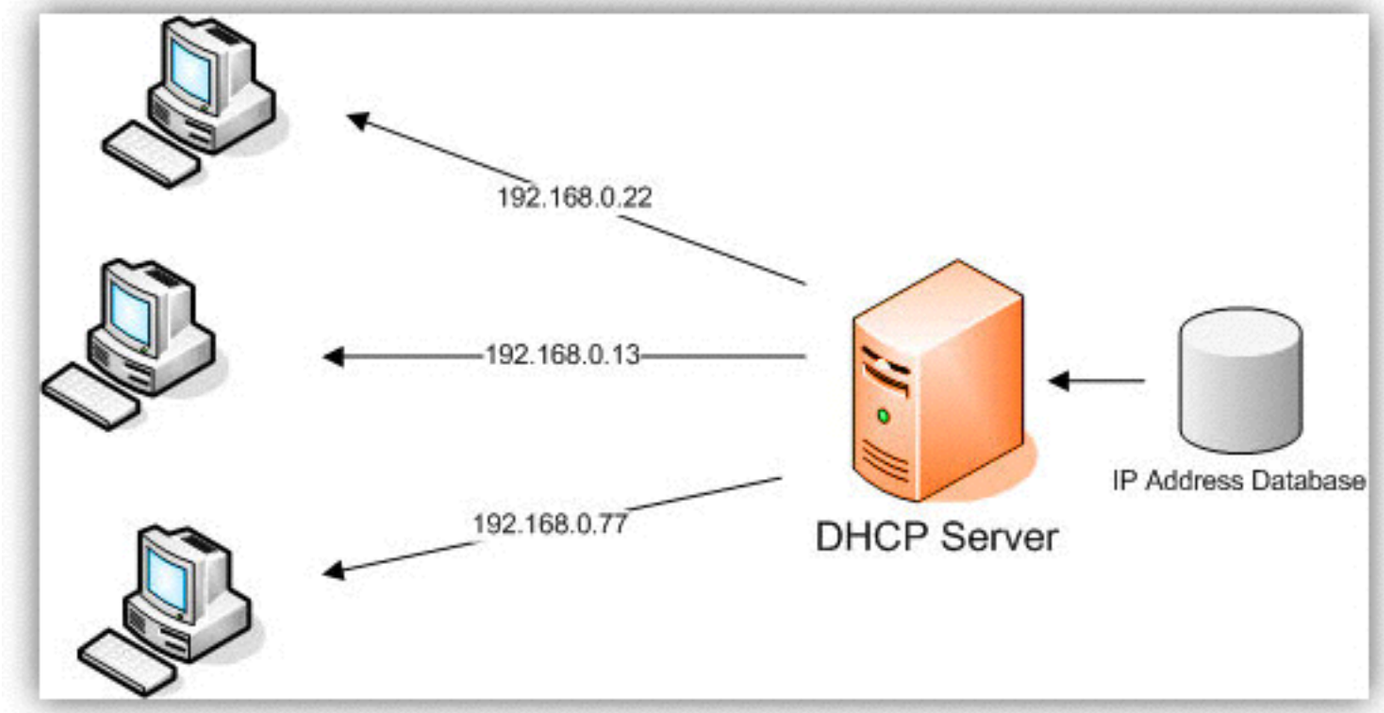
Message type	Description
Destination unreachable	Packet could not be delivered
Time exceeded	Time to live field hit 0
Parameter problem	Invalid header field
Source quench	Choke packet
Redirect	Teach a router about geography
Echo and echo reply	Check if a machine is alive
Timestamp request/reply	Same as Echo, but with timestamp
Router advertisement/solicitation	Find a nearby router

