



- (51) **International Patent Classification:**
H04L 12/28 (2006.01) *H04L 12/801* (2013.01)
- (21) **International Application Number:**
PCT/US2013/047351
- (22) **International Filing Date:**
24 June 2013 (24.06.2013)
- (25) **Filing Language:** English
- (26) **Publication Language:** English
- (71) **Applicant:** HEWLETT PACKARD DEVELOPMENT COMPANY, L.P. [US/US]; 11445 Compaq Center Drive West, Houston, TX 77070 (US).
- (72) **Inventor:** AYANDEH, Siamack; 153 Taylor Street, Littleton, MA 01460-1407 (US).
- (74) **Agents:** FEBBO, Michael et al.; Hewlett-Packard Company, Intellectual Property Administration, 3404 East Harmony Road, Mail Stop 35, Fort Collins, CO 80528 (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, 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).

Declarations under Rule 4.17:

— as to the identity of the inventor (Rule 4.17(i))

[Continued on next page]

- (54) **Title:** HARD ZONING CORRESPONDING TO FLOW

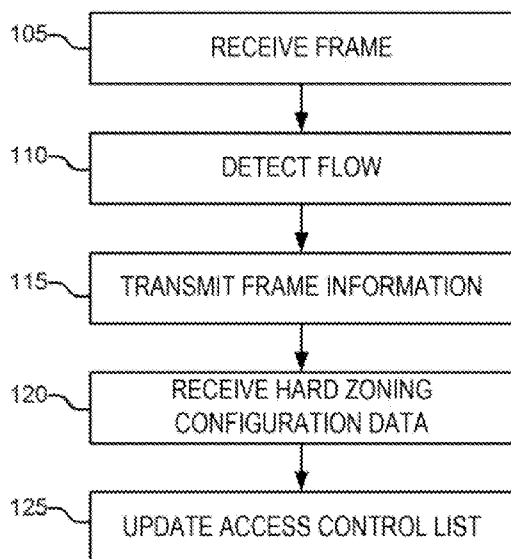


FIG. 1

(57) **Abstract:** A network controller may include a flow identifier to identify a flow using frame information. The frame information may be transmitted by a network switch. The network controller may include a retriever to retrieve hard zoning configuration data corresponding to the flow. The hard zoning configuration data may be used by the network switch to update an access control list.



— *as to applicant's entitlement to apply for and be granted
a patent (Rule 4.17(ii))*

Published:

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

HARD ZONING CORRESPONDING TO FLOW

BACKGROUND

[1] Computer networks may include multiple nodes, which may include network devices such as routers, switches, hubs, and computing devices such as servers, personal computers (PCs), laptops, workstations, mobile devices, storage devices, and peripheral devices. Such computer networks may be connected using wireless or wired links in local or wide area networks (LANs or WANs). Various networking protocols may be used to implement LANs or WANs.

[2] A storage area network (SAN) is a network that provides access to consolidated, block level data storage. Various transport protocols may be used in implementing a SAN. Transport protocols offering high bandwidth and low latency, such as connection-based protocols, including Fibre Channel (FC) and Fibre Channel over Ethernet (FCoE); and session-based protocols, such as Remote Direct Memory Access over Converged Ethernet (RoCE) and Internet Small Computer System Interface (iSCSI), may be used in some SANs. Several transport technologies may exist independently or as separate traffic classes within the same network.

BRIEF DESCRIPTION OF THE DRAWINGS

[3] Certain examples are described in the following detailed description and in reference to the drawings, in which:

[4] Figure 1 illustrates an example method of network switch operation for updating an access control list according to hard zoning configuration data provided by a network controller;

[5] Figure 2 illustrates an example network switch having an access control list based on hard zoning configuration data provided by a network controller; and

[6] Figure 3 illustrates an example network controller, including a non-transitory computer readable medium, for transmitting hard zoning configuration data to a network switch.

