Week 5 – Network Layer (1)

COMP90007

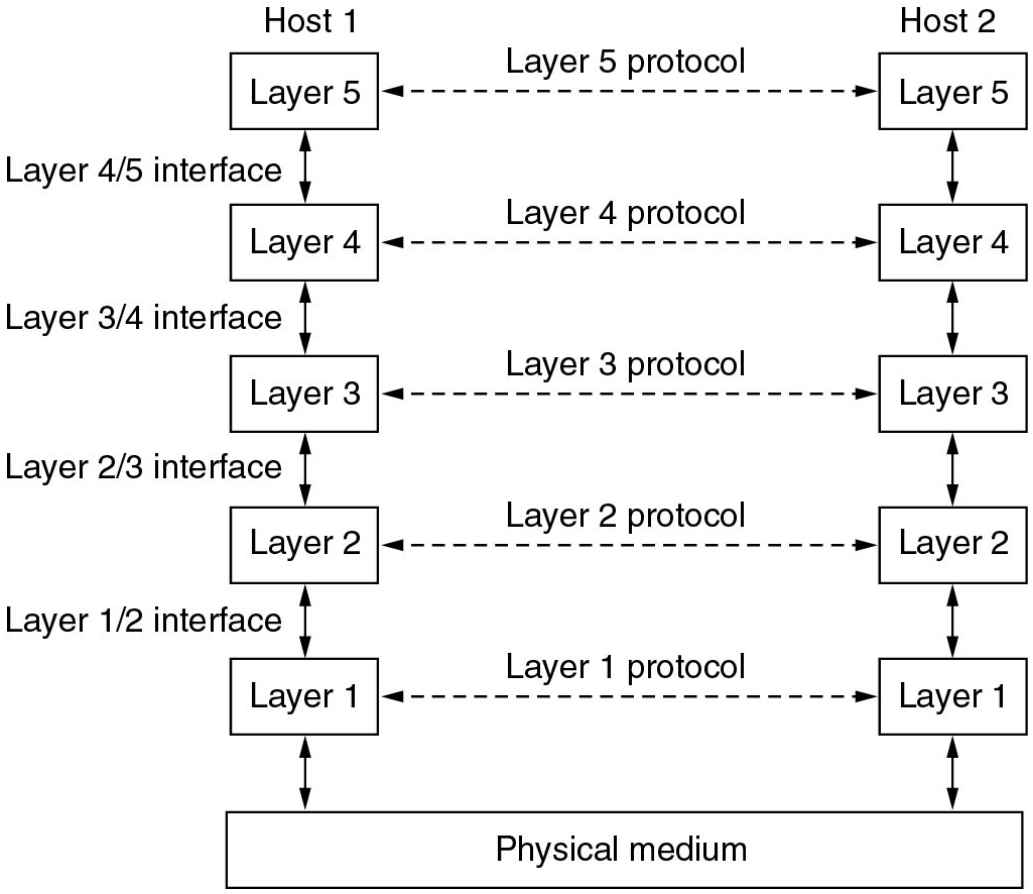
Internet Technologies

Network Layer

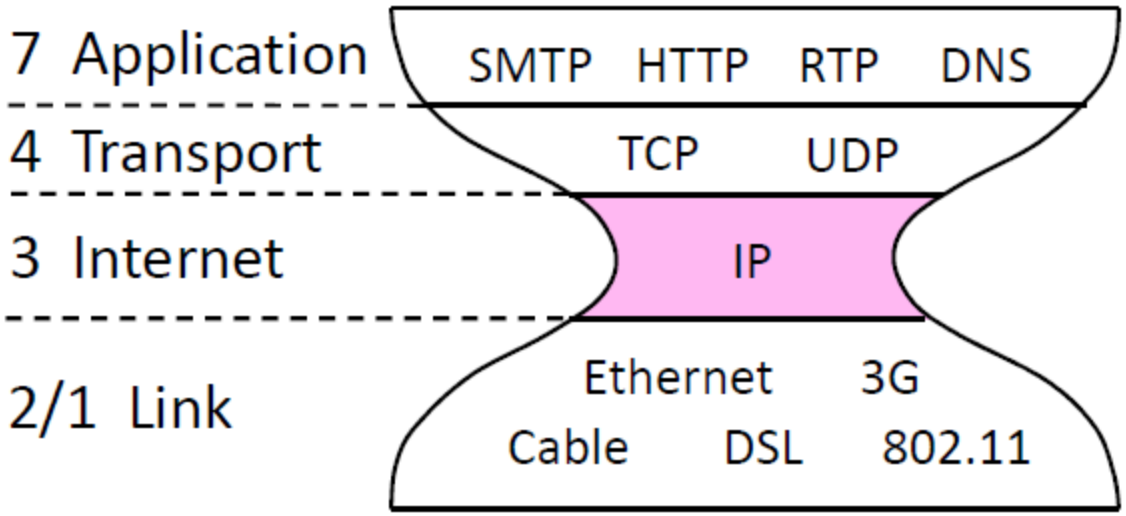
Connecting different networks (internetworking)

