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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
14 February 2013 (14.02.2013)

WIPO | PCT

(10) International Publication Number
WO 2013/023153 A1

(51) International Patent Classification:
H04L 12/28 (2006.01) *H04L 29/06* (2006.01)

(21) International Application Number:
PCT/US2012/050373

(22) International Filing Date:
10 August 2012 (10.08.2012)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:

61/522,158	10 August 2011 (10.08.2011)	US
61/533,436	12 September 2011 (12.09.2011)	US
61/550,315	21 October 2011 (21.10.2011)	US
13/571,870	10 August 2012 (10.08.2012)	US

(71) Applicant *(for all designated States except US)*: **MARVELL WORLD TRADE LTD.** [BB/BB]; L'Horizon Gunsite Road, Brittons Hill, St. Michael, BB 14027 (BB).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **SUTARDJA, Sehat** [US/US]; 27330 Elena Road, Los Altos Hills, California 94022 (US). **DANIEL, Tsahi** [IL/US]; 3517 Greer Road, Palo Alto, California 94303 (US). **MELTS, Dimitry** [IL/US]; 6450 Myrtlewood Drive, Cupertino, California 95014 (US).

(74) Agents: **WIGGINS, Michael D.** et al.; Harness, Dickey & Pierce, P.L.C., P.O. Box 828, Bloomfield Hills, Michigan 48303 (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, KM, 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, 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, ML, MR, NE, SN, TD, TG).

Published:

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

[Continued on next page]

(54) Title: INTELLIGENT PHY WITH SECURITY DETECTION FOR ETHERNET NETWORKS

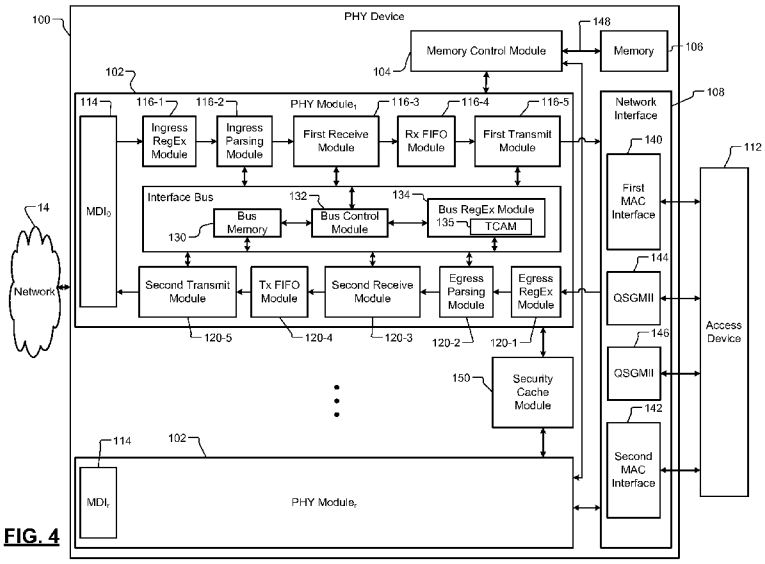

FIG. 4

(57) Abstract: A physical layer device includes memory, a memory control module, and a physical layer module. The memory control module is configured to control access to the memory. The physical layer module is configured to store packets in the memory via the memory control module. The physical layer module includes an interface configured to receive the packets from a network device via a network and an interface bus. The interface bus includes at least one of a control module and a regular expression module. The at least one of the control module and the regular expression module is configured to inspect the packets to determine a security level of the packets. A network interface is configured to, based on the security level, provide the packets to a device separate from the physical layer device.

WO 2013/023153 A1

— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments (Rule 48.2(h))*

INTELLIGENT PHY WITH SECURITY DETECTION FOR ETHERNET NETWORKS

CROSS-REFERENCE TO RELATED APPLICATIONS

[0001] This application claims priority to U.S. Nonprovisional Application No. 13/571,870, filed August 10, 2012 and also claims the benefit of U.S. Provisional Application No. 61/522,158 filed August 10, 2011; U.S. Provisional Application No. 61/533,436, filed September 12, 2011; and U.S. Provisional Application No. 61/550,315, filed October 21, 2011. The disclosures of the above application are incorporated herein by reference in their entirety.

