(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
27 March 2014 (27.03.2014)

WIPO | PCT

(10) International Publication Number
WO 2014/046932 A1

(51) International Patent Classification:
H04L 12/70 (2013.01)

(21) International Application Number:
PCT/US2013/059180

(22) International Filing Date:
11 September 2013 (11.09.2013)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
61/702,320 18 September 2012 (18.09.2012) US
13/708,265 7 December 2012 (07.12.2012) US

(71) Applicant: **CISCO TECHNOLOGY, INC.** [US/US]; 170 West Tasman Drive, San Jose, CA 95134-1706 (US).

(72) Inventors: **EDSALL, Thomas, J.**; 35 Palm Avenue, Los Gatos, CA 95030 (US). **YANG, Yue, J.**; 10831 Ridgeview Way, San Jose, CA 95127 (US). **HUANG, Wei-jen**; 3109 Atwater Drive, Burlingame, CA 94010 (US). **HUANG, Chih-tsung**; 3109 Atwater Drive, Burlingame, CA 94010 (US).

(74) Agents: **FLOAM, D., Andrew** et al.; Edell, Shapiro & Finnan, LLC, 9801 Washingtonian Blvd., Suite 750, Gaithersburg, MD 20878 (US).

(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, BN, 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, KN, KP, KR, 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, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, 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, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, 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, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

Published:

— *with international search report (Art. 21(3))*

(54) Title: EXPORTING REAL TIME NETWORK TRAFFIC LATENCY AND BUFFER OCCUPANCY

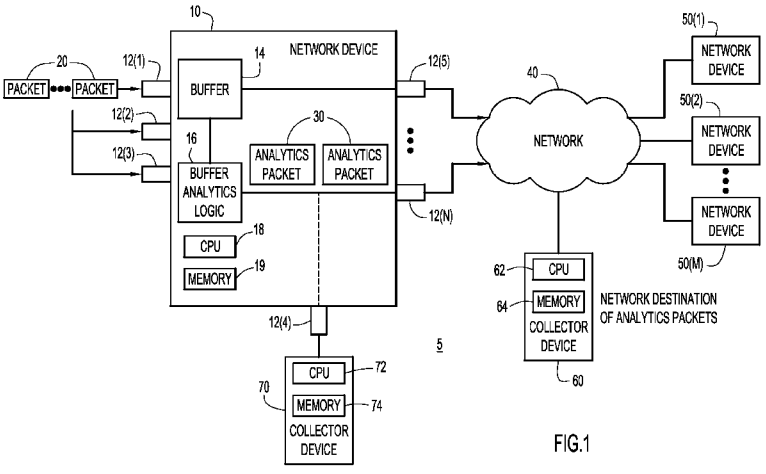

FIG.1

(57) Abstract: Techniques are presented herein to facilitate the monitoring of occupancy of a buffer in a network device. Packets are received at a network device. Information is captured describing occupancy of the buffer caused by packet flow through the buffer in the network device. Analytics packets are generated containing the information. The analytics packets from the network device for retrieval of the information contained therein for analysis, replay of buffer occupancy, etc.

WO 2014/046932 A1

EXPORTING REAL TIME NETWORK TRAFFIC LATENCY AND BUFFER OCCUPANCY

RELATED APPLICATIONS

[0001] This application claims priority to U.S. Provisional Application No. 61/702,320, filed September 18, 2012, entitled "Exporting Real Time Network Traffic Latency and Buffer Occupancy," the entirety of which is incorporated herein by reference.

TECHNICAL FIELD

[0002] The present disclosure relates generally to analysis of occupancy of a buffer in a network device.

BACKGROUND

[0003] In a computer network, data is transmitted from a source to a destination in the form of packets that generally pass through one or more network devices (e.g., switches, routers, firewalls, etc.). During the transmission, certain errors may arise that result in, for example, redundant data being added to the original data, dropped packets, etc. Massively Scalable Data Center and Cloud Computing systems are putting more traffic load on network equipment such that over-provisioned networks are no longer possible. Monitoring of a buffer in a network device is useful to gain knowledge for network administration, analysis, and performance.

BRIEF DESCRIPTION OF THE DRAWINGS

[0004] FIG. 1 is a diagram illustrating a network device configured to generate buffer analytics packets based on occupancy of a buffer in the network device.

[0005] FIG. 2 is a block diagram illustrating one example implementation of the buffer analytics logic.

[0006] FIG. 3 is a diagram that generally illustrates a format of a buffer analytics packet.

[0007] FIG. 4 is a flow chart depicting operations in a network device to generate and output buffer analytics packets.

[0008] FIG. 5 is a flow chart depicting operations in a device that receives and retrieves information from the buffer analytics packets.

[0009] FIG. 6 is a diagram illustrating an example of playback of buffer occupancy from buffer analytics packets.

DESCRIPTION OF EXAMPLE EMBODIMENTS

Overview

[0010] Techniques are presented herein to facilitate the monitoring of occupancy of a buffer in a network device. Packets are received at a network device. Information is captured describing occupancy of the buffer caused by packet flow through the buffer in the network device. Analytics packets are generated containing the information. The analytics packets from the network device for retrieval of the information contained therein for analysis, replay of buffer occupancy, etc.

Example Embodiments

[0011] Complete network visibility into buffer occupancy and the ability to replay occupancy via export and post processing is important since network disruptions (e.g., microbursts) can occur at any time. Furthermore, the ability to replay buffer occupancy allows for effective diagnosis of network issues to provide corrective actions. Existing solutions such as port mirroring (i.e., Switched Port Analyzer (SPAN)) do not provide visibility of buffer occupancy. As such, presented herein are techniques for monitoring and replaying buffer occupancy.

