IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Volume-2, Issue-4 E-ISSN: 2347-2693

IP Packet Fragmentation and Reassembly at Intermediate Routers

Gajam Pavithra[1*] and D. Teja Santosh[2]

[1*,2] *Department of Computer science & engg, Gitam University, Hyderabad*

www.ijcaonline.org

Received: 17/03/2014 Revised: 25/03/2014 Accepted: 22/04/2014 Published: 30/04/2014

***Abstract*—** IP packet fragmentation and reassembly is that, a packet is split into several pieces (fragments) that fit into packet size of the link to be traversed and combine (reassemble) these pieces or fragments at the receiving node to form original packet or datagram. In this paper, we consider reassembly of fragments allowed at the intermediate routers based on the Maximum Transmission Unit (MTU). Without waiting for the destination to reassemble it can be done at the intermediate hops where ever needed. The three fields of IP header used for fragmentation and reassemble are the packet identifier, each fragment is attached with the identifier and reassembling of fragments is done based on the identifier of the fragments. The fragment offset field gives the position of the fragment along with More Fragment (MF bit) and Don't Fragment (DF bit) flags and the total length field. These two fields fragment offset and fragment length are combinedly used to place the fragments of a packet in right order. This paper, the IP packet fragmentation and reassembly at intermediate routers will be an option to reduce the load on routers due to more number of fragmented packets and improves the performance and increase the efficiency of the router.

***Keywords*—** IP, Packet, Datagram, Fragmentation, Reassembly, MTU size, Router, Source, Destination

I. Introduction

The Internet Protocol (IP) is the method or protocol which enables communication between the networks. Each computer or host has unique IP address on the internet and across the network data can be delivered from source host to the destination host solely based on the IP addresses.

The internet layer has the IP data attached with the IP header. The IP header is 20 to 60 bytes in length and contains information which is essential to routing and delivery (IP header format includes the fields used to fragment and reassemble internet datagrams when necessary for transmission through networks). The IP Data is 65536 bytes in length and should not exceed this length.

The fields of IP header mainly used for fragmentation and reassembly are:

Total length: 8 bit field. This specifies the total number of bytes of the data plus the header.
Identification field: The identification is 16 bits. Each IP datagram is given the identifier which is assigned by the sender to aid in reassembling the fragments of a datagram.
Flags: The flags are 3 bit field. Bit 0, bit 1 and bit 2. These flag bits are important while fragmentation and reassembly. The bit 0 is reserved and always set to 0. The bit 1 is DF bit tells whether the packet is to fragment or not and the bit 2 is MF bit tells whether the fragment is last fragment or there may be some more fragments to reassemble.
Bit 0: is reserved, and is always set to 0.
Bit 1: DF bit (DF = 0 May Fragment, DF = 1 Don't Fragment).
Bit 2: MF bit (MF = 0 Last Fragment, MF = 1 More Fragments).

Corresponding Author: *Pavithra Gajam, pavithra0428@gmail.com*
Department of Computer science & engg, Gitam University, Hyderabad

Fragment offset: The fragment offset is 13 bits field. This value is a multiple of eight bytes. This fragment offset gives the position of the fragment and places where a fragment belongs in the original IP datagram.
Source IP Address: 32 bit internet address of the original sender.
Destination IP Address: 32 bit internet address of the receiver.

1.1. MTU size

The standardized technique in computer networks to determine the maximum transmission unit (MTU) size is pathMTU Discovery (PMTUD) between two IP hosts, usually with the goal of avoiding IP fragmentation.

When a datagram arrives at the router whose size is larger than the MTU size, than the packet is dropped and send back with an Internet Control message Protocol (ICMP) as the fragmentation is needed containing its MTU, allowing the source host to reduce its path MTU appropriately. The process is repeated until the MTU is small enough to traverse the entire path without fragmentation.