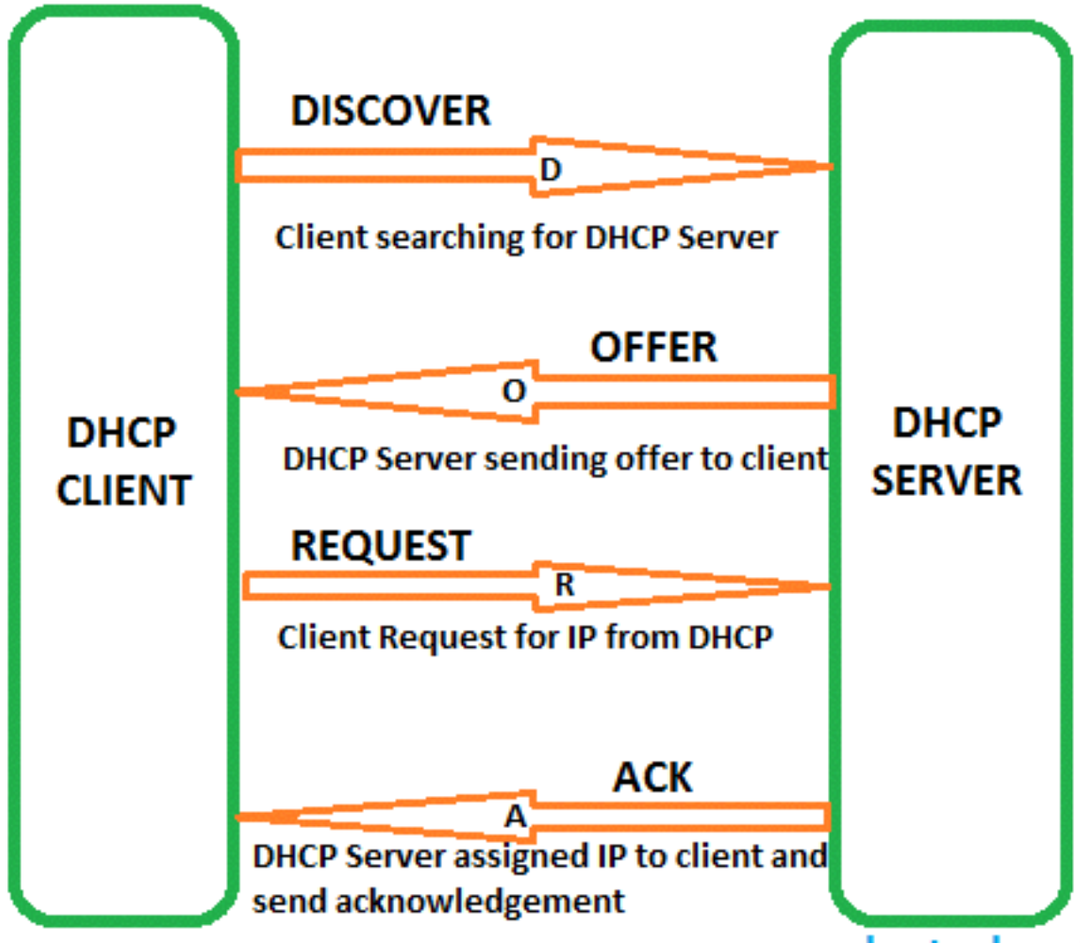
ARP—The Address Resolution Protocol



Frame	Source IP	Source Eth.	Destination IP	Destination Eth.
Host 1 to 2, on CS net	IP1	E1	IP2	E2
Host 1 to 4, on CS net	IP1	E1	IP4	E3
Host 1 to 4, on EE net	IP1	E4	IP4	E6