[0012] Referring now to FIG. 1, a diagram is shown of a network environment 5 in which a network device 10 is provided that is configured to generate buffer analytics packets based on occupancy of a buffer the network device 10. The network device 10 comprises a plurality of ports 12(1)-12(N), any of which can serve as an ingress port or egress port at any time. The network device includes a buffer 14, buffer analytics logic 16, a central processing unit (CPU) 18 and memory 19. It should be understood that there are other components of the network device 10, such as a switch fabric or application specific integrated circuit (ASIC), and the buffer 14 may reside the switch fabric. There are typically numerous buffers in the network device 10, but for simplicity only one is shown in FIG. 1. It should be understood that the techniques presented

herein are useful for each of a plurality of buffers in a network device. The buffer analytics logic 14 may be implemented in hardware by digital logic gates (and embedded in the switch fabric) or by software stored in memory 19 and executed by CPU 18.

[0013] Packets 20 arrive at the network device 10 via any of the ports 12(1)-12(N). FIG. 1 shows an example where packets are arriving at ports 12(1), 12(2) and 12(3). The network device 10 is coupled to a network 40, e.g., a local area network or wide area network (the Internet), via ports 12(5)-12(N) to ultimately communicate with any one or more of the network devices 50(1)-50(M).

[0014] Generally, the buffer analytics logic 16 captures information describing occupancy of the buffer 14 caused by packet flow through the buffer in the network device 10, and generates buffer analytics packets 30 containing the information. As will become apparent from the description below in connection with FIG. 2, there are two types of buffer analytics packets: enqueue buffer analytics packets and dequeue buffer analytics packets. The buffer analytics packets 30 are then output from the network device 10 at a programmable time schedule (or based of packet size) in any one of several ways to allow for replay of the occupancy of the buffer.

[0015] First, the network device 10 may insert into buffer analytics packets 30 an address for a destination of the buffer analytics packet, e.g., address for any device connected to the network 40, such as collector device 60 having a CPU 62 and memory 64. The network device 10 sends the analytics packet 30 via network 40 to the destination collector device 60, which may be at any location, local or remote from network device 10.

[0016] Second, the network device 10 may output the analytics packet 30 to a dedicated port, e.g., port 12(4) of the network device 10 to which a collector device 70 is connected. The dedicated analytics port 12(4) can participate in port channel or fixed port distribution to expand bandwidth to a single or multiple monitor ports. The collector device 70, since it is connected directly to port 12(4), is usually local to the network device 10. The collector device 70 includes a CPU 72 and memory 74.

[0017] Third, the analytics packets 30 may be output to the onboard CPU 18 and memory 19 in the network device 10, such that CPU 18 and memory 19 also serve as a collector device. In any of these scenarios, the CPUs 18, 62 and 72 may replay and analyze the occupancy of the buffer 14 based on software instructions stored in its associated memory 19, 64 and 74, respectively. Moreover, the analytics packets are stored in the memory 19, 64 and 74 for the associated CPU 18, 62 and 72, respectively.

[0018] The network device 10 can be any network device now known or hereinafter developed, including a switch, router, gateway, a software stack on a host device, virtual network interface cards (VNICs) virtual switches, physical network interface cards (including those that support virtualization).

[0019] Memory 19, 64 and 74 may comprise read only memory (ROM), random access memory (RAM), magnetic disk storage media devices, optical storage media devices, flash memory devices, electrical, optical, or other physical/tangible memory storage devices. Thus, in general, the memory 19, 64 and 74 may comprise one or more tangible (non-transitory) computer readable storage media (e.g., a memory device) encoded with software comprising computer executable instructions and when the software is executed (by the associated CPU) it is operable to perform the operations described herein.

[0020] Reference is now made to FIG. 2 for a more detailed description of the buffer analytics logic 16. FIG. 2 shows that the buffer analytics logic 16 comprises an enqueue analytics packet generator 80 and a dequeue analytics packet generator 82. In addition, there are an admission control block 84, a departure control block 86, a packet assembler 88 and a multiplexer 90. The admission control block 84 and departure control block 86 are commonly found in a network device and are hardware (or software) blocks used to make processing decisions, such as a drop, scheduling, rate limiting, policing, shaping, etc.

[0021] The enqueue analytics packet generator 80 is configured to generate an analytics packet, called an enqueue buffer analytics packet shown at reference numeral 32, that describes/summarizes a packet being enqueued into buffer 14. Similarly, the dequeue analytics packet generator 82 is configured to generate an analytics packet, called a dequeue buffer analytics packet shown at reference numeral 34, that describes/summarizes a packet being

dequeued from buffer 14. The packet assembler 88 assembles a packet 20 ready out from the buffer 14 for output from the network device.

[0022] The enqueue analytics packet generator 80 captures, for a packet enqueued to buffer 14, information describing one or more of identification of ingress port of arrival of the packet at the network device, Layer 2 source address and destination address, Layer 3 source address and destination address, Layer 4 source address and destination address, class of service, and timestamp of arrival at the ingress port. Similarly, the dequeue analytics packet generator 82 captures, for a packet dequeued from the buffer 14, information describing one or more of identification of egress port for departure of the packet from the network device, Layer 2 source address and destination address, Layer 3 source address and destination address, and timestamp of departure from the egress port.