DETAILED DESCRIPTION OF SPECIFIC EXAMPLES

[7] Switched fabric network topologies (fabrics) may be used as transport infrastructures in LANs or WANs, and SANs. In a fabric, devices are interconnected via intermediate network switch. Each device, or node, connects to a switch, called an "edge switch," of the fabric. Accordingly, when a first device sends a frame to a second device, the first device transmits the frame via the switch to which it is directly connected, termed the "ingress switch." The frame is sent through the fabric to the switch to which the second device is directly connected, termed the "egress switch." The frame is sent by the egress switch to the second device.

[8] Hardware enforced closed user groups (CUGs) may be created in fabrics using hard zoning. In hard zoning, connectivity and visibility is limited to devices in the same CUG. A device in a hard zoned CUG can only see and communicate with devices in the same CUG. In contrast, in soft zoning, visibility, but not connectivity, is limited to devices in the same CUG. A device in a soft zoned CUG can communicate with a device outside the CUG if it knows the address of the device outside the CUG.

[9] Some transport protocols used in SANs or other datacenter applications, such as RoCE, lack zoning schemes. Other transport protocols, such as iSCSI, only have soft zoning schemes. Although some transport protocols, such as FC and FCoE, provide hard zoning schemes, the schemes may be specific to the transport protocol and may require dedicated hardware resources at the edge switches.

[10] Some implementations of the disclosed technology may be used to provide hard zoning to fabrics in a transport independent manner. For example, a network controller may be used to instantiate hard zoning in a transport independent manner in a controlled fabric. This may allow hard zoning to be applied to various transport protocols that otherwise lack hard zoning capability.

[11] Additionally, a common hard zoning scheme may be applied to various different transport protocols. This may allow the same hardware resources, such as ternary content addressable memory (TCAM) tables, to be

used to implement common hard zoning techniques across different transport technologies. For example, the same hardware resources may be used by a switch to implement a CUG for devices using RoCE and to implement a CUG for devices using FCoE. Additionally, this may avoid a requirement for specific transport protocols to include hard zoning schemes, which may decrease the complexity of the protocols and simplify protocol stack implementations.

[12] Further, aspects of the disclosed technology may remove the need for login and logout procedures to implement hard zoning. This may reduce network overhead and simplify network administration.

[13] Figure 1 illustrates an example method of network switch operation for updating an access control list according to hard zoning configuration data provided by a network controller. The illustrated process may be performed to implement a CUG on a switch fabric in a transport independent manner.

[14] The process includes receiving a frame 105. The frame may be any digital data transmission unit transmitted in accordance with any of various transport protocols. For example, the frame may comprise an Ethernet frame used to transmit iSCSI, FCoE, or RoCE packets. As another example, the frame may comprise a FC frame.

[15] The process further includes detecting a flow corresponding to the frame 110. The term "flow" refers to a sequence of frames used for communication between two network nodes. For example, a flow may comprise a connection in compliance with an FC protocol or an FCoE protocol. As another example, a flow may comprise a session in compliance with an iSCSI protocol or a RoCE protocol.

[16] The network switch may maintain an access control list listing allowed and disallowed flows. Detecting the flow 110 may comprise determining if the frame is part of a flow listed in the access control list. For example, detecting a flow 110 may comprise evaluating information elements of the received frame according to various matching criteria. Additionally, detecting a flow corresponding to the frame 110 may comprise detecting with which of a plurality of transport protocols the frame complies. Detecting a flow

110 may be performed in different manners depending on the transport protocol with which the frame comprises.

[17] For iSCSI flows, detecting a flow 110 may comprise detecting a flow 110 based on Ethernet MAC source and destination address, or IP source and destination address. Detecting an iSCSI flow may also include evaluating TCP connection establishment information, session Initiator_Target Nexus information for a plurality of TCP connections associated with an Initiator, or iSCSI control commands.

[18] For RoCE flows, Ethernet frames may be sent from a source to a destination over a single subnet. Various matching criteria, such as Ethernet MAC source and destination address, RoCE layer-3 source and destination address, and Ethertype, may be used to detect a RoCE flow.

