The Internet Protocol (IP)

Forwarding and Addressing in the Internet

- Internet addressing and forwarding are important components of the Internet Protocol (IP).
- There are two versions of IP in use today.

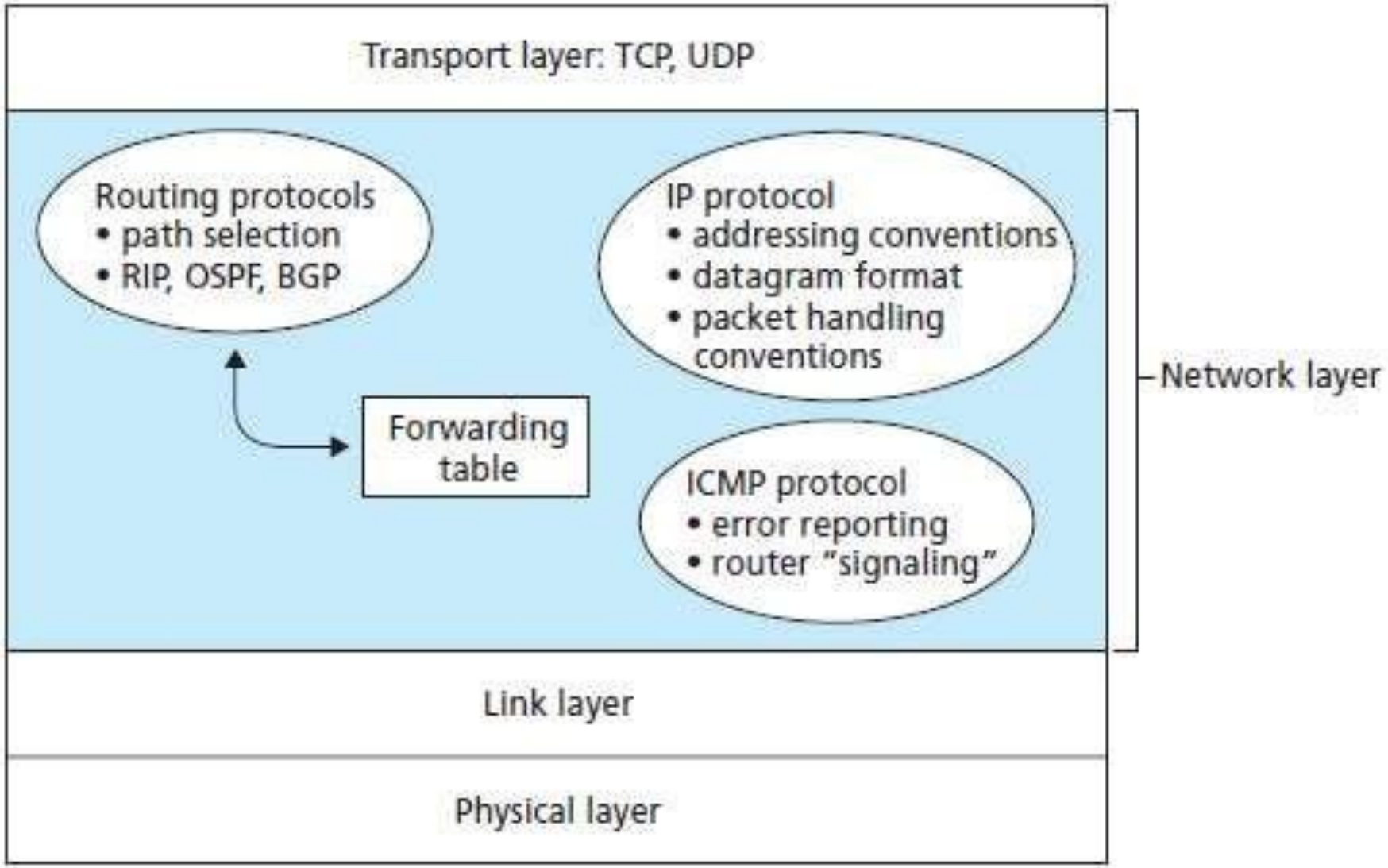
  IP protocol version 4, which is usually referred to simply as IPv4

