

(19) World Intellectual Property Organization
International Bureau(43) International Publication Date
3 June 2010 (03.06.2010)(10) International Publication Number
WO 2010/062020 A2

PCT

(51) International Patent Classification:
H04L 12/56 (2006.01)(21) International Application Number:
PCT/KR2009/003972(22) International Filing Date:
17 July 2009 (17.07.2009)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
10-2008-0119464
28 November 2008 (28.11.2008) KR(71) Applicant (for all designated States except US): **ELECTRONICS AND TELECOMMUNICATIONS RESEARCH INSTITUTE** [KR/KR]; 161 Gajeong-dong, Yuseong-gu, Daejeon-si 305-700 (KR).

(72) Inventors; and

(75) Inventors/Applicants (for US only): **OH, Seung-hun** [KR/KR]; 505-2401 Hoban 5cha, Sinchang-dong, Gwangsan-gu, Gwangju-si 506-745 (KR). **PARK, Il-kyun** [KR/KR]; 103-1004 Daewoo Apt., Gocheok 2-dong, Guro-gu, Seoul 152-794 (KR). **LEE, Byung-tak** [KR/KR]; 412-1203 Hwaseo Jugong Apt., 650 Hwaseo-dong, Paldal-gu, Suwon-si, Gyeonggi-do 442-150 (KR). **KIM, Kyung-hun** [KR/KR]; 204-1302 Buyeong 2chaApt., Sinchang-dong, Gwangsan-gu, Gwangju-si 506-834 (KR). **KOH, Jai-sang** [KR/KR]; 106-207 Cheomdan Jugong Apt., Wolgye-dong, Gwangsan-gu, Gwangju-si 506-302 (KR).(74) Agents: **LEE, Houn-su** et al.; BYC Bldg. 15Fl., 648-1, Yeoksam-dong, Gangnam-gu, Seoul 135-080 (KR).

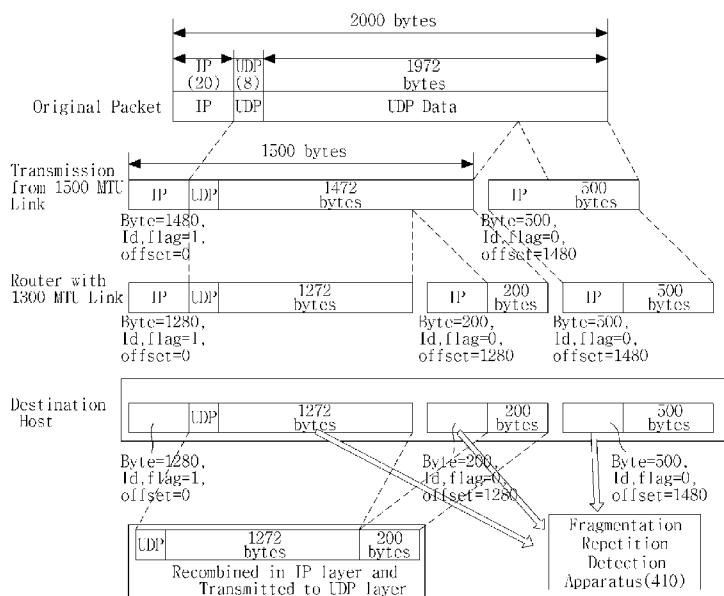
(81) Designated States (unless otherwise indicated, for every kind of national protection available): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PE, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States (unless otherwise indicated, for every kind of regional protection available): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

[Continued on next page]

(54) Title: SYSTEM FOR CONTROLLING PATH MAXIMUM TRANSMISSION UNIT BY DETECTING REPETITIONAL IP PACKET FRAGMENTATION AND METHOD THEREOF

[Fig. 4]



(57) Abstract: A fragmentation repetition detection apparatus for detecting an IP fragmentation repetition which may occur in a multicast or unicast environment is provided. The fragmentation repetition detection apparatus includes a packet capturing unit which captures a received packet, a fragmentation repetition detector which detects whether or not the captured packet is a packet which is repetitively fragmented, and a path maximum transmission unit (PMTU) transmitter which transmits PMTU information acquired by the fragmentation repetition detector to a server which transmits the packet when the captured packet is a packet which is repetitively fragmented. Since a packet is transmitted by readjusting a PMTU, a fragmentation repetition of an IP packet can be prevented.



Published:

- *without international search report and to be republished
upon receipt of that report (Rule 48.2(g))*

Description

SYSTEM FOR CONTROLLING PATH MAXIMUM TRANSMISSION UNIT BY DETECTING REPETITIONAL IP PACKET FRAGMENTATION AND METHOD THEREOF

Technical Field

- [1] The present invention relates to packet communication, and more particularly, to a technique for preventing an IP packet fragmentation repetition which may occur in a multicast environment.

Background Art

- [2] In end-to-end communication, for the sake of efficient communication, the smallest number of packets need to be transmitted, and thus packets with the largest packet size which can be supported in an end-to-end path need to be transmitted. The smallest one among maximum transmission units (MTUs) which can be supported in each link on a network path is referred to as a path MTU (PMTU). An IP packet transmission server transmits packets according to a PMTU to thereby transmit the smallest number of packets while avoiding an IP packet fragmentation.
- [3] In an Internet protocol version 4 (IPv4) unicast method, a PMTU can be detected using a traditional technique (RFC1063) established by the Internet engineering task force (IETF) in which an error message "Packet Too Big (PTB)" of an Internet control message protocol (ICMP) is used. However, a network operator and a network service provider currently do not support the ICMP due to a network security problem. Therefore, a method using the ICMP cannot actually be used.
- [4] A tool which detects a PMTU discovery failure, searches for a PMTU using a probe packet and ICMP feedback information and finds a PMTU discovery failure point was suggested by Matthew Luckie et al. in "Inferring and Debugging Path MTU Discovery Failures", Internet Measurement Conference 2005 (IMC2005). However, this tool does not consider the multicast environment.
- [5] Recently, the IETF established a stand (RFC 4821) in which a PMTU is discovered by transmitting a probe packet to a network through a packetization layer such as a transmission control protocol (TCP). However, this standard mentioned the multicast environment but did not suggest a concrete technique.

Disclosure of Invention

Technical Problem

- [6] It is an object of the present invention to provide a fragmentation repetition detection apparatus, a path MTU control apparatus, and a path MTU control method based on

detection of a packet fragmentation repetition in which an IP packet fragmentation repetition which may occur in the multicast environment is prevented, thereby preventing a packet loss which deteriorates an application service.