[19] For FCoE flows, FC frames, including the FC header and cyclic redundancy check sequence (CRC), may be encapsulated in an FCoE header, which may be in turn carried by a virtual LAN (VLAN) tagged Ethernet frame. For FCoE frames, detecting a flow 110 may comprise inspecting the virtual LAN (VLAN) information element and Ethertype of the encapsulating Ethernet frame. For example, VLAN and Ethertype may be used in implementations where frames are carried from source to destination via the same Ethernet frame with no header rewrites. As another example, FC header information elements such as Destination Address (D_ID), Source Address (S_ID), frame type (R_CTL), protocol type (TYPE), class of service (CS_CTL), and Frame Control (F_CTL) may be used as match criteria to detect a flow. In some example implementations, the network switch and network controller communicate using an OpenFlow protocol. In some such implementations, the OpenFlow protocol may be extended to include these FC header information elements as match fields.

[20] For FC flows, the FC header information elements, such as as Destination Address (D_ID), Source Address (S_ID), frame type (R_CTL), protocol type (TYPE), class of service (CS_CTL), and Frame Control (F_CTL) may be used as match criteria to detect a flow. In implementations utilizing

OpenFlow, the OpenFlow protocol may be extended to include these FC header information elements as match fields.

[21] For flows complying with other transport protocols, other evaluation criteria may be used to detect a flow 110. Such criteria may be defined by the network administrator according to the CUG or CUGs to be implemented on the switch fabric. For example, such additional evaluation criteria may be provided by a network controller.

[22] The process further includes transmitting, to a network controller, frame information corresponding to the flow 115. In some examples, transmitting the frame information corresponding to the flow 115 comprises transmitting all or a portion of the received frame's header to the network controller. In other examples, the frame information may comprise flow identifiers or other information extracted from the frame for identifying the flow.

[23] In some cases, transmitting the frame information 115 is only performed if the detected flow is a new flow. For example, the frame information is transmitted 115 if the flow is not listed on the network switch's access control list. If the flow is on the access control list, then the switch may not transmit the frame information 115. Instead, the switch may treat the frame according to the flow's entry in the access control list.

[24] The process includes receiving, from the network controller, hard zoning configuration data corresponding to the flow 120. For example, the hard zoning configuration data may indicate whether the flow is between two members of a CUG. The hard zoning configuration data may also include matching criteria to allow the network switch to identify the flow in future frames. For example, the hard zoning configuration data may include a destination address, source address, and protocol type.

[25] The process includes updating an access control list according to the hard zoning configuration data 125. For example, the network switch may add an entry in its access control list including the matching criteria included in the hard zoning configuration data. In some cases, the entries in the access control list may indicate if the flow is disallowed or allowed. If the flow is disallowed, then the network switch may implement hard zoning by discarding

the frame. Additionally, future frames of the flow may be evaluated according to the updated access control list. In some examples, the access control list may be implemented using switch hardware resources, such as ternary content addressable memory (TCAM).

[26] In some implementations, the flow may comply with a first networking protocol, and the access control list may include hard zoning configuration data corresponding to a second flow, the second flow complying with a second networking protocol different from the first networking protocol. For example, the switch may use a single access control list to evaluate frames transmitted using multiple transport protocols. For example, RoCE flows and FCoE flows may be included in the same access control list. In such an example, the same hardware resources may be used to implement hard zoning for multiple transport protocols. For example, a single TCAM table may be used to implement an access control list that includes multiple transport protocols.

[27] Figure 2 illustrates an example network switch 205. The example network switch 205 may be a switch in a fabric controlled by a network controller to implement hard zoning in a transport independent manner. For example, the switch 205 may perform the process illustrated in Figure 1. In some implementations, the switch 205 may be one of several edge switches in a three-tier network, a fat tree flat network, a full mesh network, or other data center or SAN network.

[28] The switch 205 includes a processor 210, and a memory 220, a network interface 215, and switch hardware 240 coupled to the processor 210. The processor 210 may be any processing unit capable of executing instructions stored in memory 220, configuring the switch hardware 240, and communicating using the network interface 215.

[29] Memory 220 may be a non-transitory computer readable medium capable of being read and written by the processor 210. In this example, the memory 220 contains computer executable instructions, including a protocol control stack 225, a software defined network (SDN) client, an access control list 235, and a control module 235.