  IP version 6

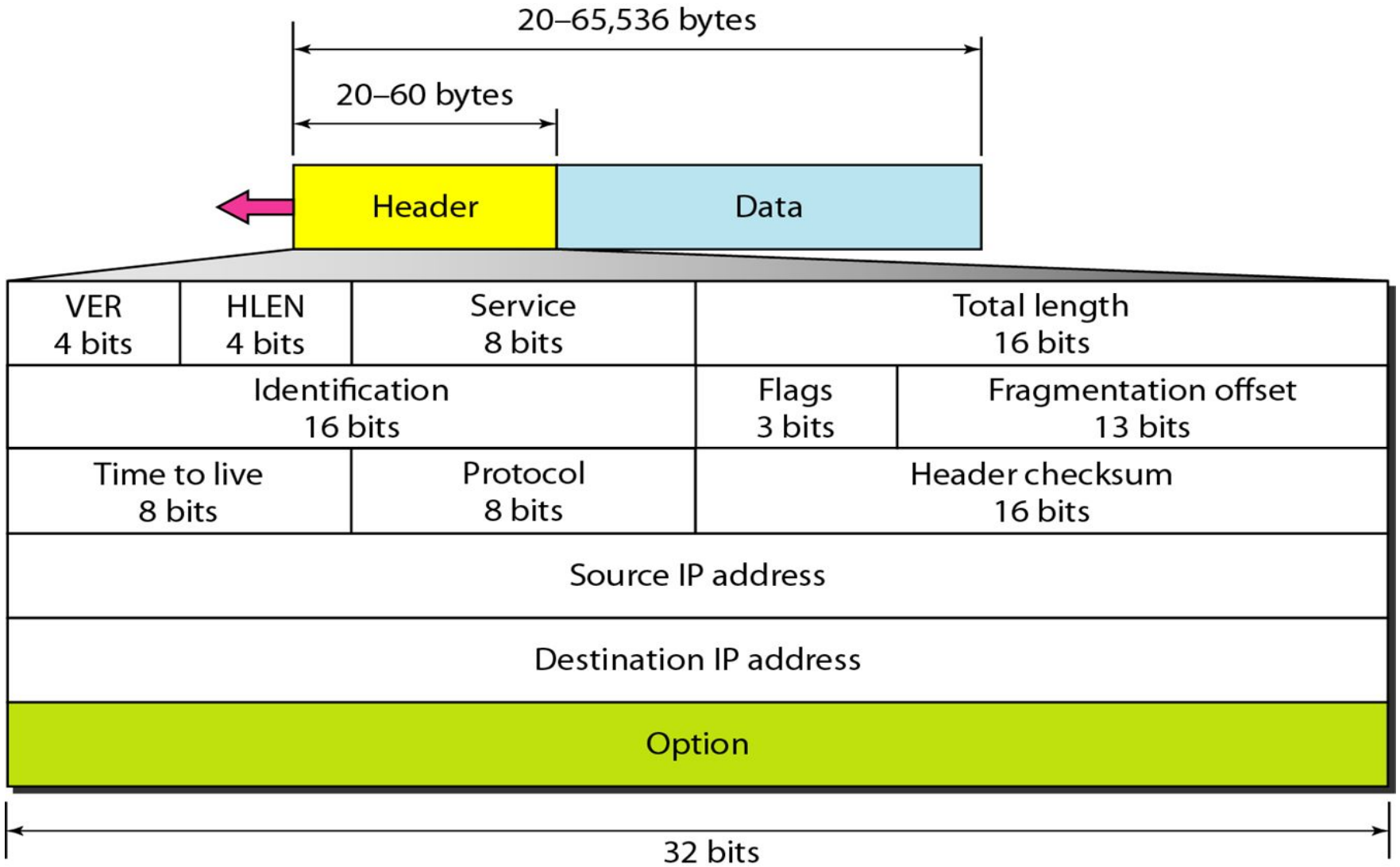
Internet's network layer has three major components.