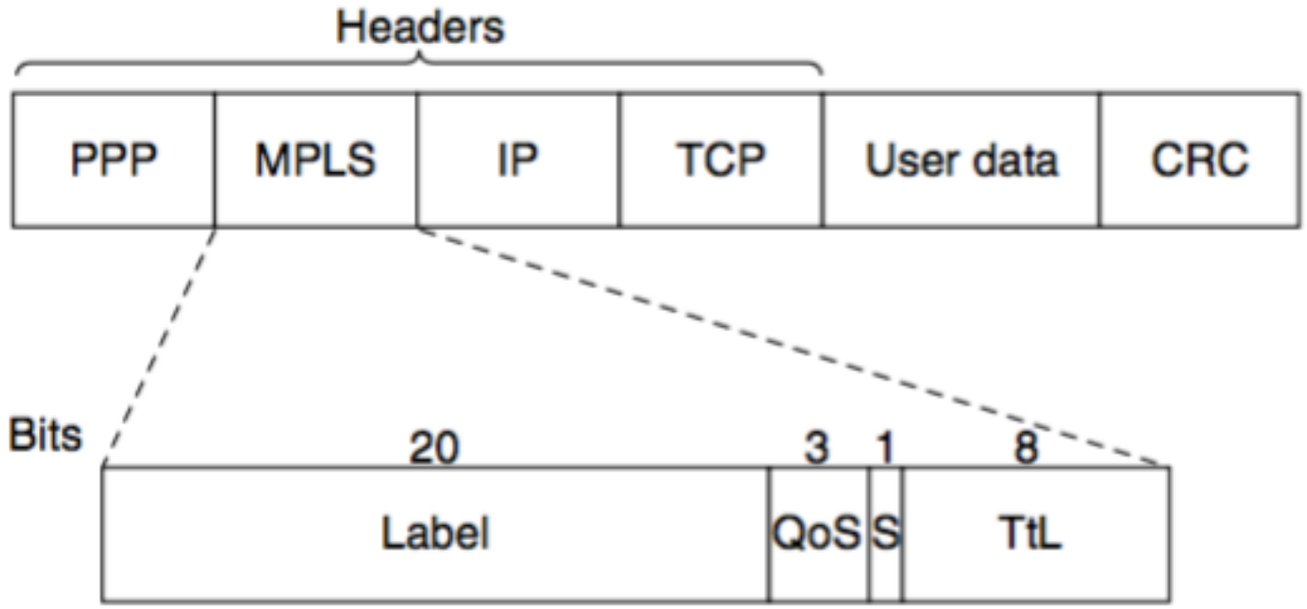
DHCP—The Dynamic Host Configuration Protocol

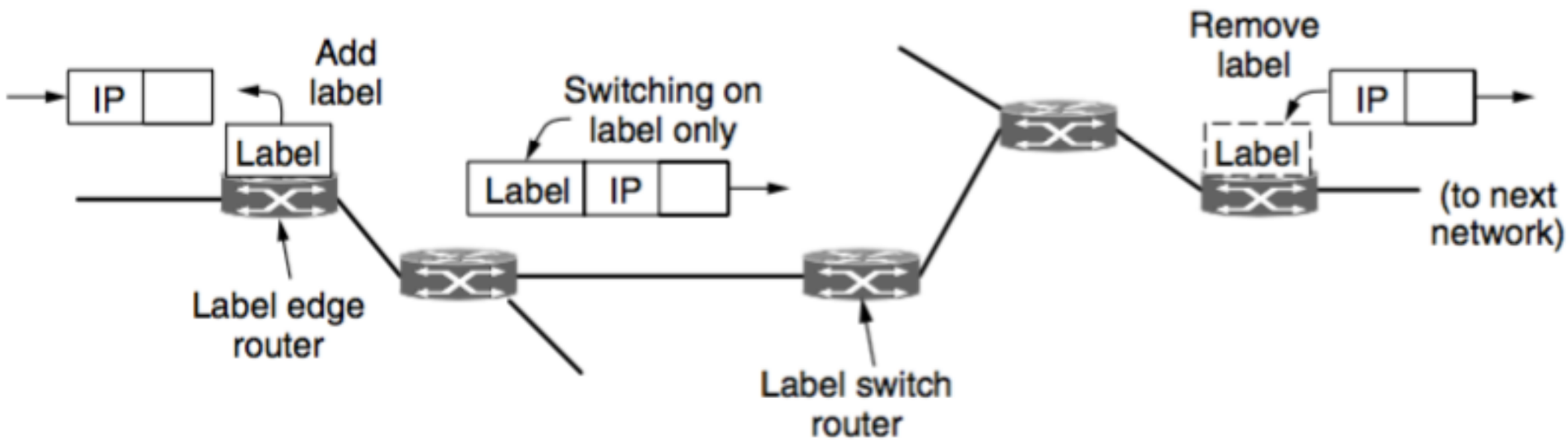




Label Switching and MPLS

MPLS adds a label in front of each packet, and forwarding is based on the label rather than on the destination address.