Framing, reliability and flow control, MAC, direct conn.

Different cables, wireless, Signal, digital to analogue



Internet

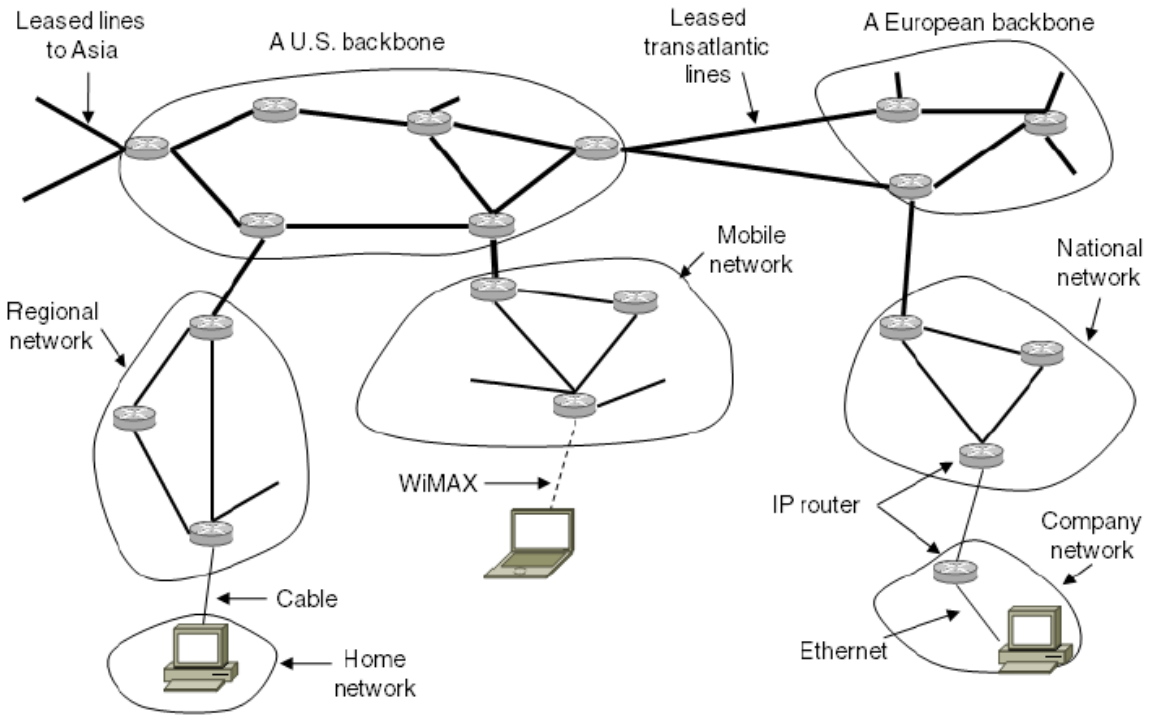

7 Application
SMTP HTTP RTP DNS
4 Transport
TCP UDP
3 Internet
IP
2/1 Link
Ethernet 3G
Cable DSL 802.11

Principles of Internet Design

- RFC 1958 “Architectural Principles of the Internet”
- Core Principles
  - Make sure it works
  - Keep it simple
  - Make clear choices
  - Exploit modularity
  - Expect heterogeneity
  - Avoid static options and parameters
  - Choose a good, but not necessarily perfect design
  - Be strict in sending and tolerant in receiving
  - Consider scalability
  - Consider performance vs cost

