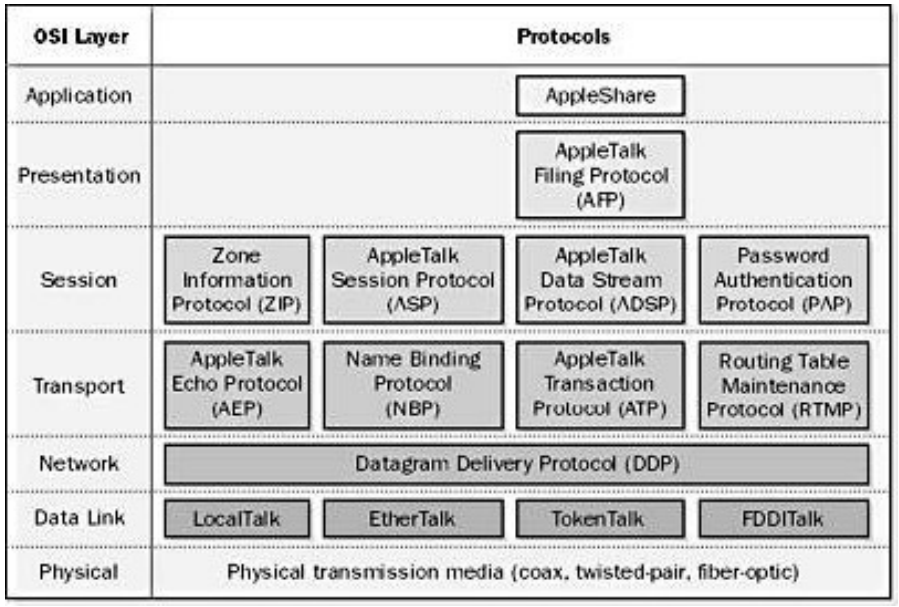
Internetworking

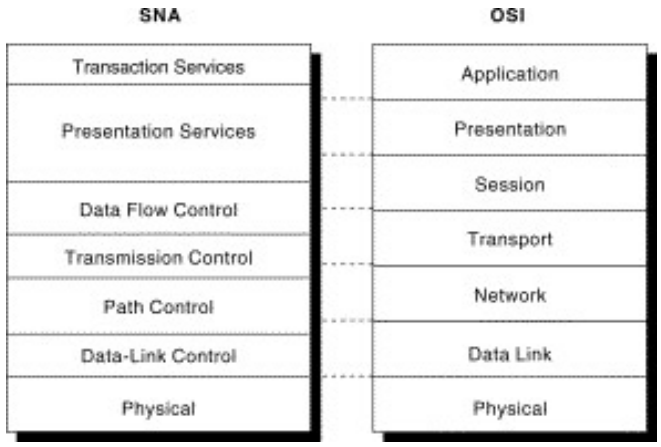
- Different networks exist, including LANs, MANs, and WANs.
- Numerous protocols are in widespread use in every layer.
- Internetworking is to connect two or more networks that are connected to form an internet.

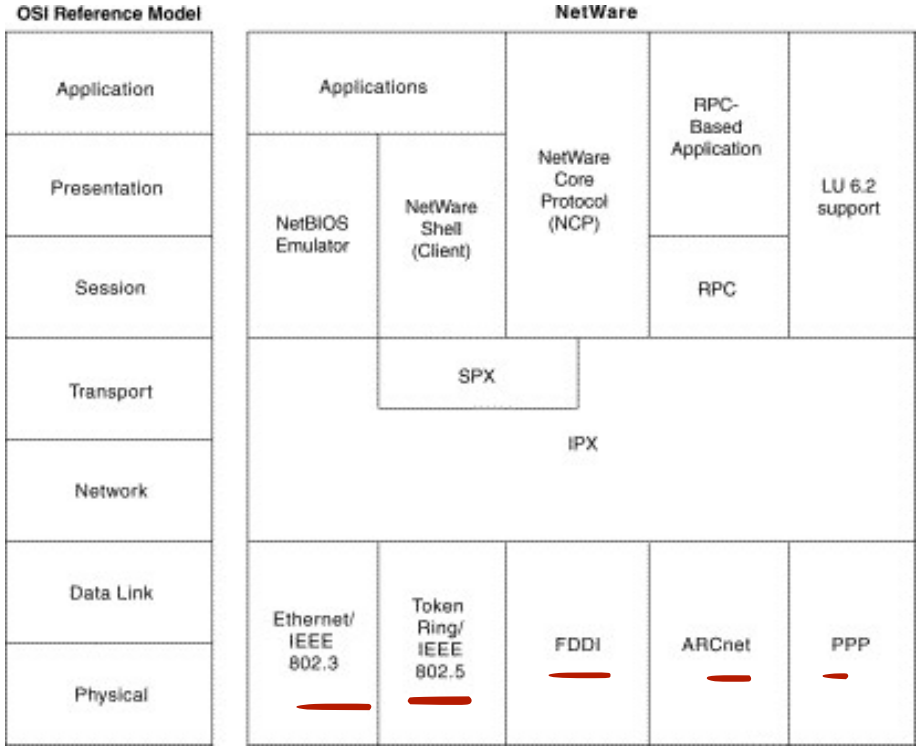
Why different networks and different protocols?