FIELD

[0002] The present disclosure relates to security detection systems within network devices.

BACKGROUND

[0003] The background description provided herein is for the purpose of generally presenting the context of the disclosure. Work of the presently named inventors, to the extent the work is described in this background section, as well as aspects of the description that may not otherwise qualify as prior art at the time of filing, are neither expressly nor impliedly admitted as prior art against the present disclosure.

[0004] Access networks provide connections between two or more network devices and/or between a network device and an Internet. The network devices may include, for example, user devices, peripheral devices, and data storage devices. The devices may be located in one or more networks. The connections are established to uplink and/or downlink signals between the devices and/or between the devices and the Internet.

[0005] As an example, an Ethernet-based access network may include an access chassis. The access chassis provides connections between network devices and/or between the network devices and the Internet. The access chassis may include, for example, fabric cards (e.g., 2 fabric cards) and line cards (e.g., 16 line cards). Each of the fabric cards can be connected to each of the line cards. The line cards are

connected to the network devices via an Ethernet network. Predetermined ports or uplink ports of one or more of the line cards may be connected to the Internet. The fabric cards provide connections between the line cards. The line cards provide connections between the network devices and the fabric cards and/or between the fabric cards and the Internet.

[0006] Each of the fabric cards typically includes an aggregation switch and a central control module. The aggregation switch provides connections between the line cards to route, for example, signals from a) a first user device connected to a first line card to b) a second user device or the Internet connected to a second line card. The central control module controls states of the connections and the transfer of packets between the line cards. Each of the line cards typically includes an access switch and multiple PHY devices (e.g., 6 PHY devices). Each of the PHY devices includes one or more PHY modules. The access switch provides connections between the aggregation switch located on the fabric card and the PHY modules.

SUMMARY

[0007] A physical layer device is provided and includes memory, a memory control module, and a physical layer module. The memory control module is configured to control access to the memory. The physical layer module is configured to store packets in the memory via the memory control module. The physical layer module includes an interface configured to receive the packets from a network device via a network and an interface bus. The interface bus includes at least one of a control module and a regular expression module. The at least one of the control module and the regular expression module is configured to inspect the packets to determine a security level of the packets. A network interface is configured to, based on the security level, provide the packets to a device separate from the physical layer device.

[0008] In other features, a method is provided and includes receiving packets from a network device via a network at an interface of a physical layer module. The packets are transferred from a physical layer device to a memory control module to store the packets in a memory. The physical layer device includes the physical layer module. The physical layer module includes an interface bus. The packets are inspected to

determine a security level of the packets via at least one of a control module and a regular expression module. The interface bus includes the at least one of the control module and the regular expression module. Based on the security level, the packets are provided via a physical layer interface to a device separate from the physical layer device.

[0009] In other features, a physical layer device is also provided and includes a memory interface, a memory control module, a physical layer module, and a second network interface. The memory interface is connected to the memory. The memory control module is configured to control access to the memory. The physical layer module is configured to receive packets from a network device via a network at a first network interface and store the packets in the memory via the memory control module. The physical layer module is separate from the memory. The second network interface is configured to provide the packets to a device separate from the physical layer device and the memory.

[0010] Further areas of applicability of the present disclosure will become apparent from the detailed description, the claims and the drawings. The detailed description and specific examples are intended for purposes of illustration only and are not intended to limit the scope of the disclosure.

BRIEF DESCRIPTION OF DRAWINGS

[0011] The present disclosure will become more fully understood from the detailed description and the accompanying drawings, wherein:

[0012] FIG. 1 is a functional block diagram of an access network incorporating an access chassis in accordance with the present disclosure;

[0013] FIG. 2 is a functional block diagram of a portion of the access chassis of FIG. 1;

[0014] FIG. 3 is a functional block diagram of another access network incorporating PHY devices in accordance with the present disclosure;

[0015] FIG. 4 is a functional block diagram of a PHY device in accordance with the present disclosure;

[0016] FIG. 5 is a functional block diagram of an ingress portion of a PHY module providing multi-level security detection in accordance with the present disclosure;

[0017] FIG. 6 is a functional block diagram of a network interface in accordance with the present disclosure; and

[0018] FIG. 7 illustrates a network access method including a security detection method in accordance with the present disclosure.