Technical Solution

- [7] According to an aspect, there is provided a fragmentation repetition detection apparatus, including a packet capturing unit which captures a received packet, a fragmentation repetition detector which detects whether or not the captured packet is a packet which is repetitively fragmented, and a path maximum transmission unit (PMTU) transmitter which transmits PMTU information acquired by the fragmentation repetition detector to a server which transmits the packet when the captured packet is a packet which is repetitively fragmented.
- [8] The packet capturing unit may capture the received packet in a data link layer.
- [9] The fragmentation repetition detector may detect whether the captured packet is a packet which is repetitively fragmented using information included in an IP header of the captured packet.
- [10] The PMTU information transmitter may transmit the PMTU information to the server which transmits the packet using a port number which is previously designated.
- [11] According to another aspect, there is provided a path maximum transmission unit (PMTU) control apparatus installed in a server which transmits service traffic, including a PMTU information receiver which receives PMTU information from an apparatus which receives a packet transmitted from the server and detects a fragmentation repetition of the packet, and a PMTU information application unit which applies the largest size of a packet to be transmitted according to the received PMTU information to traffic to be transmitted from the server.
- [12] The PMTU information receiver may receive PMTU information through a port number which is previously designated.
- [13] The PMTU information application unit may apply the received PMTU information to a data link layer to control a unit of a packet to be transmitted.
- [14] According to yet another aspect, there is provided a path maximum transmission unit (PMTU) control method based on detection of a fragmentation repetition which is performed in an apparatus which is installed in an access network to receive a packet transmitted from a server, including capturing a received packet, detecting whether or not the captured packet is a packet which is repetitively fragmented, and transmitting PMTU information acquired in the detecting of whether or not the captured packet is a packet which is repetitively fragmented to a server which transmits the packet when the captured packet is a packet which is repetitively fragmented.
- [15] Additional features of the invention will be set forth in the description which follows,

and in part will be apparent from the description, or may be learned by practice of the invention.

Advantageous Effects

- [16] According to exemplary embodiments of the present invention, there is an effect of preventing a packet loss and improving service quality by detecting an IP packet fragmentation repetition which may occur in the multicast environment and applying a new PMTU value. This effect can be achieved in the unicasting environment as well as the multicast environment.

Brief Description of Drawings

- [17] The accompanying drawings, which are included to provide a further understanding of the invention and are incorporated in and constitute a part of this specification, illustrate embodiments of the invention, and together with the description serve to explain the principles of the invention.
- [18] FIG. 1 is a schematic diagram illustrating a network configuration in which an IP packet fragmentation repetition occurs and a PMTU discovery procedure according to an exemplary embodiment of the present invention;
- [19] FIG. 2 is a view illustrating a packet fragmentation process and a packet loss which occurs due to an IP fragment repetition;
- [20] FIG. 3 is a block diagram of an IPTV quality measurement apparatus including a fragmentation repetition detection apparatus according to an exemplary embodiment of the present invention;
- [21] FIG. 4 illustrates a pattern of a packet which is captured to detect an IP fragmentation repetition;
- [22] FIG. 5 is a diagram of a state transition necessary for detecting an IP fragmentation repetition;
- [23] FIG. 6 is a block diagram of a media server including a PMTU control apparatus which applies PMTU information to a system according to an exemplary embodiment of the present invention; and
- [24] FIGS. 7 to 9 are flowcharts illustrating a procedure of detecting an IP fragmentation repetition.

Mode for the Invention

- [25] The invention is described more fully hereinafter with reference to the accompanying drawings, in which exemplary embodiments of the invention are shown. This invention may, however, be embodied in many different forms and should not be construed as limited to the embodiments set forth herein. Rather, these embodiments are provided so that this disclosure is thorough, and will fully convey the scope of the invention to those skilled in the art. In the drawings, the size and relative sizes of layers and regions

may be exaggerated for clarity. Like reference numerals in the drawings denote like elements.

- [26] It will be understood that when an element or layer is referred to as being on or connected to another element or layer, it can be directly on or directly connected to the other element or layer, or intervening elements or layers may be present. In contrast, when an element is referred to as being directly on or directly connected to another element or layer, there are no intervening elements or layers present.
- [27] FIG. 1 is a schematic diagram illustrating a network configuration in which an IP packet fragmentation repetition occurs and a PMTU discovery procedure according to an exemplary embodiment of the present invention.
- [28] FIG. 1 illustrates an example of a network in which an IP packet fragmentation (hereinafter, "IP fragmentation") repetition may occur and a situation in which a packet loss occurs in the multicast environment. A media traffic packet transmitted from a media server 100 is transmitted in units of 1,500 bytes which is a MTU value. The transmitted media traffic packet undergoes a first IP fragmentation in a first router 210. At this time, the media traffic packet is fragmented into packets of units of a maximum of 1,400 bytes and transmitted to the next node. Then, the fragmented packets undergo a second IP fragmentation in a second router 220. At this time, each fragmented packet is fragmented into packets of units of 1,300 bytes and transmitted to the next node. Therefore, packets are received in a client terminal 300 with a packet loss.
- [29] As described above, in the network environment of FIG. 1, links which may perform an IP fragmentation twice exist in the middle of the network, and so an IP fragmentation repetition occurs. An IP fragmentation is commonly performed based on a MTU value of an output link of each router, and it may be alternatively performed by including data in a packet in a middle box during end-to-end communication. For example, in several IPTV digital right management (DRM) systems, an IPTV stream is encoded in real time in a middle box, and information necessary for decoding may be included in an IPTV stream. At this time, a packet which is larger in size than a MTU of an output interface of a middle box which performs encoding may be generated, and in this case, an IP fragment is performed. Meanwhile, reference numeral 400 in FIG. 1 is not described above but will be described later.
- [30] FIG. 2 is a view illustrating a packet loss which occurs due to an IP fragment repetition.
- [31] As shown in FIG. 2, an original packet is repetitively fragmented according to a MTU, and each fragmented packet is transmitted to a destination host. An IP layer of the destination host recombines fragmented packets and transfers a recombined packet to a UDP layer, and the UDP layer computes a checksum and then finally transfers the recombined packet to an application program. At this time, in the process of computing

a checksum through the UDP layer, second-fragmented packets are discarded due to a checksum error, leading to a packet loss.