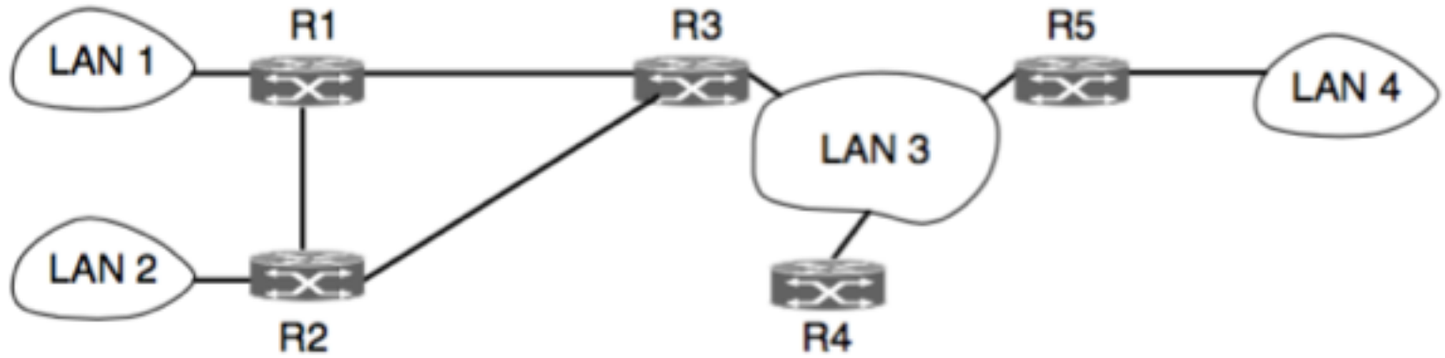


OSPF—An Interior Gateway Routing Protocol

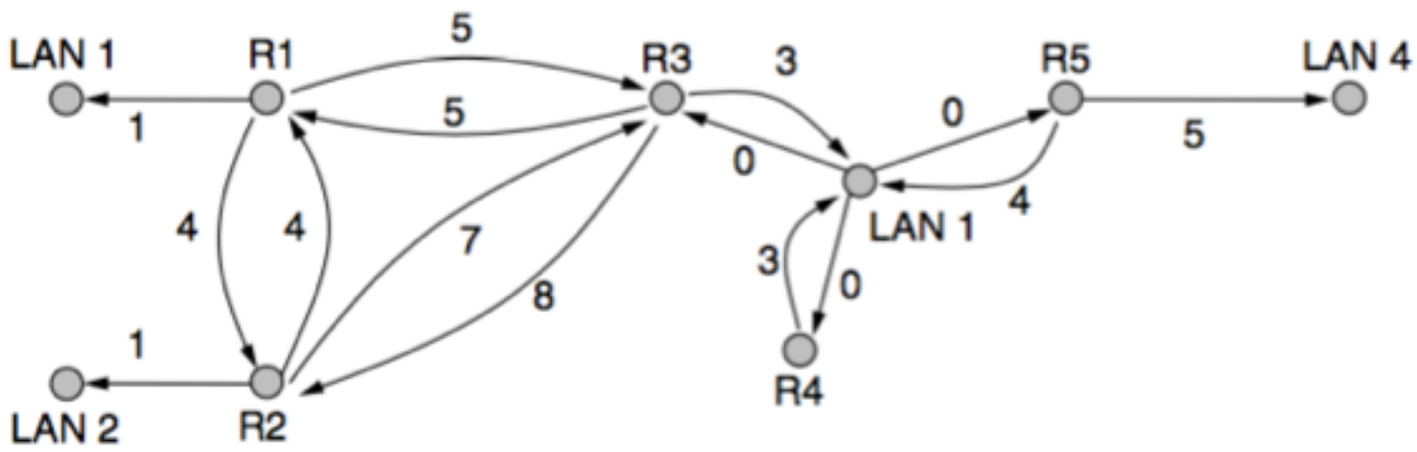
Link state protocol for intradomain routing.