[30] The protocol control stack 225 may include instructions allowing the network switch 205 to operate in compliance with a transport protocol. For example, the control stack 225 may be an Ethernet control stack, allowing the switch 205 to operate in compliance with the Ethernet protocol and protocols using the Ethernet protocol, such as RoCE, FCoE, or iSCSI. As another example, the control stack 225 may be a FC control stack. As a further example, the control stack 225 may be a converged network control stack, including instructions to allow the switch 205 to operate in compliance with multiple transport protocols, such as Ethernet and FC.

[31] The SDN client 230 may include instructions to cause the switch 205 to communicate with a network controller to receive configuration data to implement a software defined network. For example, the SDN client 230 may comprise an OpenFlow client, which may include extensions to allow the switch 205 to identify additional flows, such as FC and FCoE flows. The SDN client 230 may cause the processor 210 to communicate with a network controller via the network interface 215. In some implementations, the network interface 215 may connect to the fabric that the switch 205 is a part of. For example, both the switch 205 and the network controller may be nodes of the fabric. In other implementations, the network interface 215 may connect to a separate transport network connecting the switches of the fabric to the network controller.

[32] The access control list 235 may comprise a list reflecting membership in a CUG implemented using the switch. For example, the access control list 235 may comprise a list of allowed flows representing pairwise connections between network nodes that are members of the same CUG. The access control list 235 may be populated using hard zoning configuration data obtained from a network controller via operation of the SDN client 230. The hard zoning configuration data may correspond to flows of various protocols. Accordingly, the access control list 235 may include flows from different protocols.

[33] The control module 235 may include instructions to cause the processor 210 to implement the protocol control stack 225 and the SDN client 230. Additionally, the control module 235 may include instruction to cause the

processor 210 to configure the switch hardware 245 to implement the switch's 205 network behaviors. For example, the control module 235 may cause the processor 210 to configure a ternary content addressable memory (TCAM) table of the hardware 245 to reflect the contents of the access control list 235.

[34] The hardware 245 may comprise application specific integrated circuits (ASICs) and TCAM tables, and may be coupled to a plurality of ports 250. The hardware 245 may operate to implement the switch behavior configured by the processor 210 without further processor operation. For example, the hardware 245 may implement the hard zoning behavior reflected in the access control list 235. The hardware 245 may evaluate frames received via a port 250 according to the TCAM table. If the frame is in an allowed flow, the hardware 245 may forward or switch the frame to another port 250. If the access control list 235 includes flows from multiple protocols, then a single TCAM table may be used to implement hard zoning for multiple protocols.

[35] Figure 3 illustrates an example network controller 305, including a non-transitory computer readable medium 320, for transmitting hard zoning configuration data to a network switch. For example, the network controller 305 may connect to a network switch as illustrated in Figure 2.

[36] The example network controller 305 includes a non-transitory computer readable medium having computer executable instructions stored thereon. For example, the non-transitory computer readable medium 320 may comprise read-only memory (ROM), random access memory (RAM), storage, or a combination thereof. In this example, when executed by the processor 310, the instructions implement a flow identifier 330, a retriever 335, and a connection manager 340. In other examples, these modules may be implemented by hardware logic or by a combination of software and hardware logical elements.

[37] The example network controller 305 includes a network interface 315. The network interface 315 may allow the controller to receive frame information from a network switch. The frame information may be information corresponding to a flow. For example, the frame information may be a copy of a frame header or a portion of a frame header. In some implementations, the

frame information may be transmitted by a network switch performing the process illustrated in Figure 1.

[38] The example network controller 305 also includes a flow identifier 330. The flow identifier 330 may use the frame information to identify a flow corresponding to the frame. For example, the flow identifier 330 may use the frame information to determine a source node and a destination node to identify the flow. Additionally, the flow identifier 330 may use the frame information to determine a transport protocol to which the flow complies. The flow identifier 330 may use the transport protocol to identify the flow. Flows identified by the flow identifier 330 may include connections in compliance with an FC or FCoE protocol, or sessions in compliance with an iSCSI or a RoCE protocol.