[0023] The enqueue buffer analytics packet 32 generated by the enqueue analytics packet generator 80, dequeue buffer analytics packet 34 generated by the dequeue analytics packet generator 82, and packet 20 output by the packet assembler 88, are all supplied to a corresponding input of the multiplexer 90. The multiplexer 90 selectively outputs, at any given time, either a packet 20, an enqueue buffer analytics packet 32 or a dequeue buffer analytics packet 34. Priority is given to output of a packet 20 in order to maintain proper flow of network traffic through the network device 10. Trigger for output of an analytics packet may be based on time (according to a schedule) or size of a packet enqueued to the buffer or dequeued from the buffer.

[0024] Reference is now made to FIG. 3. FIG. 3 shows an example format of an enqueue buffer analytics packet 32 or dequeue buffer analytics packet 34. As explained above, an enqueue buffer analytics packet 32 summarizes a packet that is being enqueued to a buffer and a dequeue buffer analytics packet 34 summarizes a packet that is being dequeued from the buffer. These analytics packets, when accumulated over time for packets that pass through the buffer, allow for playback of occupancy characteristics of the buffer and traffic flow of packets through the buffer. As shown in FIG. 3, an enqueue buffer analytics packet 32 and a dequeue buffer analytics packet 34 includes an Ethernet Header field 100, a Common Header field 110, one or more Records fields 120(1)-120(N) and a cyclic redundancy check (CRC) field 130.

[0025] The Ethernet header field 110 is field that is used to encapsulate the destination address of the analytics packet, e.g., to direct the analytics packet to a destination, i.e., a local or remote collector device (as indicated in FIG. 1), including to the CPU of the network device itself. To this end, the Ethernet header field 110 includes information, such as media access control (MAC) destination address/source address (DA/SA), optional IEEE 802.1q virtual local area network (VLAN) routing information, an optional Internet Protocol (IP) header including an IP SA and IP DA. Again, the Ethernet header field 110 contains information used to route the buffer analytics packet to its desired destination.

[0026] The common header field 110 contains information captured from the header of a packet that has been enqueued to or dequeued (as the case may be) from the buffer. Thus, the common header field summarizes the header of a packet that is enqueued to and dequeued from the buffer in the network device. For example, the common header field includes information for a common header version (to allow for backward/future compatibility), timescale information representing the timescale of the enqueued or dequeued packet, a timestamp of the packet arrival and/or departure to/from the buffer to allow for replay, a record number to allow a collector to determine how many, if any records, have been lost in between the current analytics packet and the last received analytics packet, and one or more user defined fields such as class of service, type of service, etc.

[0027] The record field 120 contains data for an enqueued or dequeued packet that a user configures the buffer analytics logic to capture. Examples of data that may be include in a record field includes:

Format version to indicate a format version of the record field for backward/future compatibility.

L2 Header Fields (MAC SA/DA) or compressed versions (i.e. last 24 bits) and priority

L3 Header (IP SA/DA) or compressed versions (i.e. last 16 bits) and priority and protocol type

L4 Header (TCP/UDP SA/DA)

User defined fields, including one or more of:

Input/output port

Drop—an indication of whether the packet was dropped.

Queue id—identifier of the queue (unicast or multicast) to which the packet is associated.

Queue length—length of the queue to which the packet is associated.

Packet length—overall length of size of the packet.

Timestamp (absolute or relative to common header from protocols such as Precision Time Protocol (PTP) or Network Time Protocol (NTP))

Programmable bytes—any user configurable one or more bytes of the payload of a packet

Internally specific fields such as logical interface mapped from table with keys such as {ingress/egress port, vlan}

Last record—to indicate that this is last record field in the analytics packet.

[0028] Thus, to summarize, the record field 120 for an analytics packet contains information about an enqueued packet or dequeued packet to describe buffer occupancy characteristics such as overall buffer occupancy, buffer occupancy based on packet priority, unicast queue length, multicast queue length; packet properties such as drop, port mirrored, load balanced, bridged or routed, and packet length; and packet error properties such as Cyclic Redundancy Check (CRC), and various error protocols such as Runt, Giant, and Jabber. More specifically, for a packet enqueued to the buffer, information is included in the record field describing one or more of identification of ingress port of arrival of the packet at the network device, Layer 2 source address and destination address, Layer 3 source address and destination address, Layer 4 source address and destination address, class of service, and timestamp of arrival at the ingress port. Similarly, for a packet dequeued from the buffer, information is included in the record field describing one or more of identification of egress port for departure of the packet from the network device, Layer 2 source address and destination address, Layer 3 source address and destination address, and timestamp of departure from the egress port. Other examples of data captured into user defined fields include an indication of a packet being rate limited, shaped, policed as well as any programmable bytes of the packet including payload.

[0029] The size of the analytics packet (Ethernet header field, common header field and records) may be the Maximum Transmit Unit (MTU), a switch specific analytics MTU,

determined using a time-based method (e.g., analytics packet generated and transmitted at predetermined times), determined based on a selected number of packets, or by other techniques.

[0030] Reference is now made to FIG. 4. FIG. 4 provides a flow chart that depicts the high level operations performed in a network device in generating and outputting analytics packets. At 200, a network device receives a packet. At 210, the network device captures information describing occupancy of a buffer caused by packet flow through the buffer in the network device. At 220, an analytics packet is generated for each packet that is enqueued to and/or dequeued from the buffer. At 230, a destination address is inserted into the analytics packet. At 240, the network device processes the packet in the normal course, and outputs an analytics packet to its destination (local or remote network destination) or to a local CPU of the network device. The capturing, generating, and outputting operations are triggered to be performed based on at least one of time and size of enqueued packet or dequeued packet.