<u>OSPF requirements</u>

1. Published in the open literature
2. Support a variety of distance metrics
3. Dynamic algorithm
4. Support routing based on type of service
5. Load balancing, splitting the load over multiple lines
6. Support for hierarchical systems
7. Security

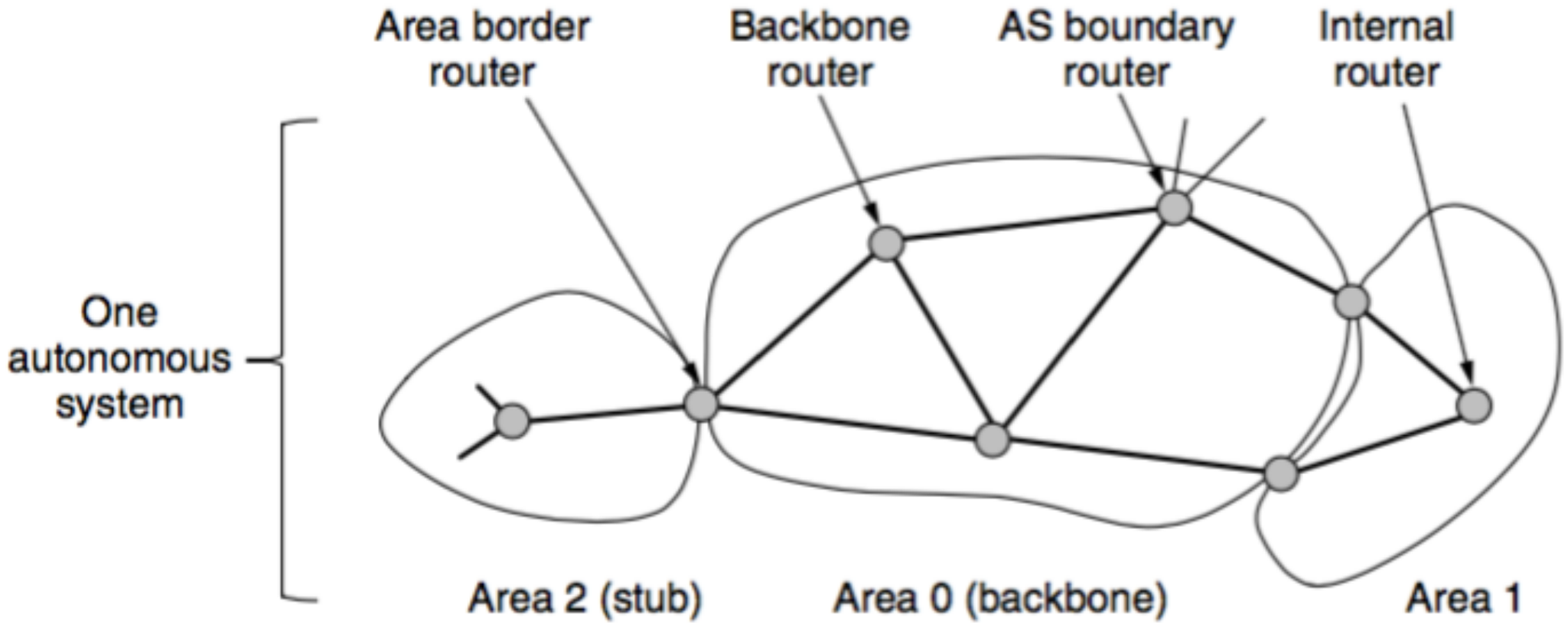


(a)



(b)