[39] The example network controller 305 also includes a retriever 335 to retrieve hard zoning configuration data corresponding to the flow. For example, the retriever 335 may retrieve the hard zoning configuration data from a configuration database 350. The configuration database 350 may include a table of allowed pairwise flows forming a closed user group. If the configuration database 350 includes the flow identified by the flow identifier 330, then the hard zoning configuration data may indicate that the flow is an allowed flow. If the configuration database 350 does not include the flow, then the controller 305 may generate hard zoning configuration data indicated that the flow is a disallowed flow. In the illustrated example, the configuration database 350 is stored on medium 320. For example, the configuration database 350 may be provided to the controller 305 by a network administrator via the network interface 315. In other examples, the configuration database may be stored at an external location, and the controller 305 may query the configuration database via the network interface 315.

[40] The example network controller 305 also includes a connection manager 340. The connection manager 340 may cause the network controller 305 to transmit the hard zoning configuration data to a network switch. For example, the connection manager 340 may cause the network controller 305 to transmit the hard zoning configuration data to the network switch via the network interface 315. In some implementations, the connection manager 340

may include an SDN protocol stack, such as an OpenFlow protocol stack. If the flows identified by the flow identifier 330 include FC or FCoE flows, the OpenFlow protocol stack may be extended to include FC or FCoE flows. Accordingly, the connection manager 340 may cause the network interface 315 to transmit the hard zoning configuration data in compliance with an OpenFlow protocol extended to include FC or FCoE flows. The network switch may be an ingress edge switch or an egress edge switch. In some cases, the connection manager 340 may cause the controller 305 to transmit to an ingress edge switch and an egress edge switch. For example, the ingress edge switch and the egress edge switch may be the switches corresponding to the flow source and destination, respectively.

[41] In the foregoing description, numerous details are set forth to provide an understanding of the subject disclosed herein. However, implementations may be practiced without some or all of these details. Other implementations may include modifications and variations from the details discussed above. It is intended that the appended claims cover such modifications and variations.

CLAIMS

1. A method of network switch operation, comprising:
 - receiving a frame;
 - detecting a flow corresponding to the frame;
 - transmitting, to a network controller, frame information corresponding to the flow;
 - receiving, from the network controller, hard zoning configuration data corresponding to the flow; and
 - updating an access control list according to the hard zoning configuration data.
2. The method of claim 1, wherein detecting a flow corresponding to the frame comprises detecting with which of a plurality of transport protocols the frame complies.
3. The method of claim 1, wherein:
 - the first flow complies with a first networking protocol; and
 - the access control list includes hard zoning configuration data corresponding to a second flow, the second flow complying with a second networking protocol different from the first networking protocol.
4. The method of claim 3, wherein the access control list is implemented using a single ternary content-addressable memory table.
5. A network controller, comprising:
 - a network interface to receive, from a network switch, frame information corresponding to a flow;
 - a flow identifier to use the frame information to determine a source node and a destination node to identify the flow;
 - a retriever to retrieve hard zoning configuration data corresponding to the flow; and
 - the network interface to transmit, to the network switch, the hard zoning configuration data.

6. The controller of claim 5, wherein the retriever is to retrieve the hard zoning configuration data from a configuration database comprising a table of allowed pairwise flows, the allowed pairwise flows forming a closed user group.
7. The controller of claim 5, wherein the network switch comprises an ingress edge switch, and wherein the transmitter is to transmit the hard zoning configuration data to an egress edge switch corresponding to the flow.
8. The controller of claim 5, wherein the flow identifier is to:
 - use the frame information to determine a transport protocol to which the flow complies; and
 - use the transport protocol to identify the flow.
9. The controller of claim 5, wherein the flow comprises:
 - a connection in compliance with a Fibre Channel protocol or Fibre Channel over Ethernet protocol, or
 - a session in compliance with an Internet Small Computer System Interface protocol or a Remote Direct Memory Access over Converged Ethernet protocol.
10. The controller of claim 5, wherein the network interface is to transmit the hard zoning configuration data in compliance with an OpenFlow protocol extended to include Fibre Channel or Fibre Channel over Ethernet flows.
11. A non-transitory computer readable medium having computer executable instructions stored thereon, the instructions to implement, when executed by a processor:
 - a flow identifier to use information from a frame to identify a flow corresponding to the frame;
 - a retriever to retrieve hard zoning configuration data corresponding to the flow; and
 - a connection manager to cause a network controller to transmit the hard zoning configuration data to a network switch.