II. IP FRAGMENTATION AND REASSEMBLY

IP fragmentation and reassembly is one of the mechanisms of IP. Under certain circumstances, when a datagram is small enough, it is originally transmitted as a single unit and arrives at its final destination. When a datagram is larger than the MTU size, then the datagram is broken into several fragments and traversed along the link and at the receiving host must accumulate these fragments until enough have arrived to completely reconstitute the original datagram.

This paper describes a way of dealing with reassembly which reduces the bookkeeping problem to a minimum, which requires for storage only one buffer equal in size to the final datagram being reassembled, which can reassemble a datagram from any number of fragments arriving in any order with any possible pattern of overlap and duplication, and which is appropriate for almost any sort of operating system.

2.1. Fragmentation

When an IP datagram size is too large than the maximum packet size (MTU size) to be traversed, then datagram has to be split into several pieces (called fragments) that fits into the packet size of the link to be traversed called as fragmentation. It allows the fragments to be further fragmented and fragments are allowed to take the different routes to traverse and reach destination host.

The three fields in the IP header mainly allow this versatility are the identification field, total length field and the fragment offset field. Each datagram is given a packet identifier, when fragmentation is done, each fragment is attached with the identifier; each fragment also carries an offset field (which is used at reassembly) and a fragment length.

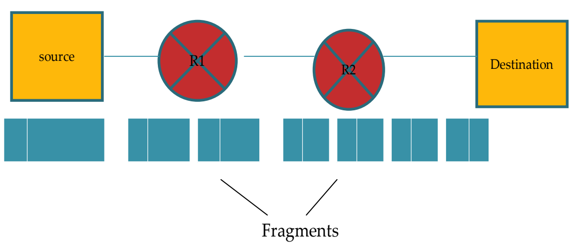

Fig 1. Fragmentation

2.2. Reassembly

It's important to understand that while reassembly is the compliment to fragmentation, the two processes are not symmetric.

The fragments or pieces of a datagram have to be combined (reassemble) at the receiving node called as reassembly. If all the fragments arrive at the receiver, the packet identifier allows the receiver to reassemble all the fragments with a single packet. The fragment offset field (which gives the position of the fragment) and total length are together used to place all the fragments in the right order. The reassembled packet can be passed to the upper layer for further processing. This process combinedly known as fragmentation and reassembly.

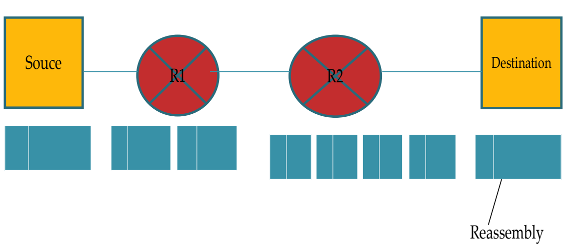

Fig 2. Reassembly

III. RELATED WORK

When a source has to send a packet to the destination, it has to query the nearest router to find the smallest MTU to deliver the packet. Routing protocols can help in finding out smallest MTU to the destination. In this, each router keeps the information about the smallest MTU to the destination along with next hop to send the packets. This method works well in interconnected LANs and it does not support with hierarchical routing, since the information about all destinations can not be maintained at all routers. Thus for packets traveling across the network, the router which is nearest to the source does not have the information about the smallest MTU size in the portion of the path that lies in the destination. Each have a smallest MTU size as the default MTU size in the area; this can lead to using too small a packet size.

IV. PROPOSED WORK

The reassembly process at intermediate routers is a new reassembly scheme that always outperforms the older notion of hop reassembly.

IP reassembly has to handle out of order fragments, lost fragments and duplicate fragments which make the implementation complex. If in case, fragments arrive in order without any loss of fragments or duplication of fragments, then reassembly process is simple. The fragments can be reassembled as they arrive until the last fragment arrives and the reassembled packet can pass to higher layer.