[32] FIG. 3 is a block diagram of an IPTV quality measurement apparatus including a fragmentation repetition detection apparatus according to an exemplary embodiment of the present invention. The fragmentation repetition detection apparatus detects whether or not an IP fragmentation is repetitively performed for media traffic received by the IPTV quality measurement apparatus.

[33] The IPTV quality measurement apparatus 400 including the fragmentation repetition detection apparatus 410 is preferably disposed on a network, for example, an access network, as shown in FIG. 1. Here, the fragmentation repetition detection apparatus 410 is implemented in the IPTV quality measurement apparatus 400, but it may be implemented in a general traffic monitoring apparatus or a client terminal 300 which finally receives media traffic.

[34] The fragmentation repetition detection apparatus 410 includes a packet capturing unit 411, a fragmentation repetition detector 412, a PMTU information storing unit 413, and a PMTU information transmitter 414. The packet capturing unit 411 captures a packet which is received in the IPTV quality measurement apparatus 400. Preferably, the packet capturing unit 411 captures a packet which is received in a data link layer. In media traffic, some of packets in which an IP fragmentation is performed twice or more are discarded due to an error in an error check process of an IDP layer, and some packets are regarded as abnormal packets and discarded in an IP layer. For this reason, the packet capturing unit 411 preferably captures packets in the data link layer before some of received packets are discarded. Packets captured in the data link layer are illustrated in FIG. 4.

[35] The packet capturing unit 411 transfers captured packets to the fragmentation repetition detector 412. At this time, the packet capturing unit 411 may transfer desired packets to the fragmentation repetition detector 412 through filtering. For example, packets which belong to a predetermined IP address band may be filtered.

[36] The fragmentation repetition detector 412 detects whether or not packets transferred from the packet capturing unit 411 are packets in which an IP fragmentation is repetitively performed. Here, the fragmentation repetition detector 412 may detect whether or not packets transferred from the packet capturing unit 411 are packets in which an IP fragmentation is repetitively performed using a header length, a total length, an identification, a flag, or offset information. The fragmentation repetition detector 412 acquires PMTU information in the process of detecting an IP fragmentation repetition and stores the acquired PMTU information in the PMTU information storing unit 413. At this time, source address information among information included in an IP header is preferably stored in the PMTU information

storing unit 413 together with PMTU information. After storing PMTU information in the PMTU information storing unit 413, the fragmentation repetition detector 412 transfers an event for requesting transmission of PMTU information to the PMTU information transmitter 414. A concrete algorithm of detecting an IP fragmentation repetition and acquiring PMTU information through the fragmentation repetition detector 412 will be described later.

- [37] The PMTU information transmitter 414 which receives the event transmits PMTU information stored in the PMTU information storing unit 413 to the media server 100 which has transmitted a media traffic packet. Since source address information of the media server 100 is stored in the PMTU information transmitter 414 together with PMTU information, the PMTU information transmitter 414 transmits PMTU information to the media server 100 using the source address information. The PMTU information transmitter 414 may transmit PMTU information to the media server 100 using a port number which is previously designated.
- [38] The media server 100 receives the PMTU information transmitted from the IPTV quality measurement apparatus 400 and applies the received PMTU information to a packet transmission system, so that a packet loss resulting from an IP fragmentation repetition can be prevented.
- [39] Meanwhile, the IPTV quality measurement apparatus 400 is disposed in an access network into which service traffic flows to measure a plurality of service sessions and thus preferably designed in view of an extension.
- [40] FIG. 5 is a diagram of a state transition necessary for detecting an IP fragmentation repetition through the fragmentation repetition detector 412 of FIG. 3.
- [41] A received packet is managed according to an IP identification. In an initial state, when a first packet which undergoes an IP fragmentation is received, that is, when a packet in which a flag value and an offset value included in an IP header are "Flags == 1 && Offset == 0" is received, it transits to a "1stPkt_Frag" state. Here, the "1stPkt_Frag" state means a state in which a first packet which undergoes an IP fragmentation is received.
- [42] In the "1stPkt_Frag" state, when a last fragmented packet, that is, a packet which has the same identification and 0 as a flag value, is received, it transits to a "LstPkt_Frag" state, while when a last fragmented packet is not received during a predetermined time period, it transits to the initial state. Here, the "LstPkt_Frag" state means a state in which a last fragmented packet is received after a first packet which undergoes an IP fragmentation is received.
- [43] In "LstPkt_Frag" state, when a packet which represents a last fragmented packet, that is, a packet which has the same identification and 0 as a flag value, is received again, it transits to a "Dup_Frag" state if a condition of Equation 1 is satisfied. Here, the

"Dup_Frag" state means a state in which an IP fragmentation repetition is detected.

[44] $(D.C_1 == \text{Offset}_2) \parallel (D.C_2 == \text{Offset}_1)$ Equation 1

[45] It is determined whether or not $D.C_1$ is identical to Offset_2 or $D.C_2$ is identical to Offset_1 . Here, D.C stands for Detection Clue and means information necessary for detecting an IP fragmentation repetition. $D.C_1$ is a D.C value (a first value) computed from a packet received when it transits to the "LstPkt_Frag" state, and Offset_1 is a value obtained from a header thereof. $D.C_2$ is a D.C value (a second value) computed from a packet received when it transits to the "Dup_Frag" state, and Offset_2 is a value obtained from a header thereof. The D.C value may be computed as in Equation 2. In Equation 2, an "IP header length" value is multiplied by 4 to express an "IP header length" value read from a packet header in units of bytes. For example, in the case in which an "IP header length" is 20 bytes, a value read from a header is 5, which is multiplied by 4 to be expressed in units of bytes.

[46] $D.C = (\text{Offset}) + (\text{total length}) - (\text{IP header length} * 4)$ Equation 2.

[47] In the "Dup_Frag" state, an event for transmitting discovered PMTU information to a server is generated, and it transits to the initial state again.

[48] In the present embodiment, it is determined whether or not a condition of $(D.C_1 == \text{Offset}_2) \parallel (D.C_2 == \text{Offset}_1)$ is satisfied as described above, but it may be determined whether or not a condition of $D.C_1 == \text{Offset}_2$ is satisfied. In Equation 1, the reason for additionally determining whether or not a condition of $D.C_1 == \text{Offset}_2$ is satisfied is to consider a packet order since a problem may occur in a packet order.

