# IP fragmentation

**IP fragmentation** is an Internet Protocol (IP) process that breaks datagrams into smaller pieces (fragments), so that packets may be formed that can pass through a link with a smaller maximum transmission unit (MTU) than the original datagram size. The fragments are reassembled by the receiving host.

RFC 791 describes the procedure for IP fragmentation, and transmission and reassembly of datagrams. RFC 815 describes a simplified reassembly algorithm.

The *Identification* field along with the *foreign* and *local internet address* and the *protocol ID*, and *Fragment* offset field along with *Don't Fragment* and *More Fragment* flags in the IP protocol header are used for fragmentation and reassembly of IP datagrams.[:24:9]

Under IPv4, a router that receives a protocol data unit (PDU) larger than the next hop's MTU has two options: drop the PDU and send an Internet Control Message Protocol (ICMP) message which indicates the condition *Packet too Big*, or fragment the IP packet and send it over the link with a smaller MTU. IPv6 hosts are required to determine the optimal Path MTU before sending packets; however, it is guaranteed that any IPv6 packet smaller than or equal to 1280 bytes must be deliverable.

If a receiving host receives a fragmented IP packet, it has to reassemble the datagram and pass it to the higher protocol layer. Reassembly is intended to happen in the receiving host but in practice it may be done by an intermediate router, for example, network address translation (NAT) *may* need to re-assemble fragments in order to translate data streams.

IP fragmentation can cause excessive retransmissions when fragments encounter packet loss and reliable protocols such as TCP must retransmit all of the fragments in order to recover from the loss of a single fragment. Thus, senders typically use two approaches to decide the size of IP

datagrams to send over the network. The first is for the sending host to send an IP datagram of size equal to the MTU of the first hop of the source destination pair. The second is to run the path MTU discovery algorithm, described in RFC 1191, to determine the path MTU between two IP hosts, so that IP fragmentation can be avoided.

## Impact of fragmentation on network forwarding

When a network has multiple parallel paths, technologies like LAG and CEF split traffic across the paths according to a hash algorithm. One goal of the algorithm is to ensure all packets of the same flow are sent out the same path to minimize unnecessary packet reordering.

## IPv4 and IPv6 differences

The details of the fragmentation mechanism, as well as the overall architectural approach to fragmentation, are different between IPv4, the first official version of the Internet Protocol, and IPv6, the newer version. In IPv4, routers perform fragmentation, whereas in IPv6, routers do not fragment, but drop the packets that are larger than their MTU. Though the header formats are different for IPv4 and IPv6, analogous fields are used for fragmentation, so the same algorithm can be reused for IPv4 and IPv6 fragmentation and reassembly.

In IPv4, hosts must make a best-effort attempt to reassemble fragmented IP datagrams with a total reassembled size of up to 576 bytes. They may also attempt to reassemble fragmented IP datagrams larger than 576 bytes, but they are also permitted to silently discard such larger datagrams. Applications are recommended to refrain from sending datagrams larger than 576 bytes unless they have prior knowledge that the remote host is capable of accepting or reassembling them.:12

In IPv6, hosts must make a best-effort attempt to reassemble fragmented datagrams with a total reassembled size of up to 1500 bytes, larger than IPv6's minimum MTU of 1280 bytes. Fragmented datagrams with a total reassembled size larger than 1500 bytes may optionally be silently

discarded. Applications relying upon IPv6 fragmentation to overcome a path MTU limitation must explicitly fragment the datagram at the point of origin; however, they should not attempt to send fragmented datagrams with a total size larger than 1500 bytes unless they know in advance that the remote host is capable of reassembly.

## See also

- IPv4 § Fragmentation and reassembly
- IPv6 packet § Fragmentation
- IP fragmentation attacks

## References


1. ^ **a b c** *Internet Protocol, Information Sciences Institute, September 1981, RFC 791*
2. ^ **a b** *David D. Clark (July 1982), IP Datagram Reassembly Algorithms, RFC 815*
3. **^** *Architectural Implications of NAT, November 2000, RFC 2993*
4. **^** *Christopher A. Kent, Jeffrey C. Mogul. "Fragmentation Considered Harmful" (PDF).*
5. **^** *Path MTU Discovery, November 1990, RFC 1191*
6. **^** *S. Deering; R. Hinden (December 1998), Internet Protocol, Version 6 (IPv6) Specification, RFC 2460*


## External links

- What is packet fragmentation?
- The Never-Ending Story of IP Fragmentation