ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 7, July 2016

A Survey on IP Fragmentation Effectiveness and Protocol`s Techniques for Higher Performance

Ahmed Alahda[1], Dr.G.N.Shinde[2]

Research Scholar, Dept. of Computer Sciences, SRTM University, Nanded, Maharashtra, India[1]

Pro.Vice. Chancellor, SRTM University, Nanded, Maharashtra, India[2]

ABSTRACT: The work investigates the existing techniques to avoid fragmentation (IP fragmentation) process in IPv4. It also explains the fragmentation process in IPv4 to gain a clear idea of how fragmentation process is being handled. This work discusses the Path Maximum Transmission Unit discovery (PMTU), which is a standardized technology that works to protect the segments from being fragmented. It also explains how IPv6 protocol prevents fragmentation at intermediate routers. Furthermore, the work discusses the effectiveness of fragmentation as well solutions introduced for this matter. Also the work discusses the issues caused by IP fragmentation at intermediate routers which usually affect the performance of the network.

KEYWORDS: Fragmentation, IPv4, IPv6, Segmentation, PMTUD, Protocols

I. INTRODUCTION

IP fragmentation is a process of dividing the segments at intermediate router, where IP fragmentation can cause various issues during the data transfer from source to destination, in fact the source host is not aware of the MTU of each intermediate router to host destination. Therefore, IP fragmentation can occur. Generally, the segment size is not fixed as it differs from one protocol to another, for example the segment size of an Ethernet is 1500 bytes which may not pass a router that has less maximum transmission unit (MTU) allowance. The segments are a divided data packets that do not have a specific size as their size depends on the protocol used and the type of network it adapts.

Fragmentation process can create several security issues and decreases the performance of the transfer rate of data from source to destination. Basically, there is always a potential threat if fragmentation process occurs during the transfer process, such fact encourages the software designers to find solution such as PMTUD that works to avoid fragmentation at intermediate routes. When segments travel from source to destination it is not preferable to be fragmented but the process happen anyway in IPv4 as there is no other option if the MTU of the intermediate router is less than the segment size.

II. RELATED WORK

To move packets from a network with smaller MTU to one with a larger MTU is trivial, but the reverse is not. In order to handle this, IPv4 protocol uses fragmentation. It is the process of breaking up of the original packet into smaller fragments. Most of the fields of this header are inherited from the IP header of the original datagram. Thus, each fragment has same Identification (ID) field, protocol, source address and destination address but different offset field which for each fragment contains the distance, measured in 8-byte units, between the original datagram and the beginning of the particular fragment [1]. IP fragmentation breaks a packet into smaller fragments so that the fragments, which collectively form the entire packet, can pass through links with smaller Maximum Transfer Unit (MTU) than the actual packet size [2]. Packet fragmentation occurs when a device tries to transmit a packet that is larger than the maximum transmission unit size, or MTU, allowed by the link layer. When this occurs, the device can either drop the packet or fragment the packet into several smaller packets so that each will be no larger than the MTU. Using standard IP protocols, if the packet is fragmented and not dropped, then the original packet can be reassembled when all of the

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 7, July 2016

packets are received [3]. If a malicious entity knows that pair of hosts is communicating using a fragmented stream, it may present an opportunity for this entity to corrupt the flow. By sending high fragments (those with offset greater than zero) with a forged source address, the attacker can deliberately cause corruption as described above. Exploiting this vulnerability requires only knowledge of the source and destination addresses of the flow, and fragment boundaries. It does not require knowledge of port or sequence numbers [RFC 4963]. In order to assist in avoiding IP fragmentation at the endpoints of the TCP connection, the selection of the MSS value was changed to the minimum buffer size and the MTU of the outgoing interface (- 40). MSS numbers are 40 bytes smaller than MTU numbers because MSS is just the TCP data size, which does not include the 20 byte IP header and the 20 byte TCP header. MSS is based on default header sizes; the sender stack must subtract the appropriate values for the IP header and the TCP header depending on what TCP or IP options are being used, TCP MSS as described above takes care of fragmentation at the two endpoints of a TCP connection, but it doesn't handle the case where there is a smaller MTU link in the middle between these two endpoints [4]. IP address fragmentation is a critical factor that impacts addressing and routing scalability, it is also a key problem in IPv4 today. Address fragmentation is the phenomenon in which a single entity on the network has multiple noncontiguous IP address blocks or prefixes instead of a single prefix in the routing table. Address fragmentation increases routing table size, therefore degrades scalability as well as IP address lookup and routing performance in routers [5].

III. PROTOCOLS OVERVIEW

A- Fragmentation in IPv4:

The internet protocol version 4 has a major issue but a rescue process too with respect to data fragmentation, if a segment of such size, let's assume a 1500 bytes did pass the source router during its travel to the host destination while an intermediate router happened to have less capacity of passing such segment size, time to panic what could be done, so the designer of IPv4 solved the problem by introducing the fragmentation process. Fragmentation is a process that occurs when the size of the segment is larger than the MTU of any an intermediate router.