- The first component is the IP protocol.
- The second major component is the routing component, which determines the path a datagram follows from source to destination.
- The final component of the network layer is a facility to report errors in datagrams and respond to requests for certain network-layer information.

Inside the Internet's network layer



IPv4 datagram format



A network-layer packet is referred to as a *datagram.*

IPv4 datagram format

- ***Version number.*** These 4 bits specify the IP protocol version of the datagram.By looking at the version number, the router can determine how to interpret the remainder of the IP datagram.

- ***Header length***. Because an IPv4 datagram can contain a variable number of options (which are included in the IPv4 datagram header), these 4 bits are needed to determine where in the IP datagram the data actually begins. Most IP datagrams do not contain options, so the typical IP datagram has a 20-byte header

.

IPv4 datagram format

- ***Type of service.*** The type of service (TOS) bits were included in the IPv4 header to allow different types of IP datagrams (for example, datagrams particularly requiring low delay, high throughput, or reliability) to be distinguished from each other.

- ***Datagram length.*** This is the total length of the IP datagram (header plus data), measured in bytes. Since this field is 16 bits long, the theoretical maximum size of the IP datagram is 65,535 bytes. However, datagrams are rarely larger than 1,500 bytes.

IPv4 datagram format

- ***Identifier, flags, fragmentation offset.*** These three fields have to do with so-called IP fragmentation.

- ***Time-to-live***. The time-to-live (TTL) field is included to ensure that datagrams do not circulate forever in the network. This field is decremented by one each time the datagram is processed by a router. If the TTL field reaches 0, the datagram must be dropped.

IPv4 datagram format

- ***Protocol.*** This field is used only when an IP datagram reaches its final destination. The value of this field indicates the specific transport layer protocol. For example, a value of 6 indicates that the data portion is passed to TCP, while a value of 17 indicates that the data is passed to UDP.

- ***Header checksum.*** The header checksum aids a router in detecting bit errors in a received IP datagram. The header checksum is computed by treating each 2 bytes in the header as a number and summing these numbers using 1s complement arithmetic.

IPv4 datagram format

- ***Source and destination IP addresses :*** When a source creates a datagram, it inserts its IP address into the source IP address field and inserts the address of the ultimate destination into the destination IP address field. Often the source host determines the destination address via a DNS lookup,

- ***Options :*** The options fields allow an IP header to be extended.

- ***Data(payload) :*** *T*he data field of the IP datagram contains the transport-layer segment (TCP or UDP) to be delivered to the destination. The data field of the IP datagram contains the transport-layer segment (TCP or UDP) to be delivered to the destination. However, the data field can carry other types of data, such as ICMP messages.

IP Datagram Fragmentation

- Not all link-layer protocols can carry network-layer packets of the same size.
- Some protocols can carry big datagrams, whereas other protocols can carry only little packets.
- For example, Ethernet frames can carry up to 1,500 bytes of data, whereas frames for some wide-area links can carry no more than 576 bytes.
- The maximum amount of data that a link-layer frame can carry is called the maximum transmission unit (MTU).
- A router that interconnects several links, each running different link layer protocols with different MTUs.
- Suppose it receive an IP datagram from one link. The forwarding table determine the outgoing link, and this outgoing link has an MTU that is smaller than the length of the IP datagram.

IP Datagram Fragmentation

MTUs for some networks

Protocol	*MTU*
Hyperchannel	65,535
Token Ring (16 Mbps)	17,914
Token Ring (4 Mbps)	4,464
FDDI	4,352
Ethernet	1,500
X.25	576
PPP	296

IP Datagram Fragmentation

- The solution is to fragment the data in the IP datagram into two or more smaller IP datagrams, encapsulate each of these smaller IP datagrams in a separate link-layer frame; and send these frames over the outgoing link.