- First, the installed base of different networks is large – PC's run TCP/IP or Apple Talk or Novell NCP/IPX , Mainframes run IBM's SNA, Telephone systems use ATM Networks, Wireless use variety of different protocols.
- With new technology the protocols change.

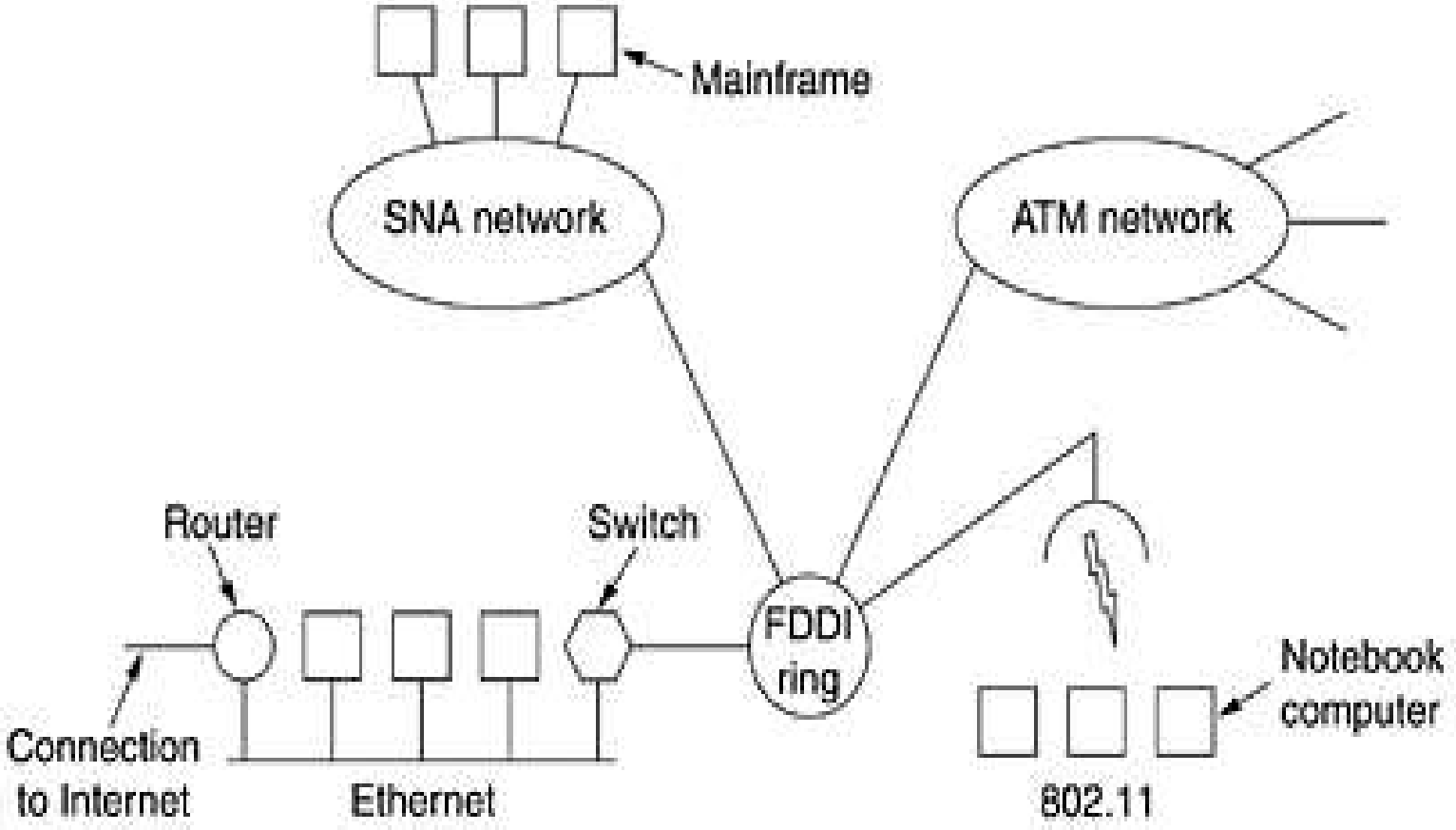
- Second, Different OS- UNIX and running TCP/IP and some systems with Macs and Apple Talk.
- Third, different networks (e.g., ATM and wireless) have radically different technology hence different hardware.