Network Layer in the Internet

- Internet is an interconnected collection of many networks or Autonomous Systems that is held together by the IP protocol

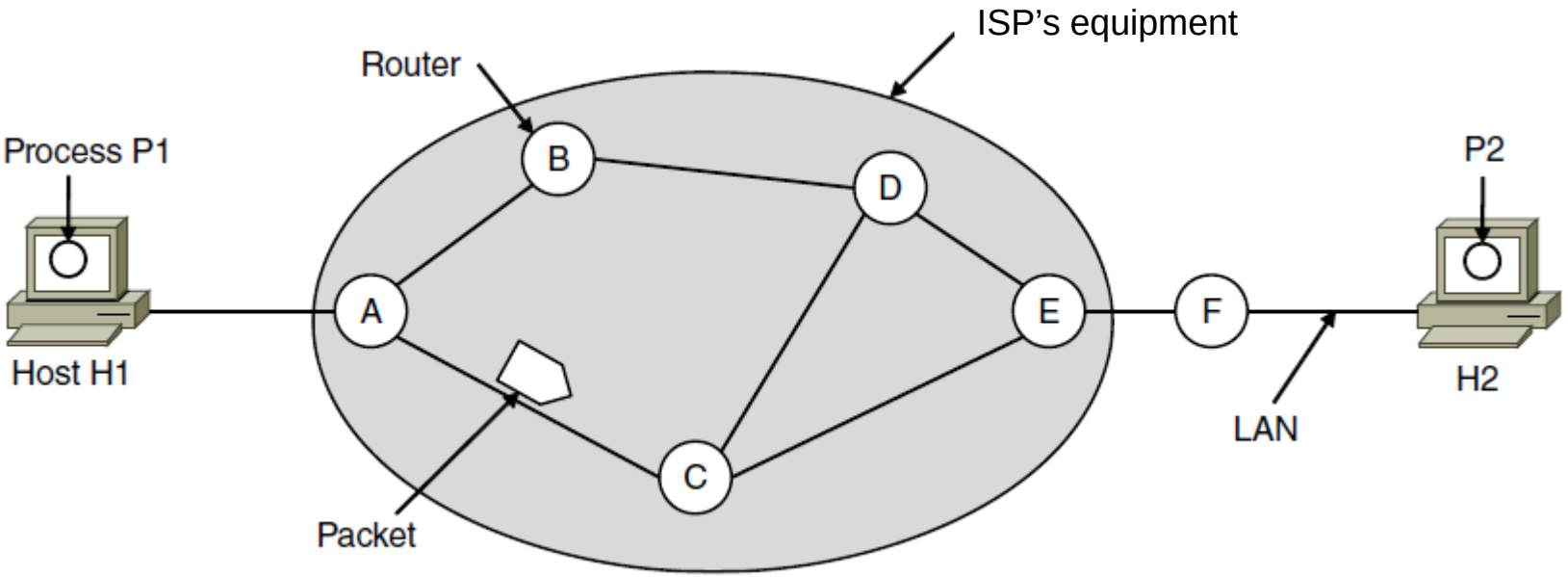


Internet Protocol (IP)

- The glue that holds the whole Internet together is the network layer protocol, IP (Internet Protocol)
- Provides a best-effort service to **route datagrams** from source host to destination host
- These hosts may be
  - On the same network
  - On different networks
- Each network is called an **Autonomous System** (AS)

Store-and-Forward Packet Switching

- Hosts generate packets and inject into the network
- Routers treat packets as messages, receiving (storing) them and then forwarding them based on how the message is addressed
- **Router routes packets through the network**