[0031] FIG. 5 illustrates a high level flow chart depicting the operations performed at a destination of the analytics packets. At 300, a collector device receives the analytics packets over time. At 310, the collector device parses the analytics packets to retrieve information in the individual records as well as the common header, and uses this information to replay buffer occupancy, perform traffic latency and perform other analysis.

[0032] FIG. 6 shows an example of how a replay of buffer occupancy, subject to certain filtering criteria, may be made. In FIG. 6, a "*" represents data that has been stored into buffer and lack of "*" represents absence or removal of data from the buffer.

[0033] By generating and exporting analytics packets that summarize properties of packets enqueued to and dequeued from a buffer in a network device, a replay of the buffer may be achieved using specific pieces of information that are of interest to network administrators and application developers. Recording each of these categories would require enormous bandwidth if a complete enqueued or dequeued packet is captured.

[0034] In summary, presented herein are techniques that enable a time-based complete replay of the buffer occupancy with resolution determined by a sampling period. These techniques provide visibility of traffic flows received by network devices. The information provided can be

used by network administrators to gain insight into their specific network traffic, such as per-packet latency, buffer occupancy, and possible congestion sources. This information can lead to better allocation and provisioning of network resources, reduced congestion, and higher overall throughput. By parsing and aggregating relevant characteristics from each packet according to the techniques presented herein, bandwidth requirements associated with network monitoring are greatly reduced. As such, these techniques assist in reducing the amount of data exported for analysis.

[0035] The above description is intended by way of example only.

What is claimed is:

1. A method comprising:

receiving packets at a network device;

capturing information describing occupancy of a buffer caused by packet flow through the buffer in the network device;

generating analytics packets containing the information; and

outputting the analytics packets from the network device.

2. The method of claim 1, wherein outputting comprises:

inserting into the analytics packets an address for a destination of the analytics packet; and

sending the analytics packets into a network to the destination.

3. The method of claim 1, wherein outputting comprises outputting the analytics packet to a dedicated port of the network device to which a collector device is connected.

4. The method of claim 1, wherein capturing comprises capturing, for a packet enqueued to the buffer, information describing one or more of identification of ingress port of arrival of the packet at the network device, Layer 2 source address and destination address, Layer 3 source address and destination address, Layer 4 source address and destination address, class of service, and timestamp of arrival at the ingress port.

5. The method of claim 1, wherein capturing comprises capturing, for a packet dequeued from the buffer, information describing one or more of identification of egress port for departure of the packet from the network device, Layer 2 source address and destination address, Layer 3 source address and destination address, and timestamp of departure from the egress port.

6. The method of claim 1, wherein generating comprises generating at least one of an enqueue analytics packet and a dequeue analytics packet, the enqueue analytics packet comprising information describing properties associated with a packet being enqueued to the buffer in the network device and the dequeue analytics packet comprising information describing

properties associated with a packet being dequeued from the buffer in the network device, and further comprising inserting an address into the enqueue analytics packet and into the dequeue analytics packet, and sending the enqueue analytics packet and dequeue analytics packet into the network to a destination.

7. The method of claim 1, wherein generating the analytics packets comprises generating packets each comprising a header containing information to be used for directing the analytics packet to a destination, and a records summarizing a packet enqueued in the buffer or a packet dequeued from the buffer.

8. The method of claim 1, wherein capturing comprises capturing information describing buffer occupancy characteristics of the buffer including at least one of: overall buffer occupancy, buffer occupancy for based on packet priority, unicast queue length and multicast queue length.

9. The method of claim 1, wherein capturing comprises capturing information describing packet processing properties for packets processed by the network device including at least one of: drop, port mirrored, load balanced, bridged or routed, and packet length.

10. The method of claim 1, wherein capturing comprises capturing information describing packet processing properties for packets corresponding to user defined parameters for one or more of: rate limited, shaped, policed and any programmable bytes of the packet including payload.

11. The method of claim 1, wherein capturing, generating, and outputting are triggered to be performed based on at least one of time and size of packet.

12. An apparatus comprising:

a buffer configured to buffer packets that are received at a network device and are to be processed for routing in the network by the network device; and

a processor unit coupled to the buffer and configured to:

capture information describing occupancy of a buffer caused by packet flow through the buffer in the network device;

generate analytics packets containing the information; and

output the analytics packets.

13. The apparatus of claim 12, wherein the processor unit is further configured to insert into the analytics packets an address for a destination of the analytics packet, and to send the analytics packets into a network to the destination.

14. The apparatus of claim 12, wherein the processor unit is configured to generate at least one of an enqueue analytics packet and a dequeue analytics packet, the enqueue analytics packet comprising information describing properties associated with a packet being enqueued to the buffer in the network device and the dequeue analytics packet comprising information describing properties associated with a packet being dequeued from the buffer in the network device.

15. The apparatus of claim 12, wherein the processor unit is configured to generate the analytics packets, each analytics packet comprising an Ethernet header field containing information to be used for directing the analytics packet to a destination, a common header containing information derived from a header of a packet enqueued to the buffer or dequeued from the buffer and one or more record fields containing user defined information summarizing data contained in a packet enqueued in the buffer or a packet dequeued from the buffer.