- Each of these smaller datagrams is referred to as a **fragment**.

- Fragments need to be reassembled before they reach the transport layer at the destination.

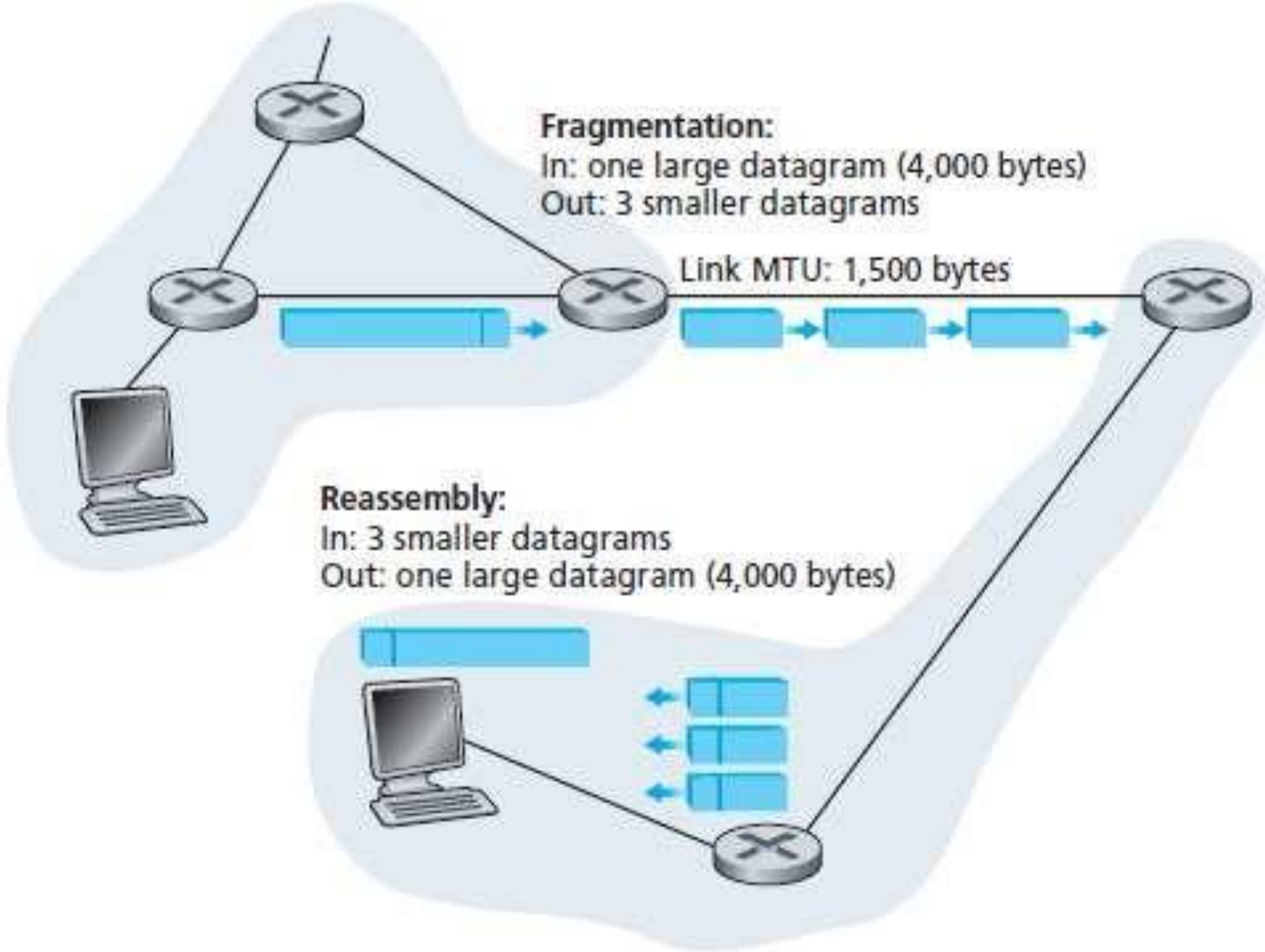
- The designers of IPv4 decided to put the job of datagram reassembly in the end systems rather than in network routers.