In the IP header four fields which enable reassembly are: a datagram identifier which tells the fragments belong to same packet. Fragment length which specifies the total length. The flags ('more fragment') which indicates whether the fragment is first or last fragment. The fragment offset which indicates the position of the fragment in the datagram. The implementation keeps a reassembly list which contains the fragmented datagrams. Each fragment in the reassembly list is kept in increasing order of their offsets to reassemble.

4.1. Intermediate reassembly

In the existing system IP fragmentation is done at any intermediate router and IP reassembly is done only at the destination called as Destination Reassembly (DR). In some networks, a packet may fragment at a router over a single link and have a next hop router which is also on the same link may reassemble the packet called as Hop Reassembly (HR). In hop reassembly, the reassembly at router is done only when the previous hop router will fragments the packet.

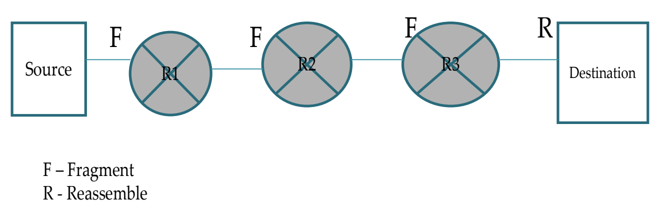

Fig 3. Destination reassembly

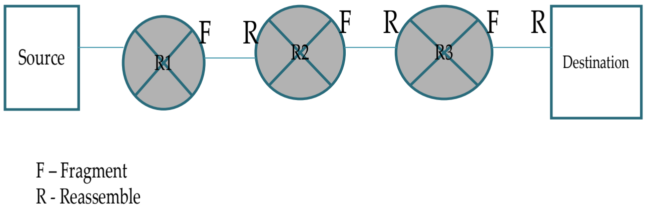

Fig 4. Hop reassembly

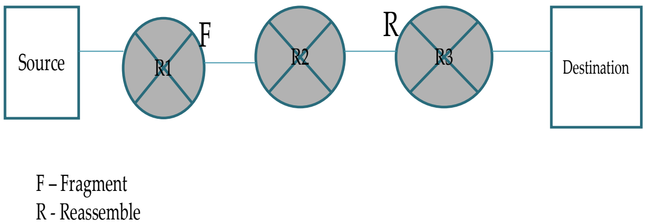

Fig 5. Intermediate reassembly

Intermediate Reassembly Algorithm

Step1. A fragment F is received.

Step2. Check fragment F with other fragments for same packet P.

Step3. If reassembly predicate is satisfied then goto step5, 6, 7.

Step4. Partially reassembled packets P that not satisfied then goto step5, 6, 7.

Step5. If packet is complete then send packet P to next hop.

Step6. Elseif (at destination or hop reassembly) then destroy packet P.

Step7. Else (Intermediate reassembly)
Send coalesced fragments to next hop.

If the router outgoing link MTU size is not large enough to travel the datagram, it has to fragment. Consider two cases: in the first case, a packet size is of 1500 bytes and is fragmented into three fragments each of 500 bytes which arrives at a router which has an outbound MTU size 1500 bytes. Here in this case router performs hop reassembly. In the second case, it is similar and the outbound link MTU size is 1000 bytes. In this case we suggest partial reassembly.

Partial Reassembly: Partial reassembly keeps reassembling the fragments until the size exceeds the outbound MTU. To store the partially reassembled packets datalink buffering is used. If the fragments arrive in same order as they fragment (FIFO) without any loss, we follow the same reassembly algorithm. If the fragments are inorder for the same packet, we coalesce it with previous fragments. Some times we may do partial reassembly at destination.

If we maintain a separate reassembly buffers for each concurrent flow then memory costs would be large. The simple approach is, for each current packet P one reassembly buffer is used. Before the reassembly predicate P is satisfied, another fragment for a different packet is arrived then P is pushed. Thus we reduce the memory cost.

