Computer Networks

-Transport/Network layer I.-

College of Information Science and Engineering
Ritsumeikan University

RITSUMEIKAN UNIVERSITY

W3 short test (1)

- What is the difference between the Internet and an internet?
  - Any collection of interconnected networks is called an internetwork or internet. The Internet is a specific internet that refers to the world-wide publicly available Internet Protocol network.
- Why evolvability is an important design goal for networks?
  - Mainly because networks grow larger and new designs emerge that need to be connected to the existing network.

W3 short test (2)

- What is the difference between services and protocols?
  - A service is a set of primitives that a layer provides to the layer above it, and it is not about how the operations are implemented. On the other hand, a protocol is a set of rules governing the format and meaning of the packets exchanged by the peer entities within a layer on different machines.
- Which layer is designed to allow peer entities on the source and destination hosts to carry on a conversation, and which reference models have it?
  - The transport layer. Both the OSI and TCP/IP reference models have this layer.

W3 recap (1)

- Human-readable domain names must be converted to IP addresses with the DNS
- Name resolution is the process of looking up a name a finding an address
- A DNS client issues a query to a local recursive resolver, which performs an iterative query to ultimately resolve the query
- The Internet is divided into top-level domains and many subdomains in a namespace hierarchy, involving non-overlapping zones
- The most common resource record 'A' is the IP address
- The email architecture consists of two kinds of subsystems: user agents and mail servers/message transfer agents speaking the SMTP
- RFC 5322 is the basic ASCII Internet message format
- MIME is about multimedia extensions to the basic format

W3 recap (2)

- One of the main protocols used for the final email delivery is IMAP, an improvement over POP3
- Webmail is an alternative to IMAP and SMTP for providing email service, using the Web as an interface
- The World Wide Web is a popular architectural framework for accessing linked content all over the Internet
- Fetching and rendering a static and dynamic pages involves HTTP/HTTPS requests to many servers
- Each page is assigned an URL that is the page's worldwide name with three parts
- There are several common URL protocols for a variety of purposes
- HTTP/HTTPS is a request-response protocol with different request methods

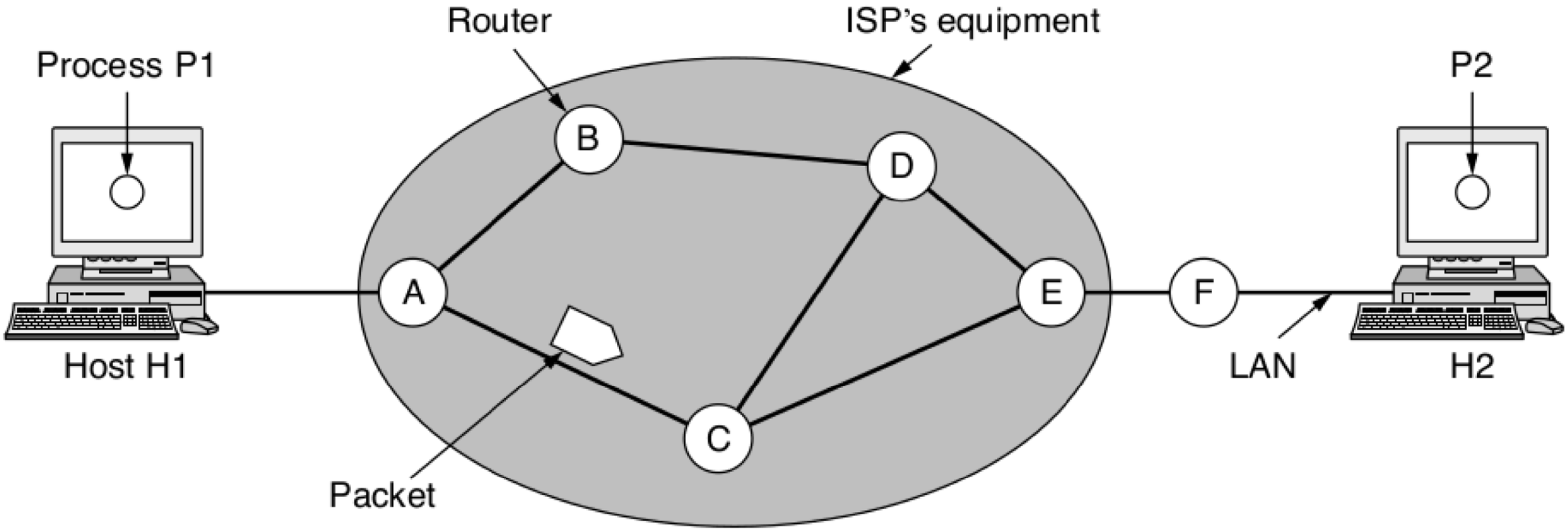
Agenda

- Network layer design
- Traffic management and QoS
- Internetworking
- The network layer in the Internet
- IP version 4 protocol
- IP addresses
- Summary