Services Provided to the Transport Layer

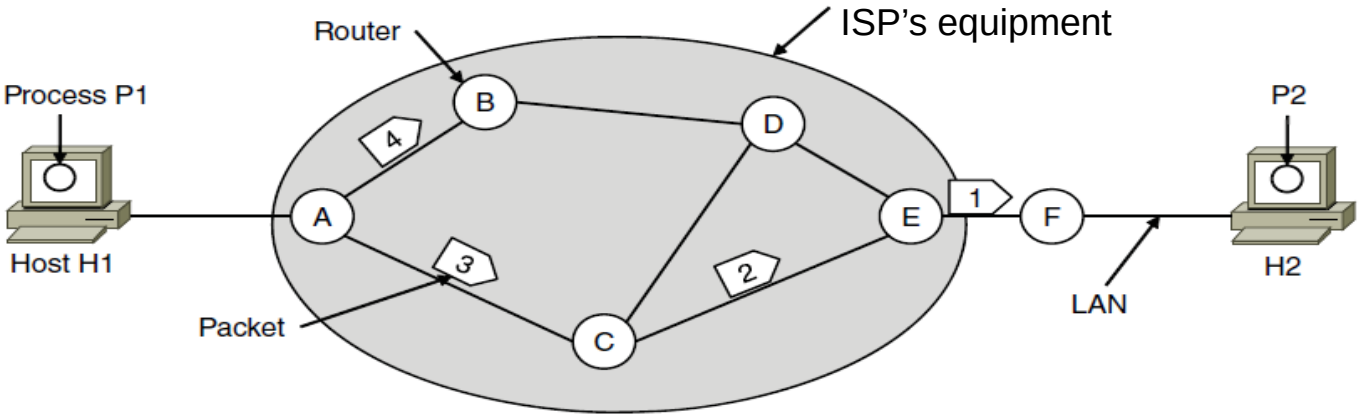
- Design goals:
  - Services should be **independent of router technologies**
  - **Transport layer should be shielded** from number, type and topology of routers
  - **Network addressing should use a uniform numbering** plan (network identifier)

Types of Services

- **Connectionless**: Packets (datagrams) are injected into subnet individually and routed independently to destination
  - Internet: move packets in a potentially unreliable subnet - QoS is not easily implemented
  - Flow and error control done by the hosts
- **Connection-oriented**: Packets travelling between destinations all use the same route
  - Telco: guarantee reliability - QoS is important

Routing within a Datagram Subnet

- **Post office model**: packets are routed individually based on destination addresses in them
- Packets can take different paths
- E.g., P1 sends a long message to P2



A's table (initially)

Dest.	Line
A	X
B	B
C	C
D	B
E	C
F	C

A's table (later)