16. The apparatus of claim 12, wherein the processor unit is configured to capture information describing buffer occupancy characteristics of the buffer including at least one of: overall buffer occupancy, buffer occupancy for based on packet priority, unicast queue length and multicast queue length.

17. The apparatus of claim 12, wherein the processor unit is configured to capture information describing packet processing properties for packets corresponding to user defined parameters for one or more of: rate limited, shaped, policed and any programmable bytes of the packet including payload.

18. A computer readable tangible storage media encoded with instructions that, when executed by a processor, cause the processor to:

capture information describing occupancy of a buffer caused by packet flow through the buffer in the network device;

generate analytics packets containing the information; and

output the analytics packets from the network device.

19. The computer readable tangible storage media of claim 18, wherein the instructions that cause the processor to generate comprise instructions that cause the processor generate at least one of an enqueue analytics packet and a dequeue analytics packet, the enqueue analytics packet comprising information describing properties associated with a packet being enqueued to the buffer in the network device and the dequeue analytics packet comprising information describing properties associated with a packet being dequeued from the buffer in the network device.

20. The computer readable tangible storage media of claim 18, wherein the instructions that cause the processor to generate comprise instructions that cause the processor generate the analytics packets, each analytics packet comprising an Ethernet header field containing information to be used for directing the analytics packet to a destination, a common header containing information derived from a header of a packet enqueued to the buffer or dequeued from the buffer and one or more record fields containing user defined information summarizing data contained in a packet enqueued in the buffer or a packet dequeued from the buffer.

21. The computer readable tangible storage media of claim 18, wherein the instructions that cause the processor to capture comprise instructions that cause the processor to capture information describing buffer occupancy characteristics of the buffer including at least one of: overall buffer occupancy, buffer occupancy for based on packet priority, unicast queue length and multicast queue length.

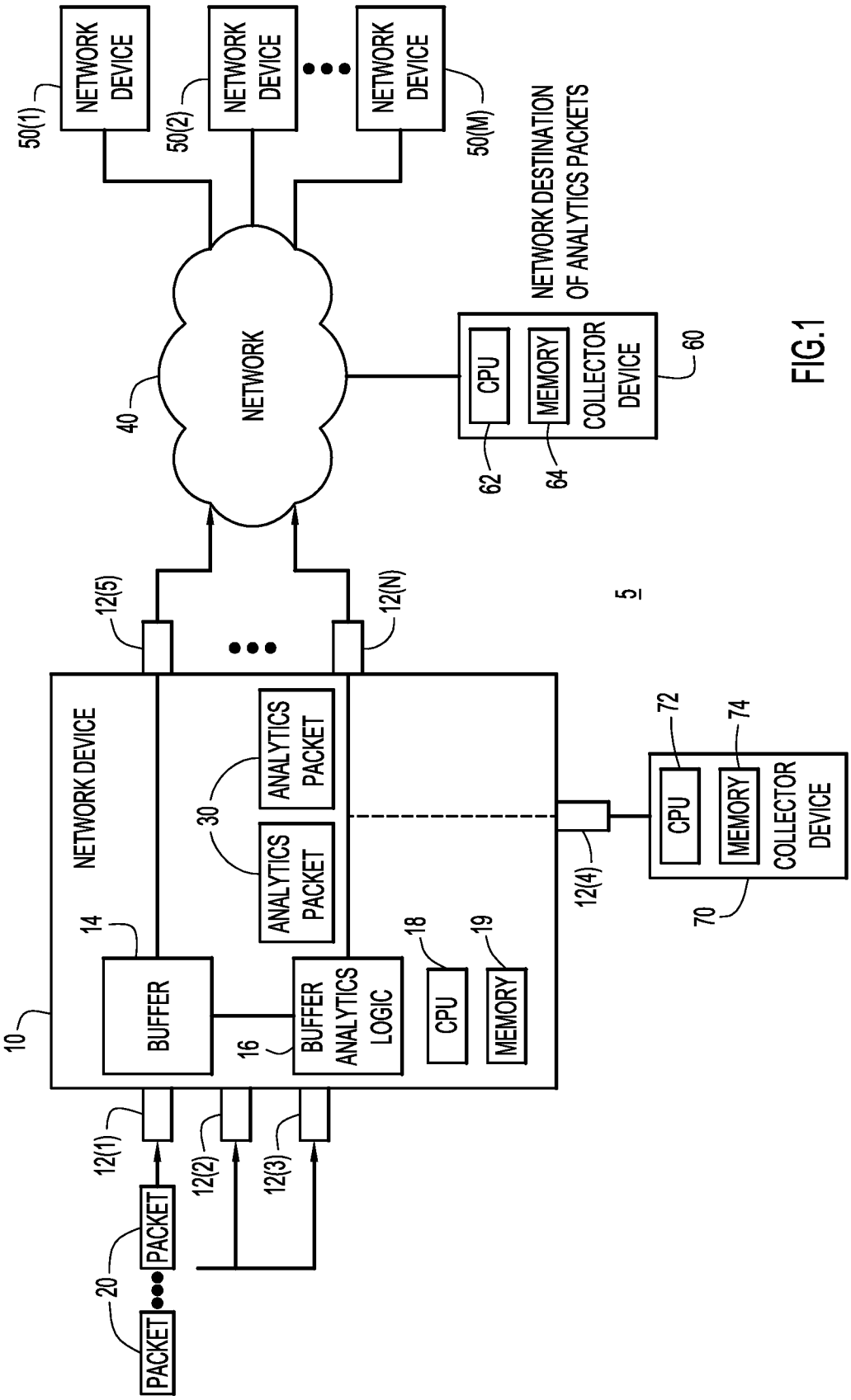
NETWORK DEVICE
50(1)
NETWORK DEVICE
50(2)
NETWORK DEVICE
50(M)
NETWORK
40
NETWORK DESTINATION OF ANALYTICS PACKETS
CPU
MEMORY
COLLECTOR DEVICE
60
62
64
12(5)
12(N)
5
NETWORK DEVICE
10
ANALYTICS PACKET
30
ANALYTICS PACKET
BUFFER
14
BUFFER ANALYTICS LOGIC
16
CPU
18
MEMORY
19
12(1)
12(2)
12(3)
12(4)
72
CPU
74
MEMORY
COLLECTOR DEVICE
70
PACKET
20
PACKET