Network layer basics

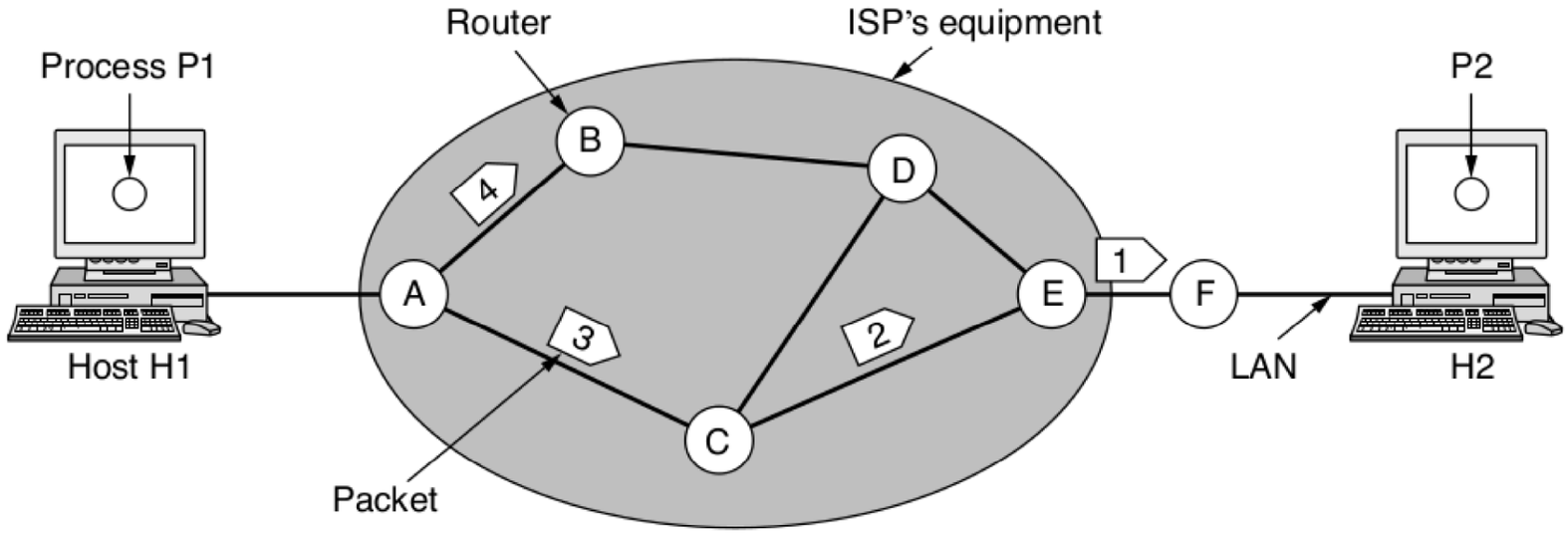
- The network layer is concerned with getting packets from the source to the destination
  - may require making many hops at intermediate routers along the way
  - the lowest layer that deals with end-to-end transmission
- **Store-and-Forward packet switching**
  - the host with a packet to send transmits it to the nearest router (LAN, ADSL, etc.), where the packet is stored until it has fully arrived and the link has finished its processing
  - then forwarded to the next router until it reaches the destination
- In the case of a connectionless service, packets or **datagrams** are injected into the network individually and routed independently of each other (e.g., IP)
- If connection-oriented service is used, a path from the source router all he way to the destination router must be established before any data packets can be sent, where the connection is called **VC** (Virtual Circuit) (e.g., ATM)

Store-and-Forward packet switching



Routing for a datagram network

- The algorithm that manages the routing tables and makes the routing decisions is called the **routing algorithm**



A's table (initially)

A	–
B	B
C	C
D	B
E	C
F	C

A's table (later)