DESCRIPTION

[0019] An access network may include an access chassis with fabric cards and line cards. The fabric cards may each include an aggregation switch and a central control module. The line cards may each include an access switch and multiple PHY devices. Because each of the fabric cards includes a central control module and an aggregation switch and each of the line cards includes an access switch, a control plane associated with the access chassis is complex. The line cards may be referred to as high cost and/or high-power cards due to the inclusion and operation of the access switch. The access chassis may be upgrade limited, as each of the line cards needs to be replaced in order to perform a control specific upgrade (e.g., upgrade to change how switch connections are provided).

[0020] In the following examples, multiple access networks are provided. A first access network is disclosed in FIGs. 1-2 and includes line cards that do not include access switches. Switching between the line cards, between network devices, and between the network devices and the Internet are provided via fabric cards. As a result, the line cards may be referred to as low cost and/or low-power line cards. The line cards include PHY modules that may be configured to perform deep packet inspection (DPI). DPI includes inspection of packets to determine whether a packet is a valid packet or an invalid packet. A packet may be an invalid packet when the packet has an incorrect format, contains a pattern associated with an attack and/or virus, has improper value(s), includes spam, introduces a security threat and/or does not satisfy predefined criteria. DPI may include inspection of headers and/or a payload of one or more packets. The headers may include, for example, an internet protocol (IP) header,

a transmission control protocol (TCP), a user datagram protocol (UDP), and/or other headers.

[0021] Since the line cards do not include access switches and the fabric cards control access, aggregation and switching functionality for the line cards, network devices, and the Internet, the access network chassis is easily upgradable. During an upgrade, control logic, software, and/or hardware may be altered and/or replaced. The access network may be upgraded by simply replacing one or more of the fabric cards and not the line cards. In addition, complexity of a control plane associated with the access network is reduced, since switching of the connections is performed in one or more centralized locations, as opposed to being performed in numerous line cards and fabric cards. The access network of FIGs. 1-2 and other example access networks and associated features are described below.

[0022] In FIG. 1, an access network 10 is shown. As an example, the access network 10 may be an application-aware network. An application-aware network is a network that directly cooperates with applications and services to maximize network responsiveness to application-specific requirements. Modules in an application-aware network may convey objects including methods to be invoked at different points in the network. Application-specific programming of switches and processing devices is performed according to the methods. The modules perform customized computations and resource management to meet application-specific requirements. An application-aware network may be used to manage security of proprietary networks and/or local area networks (LANs).

[0023] The access network 10 may include an access chassis 12, a network 14, an Internet 16, and network devices 18 (p network device are shown). The access chassis 12 is connected to the network devices 18 via the network 14. The network 14 may be, for example, an Ethernet network. The access chassis 12 routes signals between the network devices 18 and/or between the network devices 18 and the Internet 16. The network devices 18 may include user devices, peripheral devices, and/or data storage devices. The user devices may include computers, cellular phones, set top boxes, televisions, etc.

[0024] The access chassis 12 includes one or more fabric cards 20 (2 are shown), and one or more line cards 22 (n are shown). The line cards 22 include PHY devices 24. An example of a PHY device is shown in FIG. 4. In the example shown, each of the line cards 22 includes m PHY devices. As an example, the access chassis 12 may include 48 line cards, where each of the line cards includes one or more PHY devices (e.g., 6 PHY devices). Each of the fabric cards 20 includes an aggregation switch 26 that provides connections between the line cards 22, between the PHY devices 24 on the same line card, and/or between the PHY devices on different ones of the line cards 22.