FIG.1

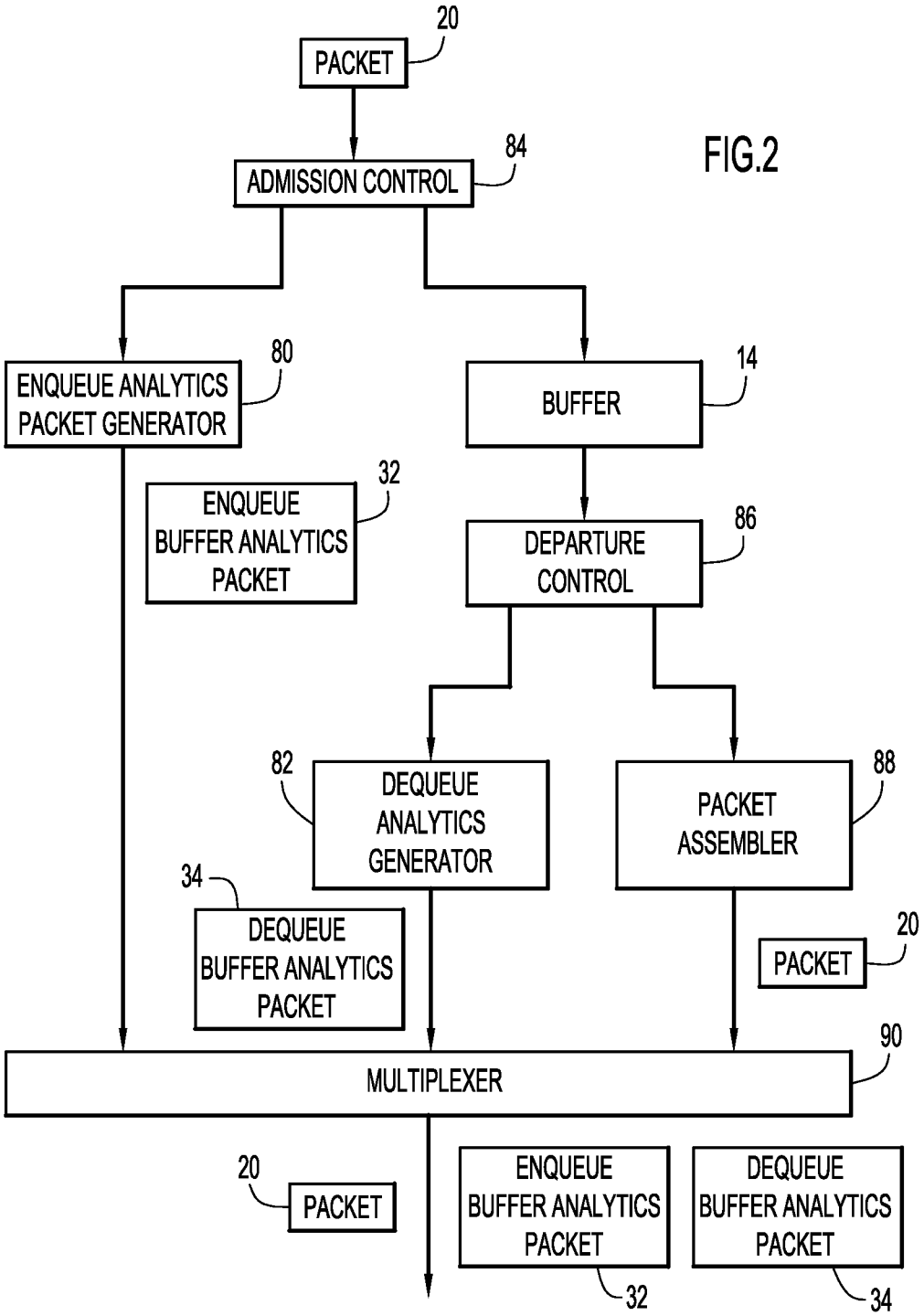
PACKET
20
ADMISSION CONTROL
84
ENQUEUE ANALYTICS PACKET GENERATOR
80
BUFFER
14
ENQUEUE BUFFER ANALYTICS PACKET
32
DEPARTURE CONTROL
86
DEQUEUE ANALYTICS GENERATOR
82
PACKET ASSEMBLER
88
DEQUEUE BUFFER ANALYTICS PACKET
34
PACKET
20
MULTIPLEXER
90
PACKET
20
ENQUEUE BUFFER ANALYTICS PACKET
32
DEQUEUE BUFFER ANALYTICS PACKET
34