A	–
B	B
C	C
D	B
E	B
F	B

C's table

A	A
B	A
C	–
D	E
E	E
F	E

E's table

A	C
B	D
C	C
D	D
E	–
F	F

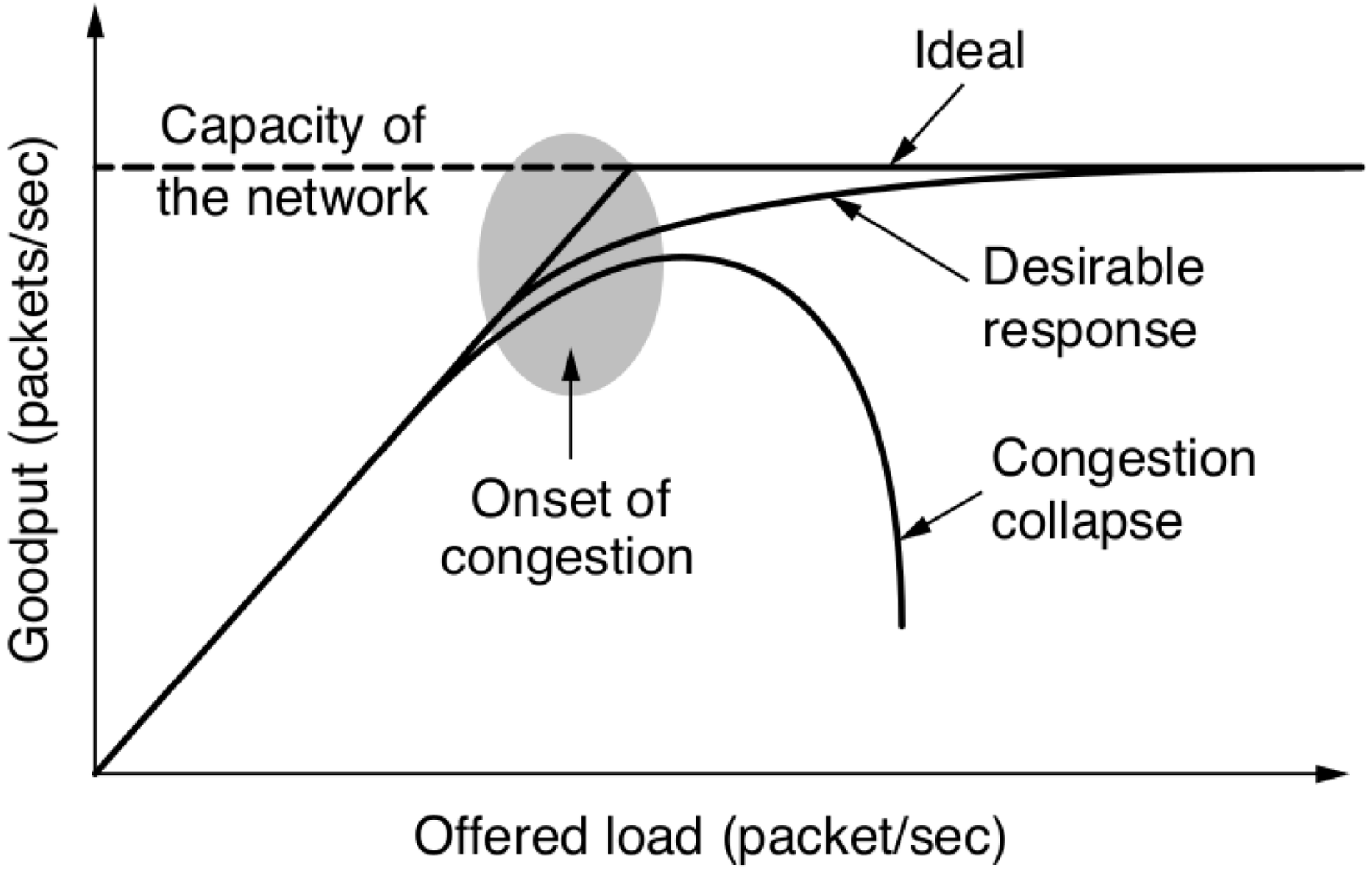
Routing algorithms

- In practice, the main function of the network layer is routing packets from source machine to destination machine
- One can think of a router as having two processes inside it:
  - one of them handles each packet as it arrives, looking up the outgoing line to use for it in the routing tables: **forwarding**
  - the other is responsible for filling in and updating the routing tables: **the routing algorithm**
- Two main types of routing algorithms
  - nonadaptive algorithms and **static routing**: the route choices are computed offline in advance, and loaded to the routers when the network is booted
  - adaptive algorithms and **dynamic routing**: change their routing decisions to reflect changes in the network topology

Congestion (1)

- **Congestion** happens when too many packets introduce packet delay and loss that degrades performance
- **Congestion management**/**Traffic management**
  - the network layer does not explicitly eliminates congestion, but routers, switches, etc. can be configured to mitigate the effects of congestion (e.g., tell the sender to reduce sending rate, using different paths in the network)
- **Congestion collapse** happens when increasing load on the network results in less traffic being successfully delivered (packets delayed inside the network are no longer useful when they leave the network)
- **Goodput** is the rate at which useful packets are delivered

Congestion (2)

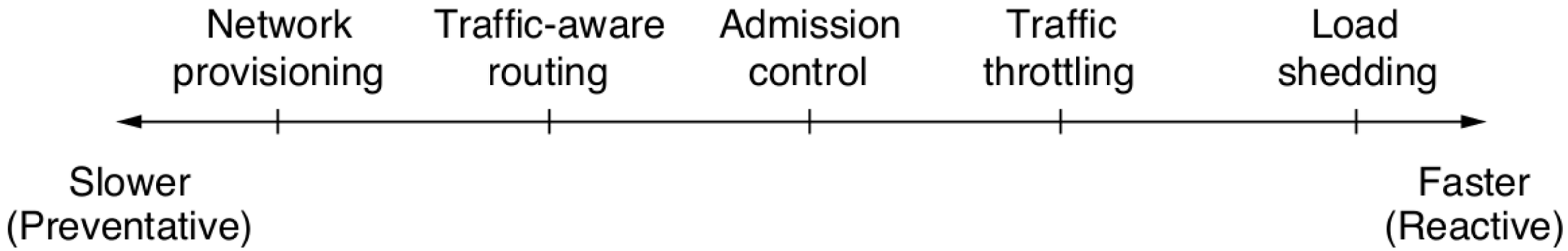


Traffic management approaches (1)

- Two main approaches to deal with congestion: increase the resources or decrease the load
- **Network provisioning** is about adding the physical resources needed to build a network that it can carry the traffic load intended (e.g., upgrade routers, add backups, etc.)
- **Traffic-aware routing** is about making the most of the existing network capacity by tailoring routes to traffic patterns that change during the day
- In simple terms, **admission control** is about denying senders the ability to send traffic if the network capacity cannot support it
- A network can request the sources of congestion to slow down sending rates or just slow down the traffic itself by **throttling**
- **Load shredding** is about discarding packets that the network cannot deliver (e.g., dropping traffic from a sender if it exceeds some rate)

Traffic management approaches (2)

- The different approaches are usually applied on different time scales to prevent congestion or react to it once it has occurred



QoS (1)

- Networks do not need to be lossless for reliable file transfer
  - some amount of loss can be repaired with retransmissions, and some amount of jitter (variation in delay or packet arrival times) can be smoothed by buffering packets at the receiver
  - there is nothing applications can do to help if the network provides too little bandwidth or there is too much delay
- **Overprovisioning** is about building a network with enough capacity for whatever traffic will be thrown at it
- **Packet scheduling algorithms** allocate router resources among the packets of a flow and between competing flows
  - Which of the buffered packets to send on the output line next? (e.g., FIFO)
- Different applications have different **QoS** (Quality of Service) requirements

QoS (2)