[49] Also, the reason for determining whether or not a condition of $(D.C_1 == \text{Offset}_2) \parallel (D.C_2 == \text{Offset}_1)$ is satisfied is to prevent any contingency problem. For example, if it is assumed that an IP fragmentation is normally performed once and a second fragmented packet is copied on a path, an apparatus for detecting it may misjudge that an IP fragmentation is performed twice based on only an ID value and a flag value. In order to prevent such a problem, offset values are computed and compared.

[50] FIG. 6 is a block diagram of the media server 100 including a PMTU control apparatus 110 which applies PMTU information to a system according to an exemplary embodiment of the present invention.

[51] The PMTU control apparatus 110 includes a PMTU information receiver 111, a PMTU information storing unit 112, and a PMTU information application unit 113. An application program module independently transmits (unicasts or multicasts) service traffic, and the PMTU information receiver 111 receives PMTU information transmitted from the PMTU information transmitter 414 of the fragmentation repetition detection apparatus 410. Since a communication socket of a corresponding port number is used as described above, the PMTU information receiver 111 receives PMTU information through a communication socket of a corresponding port number.

The PMTU information receiver 111 stores the received PMTU information in the PMTU information storing unit 112 and transmits an event for instructing that newly stored PMTU information be applied to service traffic to the PMTU information application unit 113.

- [52] The PMTU information application unit 113 which has received the event applies PMTU information newly stored in the PMTU information storing unit 112 to a system and controls a MTU of a service traffic packet to be transmitted by an application program module. For example, the PMTU information application unit 113 applies new PMTU information to the data link layer of the media server 100 and controls a MTU of a service traffic packet to be transmitted by an application program module.
- [53] FIGS. 7 to 9 are flowcharts illustrating a procedure of detecting an IP fragmentation repetition through the fragmentation repetition detection apparatus 410.
- [54] A procedure of detecting an IP fragmentation repetition according to an exemplary embodiment of the present invention is initiated, and a received packet is captured in a data link layer. In one embodiment, the fragmentation repetition detection apparatus 410 captures only a packet which belongs to a specific IP address band (operation 700). Then, an identification value included in an IP header of the captured packet is investigated to determine whether or not it is an identification value which is previously registered (operation 710).
- [55] When it is determined in operation 710 that it is a new identification (ID), it is determined whether or not the received packet is a first packet which undergoes an IP fragmentation (operation 720). This process may be performed by determining whether or not a flag value and an offset value included in an IP header of the received packet satisfies "Flags == 1 && Offset == 0."
- [56] When a flag value and an offset value included in an IP header satisfies "Flags == 1 && Offset == 0," the fragmentation repetition detection apparatus 410 generates a data structure for a new ID (operation 730) and includes a destination address, a source address, an identification value, and a total length value which are included in the IP header of the packet in the data structure (operation 740). At this time, a state transits to the "1stPkt_Frag" state (operation 750).
- [57] Meanwhile, when it is determined in operation 710 that it is not a new identification, a current state is investigated (operation 800). When it is determined that the current state is the "1stPkt_Frag" state, it is determined whether or not a last fragmented packet is received (operation 810). That is, it is determined whether or not a flag value included in the IP header is "Flags == 0." When a flag value included in the IP header is "Flags == 0," a D.C₁ value is computed and stored, and an Offset₁ value included in the IP header is stored (operation 820). Then, a state transits to the "LstPkt_Frag" state (operation 830).

- [58] Meanwhile, when it is determined in operation 800 that the current state is the "LstPkt_Frag" state, it is determined whether or not a last fragmented packet is received again (operation 900). That is, it is determined whether or not a flag value included in the IP header is "Flags==0." When a flag value included in the IP header is "Flags==0," a D.C₂ value is computed and stored, and an Offset₂ value included in the IP header is stored (operation 910). Then, a relationship between values of D.C₁ and Offset₁ and values of D.C₂ and Offset₂ is investigated. For example, it is determined whether or not the D.C₁ value is identical to the Offset₂ value or the D.C₂ value is identical to the Offset₁ value (operation 920). At this time, a state transits to a "Dup_Frag" state (operation 930). When either of the two cases is satisfied, a PMTU value is stored (operation 940). A PMTU information packet including a PMTU value is generated and transmitted to the media server 100 (operation 950). Finally, all information generated for a corresponding identification is deleted (operation 960), and a state transits to the initial state (operation 970).
- [59] As described above, the present invention suggests a PMTU discovery technique of an in-band method in which a PMTU can be discovered from actual media traffic in view of the multicast environment in which a plurality of clients are present and it can be determined whether or not an IP fragmentation is repetitively performed in the process of discovering a PMTU rather than a PMTU discovery technique of an out-of-band method of using a separate probe packet.
- [60] It will be apparent to those skilled in the art that various modifications and variation can be made in the present invention without departing from the spirit or scope of the invention. Thus, it is intended that the present invention cover the modifications and variations of this invention provided they come within the scope of the appended claims and their equivalents.
- [61]

Claims

- [1] A fragmentation repetition detection apparatus, comprising:
a packet capturing unit which captures a received packet;
a fragmentation repetition detector which detects whether or not the captured packet is a packet which is repetitively fragmented; and
a path maximum transmission unit (PMTU) transmitter which transmits PMTU information acquired by the fragmentation repetition detector to a server which transmits the packet when the captured packet is a packet which is repetitively fragmented.
- [2] The fragmentation repetition detection apparatus of claim 1, wherein the packet capturing unit captures the received packet in a data link layer.
- [3] The fragmentation repetition detection apparatus of claim 1, wherein the packet capturing unit captures a packet which belongs to a specific IP address band.
- [4] The fragmentation repetition detection apparatus of claim 1, wherein the fragmentation repetition detector detects whether the captured packet is a packet which is repetitively fragmented using information included in an IP header of the captured packet.
- [5] The fragmentation repetition detection apparatus of claim 4, wherein the fragmentation repetition detector detects whether the captured packet is a packet which is repetitively fragmented using a header length, a total length, an identification, a flag, or an offset.
- [6] The fragmentation repetition detection apparatus of claim 4, wherein PMTU information acquired by the fragmentation repetition detector is total length information of a first packet among packets having the same identification.
- [7] The fragmentation repetition detection apparatus of claim 1, wherein the PMTU information transmitter transmits the PMTU information to the server which transmits the packet using a port number which is previously designated.
- [8] The fragmentation repetition detection apparatus of claim 1, wherein the received packet is a media traffic packet.
- [9] The fragmentation repetition detection apparatus of claim 1, wherein the fragmentation repetition detection apparatus is disposed in an access network.
- [10] A path maximum transmission unit (PMTU) control apparatus installed in a server which transmits service traffic, comprising:
a PMTU information receiver which receives PMTU information from an apparatus which receives a packet transmitted from the server and detects a fragmentation repetition of the packet; and
a PMTU information application unit which applies the largest size of a packet to

be transmitted according to the received PMTU information to traffic to be transmitted from the server.