FIG.2

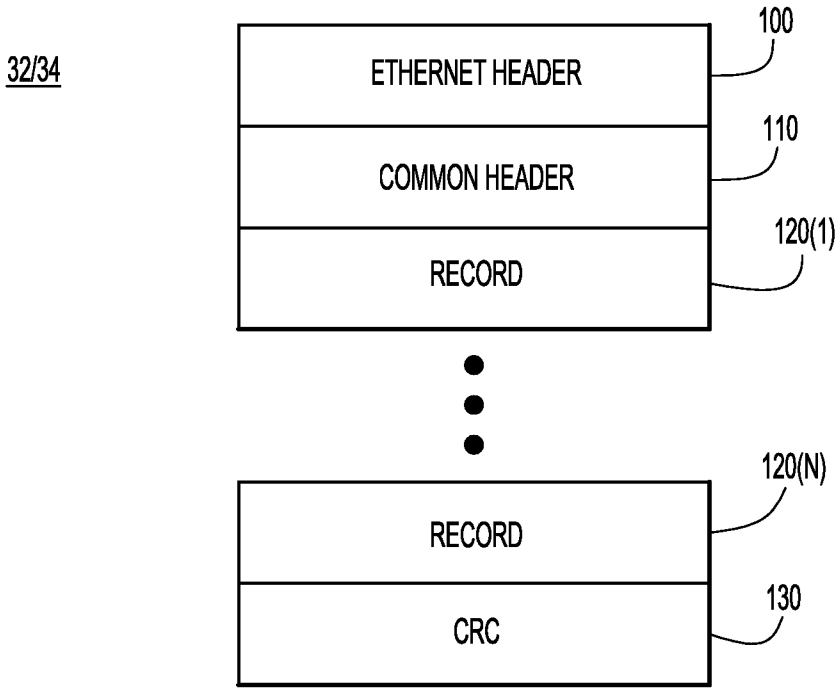
32/34
ETHERNET HEADER
100
COMMON HEADER
110
RECORD
120(1)
RECORD
120(N)
CRC
130

FIG.3

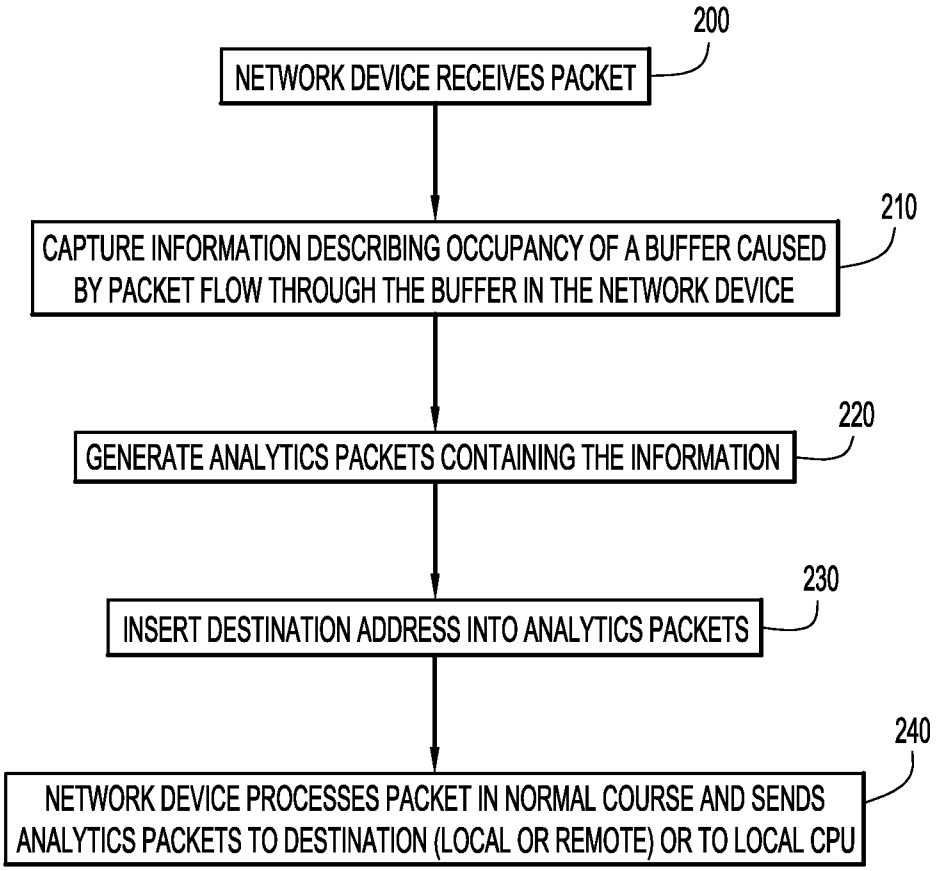
200
NETWORK DEVICE RECEIVES PACKET
210
CAPTURE INFORMATION DESCRIBING OCCUPANCY OF A BUFFER CAUSED BY PACKET FLOW THROUGH THE BUFFER IN THE NETWORK DEVICE
220
GENERATE ANALYTICS PACKETS CONTAINING THE INFORMATION
230
INSERT DESTINATION ADDRESS INTO ANALYTICS PACKETS
240
NETWORK DEVICE PROCESSES PACKET IN NORMAL COURSE AND SENDS ANALYTICS PACKETS TO DESTINATION (LOCAL OR REMOTE) OR TO LOCAL CPU