A	X
B	B
C	C
D	B
E	B
F	B

C's Table

A	A
B	A
C	X
D	E
E	E
F	E

E's Table

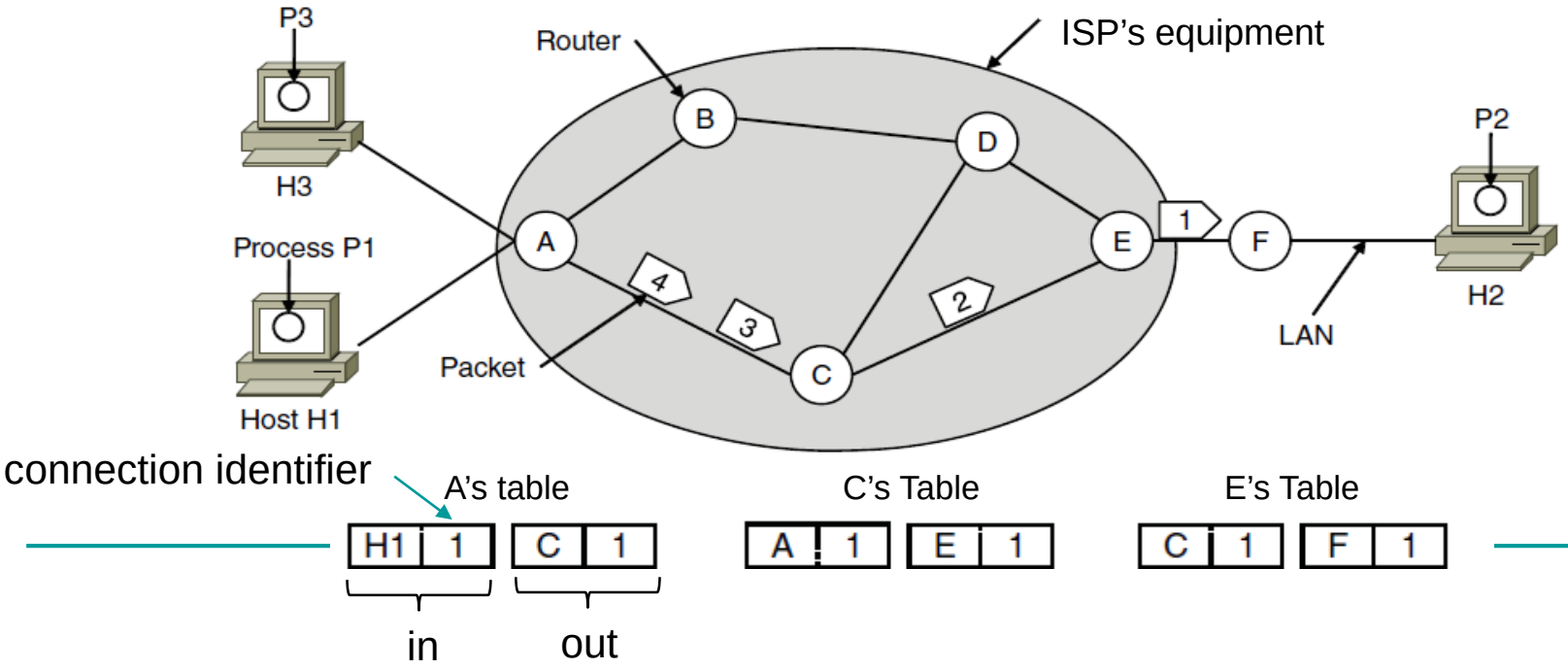
A	C
B	D
C	C
D	D
E	X
F	F

Routing table (can be fixed, can change over time)

Routing algorithm – manages the routing table

Routing within a Virtual-Circuit Subnet

- **Telephone network model:** Packets are routed through virtual circuits (created earlier) based on tag number (not full address but unique at a given link) in them
  - Packets take the same path: to avoid having to choose a new route for every packet sent
  - e.g., MultiProtocol Label Switching Network (to provide QoS) – 20 bit label or Conn. Identifier



Differences in Virtual-Circuit and Datagram Subnets

Issue	Datagram network	Virtual-circuit network
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

Compromises in VC and Datagram Subnets (1)

- Setup time vs. address parsing time
  - VC: requires setup time and resources, but packet transmission is very fast after that
  - Datagram: more complicated lookup procedure
- Memory (router)
  - VC: requires entry per virtual circuit
  - Datagram: requires large tables of every possible destination routes
- Bandwidth
  - VC: saves potential overhead in full addressing of each packet and computation of path. Still needs them during setup
  - Datagram: full destination address in every packet

Compromises in VC and Datagram Subnets (2)

- QoS and congestion avoidance
  - VC: can use a tighter QoS - able to reserve CPU, bandwidth and buffer in advance
- Longevity
  - VC: can be setup for long-running uses e.g. Permanent VC's
- Vulnerability
  - VC: particularly vulnerable to hardware/software crashes - all VC's aborted and no traffic until they are rebuilt
  - Datagram: can use an alternative route