OSPF—An Interior Gateway Routing Protocol



OSPF messages

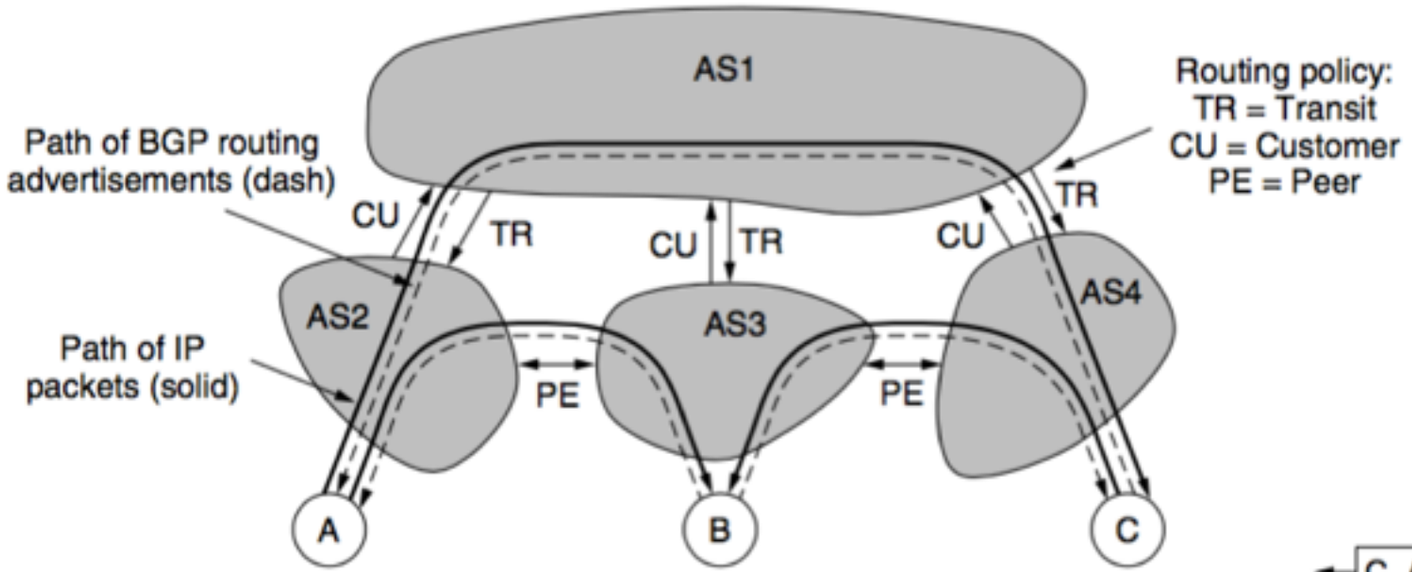
Message type	Description
Hello	Used to discover who the neighbors are
Link state update	Provides the sender's costs to its neighbors
Link state ack	Acknowledges link state update
Database description	Announces which updates the sender has
Link state request	Requests information from the partner