FIG.4

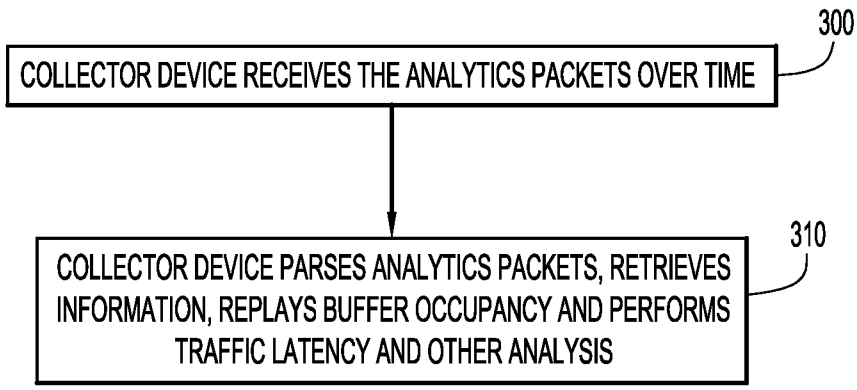
300
COLLECTOR DEVICE RECEIVES THE ANALYTICS PACKETS OVER TIME
310
COLLECTOR DEVICE PARSES ANALYTICS PACKETS, RETRIEVES INFORMATION, REPLAYS BUFFER OCCUPANCY AND PERFORMS TRAFFIC LATENCY AND OTHER ANALYSIS

FIG.5

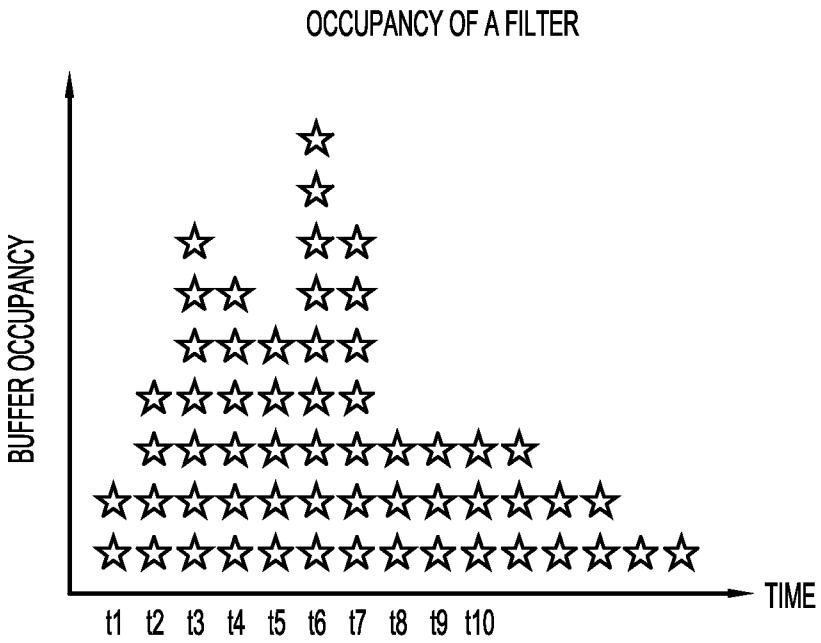
OCCUPANCY OF A FILTER
BUFFER OCCUPANCY
TIME
t1 t2 t3 t4 t5 t6 t7 t8 t9 t10

FIG.6

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2013/059180

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04L12/70
ADD.

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2010/287297 A1 (LEFEBVRE YVES [CA]) 11 November 2010 (2010-11-11) abstract paragraph [0001] - paragraph [0023] paragraph [0094] paragraph [0110] - paragraph [0113] claims 1,4,7-8,12,15 figures 1-2,9,13-15	1-21

-/--

[X] Further documents are listed in the continuation of Box C.

[X] See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
21 November 2013	28/11/2013

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Schrembs, Gerd

2

Form PCT/ISA/210 (second sheet) (April 2005)

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	GB 2 477 640 A (ORBITAL MULTI MEDIA HOLDINGS CORP [VG]) 10 August 2011 (2011-08-10) abstract page 1, line 5 - page 10, line 19 page 13, lines 12-18 page 17, line 29 - page 18, line 26 page 20, line 15 - page 22, line 8 page 30, line 31 - page 31, line 22 claims 1,9-10 figures 1,6,8	1-21
A	US 2005/240745 A1 (IYER SUNDAR [US] ET AL) 27 October 2005 (2005-10-27) abstract paragraph [0503] - paragraph [0517]	1-21
A	US 2012/093505 A1 (YEAP TET HIN [CA] ET AL) 19 April 2012 (2012-04-19) abstract paragraph [0001] paragraph [0008] - paragraph [0013] paragraph [0078] - paragraph [0081] paragraph [0087] paragraph [0098] - paragraph [0101] paragraph [0106] claims 1-8 figure 1	1-21

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/US2013/059180

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2010287297 A1	11-11-2010	CA 2749160 A1	18-11-2010
		US 2010287297 A1	11-11-2010
		US 2011238856 A1	29-09-2011
		WO 2010130023 A1	18-11-2010
GB 2477640 A	10-08-2011	EP 2532170 A1	12-12-2012
		EP 2615760 A2	17-07-2013
		GB 2477515 A	10-08-2011
		GB 2477640 A	10-08-2011
		US 2013028088 A1	31-01-2013
		WO 2011094845 A1	11-08-2011
US 2005240745 A1	27-10-2005	NONE	
US 2012093505 A1	19-04-2012	CA 2741083 A1	29-12-2010
		TW 201108710 A	01-03-2011
		US 2012093505 A1	19-04-2012
		WO 2010151099 A1	29-12-2010