[11] The PMTU control apparatus of claim 10, wherein the PMTU information receiver receives PMTU information through a port number which is previously designated.

[12] The PMTU control apparatus of claim 10, wherein the PMTU information application unit applies the received PMTU information to a data link layer to control a unit of a packet to be transmitted.

[13] A path maximum transmission unit (PMTU) control method based on detection of a fragmentation repetition which is performed in an apparatus which is installed in an access network to receive a packet transmitted from a server, comprising:

capturing a received packet;

detecting whether or not the captured packet is a packet which is repetitively fragmented; and

transmitting PMTU information acquired in the detecting of whether or not the captured packet is a packet which is repetitively fragmented to a server which transmits the packet when the captured packet is a packet which is repetitively fragmented.

[14] The method of claim 13, wherein the capturing of the received packet comprises capturing the received packet in a data link layer.

[15] The method of claim 13, wherein the detecting of whether or not the captured packet is a packet which is repetitively fragmented comprises detecting whether or not the captured packet is a packet which is repetitively fragmented using information included in an IP header of the captured packet.

[16] The method of claim 15, wherein the detecting of whether or not the captured packet is a packet which is repetitively fragmented comprises:
checking whether or not identification information of the captured packet is previously stored;
when identification information of the captured packet is not previously stored, checking a flag value and an offset value included in an IP header of the packet to determine whether or not the packet is a first fragmented packet, and when the packet is a first fragmented packet, recording a state of an identification of the captured packet as a first fragmentation state;
when identification information of the captured packet is previously stored, checking whether a state of the identification is a first fragmentation state or a last fragmentation state;
when a state of the identification is a first fragmentation state, checking a flag

value included in an IP header of the captured packet to determine whether or not the packet is a last fragmented packet, and when the packet is a last fragmented packet, recording a state of the identification as a last fragmentation state; and when a state of the identification is a last fragmentation state, checking a flag value included in an IP header of the captured packet to determine whether or not the packet is a last fragmented packet, and when the packet is a last fragmented packet, recording a state of the identification as a repetition fragmentation state and storing PMTU information.

[17] The method of claim 16, wherein the recording of the state of the identification as the last fragmentation state comprises recording the state of the identification as the last fragmentation state after storing a first value obtained by adding a total length to an offset value included in an IP header of the captured packet and subtracting an IP header length value and an offset value in the first fragmentation state, and the storing of the PMTU information comprises: storing a second value obtained by adding a total length to an offset value included in an IP header of the captured packet and subtracting an IP header length value and an offset value in the first fragmentation state, determining whether or not the first value is identical to the offset value stored in the last fragmentation state, and when the first value is identical to the offset value stored in the last fragmentation state, recording the state of the identification as the repetition fragmentation state.

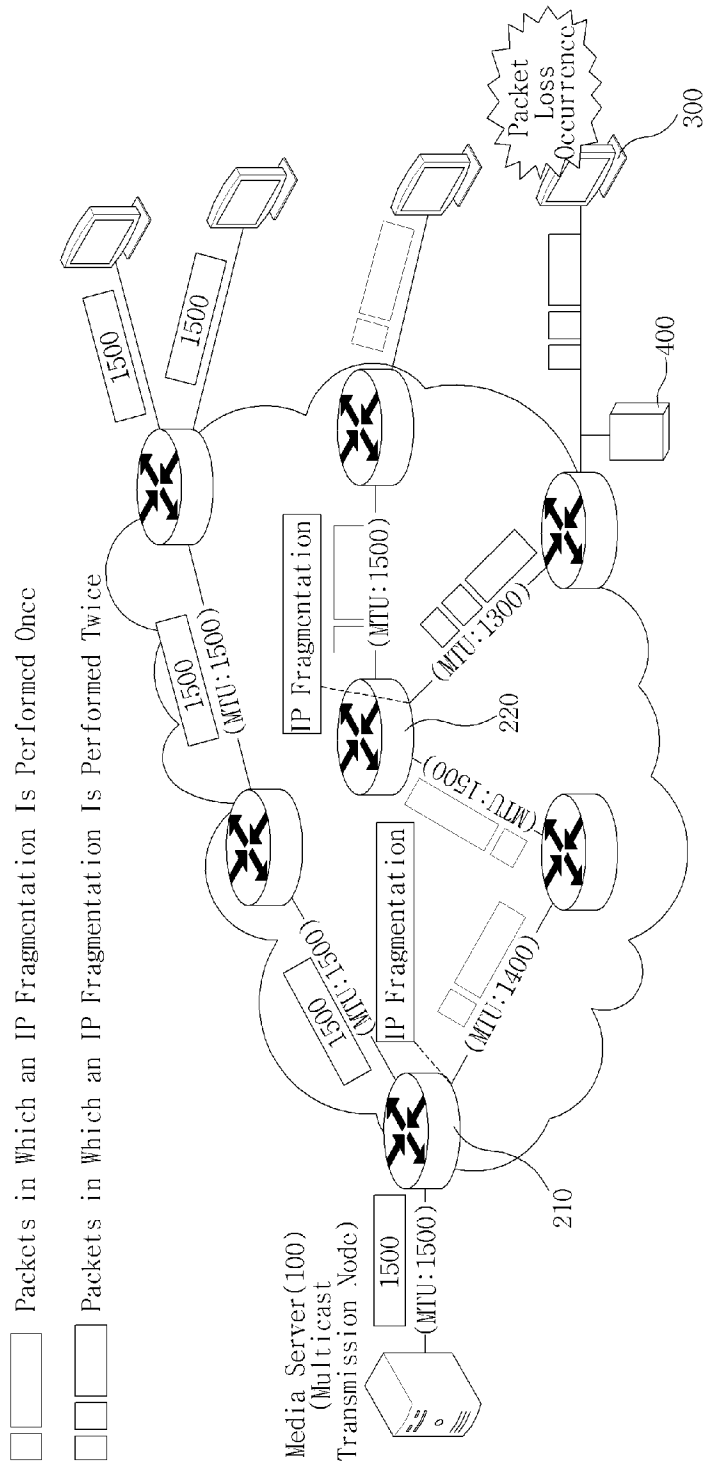
[18] The method of claim 16, wherein the recording of the state of the identification as the last fragmentation state comprises recording the state of the identification as the last fragmentation state after storing a first value obtained by adding a total length to an offset value included in an IP header of the captured packet and subtracting an IP header length value and an offset value in the first fragmentation state, and the storing of the PMTU information comprises: storing a second value obtained by adding a total length to an offset value included in an IP header of the captured packet and subtracting an IP header length value and an offset value in the first fragmentation state, determining whether or not the first value is identical to the offset value stored in the last fragmentation state or the second value is identical to the offset value stored in the last fragmentation state, and when the first value is identical to the offset value stored in the last fragmentation state or the first value is identical to the offset value stored in the last fragmentation state, recording the state of the identification as the repetition fragmentation state.