12. The non-transitory computer readable medium of claim 11, wherein the instructions, when executed by the processor, implement the flow identifier to:
 - use the information from the frame to identify a flow source address;
 - use the information from the frame to identify a flow destination address;
 - use the information from the frame to identify a transport protocol that the flow complies with; and
 - use the flow source device, the flow destination device, and transport protocol to identify the flow.
13. The non-transitory computer readable medium of claim 11, wherein the instructions, when executed by the processor, implement the connection manager to cause the network controller to transmit the hard zoning configuration data to a second network switch.
14. The non-transitory computer readable medium of claim 11, wherein the instructions, when executed by the processor, implement the retriever to retrieve the hard zoning configuration data from a configuration database.
15. The non-transitory computer readable medium of claim 14, wherein the configuration database comprises a table of pairwise flows forming a closed user group.

1/3

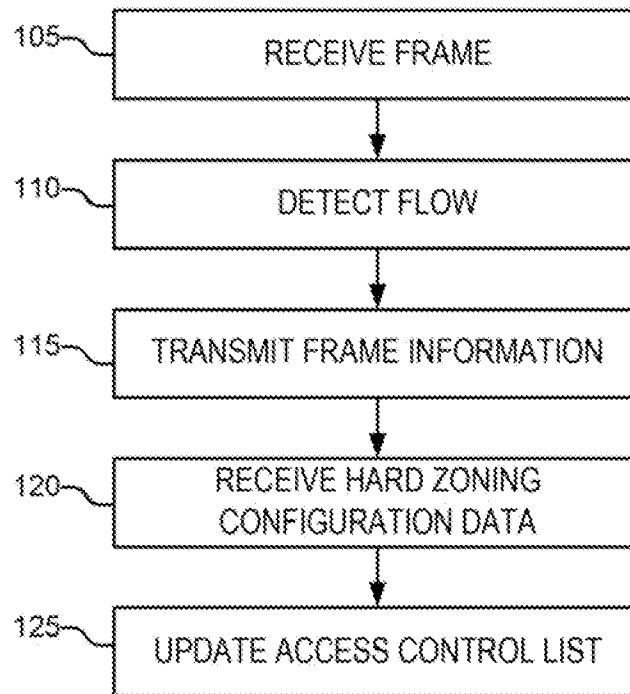
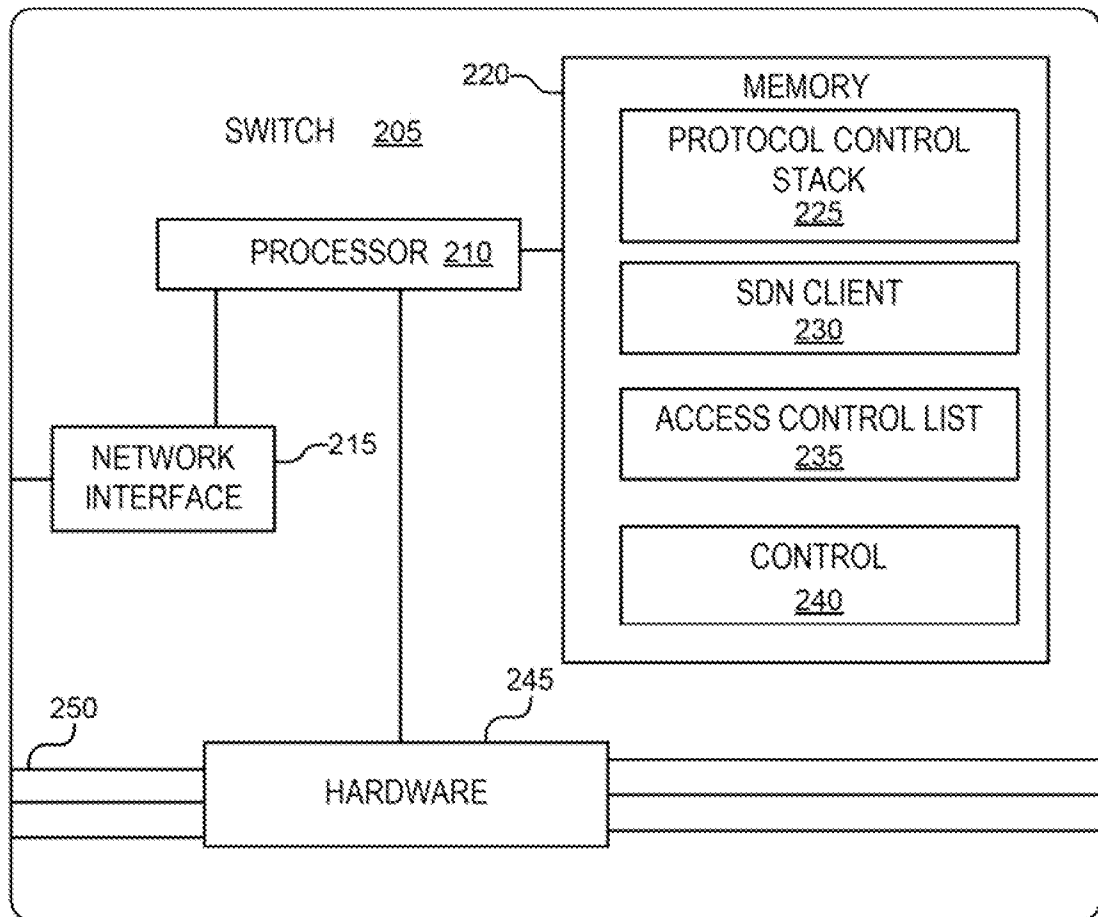
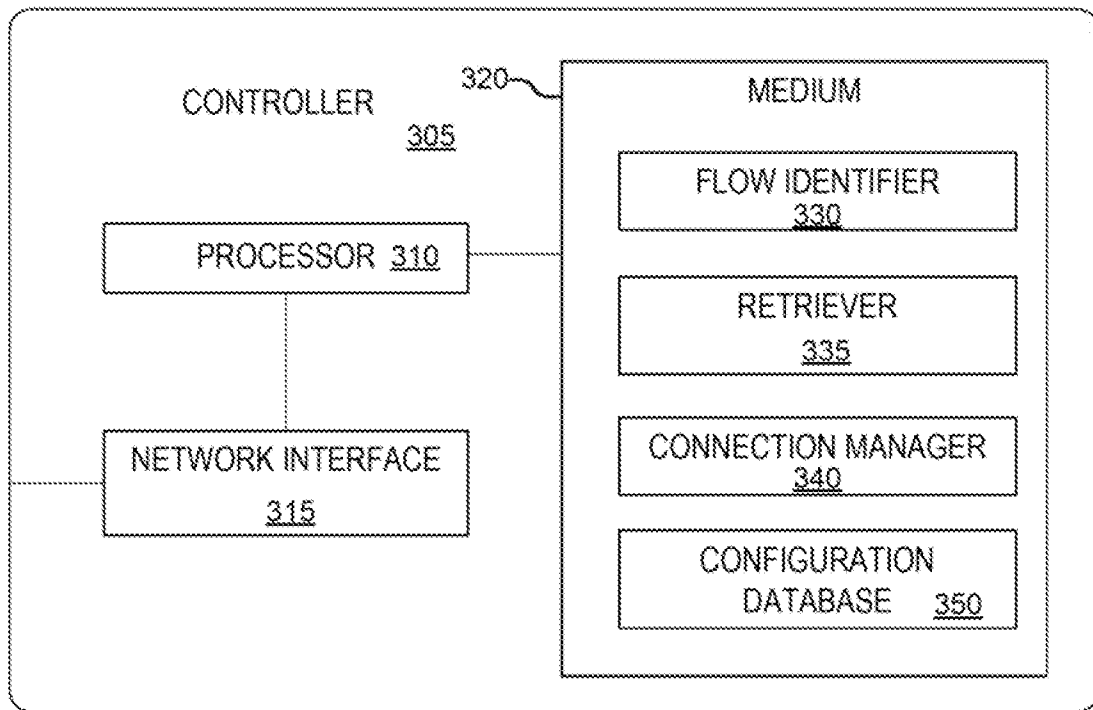