4.2. Advantages of Intermediate reassembly

Intermediate reassembly has some advantages compared with the existing one.

- Intermediate reassembly sends fragments to next hop whenever possible. It does not require cooperation from previous hop.
- More discrimination as the intermediate reassembly uses the information about next hop MTU, so it can make better choices to reassemble.
- Intermediate reassembly uses IP fragmentation header so there is no issue of protocol changes.

V. CONCLUSION

We have introduced a new form of reassembly known as intermediate reassembly as it discriminate between packets to destination can often perform better that can benefit from reassembly. Since the increase of load on the routers due to its high fragmented packets passing through the network. By reassembling the packets at the routers based on the identification field and MF bit, the performance of the routers has been increased. Reassembly of datagram fragments at intermediate routers can be done for load less travel of packets. Using FIFO reassembly, intermediate reassembly can be implemented in routers at low cost.

ACKNOWLEDGMENT

The author wish to thank Mr. D. Teja Santosh who is currently working as Assistant Professor in Gitam University, Hyderabad in the department of Computer Science and Engineering for his valuable guidance during this work. And also like to thanks to all teachers and staff for their valuable suggestions and feedback.

REFERENCES

[1] J. Mogul, S. Deering, “Path MTU Discovery”, RFC – 1191, Stanford University, November 1990.

[2] Shoch. J, "Inter-Network Naming, Addressing, and Routing", COMPCON, IEEE Computer Society, Fall 1978.

[3] Shoch. J, "Packet Fragmentation in Inter-Network Protocols", Computer Networks, v. 3, n. 1, February 1979.

[4] David D. Clark, “IP Datagram Reassembly Algorithms”, RFC – 815, MIT Laboratory for Computer Science Computer Systems and communications Group, July 1982.

[5] J. Romkey, “A Nonstandard For Transmission of IP Datagrams Over Serial Lines: SLIP”, RFC – 1055, June 1988.

[6] J. Heffner, M. Mathis, B. Chandler, “IPv4 Reassembly Errors at High Data Rates”, RFC – 4963, PSC, July 2007.

[7] C. Hedrick, “Routing Information Protocol”, RFC – 1058, Rutgers University, June 1988.

[8] D. Waitzman, “A Standard for the Transmission of IP Datagrams on Avian Carriers”, RFC - 1149, BBN STC, 1 April 1990.

[9] R. Hinden Nokia, S. Deering, “IP Version 6 Addressing Architecture”, RFC – 4291, Cisco Systems, February 2006.

[10] W. Townsley, O. Troan, "IPv6 Rapid Deployment on IPv4 Infrastructures (6rd) -- Protocol Specification", RFC – 5969, Cisco Systems, August 2010.
[11] R. Hinden Nokia, S. Deering, "Internet Protocol, Version 6 (IPv6) Specification", RFC – 2460, Cisco Systems, December 1998.
[12] J. Moy, "OSPF Version 2", RFC – 2328, Ascend Communications, Inc. April 1998.
[13] S. Krishnan Ericsson, "Handling of Overlapping IPv6 Fragments", RFC – 5722, December 2009.
[14] J. McCann, S. Deering, J. Mogul, "Path MTU Discovery for IP version 6", RFC – 1981, August 1996.
[15] Sharmeen Kaur, Raveena Singh and Shivya Gagneja, "Network Security and Methods Of Encoding and Decoding", International Journal Of Computer Science and Engineering, Volume - 2 Issue – 2, 2347 – 2693, 2014.

AUTHORS PROFILE

Gajam Pavithra
The author Gajam Pavithra is currently pursuing masters degree program in computer science and engineering in Gitam University, Hyderabad, India. E-mail: pavithra0428@gmail.com

D. Teja Santosh
Mr. D. Teja Santosh is currently working as an assistant professor in the department of computer science and engineering in Gitam University, Hyderabad, India. E–mail: dts.bond@gmail.com