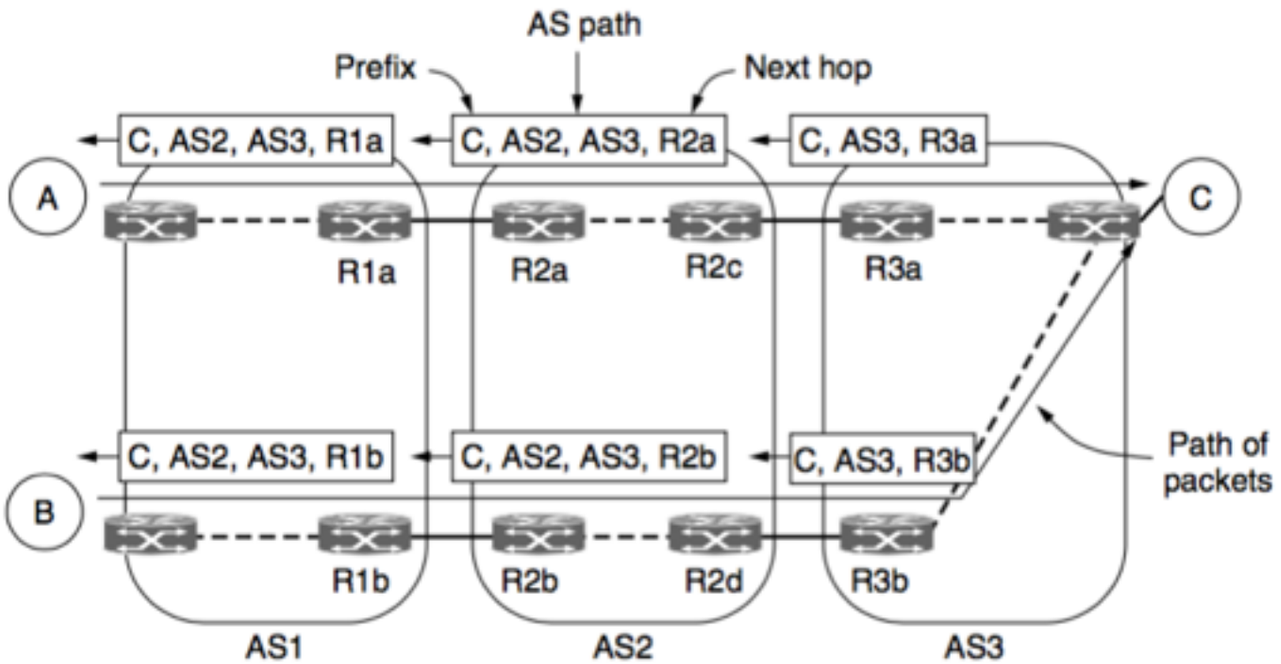
BGP—The Exterior Gateway Routing Protocol

interdomain routing protocol

Examples of policies

1. Do not carry commercial traffic on the educational network.
2. Never send traffic from the Pentagon on a route through Iraq.
3. Use TeliaSonera instead of Verizon because it is cheaper.
4. Don't use AT&T in Australia because performance is poor.
5. Traffic starting or ending at Apple should not transit Google.