Internetworking

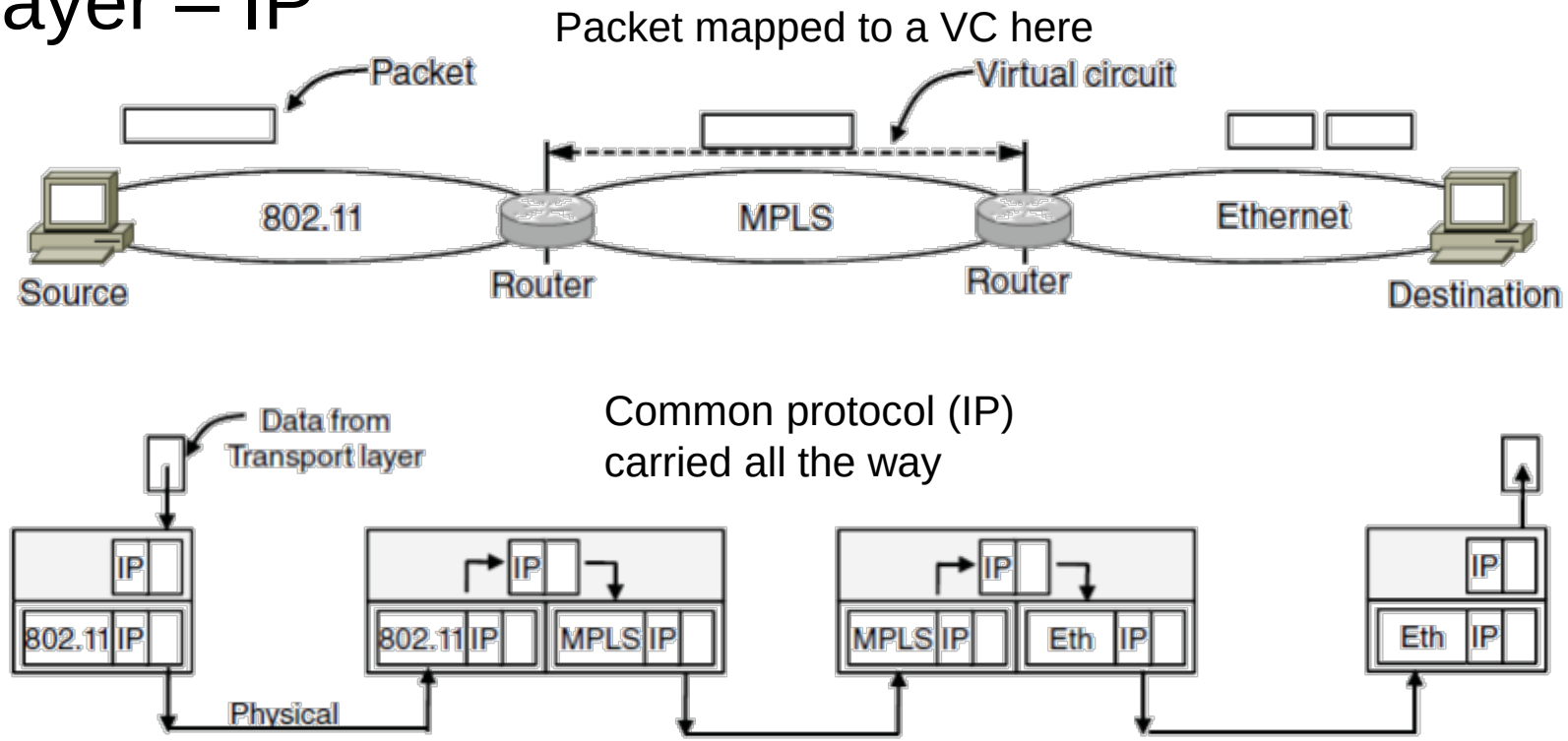
- Recall we cannot assume a single homogeneous network
- Internetworking joins multiple, different networks into a single larger network
- Issues when connecting networks:
  - Different network types and protocols
  - Different motivations for network choices
  - Different technologies at both hardware and software levels

Differences at the Network Layer

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 Different Networks are Connected

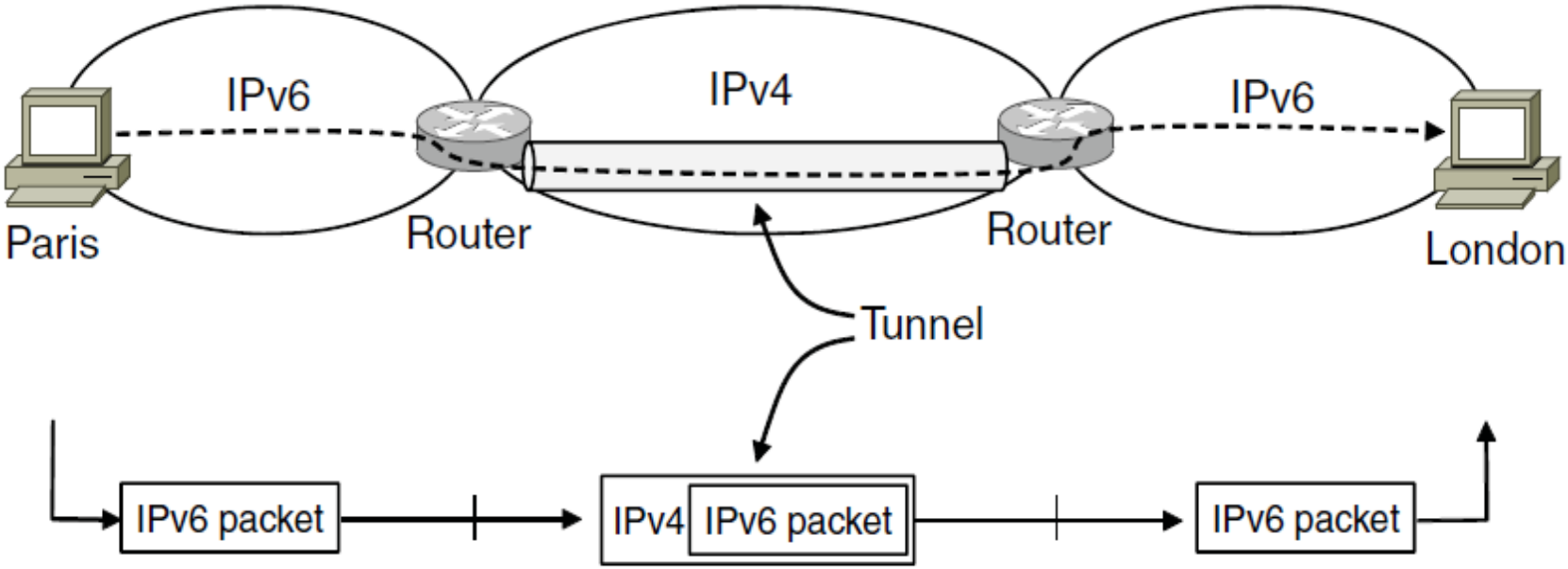
- Internetworking based on a common network layer – IP