OSI Layer
Protocols
Application
AppleShare
Presentation
AppleTalk Filing Protocol (AFP)
Session
Zone Information Protocol (ZIP)
AppleTalk Session Protocol (ASP)
AppleTalk Data Stream Protocol (ADSP)
Password Authentication Protocol (PAP)
Transport
AppleTalk Echo Protocol (AEP)
Name Binding Protocol (NBP)
AppleTalk Transaction Protocol (ATP)
Routing Table Maintenance Protocol (RTMP)
Network
Datagram Delivery Protocol (DDP)
Data Link
LocalTalk
EtherTalk
TokenTalk
FDDITalk
Physical
Physical transmission media (coax, twisted-pair, fiber-optic)


SNA
OSI
Transaction Services
Presentation Services
Data Flow Control
Transmission Control
Path Control
Data-Link Control
Physical
Application
Presentation
Session
Transport
Network
Data Link
Physical


OSI Reference Model
NetWare
Application
Presentation
Session
Transport
Network
Data Link
Physical
Applications
NetBIOS Emulator
NetWare Shell (Client)
NetWare Core Protocol (NCP)
RPC-Based Application
RPC
LU 6.2 support
SPX
IPX
Ethernet/ IEEE 802.3
Token Ring/ IEEE 802.5
FDDI
ARCnet
PPP

A collection of interconnected networks



- The purpose of interconnecting all these networks is to allow users on any of them to communicate with users on all the other ones and also to allow users on any of them to access data on any of them.
- Accomplishing this goal means sending packets from one network to another.
- Since networks often differ in important ways, getting packets from one network to another is not always so easy.

How Networks Differ?

- Networks can differ in many ways.
- Some of the differences, such as different modulation techniques or frame formats, are in the physical and data link layers.