IP Datagram Fragmentation

- When a destination host receives a series of datagrams from the same source, it needs to determine whether any of these datagrams are fragments of some original, larger datagram.

- If some datagrams are fragments, it must further determine when it has received the last fragment and how the fragments it has received should be pieced back together to form the original datagram.

- To allow the destination host to perform these reassembly tasks, the designers of IP (version 4) put ***identification***, ***flag***, **and** ***fragmentation offset*** **fields in the IP datagram header.**


Fragmentation:
In: one large datagram (4,000 bytes)
Out: 3 smaller datagrams
Link MTU: 1,500 bytes
Reassembly:
In: 3 smaller datagrams
Out: one large datagram (4,000 bytes)

IP Datagram Fragmentation

- At the destination, the payload of the datagram is passed to the transport layer only after the IP layer has fully reconstructed the original IP datagram.
- If one or more of the fragments does not arrive at the destination, the incomplete datagram is discarded and not passed to the transport layer.

Fields Related to Fragmentation

- **Identification. This 16-bit field identifies a datagram originating from the source** host.
- The combination of the identification and source IP address must uniquely define a datagram as it leaves the source host.
- When a datagram is fragmented, the value in the identification field is copied into all fragments.
- The identification number helps the destination in reassembling the datagram. It knows that all fragments having the same identification value should be assembled into one datagram

Fields Related to Fragmentation

- **Flags. This is a three-bit field. The first bit is reserved (not used).**
- **The second bit is called the *do not fragment bit.***
- *If its value is 1, the machine must not fragment the* datagram.
- If it cannot pass the datagram through any available physical network, it discards the datagram and sends an ICMP error message to the source host.
- If its value is 0, the datagram can be fragmented if necessary.

