Packet Fragmentation

Every packet based network has an MTU(Maximum Transmission Unit) size. The MTU is the size of the largest packet that that network can transmit.
Packets larger than the allowable MTU must be divided into smaller packets or fragments to enable them to traverse the network.

Network	Standard MTU
Ethernet	1500
Token Ring	4096

Packet Headers

Every IP packet has an IP (Internet Protocol) header that stores information about the packet, including:

- Version
- IHL
- Type of Service
- Total Length
- Identification
- Flags
- Fragment Offset
- Time to Live
- Protocol
- Header Checksum
- Source Address
- Destination Address
- Options

Note: For more information on the IP header, see RFC 791 – Internet Protocol.
Three of these fields are involved in packet fragmentation.

- Identification
- Flags
- Fragment Offset

Identification: 16 bits
An identifying value that the sender assigns to aid in assembling a datagram's fragments.

Flags: 3 bits
Various Control Flags.

```
Bit 0: reserved, must be zero
Bit 1: (DF) 0 = May Fragment, 1 = Don't Fragment.
Bit 2: (MF) 0 = Last Fragment, 1 = More Fragments.
```

```
 0 1 2

+---+---+---+

| | D | M |

| 0 | F | F |

+---+---+---+
```

Fragment Offset: 13 bits
This field indicates where in the datagram this fragment belongs.

The fragment offset is measured in units of 8 octets (64 bits). The first fragment has offset zero.

Much like the IP header, the TCP (Transmission Control Protocol) header stores information about the packet:

- Source Port
- Destination Port
- Sequence Number
- Acknowledgement Number
- Data Offset
- Flags
- Window
- Checksum
- Urgent Pointer
- Options

- Padding

Note: For more information on the TCP header, see RFC 793 – Transmission Control Protocol.

A Packet Fragmentation Example

If a 2,366 byte packet enters an Ethernet network with a default MTU size, it must be fragmented into two packets.
The first packet will:

- Be 1,500 bytes in length. 20 bytes will be the IP header, 24 bytes will be the TCP header, and 1,456 bytes will be data.
- Have a DF bit equal to 0 to mean "May Fragment" and an MF bit equal to 1 to mean "More Fragments."
- Have a Fragmentation Offset of 0.

The second packet will:

- Be 910 bytes in length. 20 bytes will be the IP header, 24 bytes will be the TCP header, and 866 bytes will be data.
- Have the DF bit equal to 0 to mean "May Fragment" and the MF bit equal to 0 to mean "Last Fragment."
- Have a Fragmentation Offset of 182 (Note: 182 is 1456 divided by 8).

The Packet Fragmentation Attack

Packet fragmentation can be utilized to get around blocking rules on some firewalls.

This is done by cheating with the value of the Fragment Offset. The trick is to set the Fragment Offset's value on the second packet so low that instead of appending the second packet to the first packet, it actually overwrites the data **and** part of the TCP header of the first packet.
If someone wants to `telnet` into a network where a packet filtering firewall blocks TCP port 23, SMTP port 25 is allowed into that network.

The user would have to send two packets:

The first packet would:

- Have a Fragmentation Offset of 0.

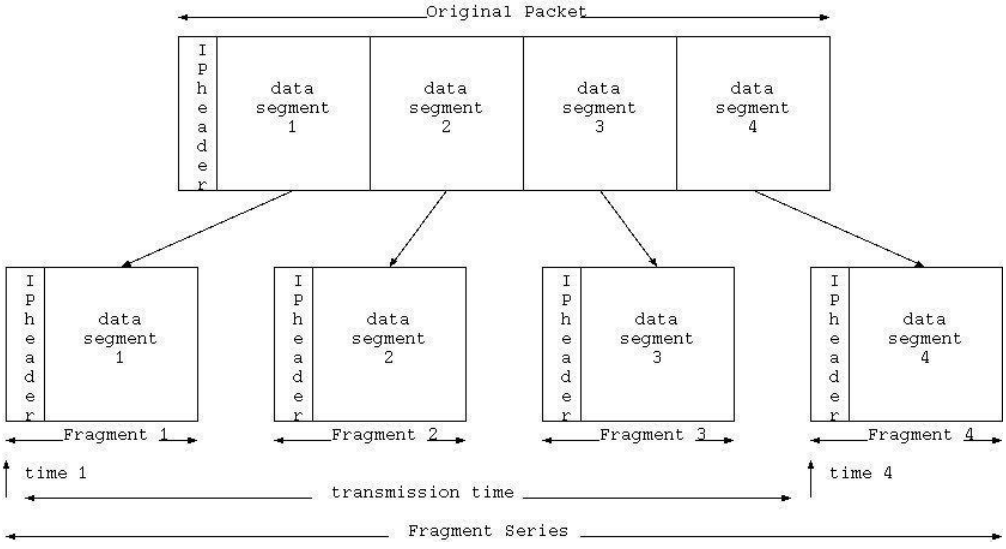
- Have a DF bit equal to 0 to mean “May Fragment” and an MF bit equal to 1 to mean “More Fragments.”
- Have a Destination Port in the TCP header of 25. TCP port 25 is allowed, so the firewall would allow that packet to enter the network.

The second packet would:

- Have a Fragmentation Offset of 1. This means that the second packet would actually overwrite everything but the first 8 bits of the first packet.
- Have a DF bit equal to 0 to mean “May Fragment” and an MF bit equal to 0 to mean “Last Fragment.”
- Have a Destination Port in the TCP header of 23. This would normally be blocked, but will not be in this case!

The packet filtering firewall will see that the Fragment Offset is greater than zero on the second packet. From this data, it will deduce that the second packet is a fragment of another packet and it will not check the second packet against the rule set.

When the two packets arrive at the target host, they will be reassembled. The second packet will overwrite most of the first packet and the contents of the combined packet will go to port 23.



Source: http://www.tech-faq.com/packet-fragmentation.html