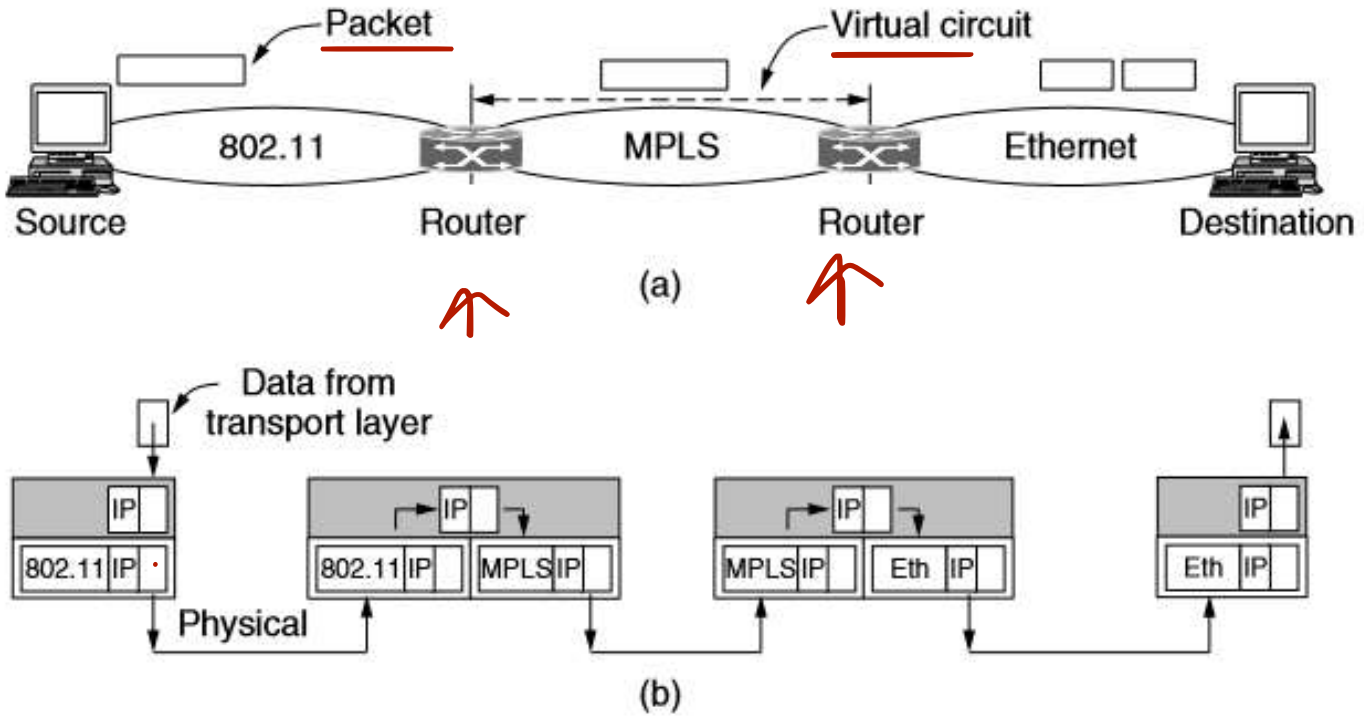
Item	Some Possibilities
Service offered	Connection oriented versus connectionless
Protocols	IP, IPX, SNA, ATM, MPLS, AppleTalk, etc.
Addressing	Flat (802) versus hierarchical (IP)
Multicasting	Present or absent (also broadcasting)
Packet size	Every network has its own maximum
Quality of service	Present 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

How the networks can be connected?

- Networks can be interconnected by different devices.
- In the physical layer, networks can be connected by repeaters or hubs, which just move the bits from one network to an identical network.
- These are mostly analog devices and do not understand anything about digital protocols.
- At data link layer- bridges and switches
- They can accept frames, examine the MAC addresses, and forward the frames to a different network while doing minor protocol translation in the process
- For example, from Ethernet to FDDI or to 802.11.

Interconnection at higher layer

- An internet comprised of 802.11, MPLS, and Ethernet networks

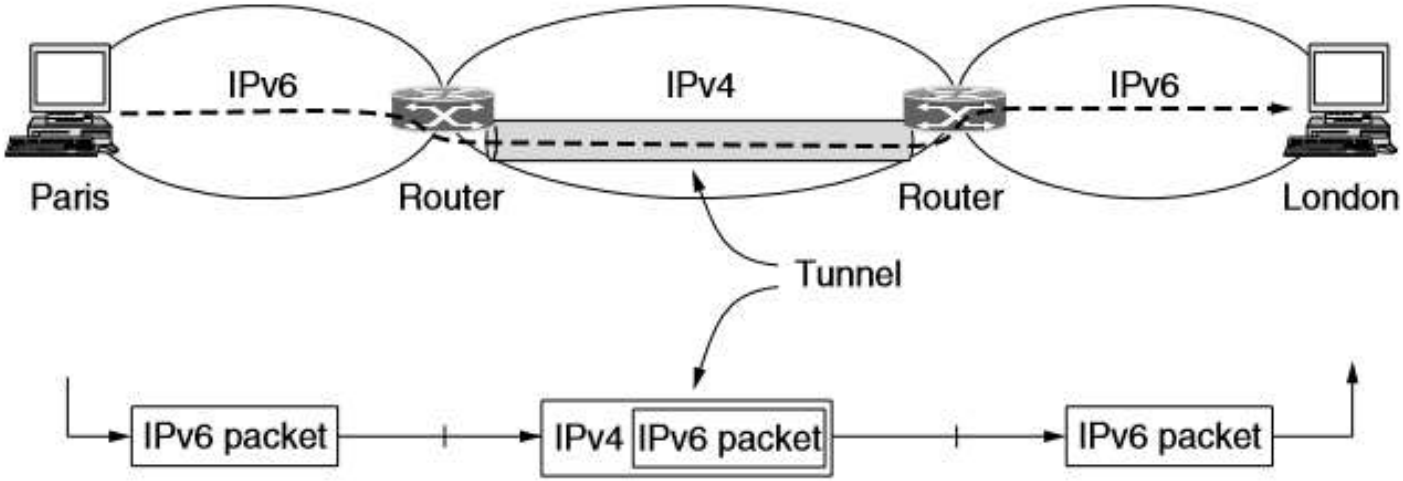


(a) A packet crossing different networks. (b) Network and link layer protocol processing.