[19] The method of claim 16, wherein the PMTU information is a total length of a first packet among packets having the same identification.

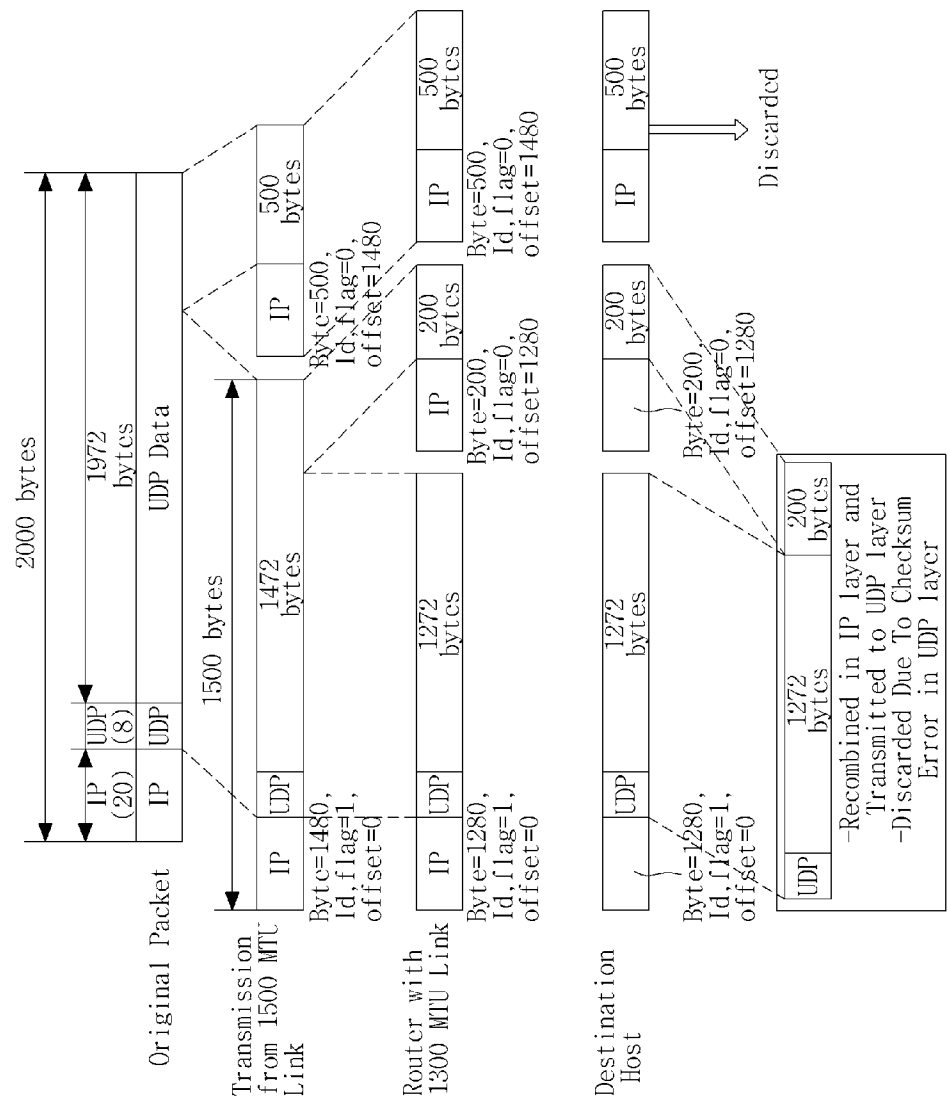
[20] The method of claim 16, further comprising, deleting the identification and in-

formation recorded related to the identification after transmitting the PMTU information.

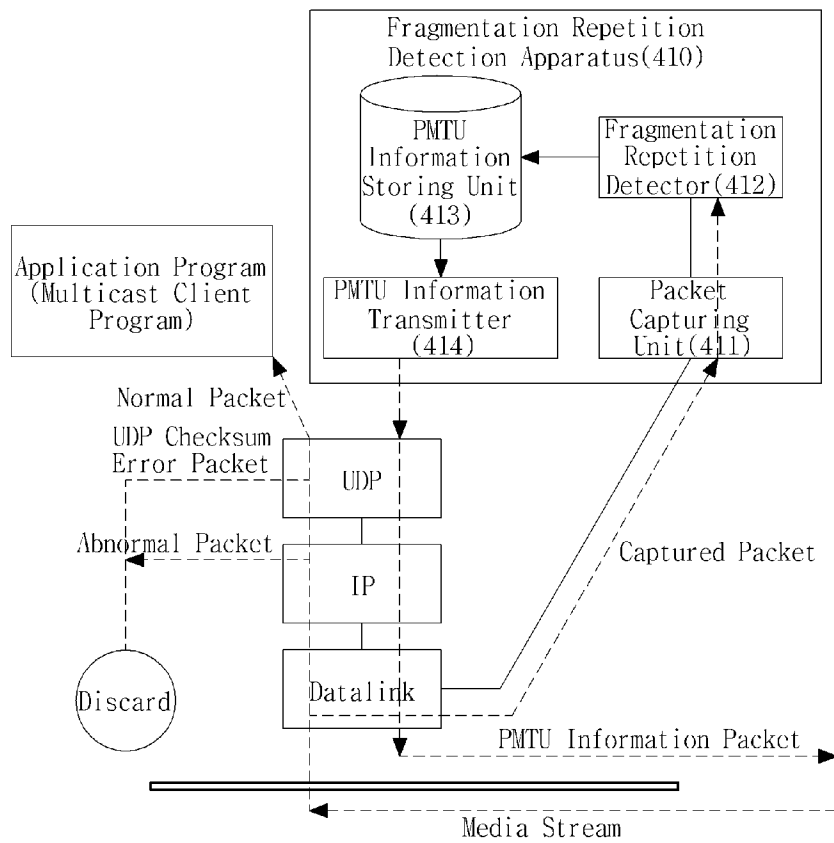
[Fig. 1]