FIG. 1

2/3



3/3



INTERNATIONAL SEARCH REPORT

International application No.
PCT/US2013/047351**A. CLASSIFICATION OF SUBJECT MATTER****H04L 12/28(2006.01)i, H04L 12/801(2013.01)i**

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 12/28; G06F 15/173; G06F 3/00; H04L 12/26; H04L 9/00; H04L 12/22; H04L 12/801

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

Korean utility models and applications for utility models

Japanese utility models and applications for utility models

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

eKOMPASS(KIPO internal) & Keywords: network, switch, frame, information, hard, zoning, access, control, list

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2009-0037977 A1 (SILVANO GAI et al.) 05 February 2009 See paragraphs [0006], [0016]-[0017], [0025]-[0028], [0031], [0038]-[0039], [0053]-[0058], [0061], [0064], [0075]; and figures 1, 3-4.	5,7,9-11,13-14
Y		1-2,8,12
A		3-4,6,15
Y	US 2012-0226801 A1 (SHRIRAM VELAGA et al.) 06 September 2012 See paragraphs [0010], [0014], [0018], [0046], [0048]; and figures 1, 3, 4i.	1-2,8,12
A		3-7,9-11,13-15
A	US 8364852 B1 (AMIT SHUKLA et al.) 29 January 2013 See column 1, lines 20-24; column 5, line 55 - column 6, line 19; and figures 3, 9.	1-15
A	US 2012-0039163 A1 (AKIO NAKAJIMA) 16 February 2012 See paragraphs [0026], [0028], [0034], [0065]; and figures 1-2, 6.	1-15
A	KR 10-2003-0036216 A (QLOGIC SWITCH PRODUCTS, INC.) 09 May 2003 See page 2, lines 1-15; page 3, lines 1-15; page 5, lines 5-11; and figures 1-2.	1-15



Further documents are listed in the continuation of Box C.



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

17 March 2014 (17.03.2014)

Date of mailing of the international search report

18 March 2014 (18.03.2014)

Name and mailing address of the ISA/KR

International Application Division
Korean Intellectual Property Office
189 Cheongsa-ro, Seo-gu, Daejeon Metropolitan City, 302-701,
Republic of Korea

Facsimile No. +82-42-472-7140

Authorized officer

LEE, Dong Yun

Telephone No. +82-42-481-8734



INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.

PCT/US2013/047351

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2009-0037977 A1	05/02/2009	US 2013-086266 A1 US 8321908 B2	04/04/2013 27/11/2012
US 2012-0226801 A1	06/09/2012	None	
US 8364852 B1	29/01/2013	None	
US 2012-0039163 A1	16/02/2012	US 8422359 B2 WO 2011-121664 A1	16/04/2013 06/10/2011
KR 10-2003-0036216 A	09/05/2003	AU 2001-75252 A1 CA 2410932 A1 CA 2410932 C EP 1290837 A2 EP 1290837 B1 JP 04741039 B2 JP 2004-501565 A US 2003-0179748 A1 US 2008-0002687 A1 US 2008-0095152 A1 US 7248580 B2 US 7684398 B2 US 7978695 B2 WO 01-95566 A2 WO 01-95566 A3	17/12/2001 13/12/2001 13/04/2010 12/03/2003 24/10/2007 03/08/2011 15/01/2004 25/09/2003 03/01/2008 24/04/2008 24/07/2007 23/03/2010 12/07/2011 13/12/2001 13/06/2002