- Different Networks- Different addressing format.
- 802.11 provides a connectionless service, but MPLS provides a connection-oriented service.
- This means that a virtual circuit must be set up to cross that network.
- If the packets are larger then must be broken down- Fragmentation and reassembled at destination.
- A router that can handle multiple network protocols is called a multiprotocol router.

Tunnelling

- Making two different networks interwork is exceedingly difficult.
- Special Case: the source and destination hosts are on the same type of network, but there is a different network in between.



- The path through the IPv4 Internet can be seen as a big tunnel extending from one multiprotocol router to the other.
- Tunneling is widely used to connect isolated hosts and networks using other networks.
- The network that results is called an **overlay** since it has effectively been overlaid on the base network.

Advantages:

1. Security: With tunnel we can create a private link across public network.
2. R1 and R2 may be multicast routers- some extra capabilities which are not available in other network.
3. To carry packets from protocols other than IP across an IP network.

Disadvantages

- Increases the length of packets; this might represent a significant waste of bandwidth for short packets.
- Longer packets might be subject to fragmentation, which has its own set of drawbacks.
- There may also be performance implications for the routers at either end of the tunnel.
- There is a management cost for the administrative entity.

Internetwork Routing

- Internetwork Routing refers to the process of determining the path for data to travel across multiple interconnected networks (i.e., an internetwork).
- Networks run by different operators lead to bigger problems.
- The operators may have different ideas about what is a good path through the network.
- This will lead the operators to use different quantities to set the shortest-path costs (e.g., milliseconds of delay vs. monetary cost).
- Shortest paths on the internet will not be well defined.

Routing algorithms can be categorized based on the scope of their operation into:

- Intra domain or interior gateway routing

Operate within a single domain or Autonomous System (AS) — such as an organization or ISP.

- Inter domain or exterior gateway routing.

Operate between multiple Autonomous Systems (ASes) — such as between two ISPs.

- Usually there will be different intra domain routing but same inter domain protocol.

Common Intra-Domain Routing Protocols:

Protocol	Type	Description
RIP (Routing Information Protocol)	Distance Vector	Uses hop count as the metric, max 15 hops, simple but limited scalability.
OSPF (Open Shortest Path First)	Link State	Uses Dijkstra's algorithm to find the shortest path; fast and scalable.
EIGRP (Enhanced Interior Gateway Routing Protocol)	Hybrid	Cisco proprietary; combines distance vector and link state benefits.

Common Inter-Domain Routing Protocol:

Protocol	Type	Description
BGP (Border Gateway Protocol)	Path Vector	Used on the global internet. Selects routes based on policy, not always shortest path.

Autonomous systems and Routing Policies.

- A network that operates independently is called as an Autonomous system- e.g- ISP.
- An ISP network may be comprised of more than one AS .
- There are business arrangements between ISPs
  - Each ISP may charge or receive money from the other ISPs for carrying traffic.
  - Routing that requires crossing international boundaries- must take care of privacy laws.

Fragmentation

- Data Fragmentation is the process of breaking a large data packet into smaller pieces (called fragments) so it can be transmitted over a network that has a smaller Maximum Transmission Unit (MTU).
- The receiving system then reassembles these fragments into the original packet.

Why Fragmentation?

- Different networks/devices have different MTU sizes.
- If a packet exceeds the MTU of a network along its path, it must be fragmented.
- Ensures reliable transmission over heterogeneous networks.

Fragmentation

- At the IP layer, fragmentation typically occurs.
- Key fields in an IPv4 header used for fragmentation:
- Identification: To group fragments of the same packet.
- Flags: Indicates if more fragments follow.
- Fragment Offset: Position of the fragment in the original packet.
- Example: A 3000-byte IP packet hits a network with MTU 1500 bytes → gets split into 2 or more fragments.