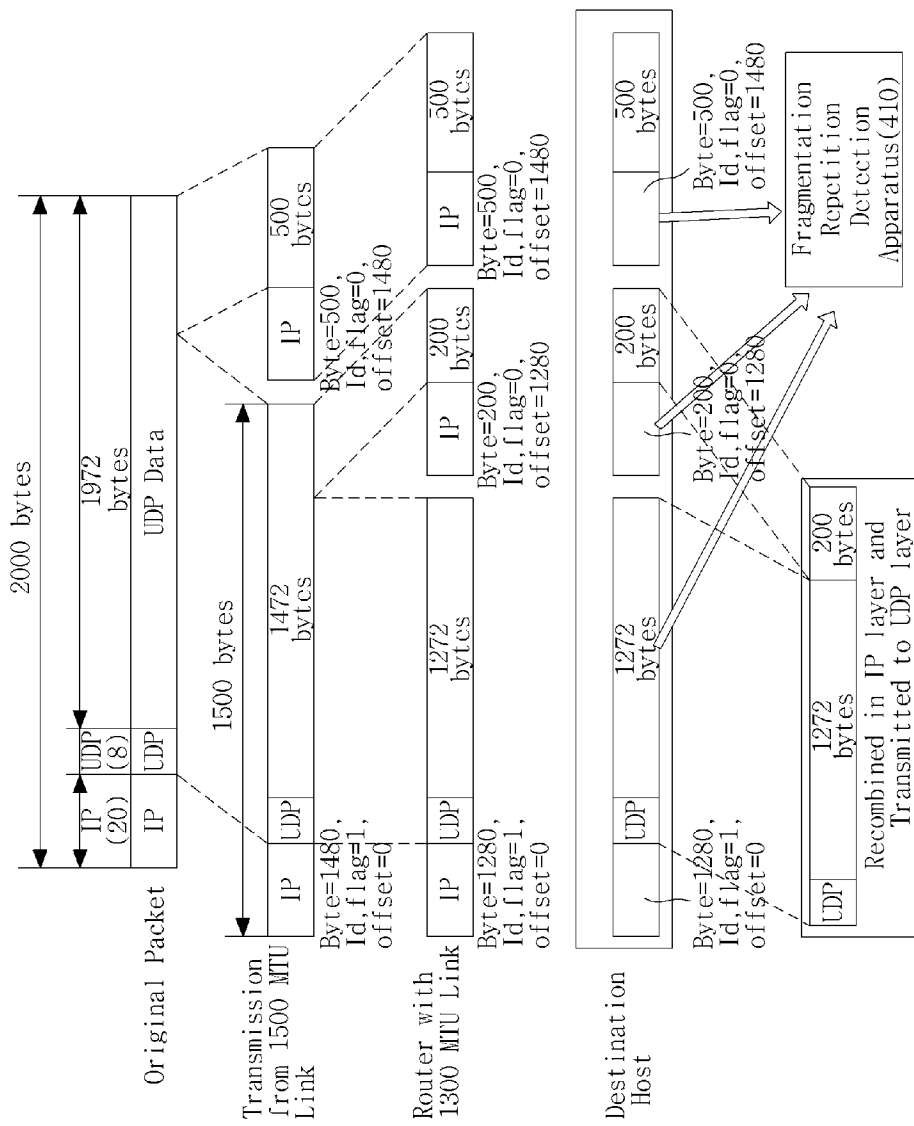
[Fig. 2]



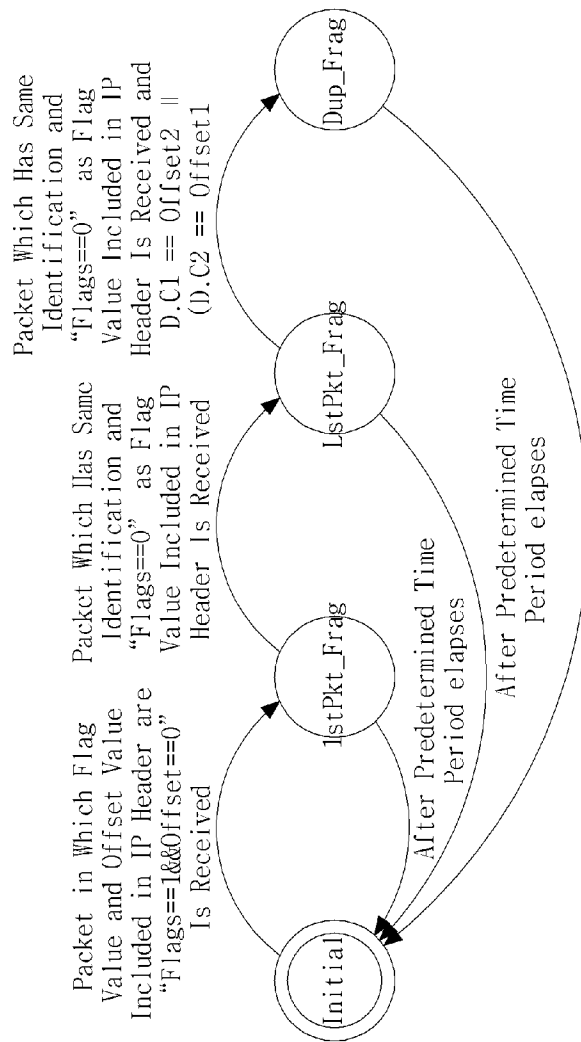
[Fig. 3]



[Fig. 4]