[0025] Referring now also to FIG. 2, a portion 30 of the access chassis 12 is shown. The portion 30 includes one of the fabric cards 20 (designated 32) and one of the line cards 22 (designated 34). Each of the fabric cards 20 may include a central control module 36, an aggregation switch (designated 38 in FIG. 2), and memory devices 40. In one implementation, the central control module 36 is not included in the aggregation switch 38. The aggregation switch 38 switches between PHY devices 24 on the line cards 22 and provides centralized switching. The central control module 36 may control states of switches 42 in the aggregation switch 38.

[0026] The memory devices 40 may each include, for example, double data rate type 3 (DDR3) synchronous random access memory (SRAM) and/or other suitable memory, such as dynamic random access memory (DRAM). Each of the line cards 22 includes respective ones of the PHY devices 24 (example PHY devices of a first line card 34 are designated 44 in FIG. 2) and does not include an access switch. An access switch refers to a switch located on a line card and configured to provide connections between the line card and a fabric card of an access chassis.

[0027] The PHY devices 44 enable centralized switching. Switching is not performed at the PHY devices 44, but rather is performed at the fabric cards 20. The PHY devices 44 forward the received packets to the fabric cards 44 to then be forwarded to expected or originally selected destinations. Each of the PHY devices 44 may perform DPI. This provides DPI at an edge of the access network 30. An edge of an access network may refer to a boundary between the access chassis 32 and the network 14 and/or at a boundary between the access chassis 32 and the network devices 18. DPI may include sending packets to the central control module 36 when a PHY module of

one of the PHY devices 44 is unable to determine whether a packet is a valid packet or an invalid packet. As an example, a packet may be forwarded from the PHY module to the central control module 36 via the aggregation switch 38 for inspection. The central control module 36 may inspect the packet to determine the validity of the packet and then either instruct the PHY module to drop (i.e. delete and/or prevent further transmission of packets similar to the packet) or forward packets similar to the first packet based on results of the inspection. An invalid packet may be dropped, whereas a valid packet may be forwarded. Similar packets may refer to packets having the same format, source address, destination address, and/or other packet parameters and/or fields.

[0028] The PHY module may inspect ingress packets, forward the ingress packets towards the aggregation switch 38, tunnel the ingress packets to the central control module 36 for further inspection, and/or drop invalid or unsecure ones of the ingress packets. During packet inspection, PHY hardware of the PHY devices 44 identifies ingress packets as: valid packets; packets for which further localized inspection is to be performed; packets for which centralized inspection is to be performed, or invalid packets. Localized inspection refers to inspection performed within the PHY devices 44 and/or by modules within the PHY devices 44. Centralized inspection refers to inspection performed external to the PHY devices 44, and in, for example, the central control module 36. A valid packet may refer to a packet that is quickly (within a predetermined period) and/or clearly determined to be safe and correct (does not have one or more errors) and/or have a proper format, signature, and/or pattern. As an example, a packet received from a particular local source may be determined to be valid based on a received address of the source.

[0029] A packet for which further centralized inspection is to be performed may refer to a packet that has been inspected by the PHY hardware and/or a module of the associated PHY device, but is not quickly and/or clearly determined to be a valid packet. Such a packet may have one or more errors, unknown format, include suspicious content, or be from a remote source outside of a local network. For this reason, the packet may be further inspected by the central control module 36.

[0030] A tunneling packet refers to: a packet that is not recognizable to the PHY device and/or module of the PHY device; may have been inspected by the PHY device and/or module of the PHY device; and/or the PHY device and/or module of the PHY device is unable to determine whether the packet is a valid packet or an invalid packet. The tunneling packet may not be inspected by the PHY device and/or module of the PHY device and may be simply forwarded to the central control module 36. An invalid packet is a packet that is determined to be invalid through inspection. The invalid packet may have an improper format, signature, pattern, and/or values. If a packet is determined to be invalid by the PHY device and/or module of the PHY device, the packet may be dropped, deleted, prevented from being forwarded to a device or module in the access chassis, and/or may not be forwarded to one of the fabric cards 20. Tunneling packets and packets for which further localized inspection is to be performed may be referred to as suspicious packets.