Fragmentation- Problems:

- Performance impact: Reassembly adds overhead.
- Security risks: Can be exploited (e.g., fragmentation attacks).
- Packet loss: If one fragment is lost, the entire packet may be dropped.
- Avoidance: Modern protocols and systems try to avoid it using Path MTU Discovery (PMTUD).

Fragmentation

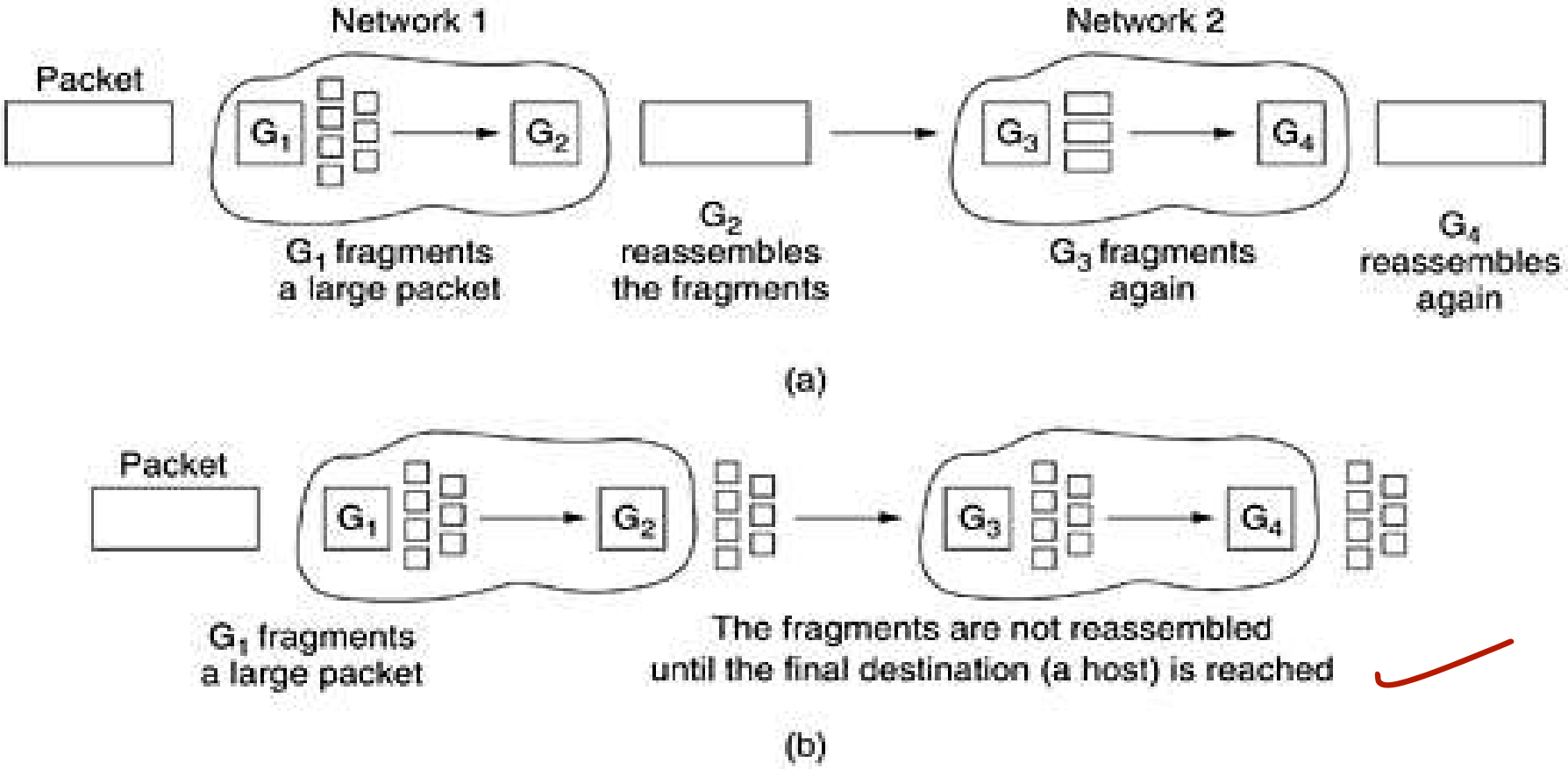
Each network imposes some maximum size on its packets. These limits have various causes, among them:

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.

