The Internet Protocol: IPV4 Packet Fragmentation & Reassembly

In this lesson, we'll study IP version 4 fragmentation and reassembly.

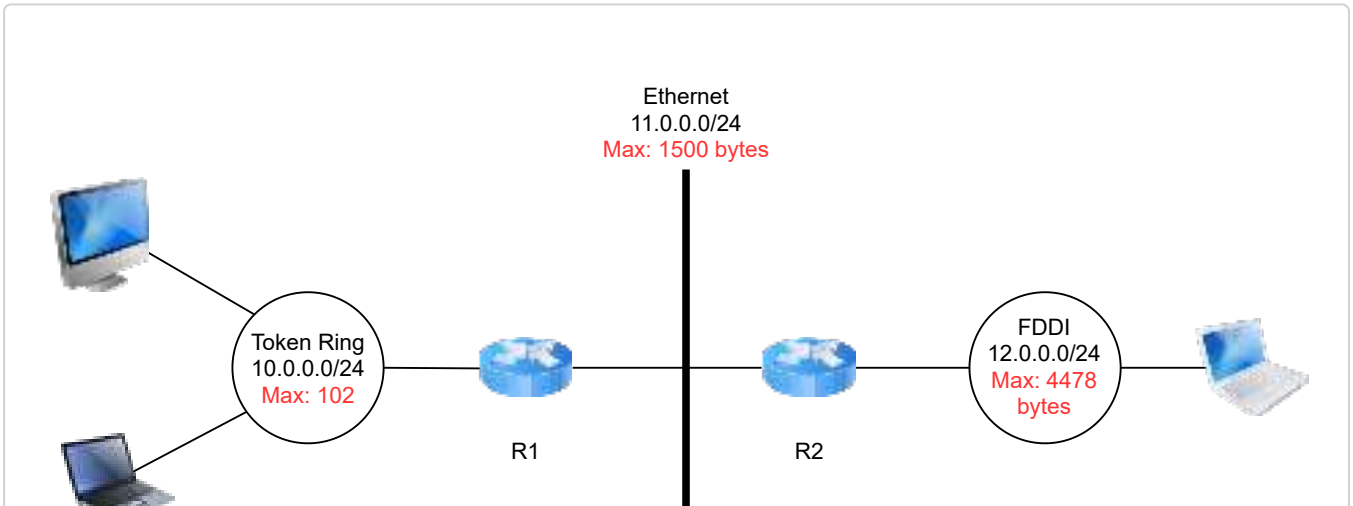
WE'LL COVER THE FOLLOWING

- Why Fragmentation?
- How Fragmentation Works
- How Reassembly Works
  - Handling Loss & Duplicates
- Quick Quiz!

Why Fragmentation?

Although IPv4 packets can be as big as 64kB, few data link layer technologies can send a 64 KB IPv4 packet inside a frame.

Furthermore, as in the figure below, if the host on the FDDI network abides by its own data link layer's maximum packet size of 4478 bytes, the resulting data link layer frame would violate the maximum frame size of the Ethernet between routers R1 and R2. Hence, a host may end up sending a packet that is too large for a data link layer technology used by (an) intermediate router(s).



The need for fragmentation and reassembly

To solve these problems, IPv4 includes a **packet fragmentation and reassembly mechanism** in both hosts and intermediate routers. In IPv4, fragmentation is completely performed in the IP layer and a large IPv4 packet is fragmented into two or more IPV4 packets (called fragments).

How Fragmentation Works

The IPv4 fragmentation mechanism relies on four fields of the IPv4 header:

- **Length**
- **Identification**
- The **flags**
  - **More fragments**
  - **Don't Fragment (DF)**. When this flag is set, it indicates that the **packet cannot be fragmented**
- **Fragment Offset**.

The **basic operation of IPv4 fragmentation** is as follows:

- A large packet is fragmented into two or more fragments where the size of all fragments, except the last one, is equal to the Maximum Transmission Unit of the link used to forward the packet.
- The Length field in each fragment indicates the length of the payload and the header **of the fragment**.
- Each IPv4 packet contains a 16 bit **Identification** field. When a packet is fragmented, the Identification of the large packet is copied in all fragments to allow the destination to reassemble the received fragments together.
- In each fragment, the **Fragment Offset** indicates, in units of 8 bytes, the position of the payload of the fragment in the payload of the original packet.
- When the **Don't Fragment (DF)** flag is set, it indicates that the **packet**

cannot be fragmented.

- Finally, the **More fragments** flag is set only in the last fragment of a large packet.

How Reassembly Works

The fragments of an IPv4 packet **may arrive at the destination in any order** since each fragment is forwarded independently in the network and may follow different paths. Furthermore, some fragments **may be lost and never reach the destination**.

The **reassembly algorithm** used by the destination host is roughly as follows:

1. First, the destination can verify whether a received IPv4 packet is a fragment or not by checking the value of the **More fragments** flag and the **Fragment Offset**. If the Fragment Offset is set to 0 and the More fragments flag is reset, the received packet has not been fragmented. Otherwise, the packet has been fragmented and must be reassembled.
2. The reassembly algorithm relies on the Identification field of the received fragments to associate a fragment with the corresponding packet being reassembled.
3. Furthermore, the Fragment Offset field indicates the position of the fragment payload in the original unfragmented packet.
4. Finally, the packet with the More fragments flag reset allows the destination to determine the total length of the original unfragmented packet.

Handling Loss & Duplicates

Note that the reassembly algorithm must **deal with the unreliability of the IP network**: fragments may be duplicated or may never reach the destination. The destination can easily **detect fragment duplication with the Fragment Offset**.

To deal with fragment losses, the reassembly algorithm must bind the time during which the fragments of a packet are stored in its buffer while the packet is being reassembled. This can be implemented by starting a timer

when the first fragment of a packet is received. If the packet has not been

reassembled upon expiration of the timer, all fragments are discarded and the packet is considered to be lost.

Quick Quiz!

1

Given the sample MTU size of 200 and an IP datagram of size 1999, how many fragments will be created?

COMPLETED 0%

1 of 9

In the next lesson, we'll study an error-reporting protocol: **ICMP**.