[0031] Each of the PHY devices 24, 44 may include a communication link to each of the fabric cards 20. In FIG. 2, FC1 refers to fabric $card_1$. FC2 refers to fabric $card_2$. Subscripts of each of the communication links FC1, FC2 refer to one of the PHY devices 44. For example, $FC1_1$ refers to communication links between fabric $card_1$ and PHY $device_1$. Two communication links are provided for load balancing and/or interface redundancy. Load balancing may including transporting equal amounts of data over two or more links during the same time period. Interface redundancy may refer to the inclusion of two or more interfaces (or communication links), where one or more of the interfaces are provided as a backup in case an interface is disabled or unusable.

[0032] The memory devices 40 may be used to store instructions, code, rules, tables, and/or packet data. The instructions, code, rules, and/or tables may be used by the central control module 36, the aggregation switch 38, and/or the PHY devices 44 when performing DPI and/or when controlling states of the switches 42. The memory devices 40 may be used to store: packets that are being inspected; copies of selected packets to be inspected; and/or packets that are to be forwarded, uplinked, and/or downlinked. A packet is uplinked when the packet is forwarded from one of the network devices 18 via the access chassis 12 to the Internet 16. A packet is downlinked

when the packet is forwarded from the Internet 16 via the access chassis 12 to one of the network devices 18.

[0033] In FIG. 3, another access network 50 is shown. As an example, the access network 50 may be an application-aware network and include one or more access chassis 52 (m are shown), the network 14, the Internet 16, and the network devices 18. The access chassis 52 may include routers, switches, computers, servers, or other suitable access devices. Each of the access chassis 52 includes a line card 54. Each of the line cards 54 includes one or more PHY devices 56. An example of a PHY device is shown in FIG. 4. Each of the PHY devices 56 includes one or more PHY modules. Example PHY modules are shown in FIG. 4. The PHY devices 56 communicate with the network devices 18 via the network 14.

[0034] The access chassis 52 may provide connections between each other, between PHY devices of the same access chassis, between PHY devices of different access chassis, and/or between the PHY devices and the Internet 16. In so doing, the access chassis 52 may provide connections between the network devices 18 and/or between the network devices 18 and the Internet 16.

[0035] The access network 50 may also include a central network device 60. The central network device 60 may be used to control the access chassis 52, to perform DPI, and/or to inspect packets that are indiscernible (referred to as tunneling packets) by the access chassis 52. A tunneling packet may be a packet that cannot be determined by an access chassis, a PHY device, and/or a module of a PHY device to be valid or invalid.

[0036] The central network device 60 may be located in a network remote from the access chassis 52 and/or may be located in a local network of the access chassis 52. The central network device 60 may be disposed within one or more of the access chassis 52. The central network device 60 and/or one or more of the access chassis 52 may be collectively a service provider providing one or more services to the network devices 18.

[0037] The PHY devices 24, 44, 56 and modules of the PHY devices 24, 44, 56 of FIGs. 1-3 may be located and/or connected, for example, between a) the network 14 or the Internet 16 and b) MAC devices and/or other higher layer devices in the line cards 22, 34 and access chassis 52. The PHY devices 24, 44, 56 may refer to devices in a physical layer of the line cards 22, 34 and access chassis 52.

[0038] Referring also to FIG. 4, a PHY device 100 is shown. The PHY device 100 may be used: to provide a security firewall between networks; for zero-day attack prevention; in access enterprise networks; etc. The PHY device 100 may be referred to as a firewall in a PHY package. The PHY device 100 may functionality provide a firewall operating across multiple International Organization for Standardization (ISO) and/or open systems interconnection (OSI) layers, not only across a PHY layer. The firewall functionality is provided across PHY layers and layers (e.g., MAC layers) higher than the PHY layers. A zero-day attack is an attack that exploits a previously unknown vulnerability in a computer application. A zero-day attack occurs on "day zero" of awareness of the vulnerability. This means there have been zero days to address and patch the vulnerability. A zero-day attack exploits software that uses a security hole to carry out an attack. Zero-day attack prevention refers to prevention of a zero-day attack. This may include preventing invalid packets, such as packets associated with a virus or a worm, from spreading (i.e. being further passed along in a network). This includes dropping (or deleting) the invalid packets upon detection of the attack. This detection and dropping of the packets may be performed by the PHY device 100 and/or one of the devices and/or modules of the PHY device 100.