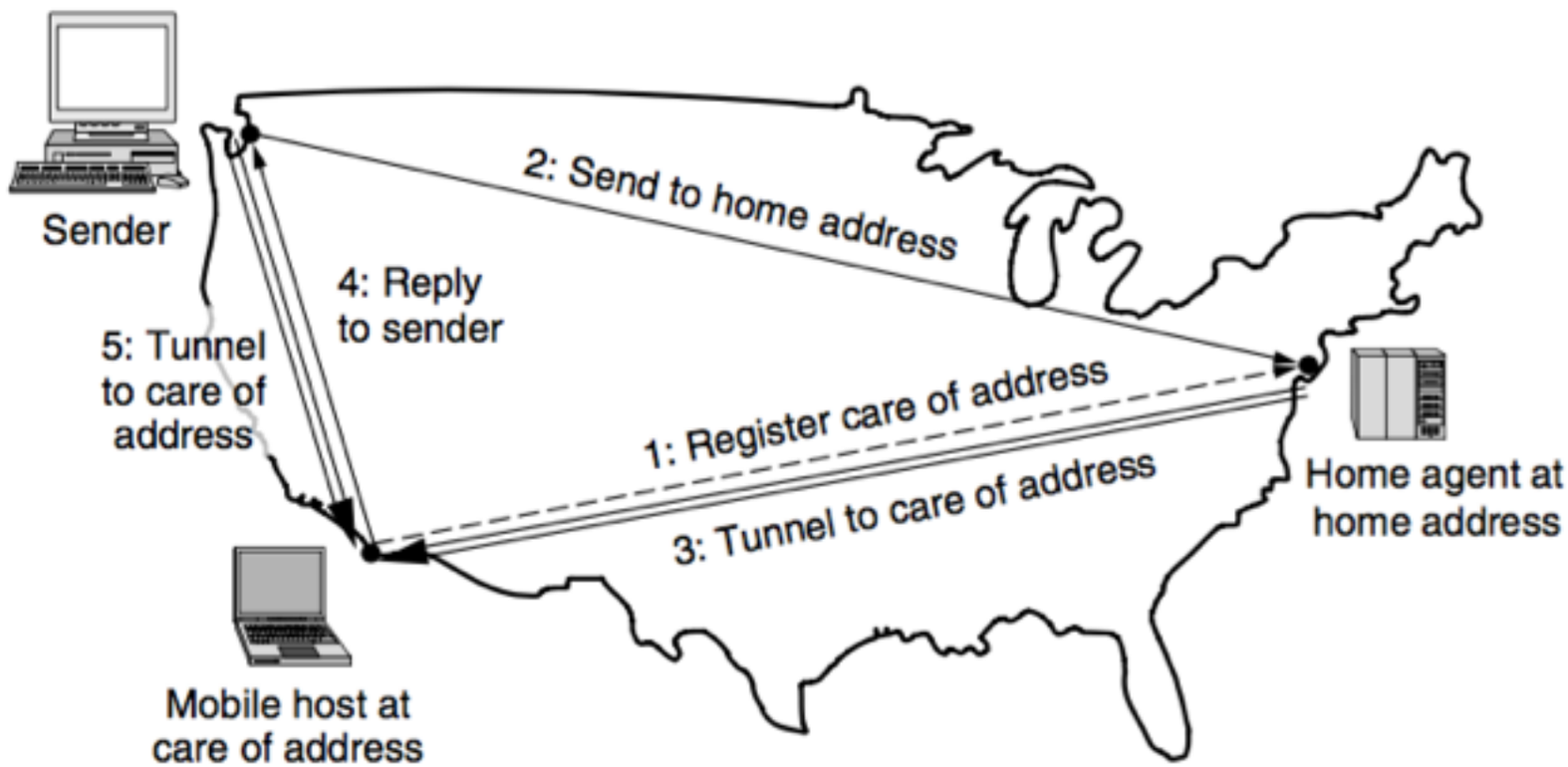


Internet Multicasting

Multicasting uses class D IP addresses
IP addresses 224.0.0.0/24 is reserved for multicast
224.0.0.1 : All systems on a LAN
224.0.0.2 : All routers on a LAN
224.0.0.5 : All OSPF routers on a LAN
224.0.0.251: All DNS servers on a LAN

Mobile IP

1. Each mobile host must be able to use its home IP address anywhere.
2. Software changes to the fixed hosts are not permitted.
3. Changes to the router software and tables are not permitted.
4. Most packets for mobile hosts should not make detours on the way.
5. No overhead should be incurred when a mobile host is at home.



講義日程（2Q）

		授業計画		課題
06/14	第９回	ネットワーク層１ ルーティング・輻輳制御	５章	ルーティングの種類を理解し 輻輳制御手法を説明できる
06/21	第１０回	ネットワーク層２ インターネットとサービス品質	５章	インターネットの制御プロトコルを理解し ネットワーク間の接続について説明できる
06/28	第１１回	トランスポート層１ トランスポート・プロトコルの要素	６章	誤り制御とフロー制御を理解し 輻輳制御について説明できる
07/05	第１２回	トランスポート層２ UDP と TCP	６章	TCP の信頼性を理解し TCP のコネクション管理を説明できる
07/12	第１３回	アプリケーション層 DNS, 電子メール, www	７章	DNS, 電子メール, www のしくみを理解し ストリーミング，P2P について説明できる
07/26	第１４回	ネットワークセキュリティ１ 対称鍵暗号，公開鍵暗号	８章	暗号アルゴリズムを理解し SHA-1,2 と RSA について説明できる
08/02	第１５回	ネットワークセキュリティ２ デジタル署名，認証プロトコル	８章	電子メール,Web のセキュリティ の脅威について把握できる