Tunneling

- Tunneling is a special case used when the source and destination are on the same network, but there is a different network in between.
  - Source Packets are encapsulated over the packets in the connecting network

Tunneling IPv6 Packets through IPv4

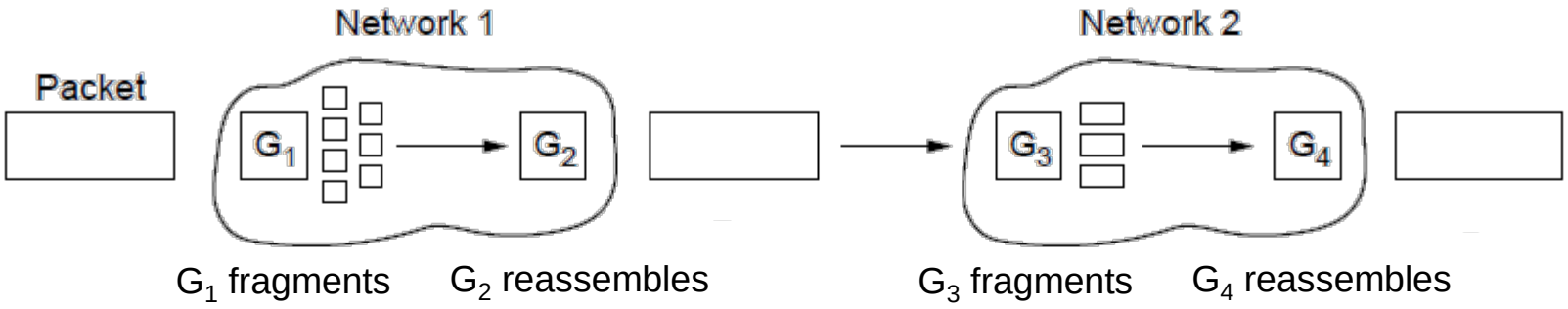


Fragmentation

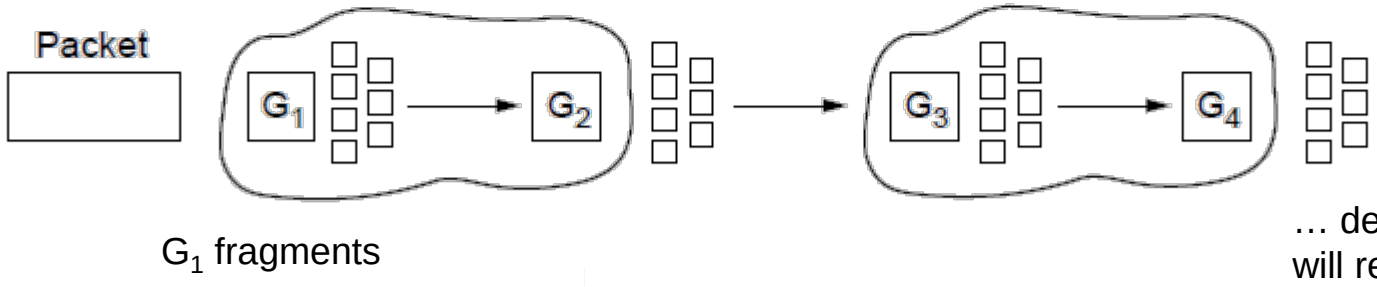
- All networks have a maximum size for packets, could be motivated by:
  - Hardware
  - Operating system
  - Protocols
  - Standards compliance
  - Desire to reduce transmissions due to errors
  - Desire for efficiency in communication channel
- Fragmentation (division of packets into fragments) allows network gateways to meet size constraints