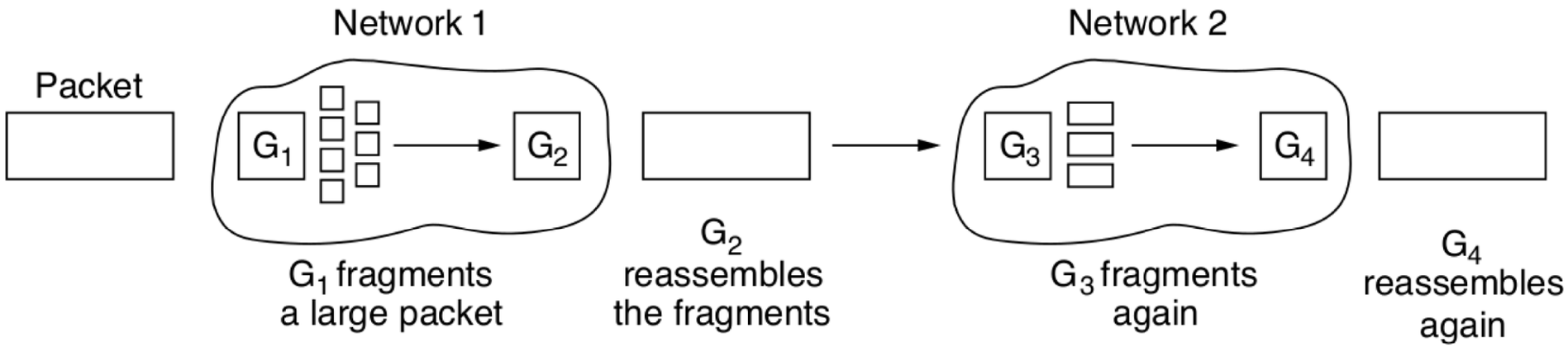
Application	Bandwidth	Delay	Jitter	Loss
Email	Low	Low	Low	Medium
File sharing	High	Low	Low	Medium
Web access	Medium	Medium	Low	Medium
Remote login	Low	Medium	Medium	Medium
Audio on demand	Low	Low	High	Low
Video on demand	High	Low	High	Low
Telephony	Low	High	High	Low
Videoconferencing	High	High	High	Low

Connecting heterogeneous network

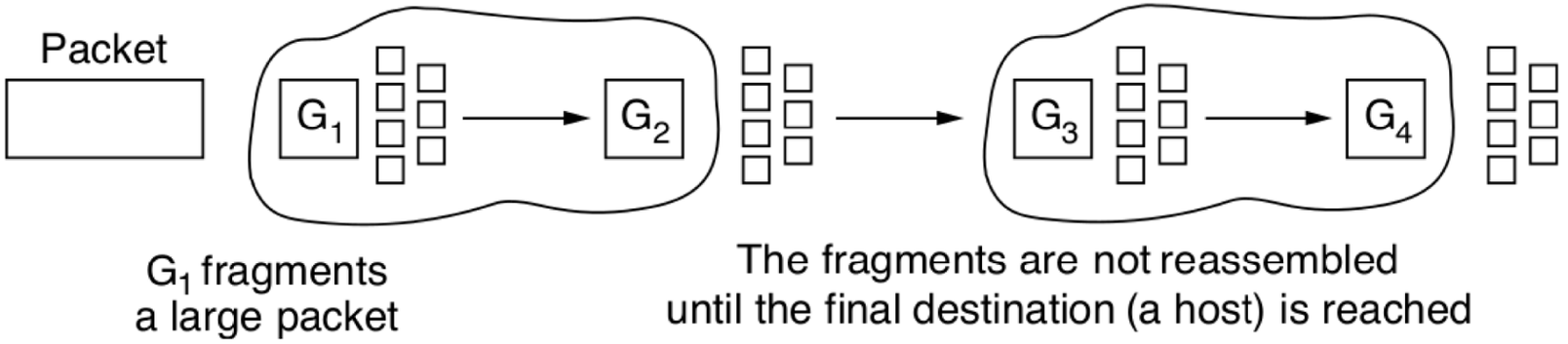
- Connecting heterogeneous networks with machines using different protocols in layers raises multiple issues
- Two basic approaches: use devices (gateways) that translate or convert packets or build a common layer on top of different networks
- Different routing algorithms, operators: two level routing
  - an intradomain gateway protocol within networks might differ
  - interdomain (exterior) gateway protocol across networks must be the same (called Border Gateway Protocol for the Internet)
- Supporting different packet sizes with **packet fragmentation**