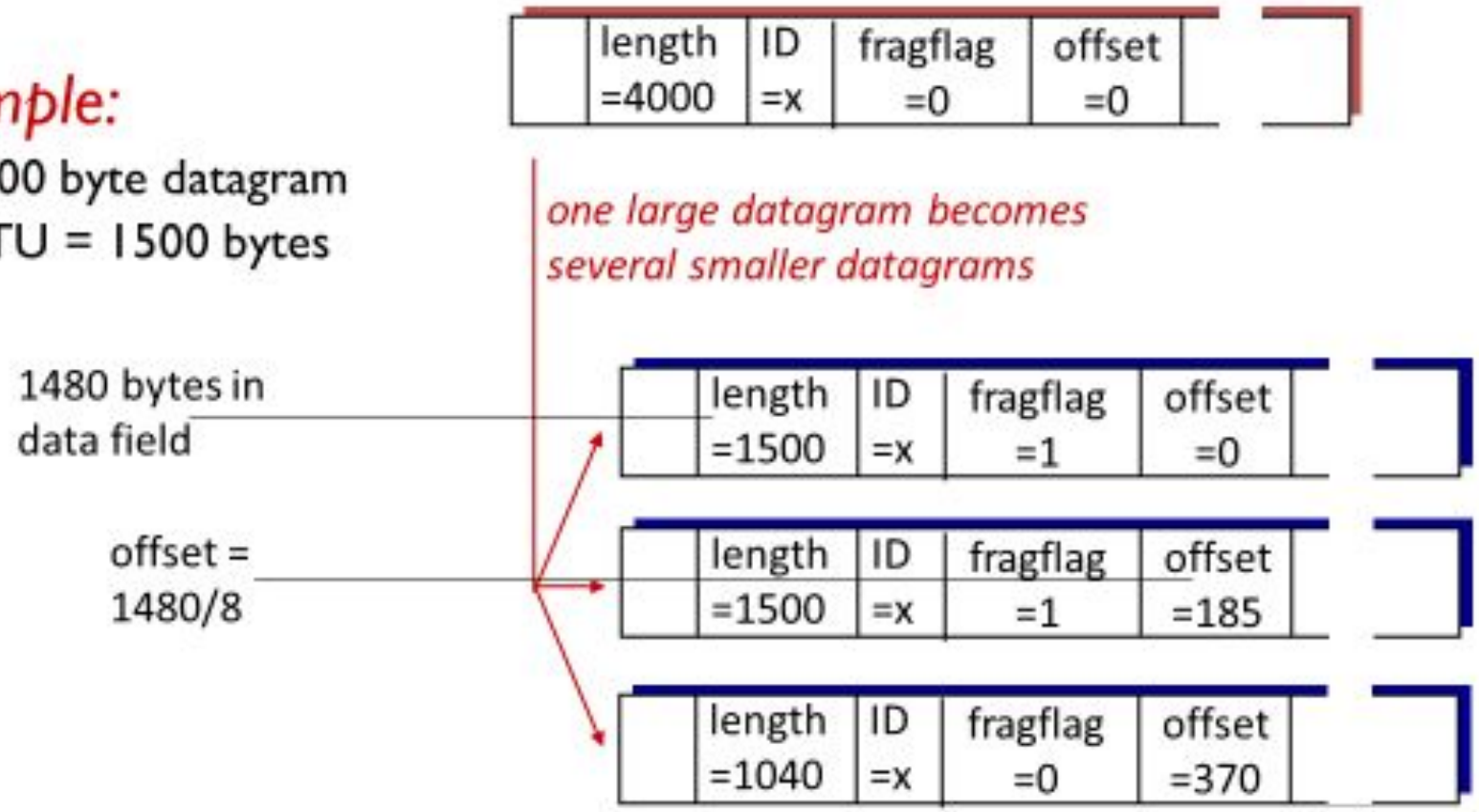
Fields Related to Fragmentation

- **The third bit is called the *more fragment bit.***
- *If its value is 1, it means the datagram is not the* last fragment; there are more fragments after this one.
- If its value is 0, it means this is the last or only fragment

IP fragmentation, reassembly

example:

- 4000 byte datagram
- MTU = 1500 bytes



IP fragments

Fragment	Bytes	ID	Offset	Flag
1st fragment	1,480 bytes in the data field of the IP datagram	identification = 777	offset = 0 (meaning the data should be inserted beginning at byte 0)	flag = 1 (meaning there is more)
2nd fragment	1,480 bytes of data	identification = 777	offset = 185 (meaning the data should be inserted beginning at byte 1,480. Note that 185 · 8 = 1,480)	flag = 1 (meaning there is more)
3rd fragment	1,020 bytes (= 3,980–1,480–1,480) of data	identification = 777	offset = 370 (meaning the data should be inserted beginning at byte 2,960. Note that 370 · 8 = 2,960)	flag = 0 (meaning this is the last fragment)

IP Datagram Fragmentation

- But fragmentation also has its costs.
- First, it complicates routers and end systems, which need to be designed to accommodate datagram fragmentation and reassembly.
- Second, fragmentation can be used to create DoS attacks, whereby the attacker sends a series of unexpected fragments, where the attacker sends a stream of small fragments to the target host, none of which has an offset of zero.

IP Datagram Fragmentation

- The target can collapse as it attempts to rebuild datagrams out of the degenerate packets.
- Another class of exploits sends overlapping IP fragments, that is, fragments whose offset values are set so that the fragments do not align properly.
- Vulnerable operating systems, not knowing what to do with overlapping fragments, can crash .
- A new version of the IP protocol, IPv6, does away with fragmentation altogether, thereby streamlining IP packet processing and making IP less vulnerable to attack.