[0039] In an access enterprise network, the PHY device 100 and/or one or more devices and/or modules of the PHY device 100 may be used to: prevent network devices from accessing the Internet 16; and/or provide limited access to the Internet 16. Example devices and modules of the PHY device 100 are described below.

[0040] The PHY device 100 includes PHY modules 102 (may be referred to as PHY channels), a memory control module 104, a PHY memory 106, and a network interface 108 (may be referred to as a fabric interface). The PHY device 100 communicates with the network 14 via the PHY modules 102 and with, for example, an aggregation switch (e.g., the aggregation switch 38) or a central network device (e.g., the central network device 60) via the network interface 108. The aggregation switch and the central network device are shown as access device 112 in FIG. 4. The aggregation switch may provide switching to route packets between the PHY modules 102 and/or between PHY modules of different PHY devices.

[0041] Each of the PHY modules 102 may include a media dependent interface (MDI) 114 (or first network interface), ingress modules 116, an interface bus 118, and egress modules 120. The MDIs 114 receive packets from, for example, one or more network devices via the network 14 and forwards the packets to the ingress modules 116. The MDIs 114 also receive packets from the egress modules 120 and transmits the packets to, for example, the network devices via the network 14. In one implementation, each of the MDIs 114 is connected to a twisted wire pair. In the implementation shown, the PHY device 100 includes 8 MDIs or other suitable interface(s).

[0042] The ingress modules 116, the egress modules 120 and/or other modules and/or devices of each of the PHY modules 102 other than the interface bus 118 may collectively be referred to as PHY hardware. The ingress modules 116 may include an ingress regular expression (RegEx) module 116-1, an ingress parsing module 116-2, a first receive module 116-3, a receive first-in-first-out (FIFO) module 116-4, and a first transmit module 116-5. The PHY modules 102 may not include one or more of the ingress modules 116. The ingress RegEx module 116-1, when included, performs a RegEx process to examine packets. The RegEx process includes comparing characters, words, signatures or patterns of data with predetermined characters, words, signatures and patterns of data. The RegEx process may be performed as part of a DPI process. The ingress RegEx process may be performed to quickly identify packets that are valid or invalid.

[0043] The ingress parsing module 116-2 may discard invalid packets and may forward valid packets and/or headers of the valid packets to the interface bus 118 and the first receive module 116-3. The first receive module 116-3 may be a direct memory access (DMA) device and copy and/or store packets, portions of the packets, packet descriptors and/or packet information received from the ingress parsing module 116-2 and/or the interface bus 118 in the PHY memory 106 and/or in a bus memory 130 of the interface bus 118. A bus control module 132 of the interface bus 118 may control storage of data in the bus memory 130. Storage in the PHY memory 106 may be performed via the memory control module 104. The portions of the packets may include one or more headers, and/or payloads of the packets. The packet information

may include information included within the headers and/or other information, such as an inspection level of the packet, a source address, a destination address, a source ID, a destination ID, a protocol ID, a length of the packet, etc. The inspection level may indicate whether the packet is: a valid packet; a packet for which additional inspection is to be performed by the bus control module 132 and/or a bus regular expression module 134; a packet to be tunneled to a central control module (e.g., the central control module 62); or an invalid packet that is to be dropped.

[0044] The ingress parsing module 116-2 may also indicate to the interface bus 118 and/or the bus control module 132 whether a packet should be inspected by the interface bus 118 and/or the bus control module 132. The first receive module 116-3 may, based on instructions from the interface bus 118, a) store packets in and/or copy packets to the PHY memory 106 and/or b) forward packets to the receive FIFO module 116-4.