So an intermediate router operates on the segment to divide it to smaller packets of data called fragments each of these fragment is a part of the original segments, these fragments reach to the host destination after dividing them into smaller packets (fragments). Therefore, when a packet of data is segmented it gets stamped by an identification number, source address and destination address taken from the original segment. Basically when the host destination receives multiple datagram (fragments) it needs to identify them to allow them enter the host destination, but how many fragments the segment was divided the destination does not know.

Therefore, one fragment may never reach, in order for the host destination to know when to stop receiving. The last fragment has a flag set to 0 where the other fragments are set to 1, so after the last fragment is reached and before it reaches the user another process is performed called reassembling, which means gathering the fragment again to form the original segment at the host destination, before it gets to the transport layer.

Finally, when it reaches the transport layer it has to be ready as it was segmented at the host source transport layer. But what happens if one fragment is lost, in fact multiple incidents of losing fragment can happen, the only possible solution for the host destination is to discard the whole packet and send an ICPM to the host source stating that the data payload is incomplete, furthermore the host source retransmits the packet again to the host destination and still it cannot ensure the delivery unless it receives an ICPM stating that.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 7, July 2016

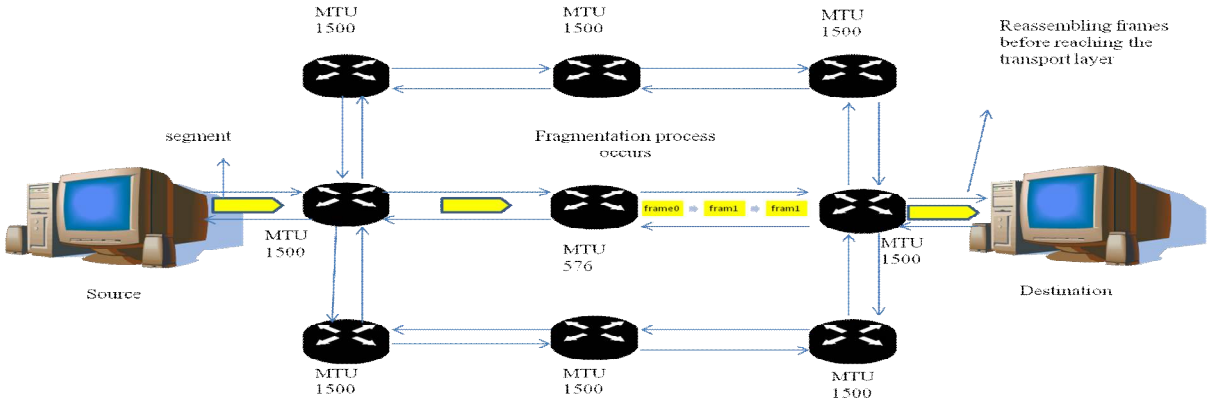

Figure 1: shows the segments and when fragmentation process occurs

Obviously everything has its cost, a fragmentation process is vulnerable to attack, causes delay in receiving data, complicates routers and it complicates the end system. Let us consider them one by one. 1- vulnerable to attack: lethal DoS attacks is an example of what may occur during the receiving and reassembling process at the host destination, actually a number of bizarre can be sent by attacker or even serial number of fragment whom don't have their flag set to 0 causing the system to collapse or overlapping of the entire packet. 2- Delay in receiving: the fact that a fragment(s) may never reaches to the host destination makes the fragmentation process insufficient, the retransmission of data packet which can happen due to the incomplete reassembling of fragments at the host destination creates a time delay because it requests a retransmission after it discard the data packet, this process may happen multiple time if same issue of MTU is met again. So the MTU allowance can cause the fragmentation process which is really unwanted by the users and the designers. Fortunately, the solution comes but unfortunately not in IPv4 in fact it was developed in the IPv6 as an improvement over IPv4. In figure1 we illustrate how segments are divided into frames by an intermediate router during the data transmission. Figure 1 shows the process in details.

B- Fragmentation in IPv6:

A common misunderstanding that there is no fragmentation process in IPv6, which is not accurate. in fact, the IPv6 does not allow fragmentation at the intermediate routers but it does allow it at source router and it sends them as a segment not a fragment. It also does not allow for reassembling because there are no fragments to reassemble, the only packet dividing and size limitation is performed at the source host (segmentation). Therefore, when a segment finds an MTU with less allowance, it discards the packet and request resending of the packet by sending an ICMP error massage back to the source host (packet is too big), than the source host retransmits the packet again with smaller packet in size (smaller segment). But still it may face the same problem if the reducing of the IP datagram is not enough.