Packet fragmentation

- Transparent vs. nontransparent

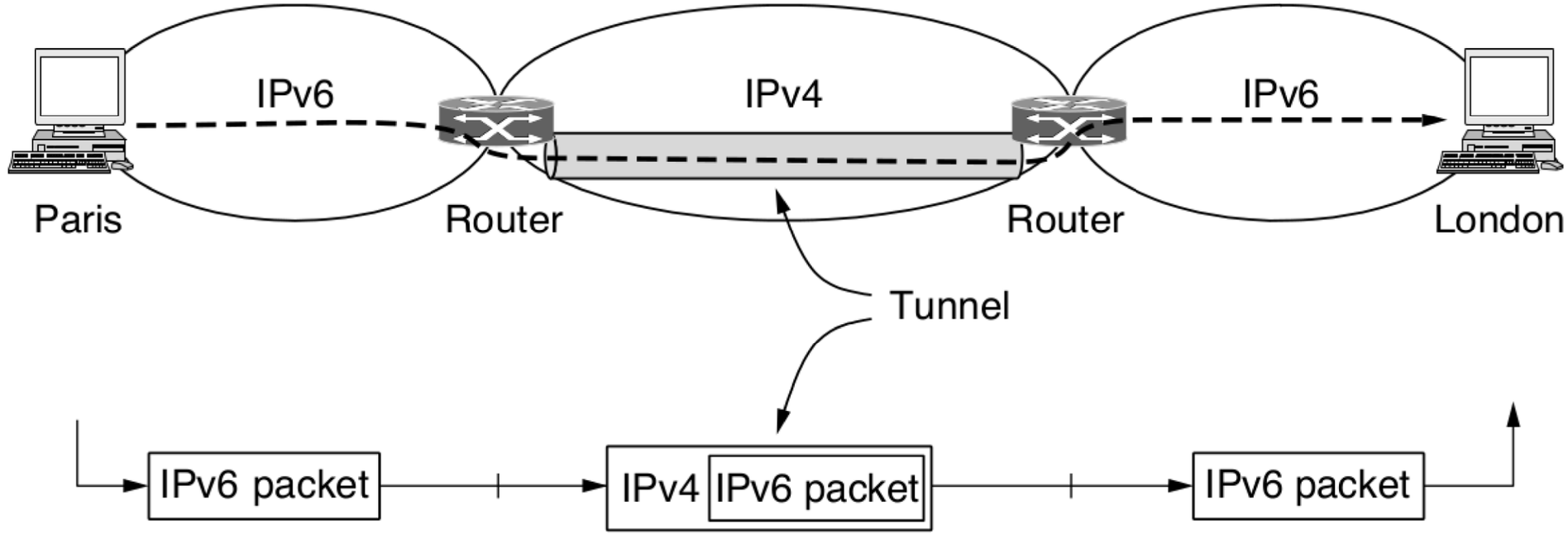


(a)



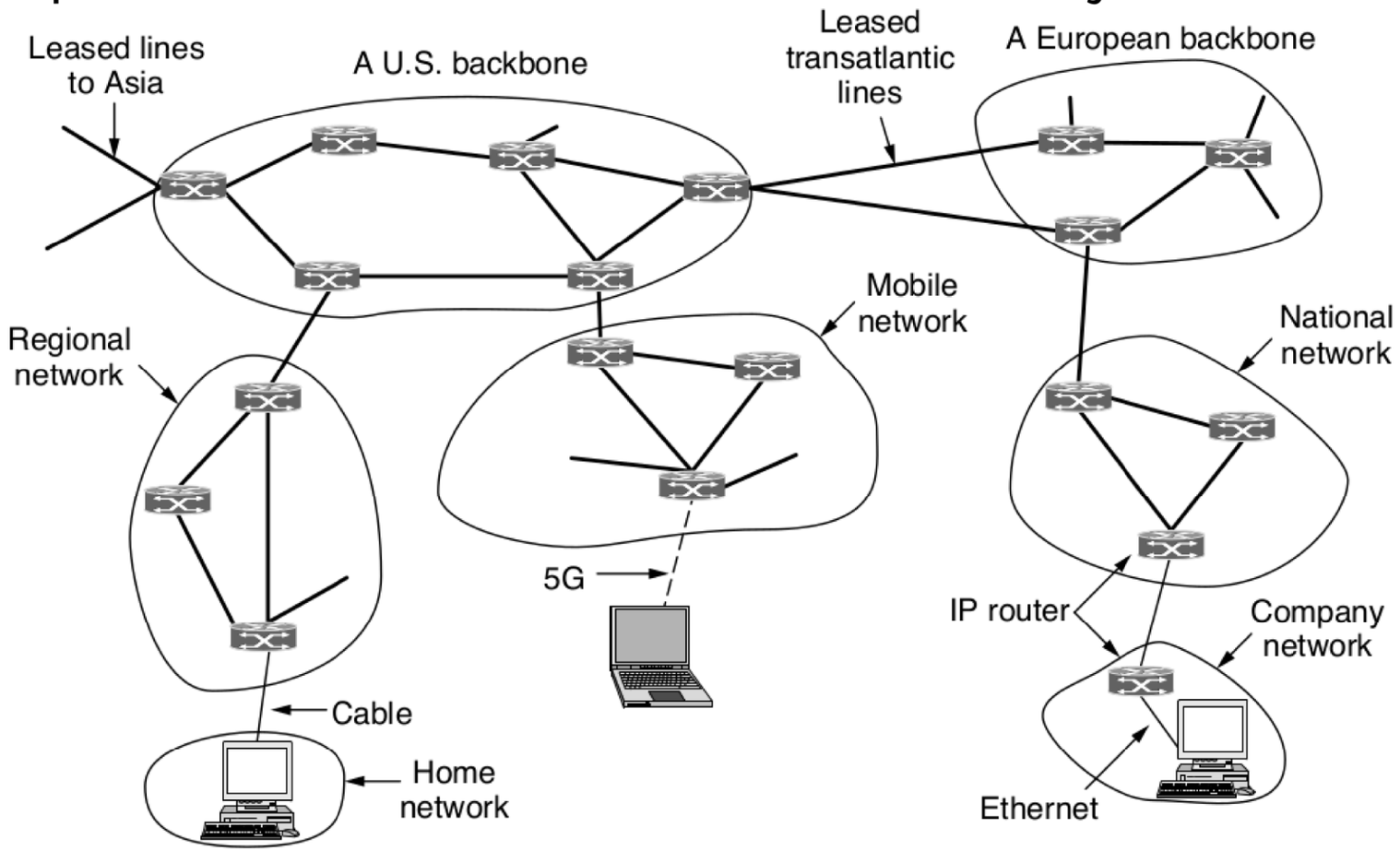
Tunneling

- If the source and destination hosts are on the same type of network but there is a different network between them, **tunneling** is used with a **multiprotocol router**
- Tunneling results in a **overlay** network (e.g., VPNs)



Interconnected collection of networks

- The Internet is a collection of networks using the **IP** (Internet Protocol)
- Without a predefined structure, but with several major backbones

