Lab 3 IP Fragmentation

1. The format of IP packet

Offsets	Octet	0								1								2								3							
Octet	Bit	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0	0	Version				IHL				DSCP						ECN		Total Length															
4	32	Identification																Flags			Fragment Offset											
8	64	Time To Live								Protocol								Header Checksum															
12	96	Source IP Address																															
16	128	Destination IP Address																															
20	160	Options (if IHL > 5)																															

Please refer to the Textbook and corresponding lecture slides for the details of IP Packet, e.g., definitions of each fields.

2. IP Fragmentation

A datagram can travel through different networks. Each router decapsulates the IPv4 datagram from the frame it receives, processes it, and then encapsulates it in another frame. The format and size of the sent frame depend on the protocol used by the physical network. For example, if a router connects a LAN to a WAN, it receives a frame in the LAN format and sends a frame in the WAN format.

2.1. Maximum Transfer Unit (MTU)

Each data link layer protocol has its own frame format in most protocols. One of the fields defined in the format is the maximum size of the data field. In other words, when a datagram is encapsulated in a frame, the total size of the datagram must be less than this maximum size, which is defined by the restrictions imposed by the hardware and software used in the network.

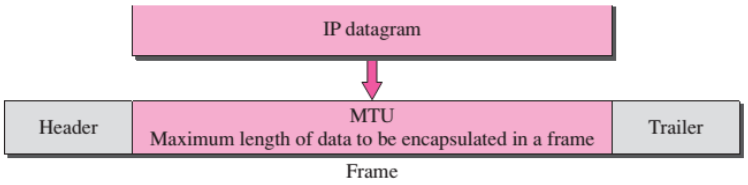

Figure 3-1 MTU

The value of the MTU depends on the physical network protocol. Following table shows the values for some protocols.

Table 3-1 MTUs in different networks

Protocol	MTU	Protocol	MTU
Hyperchannel	65,535	Ethernet	1,500

Token Ring (16Mbps)	17,914	X.25	576
Token Ring (4Mbps)	4,464	PPP	296
FDDI	4,352	--	--

To make the IPv4 protocol be independent of the physical network, the designers decided to make the maximum length of the IPv4 datagram equal to 65,535 bytes. This makes transmission more efficient if we use a protocol with an MTU of this size. However, for other physical networks, we must divide the datagram to make it possible to pass through these networks. This is called **fragmentation**.

When a datagram is fragmented, each fragment has its own header with most of the fields repeated. A fragmented datagram may itself be fragmented if it encounters a network with an even smaller MTU. In other words, a datagram can be fragmented several times before it reaches the final destination.

In IPv4, a datagram can be fragmented by the source host or any routers in the path, although there is a tendency to limit fragmentation only at the source. The reassembly of the datagram, however, is done only by the destination host, because each fragment becomes an independent datagram. Fragmented datagrams can travel through different routes, and all the fragments belonging to the same datagram should finally arrive at the destination host. So it is logical to do the reassembly at the final destination.

When a datagram is fragmented, some required parts of the header must be copied by all fragments. The option field may or may not be copied, as we will see in the next section. The host or router that fragments a datagram must change the values of three fields: ***flags, fragmentation offset, and total length***. The rest fields must be copied. Of course, the value of the ***checksum*** must be recalculated regardless of fragmentation.

2.2. Fields Related to Fragmentation

- **Identification**. This 16-bit field identifies a datagram originating from the source host. All fragments have the same identification number, the same as the original datagram. The identification number helps the destination in reassembling the datagram. All fragments having the same identification value must be assembled into one datagram.
- **Flags**. This is a 3-bit field. The first bit is reserved. The second bit is called *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. 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 (see Figure 3-10).

Figure 3-10 Flags used in fragmentation

- **Fragmentation offset**. This 13-bit field shows the relative position of this fragment with respect to the whole datagram. It is the offset of the data in the original datagram measured in units of 8 bytes. Figure 3-11 shows a datagram with a data size of 4000 bytes fragmented into three fragments.

  The bytes in the original datagram are numbered 0 to 3999. The first fragment carries bytes 0 to 1399. *The offset for this datagram is 0/8 =0*. The second fragment carries bytes

1400 to 2799; the offset value for this fragment is 1400/8 = 175. Finally, the third fragment carries bytes 2800 to 3999. The offset value for this fragment is 2800/8 = 350.

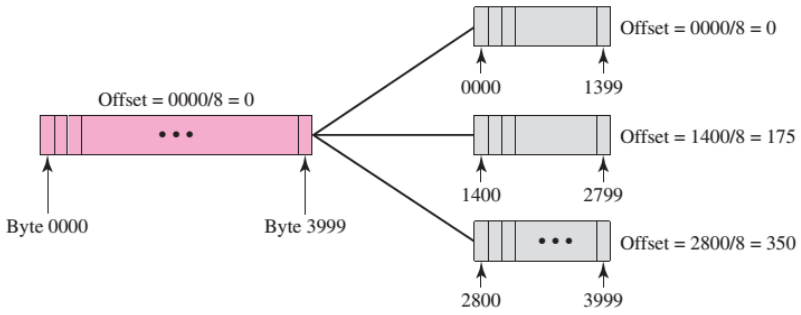

Figure 3-11 Fragmentation example

Remember that the value of the offset is measured by 8 bytes. This is done because the length of the offset field is only 13 bits and cannot represent a sequence of bytes greater than 8191. This forces hosts or routers that fragment datagrams to choose a fragment size so that the first byte number is divisible by 8.