There are two types of fragmentations

a) Transparent Fragmentation

b) Non transparent fragmentation



a) Transparent Fragmentation

- In this approach, the small-packet network has gateways (most likely, specialized routers) that interface to other networks.
- When an oversized packet arrives at a gateway, the gateway breaks it up into fragments.
- Each fragment is addressed to the same exit gateway, where the pieces are recombined.
- In this way passage through the small-packet network has been made transparent.
- Subsequent networks are not even aware that fragmentation has occurred.
- ATM networks, for example, have special hardware to provide transparent fragmentation of packets into cells and then reassembly of cells into packets.
- In the ATM world, fragmentation is called segmentation;

D’tages

- The exit gateway must know when it has received all the pieces, so either a count field or an "end of packet" bit must be provided.
- All packets must exit via the same gateway.
- Overhead required to repeatedly reassemble and then refragment a large packet passing through a series of small-packet networks.

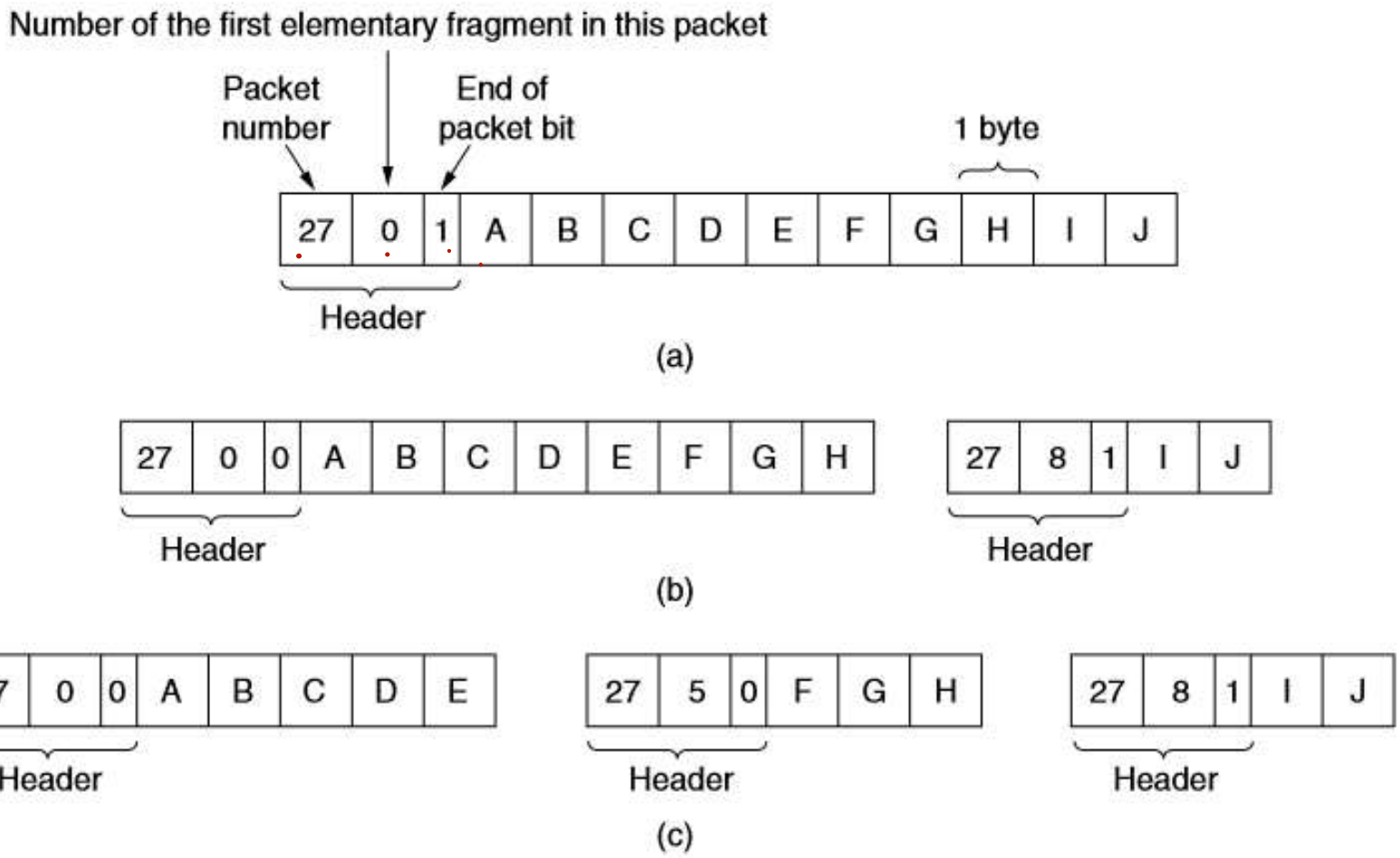
❖ATM requires transparent fragmentation.