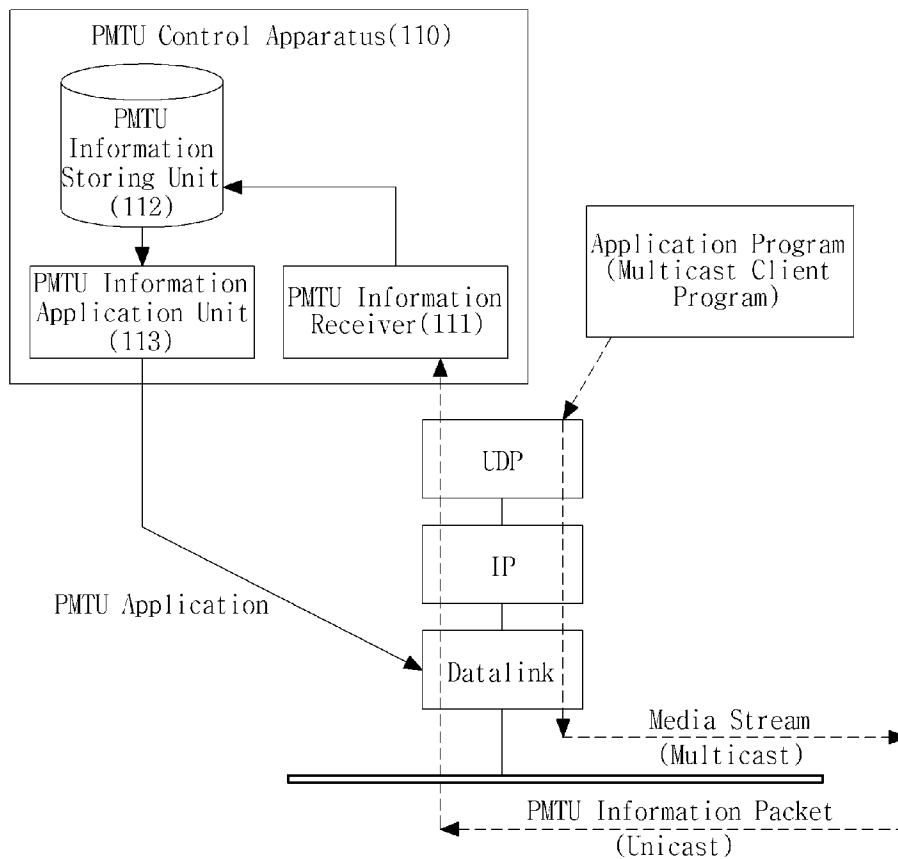


[Fig. 5]

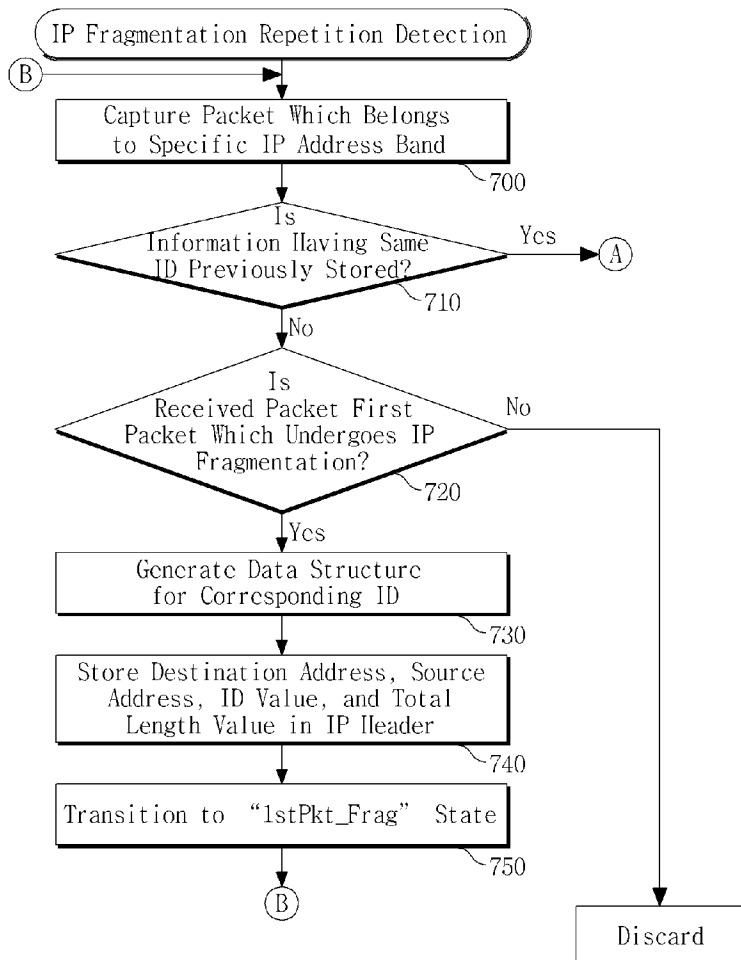


1stPkt_Frag:State in Which First Packet Which Undergoes IP Fragmentation Is Received
 LstPkt_Frag:State in Which Last Fragmented Packet Is Received After First Packet Which Undergoes IP Fragmentation Is Received
 Dup_Frag:State in Which IP Fragmentation Repetition Is Detected

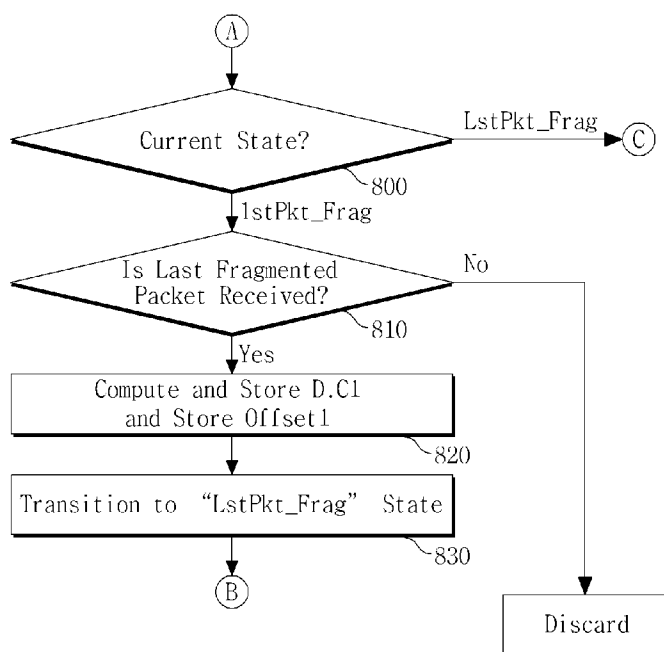
[Fig. 6]



[Fig. 7]



[Fig. 8]



[Fig. 9]