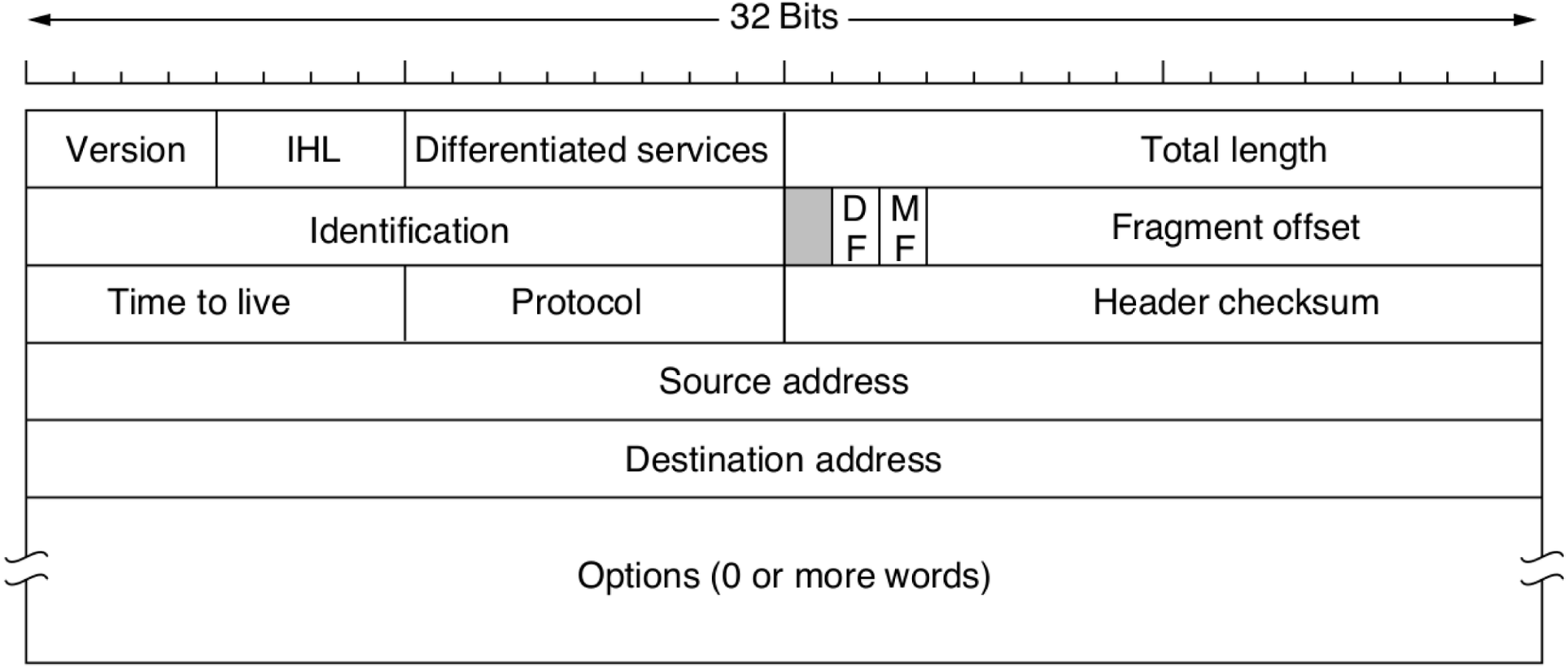


Internet communication

- The transport layer takes data streams and breaks them up so these can be sent as IP packets
- IP routers forward each packet through the Internet, along a path from one router to the next
- At the destination, the network layer reassembles the data into the original datagram, and hands it to the transport layer, which gives it to the receiving process

The IPv4 header

- The IPv4 datagram consist of a header and a body/payload part
- Bits of the header are transmitted from left to right top to bottom



IPv4 header fields (1)

- The **Version** field keeps track of the protocol version (e.g., version 4)
- **Differentiated services** is intended to distinguish between different classes of service, and **IHL** field tells how long the header is
- **Total length** of both the header and data, maximum of 65,535 bytes
- **Identification** is used to allow the destination host to determine which packet a newly arrived fragment belongs to (all fragments of a packet have the same identification value)
- Two 1-bit fields related to fragmentation: DF (Don't Fragment), and MF (More Fragments)
- The **Fragment offset** tells where in the current packet this fragment belongs
- The **TTL** (Time To Live) is a counter used to limit packet lifetimes (max 255 hops)

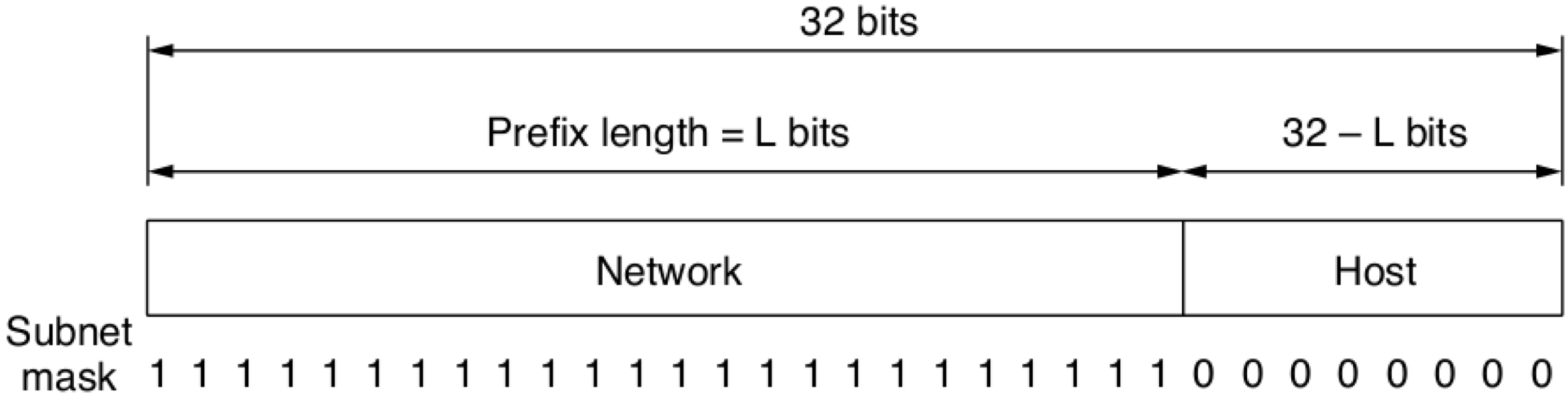
IPv4 header fields (2)