[0045] The receive FIFO module 116-4, when included, stores packets to be forwarded to the network interface 108 (or second network interface). The packets, packet descriptors, and/or packet information stored in the bus memory 130 and/or the PHY memory 106 may be stored in the receive FIFO module 116-4 for inspection by the bus control module 132 and/or a bus RegEx module 134 of the interface bus 118. The bus control module 132 and/or the bus RegEx module 134 may be individually or collectively referred to as a local control module and may perform localized inspection of packets.

[0046] The first transmit module 116-5 may also be a DMA device and may transmit packets received from the receive FIFO module 116-4, the PHY memory 106, and/or the interface bus 118 to the network interface 108. The first transmit module 116-5 may, based on instructions received from the interface bus 118 and/or modules of the interface bus 118, a) access packets stored in the PHY memory 106 and/or b) forward packets to the network interface 108. The first transmit module 116-5 may indicate to the network interface 108, the access device 112 whether a packet should be inspected by the aggregation switch and/or the central control module.

[0047] The interface bus 118 may be an advanced extensible interface (AXI) and/or have an advanced microcontroller bus architecture (AMBA) and use an AMBA protocol.

The interface bus 118 may include the bus memory 130, the bus control module 132, and the bus RegEx module 134. The bus memory 130 may include, for example, SRAM or other suitable memory. The bus memory 130 may be used by the access device 112 and/or the PHY device 100 when performing DPI and/or when controlling states of switches in the aggregation switch, a central network device (e.g., the central network device 60), and/or in an access device (e.g., the access device 112).

[0048] The bus control module 132 and/or the bus RegEx module 134 may perform DPI to determine a security level of packets received, drop invalid packets, forward valid packets, and/or tunnel packets to the central control module for further inspection. The bus control module 132 may control RegEx parsing performed by the bus RegEx module 134. The bus control module 132 may use the bus memory 130, the memory control module 104 and/or the PHY memory 106 when performing zero day attack prevention. As each of the PHY modules 102 may include a bus control module and/or one or more RegEx module(s), a bus control module and a RegEx module may be provided for each of the MDIs 114. This provides interface or port specific packet inspection and RegEx parsing.

[0049] The bus control module 132 may perform content signature recognition tasks for application-based networking and network security applications. The bus control module 132 may inspect packets at wire-speed (e.g., 1 Gbps). The bus control module 132 may analyze a packet and determine whether to drop, forward and/or mark a packet as indiscernible at a wire-speed. The bus control module 132 may be a 32-bit processor. Each bus control module in each of the PHY modules 102 may communicate with the access device 112. This communication may include: receiving rule and/or table updates for packet inspection from the central control module; and rerouting and/or reporting unusual and/or suspicious packets from the PHY modules 102 to the central control module.

[0050] The egress modules 120 may include an egress RegEx module 120-1, an egress parsing module 120-2, a second receive module 120-3, a transmit FIFO module 120-4, and a second transmit module 120-5. The PHY modules 102 may not include one or more of the egress modules 120. The egress RegEx module 120-1, when included, performs a RegEx process to examine packets received from one of the PHY modules

102 via the network interface 108. The RegEx process includes comparing characters, words, signatures, or patterns of data with predetermined characters, words, signatures and patterns of data. The RegEx process may be performed as part of a DPI process. The egress RegEx process may be performed to quickly identify packets that are valid or invalid.

[0051] The RegEx modules 116-1, 130-1, 134 may perform packet filtering based on RegEx matching. The RegEx modules 116-1, 130-1, 134 may analyze one or more packets to detect patterns in headers and/or payloads in each packet and/or across multiple packets. RegEx searching may be performed to detect patterns over sequential packets and/or over non-sequential packets to provide a full perimeter firewall. This may include complete packet Internet protocol (IP) blocking to block packets destined to predetermined destinations and/or computers. The RegEx modules 116-1, 130-1, 134 may stop or temporarily suppress an attack until a systematic corrective action can be deployed. This allows false positives of an attack and prevents missing negatives (or errors indicating an attack). The RegEx modules 116-1, 130-1, 134 may each include, be replaced with, or be used in combination with one or more ternary content addressable memories (TCAMs). In FIG. 4, a single TCAM 135 is shown.