C-Path MTU discovery:

Path maximum transmission unit discovery (PMTUD) is a standardized technology that is used to avoid IP fragmentation but what does it really do. The fact that no fragmentation is allowed enlighten us with problems caused by fragmentation process and proves that such process is unwanted. also it is forbidden in IPv6. Therefore, IP fragmentation should be avoided for better performance. In IPv6 the cost to DF process is retransmission where in PMTUD is to route through another path so protocols in that path would pass the packet datagram smoothly and easily without causing issues after passing the segment. In the figure 2 this work illustrates both scenarios of IPv6 and PMTUD in order to understand the proposed frame work and the need for it.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 7, July 2016

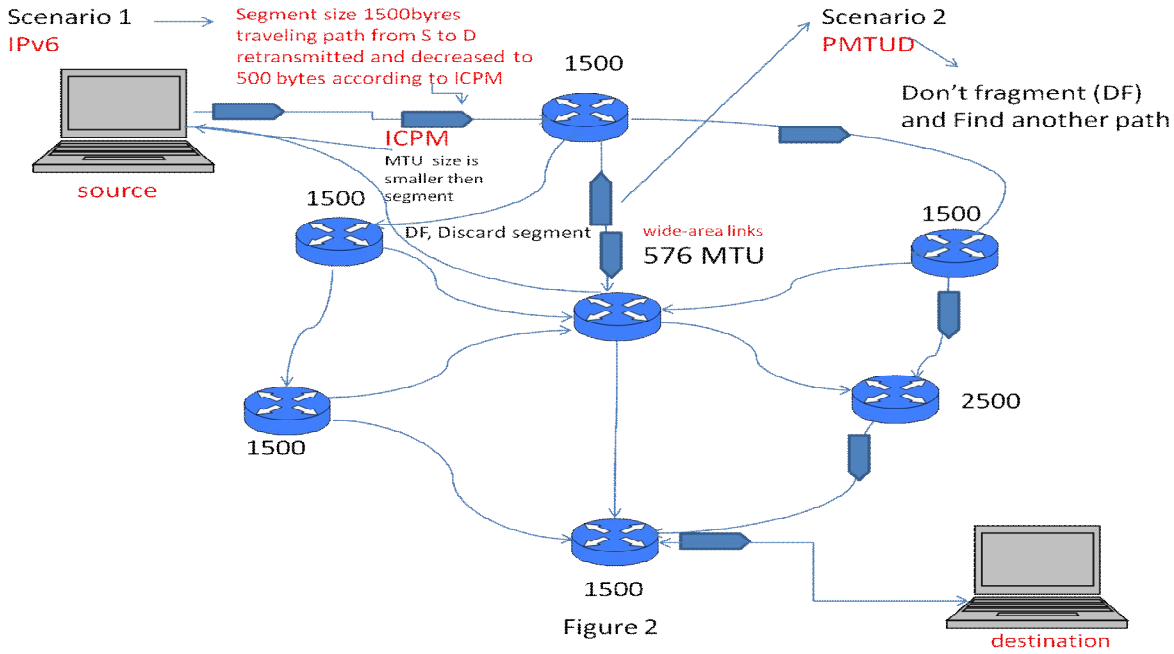

Figure 2: shows both scenario of IPv6 and PMTU to avoid fragmentation process.

IV. CONCLUSION

The IP fragmentation has been an obstacle and unwanted process but necessary to pass data of different sizes. The IP fragmentation does exist in IPv4 but it is avoided in IPv6. Therefore, this proves that IP fragmentation is not a desirable process and it causes many issues such as security issues and performances issues which this work has discussed and presented. The issues caused by the IP fragmentation process in IPv4 is due to the fact that IPv4 allows fragmentation at intermediate routers. Typically, the PMUTD introduced as an alternative solution works to avoid IP fragmentation which may slow the data transfer as it searches for paths with higher MTU allowance during the transfer time but it is still the most effective solution. Furthermore, the IPv6 does not allow fragmentation process as it prefers to reduce its size and travels again than getting fragmented. The don't fragment (DF) flag that appears when MTU size is less than the segments size is the reason why fragmentation process cannot be accomplished in IPV6.

REFERENCES

[1] Samant Saurabh, Ashok Singh Sairam "FC-DERM: Fragmentation Compatible Deterministic Edge Router Marking" 2011 17th Asia-Pacific Conference on Communications (APCC) 2nd – 5th October 2011 | Sutera Harbour Resort, Kota Kinabalu, Sabah, Malaysia.
[2] Osamah Ibrahiem Abdullaziz, Vik Tor Goh and KokSheik Wong "Using IP Identification for Fragmentation Resilient Data Embedding" 2015 International Conference on Consumer Electronics-Taiwan (ICCE-TW).
[3] J. Pope and R. Simon, "The Impact of Packet Fragmentation and Reassembly in Resource Constrained Wireless Networks," Journal of Computing and Information Technology, vol. 15, no. 1, p. 11, 2013.
[4] Resolve IP Fragmentation, MTU, MSS, and PMTUD Issues with GRE and IPSEC, http://www.cisco.com. 2016.
[5] M. Wang, L. Dunn, W. Mao and T. Chen, "Reduce IP Address Fragmentation through Allocation," in Computer Communications and Networks, 2007. ICCCN 2007. Proceedings of 16th International Conference on, Honolulu, HI, 2007.