- The **Protocol** field tells it which transport process to give the packet to (e.g., TCP, UDP)
- **Header checksum** should be zero upon arrival, used to detect error while the packet travels through the network
- **Source address** and **Destination address** indicate the IP address of the source and destination network interfaces
- **Options** is designed to avoid allocating header bits to information that is rarely needed (e.g., timestamp, record route)

Prefixes and subnet (1)

- IP addresses are hierarchical, written in dotted decimal notation from 0 to 255
- The 32-bit addresses have a variable-length network portion and a host portion
  - the network portion has the same value for all hosts on a single network
- Prefixes are written by giving the lowest IP address in the block and the size of the block (number of bits in the network portion), e.g., 128.208.2.0/24 corresponds to $2^8 = 256$ addresses, 255.254.0.0/15 corresponds to $2^{17} = 131072$ addresses
- Prefix length cannot be inferred just from the IP address, so routing protocols must carry the prefixes to routers (e.g., /16)
- Prefix length correspond to a binary mask of 1s in the network portion: **subnet mask**

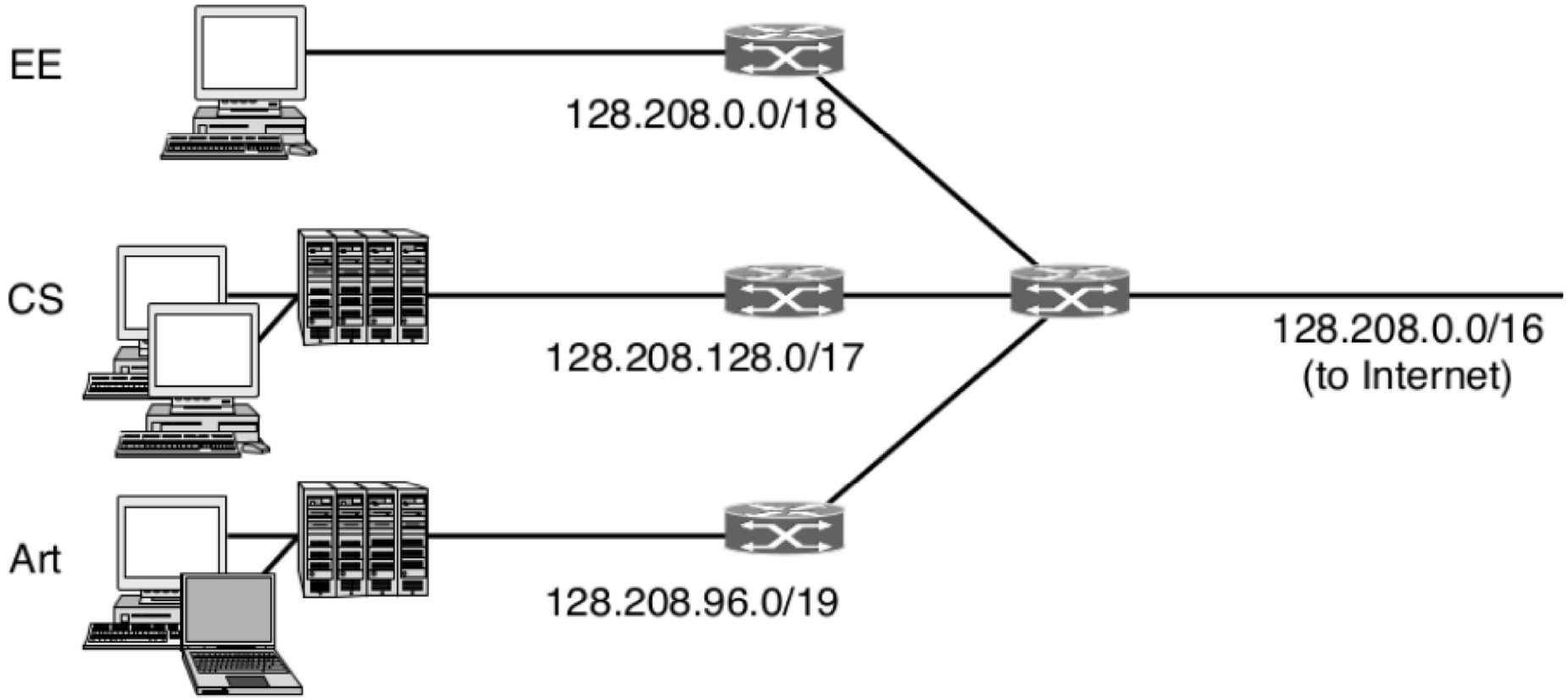
Prefixes and subnet (2)



Subnetting (1)

- Network numbers are managed by ICANN (Internet Corporation for Assigned Names and Numbers) to avoid conflicts
  - ICANN has delegated parts of the address space to regional authorities, which give out IP addresses to ISPs and other companies
- **Subnetting** is about allowing the block of addresses to be split into several parts for internal use as multiple networks while still acting like a single network to the outside
  - basically dividing up larger networks to subnets
- The router knows which subnet to give packets using the prefixes