a) Non transparent fragmentation

- In this approach the recombining of fragments does not occur at intermediate gateways.
- Once a packet has been fragmented, each fragment is treated as though it were an original packet.
- All fragments are passed through the exit gateway.
- Recombination occurs only at the destination host.

❖ Example of non transparent fragmentation is IP network.

- A complete design requires that the fragments be numbered in such a way that the original data stream can be reconstructed.
  - The design used by IP is to give every fragment a packet number (carried on all packets).
  - An absolute byte offset within the packet.
  - A flag indicating whether it is the end of the packet.


Number of the first elementary fragment in this packet
Packet number
End of packet bit
1 byte
27 0 1 A B C D E F G H I J
Header
(a)
27 0 0 A B C D E F G H
Header
27 8 1 I J
Header
(b)
27 0 0 A B C D E
Header
27 5 0 F G H
Header
27 8 1 I J
Header
(c)

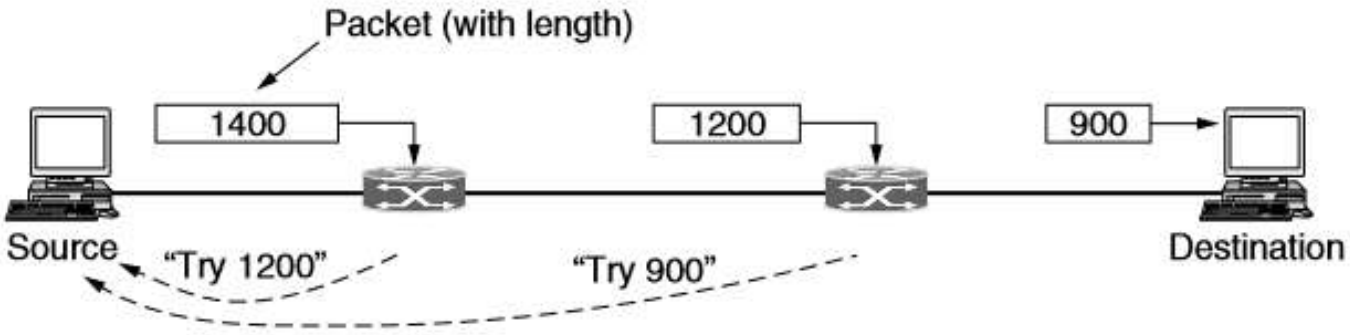
D’tages

- It requires *every host to be able to do reassembly.*
- When a large packet is fragmented, the total overhead increases because each fragment must have a header.

IPV6 and Fragmentation

- Modern Internet gets rid of the fragmentation.
- Uses the process is called path MTU discovery.
- Each IP packet is sent with its header bits set to indicate that no fragmentation is allowed to be performed.
- If a router receives a packet that is too large, it generates an error packet, returns it to the source, and drops the packet.

- When the source receives the error packet, it uses the information inside to refragment the packet into pieces that are small enough for the router to handle.
- If a router further down the path has an even smaller MTU, the process is repeated.



Advantages:

1. Source knows the packet length to be transmitted.
2. If the routes and path MTU change, new error packets will be triggered and the source will adapt to the new path.

Disadvantages:

1. Added startup delays simply to send a packet.
2. Source needs to find the MTU before transmission.

IPv4 vs. IPv6 Fragmentation

Feature	IPv4	IPv6
Who fragments?	Routers and sending hosts	Only sending host (routers do not fragment)
Header fields	Identification, Flags, Offset	Uses a separate Fragment Extension Header
Common today?	Yes	Less common due to Path MTU Discovery