Types of Fragmentation

- Large packets need to be routed through a network whose maximum packet size is too small.
- **Solution: Fragmentation and Reassembly**.



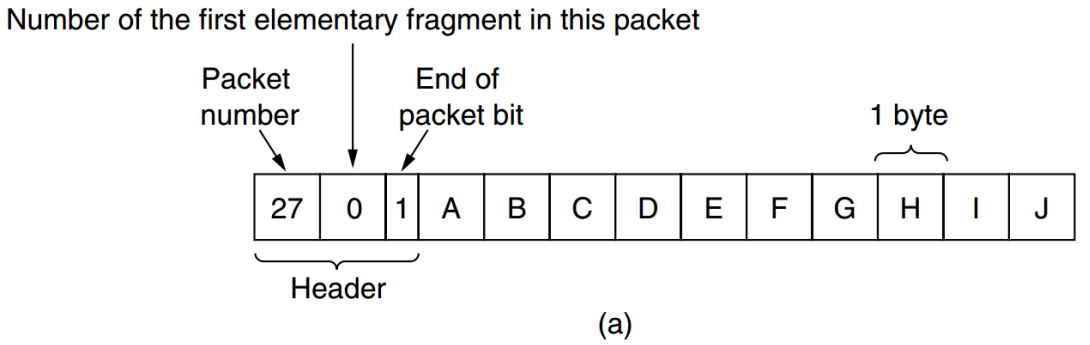
a) Transparent – packets fragmented / reassembled in each network.
Route constrained, more work



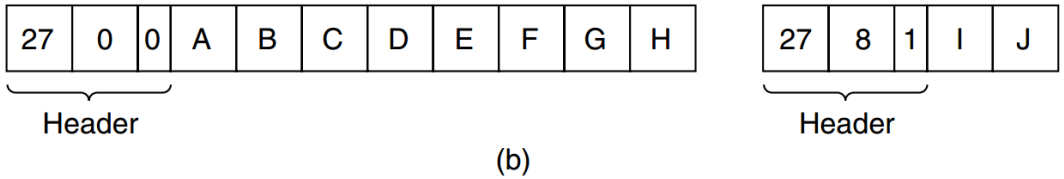
- **b) Non-transparent** – fragments are reassembled at destination.
Less work (IP works this way) – packet number, byte offset, end of packet flag

IP Style Fragmentation

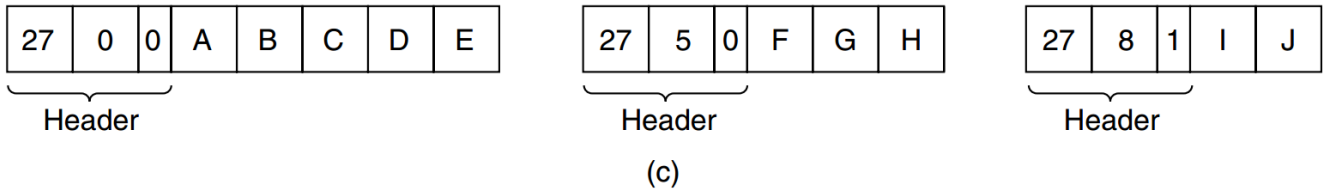
Original packet:
(10 data bytes)



Fragmented:
(to 8 data bytes)



Re-fragmented:
(to 5 bytes)



Path MTU Discovery

- Alternative to Fragmentation
- Advantage: The source now knows what length packet to send but if the routes and path MTU change, new error packets will be triggered and the source will adapt to the new path