Subnetting (2)

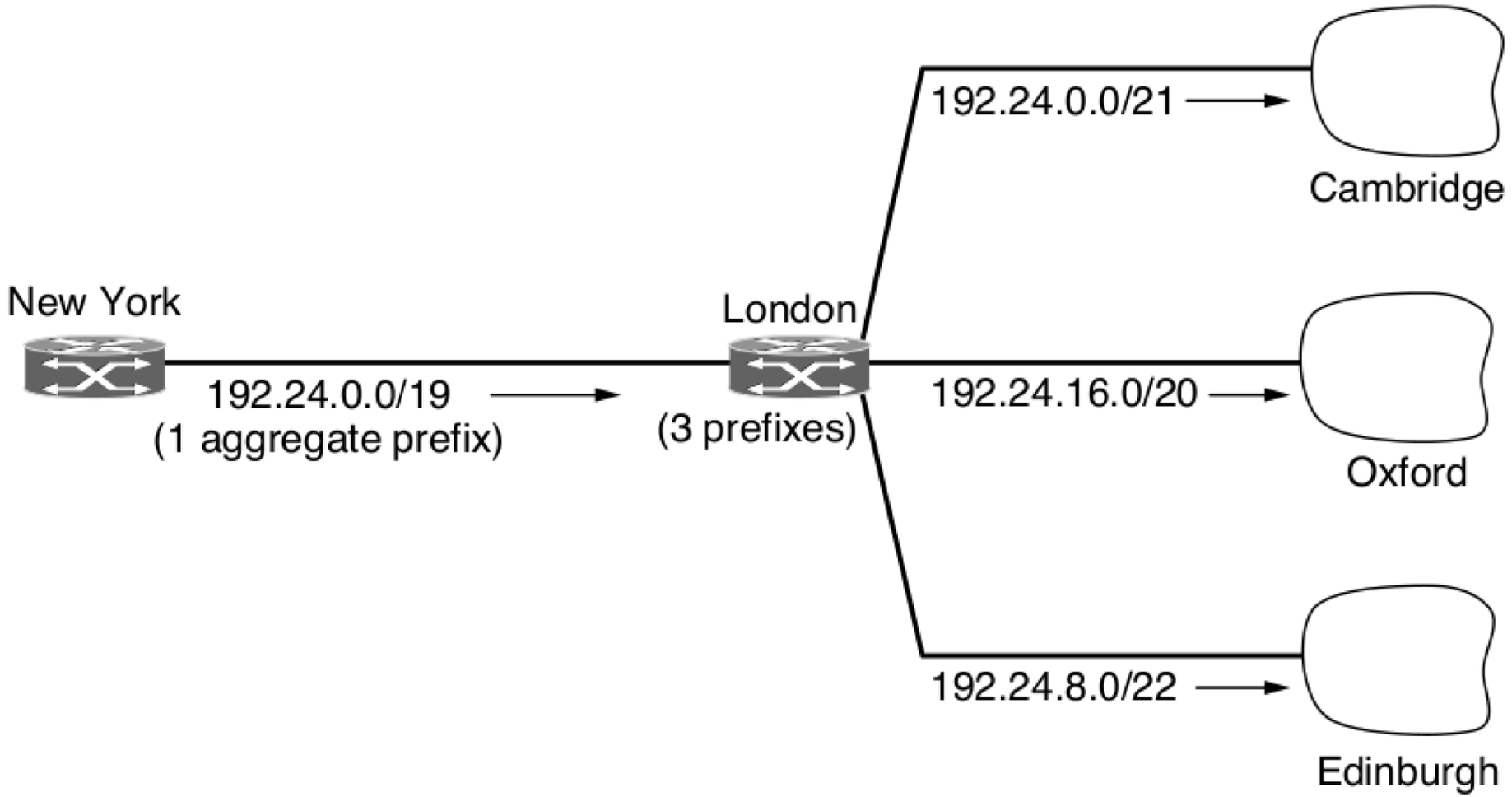


CIDR (1)

- Problem of large routing tables for ISPs and backbones
- Combining multiple small prefixes into a single, larger prefix is called **route aggregation**
- **CIDR** (Classless InterDomain Routing)

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 (2)


192.24.0.0/21
Cambridge
New York
London
192.24.0.0/19
(1 aggregate prefix)
(3 prefixes)
192.24.16.0/20
Oxford
192.24.8.0/22
Edinburgh

W4 Summary (1)

- The network layer is concerned with getting packets from the source to the destination
- Store-and-Forward packet switching: packets or datagrams are injected into the network individually and routed independently of each other then forwarded to the next router until it reaches the destination
- The algorithm that manages the routing tables and makes the routing decisions is called the routing algorithm
- Router processes: forwarding and routing (static or dynamic)
- Congestion happens when too many packets introduce packet delay and loss that degrades performance
- Two main approaches to deal with congestion: increase the resources or decrease the load
- In general, networks do not need to be lossless for reliable file transfer (QoS)

W4 Summary (2)

- Connecting heterogeneous networks with machines using different protocols in layers raises multiple issues
  - Supporting different packet sizes with packet fragmentation
- If the source and destination hosts are on the same type of network but there is a different network between them, tunneling is used
- The IPv4 datagram consist of a header and a body/payload part
- IP addresses have a network portion and host portion
- Prefix length correspond to a binary mask of 1s in the network portion: subnet mask
- Subnetting is about allowing the block of addresses to be split into several parts for internal use as multiple networks while acting like a single network
- Combining multiple small prefixes into a single, larger prefix is called route aggregation