[0052] A content addressable memory (CAM) is an application specific memory that allows its entire contents to be searched within a single clock cycle. A binary CAM performs exact-match searches, while a TCAM allows pattern matching with the use of "don't cares". Don't cares are used as wildcards during a search, and are useful in implementing longest-prefix-match searches in routing tables. The above-mentioned TCAMs may be used for packet classification and for hardware matching acceleration. TCAMs may be used to store deterministic finite automata (DFA) representations of regular expressions used during RegEx packet inspection. A DFA is a 5-tuple (e.g., Q, $\sum$, δ, q_0, A), where Q is a set of states, $\sum$ is an alphabet, δ is a transition function that is based on Q and $\sum$, q_0 is a start state, and A is a set of accepting states.

[0053] The egress parsing module 120-2 may discard invalid packets and may forward valid packets and/or headers of the valid packets to the interface bus 118 and the second receive module 120-3. The second receive module 120-3 may be a DMA device and copy and/or store packets, portions of the packets, packet descriptors,

and/or packet information received from the egress parsing module 120-2 and/or the interface bus 118 in the bus memory 130 and/or the PHY memory 106. Storage in the bus memory 130 may be performed via the bus control module 132. Storage in the PHY memory 106 may be performed via the memory control module 104. The portions of the packets may include one or more headers, and/or payloads of the packets. The packet information may include information included within the headers and/or other information, such as an inspection level of the packet, a source address, a destination address, a source ID, a destination ID, a protocol ID, a length of the packet, etc.

[0054] The egress parsing module 120-2 may also indicate to the interface bus 118 and/or the bus control module 132 whether a packet should be inspected by the interface bus 118 and/or the bus control module 132. The second receive module 120-3 may store packets in and/or copy packets to the PHY memory 106 and/or forward packets to the transmit FIFO module 120-4 based on instructions from the interface bus 118.

[0055] The transmit FIFO module 120-4 stores packets to be forwarded to the second transmit module 120-5. The packets, packet descriptors, and/or packet information stored in the bus memory 130 and/or the PHY memory 106 may be stored in the transmit FIFO module 120-4 for inspection by the bus control module 132 and/or the bus RegEx module 134. The second transmit module 120-5 may also be a DMA device and may transmit packets received from the transmit FIFO module 120-4, the PHY memory 106, and/or the interface bus 118 to a respective one of the MDIs 114. The second transmit module 120-5 may access packets stored in the PHY memory 106 and/or forward packets to a respective one of the MDIs 114 based on instructions received from the interface bus 118, the bus control module 132 and/or the bus RegEx module 134.

[0056] The memory control module 104 may perform as an arbiter to control access between the PHY modules 102 and the PHY memory 106. The memory control module 104 may permit one or more of the PHY modules 102 to have access to the PHY memory 106 and prevent one or more of the PHY modules 102 from having access to the PHY memory 106. The memory control module 104 determines access times for each of the PHY modules 102 and permits access to the PHY memory 106 accordingly.

The memory control module 104 may permit a first one of the PHY modules 102 to have access to the PHY memory 106 while a second one of the PHY modules 102 has access to the PHY memory 106. Alternatively, the memory control module 104 may prevent the first one of the PHY modules 102 from having access to the PHY memory 106 while the second one of the PHY modules 102 has access to the PHY memory 106.

[0057] The PHY memory 106 may include, for example, DDR3 SRAM and/or or other suitable memory, such as DRAM. The PHY memory 106 may have, for example, a 32 bit memory interface for transferring in parallel 32 bits of data. The PHY memory 106 may be external to the PHY device 100 and/or integrally formed on or as part of the PHY device 100. In one implementation, the PHY device 100 is an integrated circuit (IC) or system-in-a-package (SIP) and the PHY memory 106 is an IC separate from the PHY device 100. The PHY device 100 communicates with the PHY memory 106 via the memory control module 104 and/or a corresponding memory interface 148. The memory interface 148 may be connected between the memory control module 104 and the PHY memory 106.

[0058] In another implementation, the PHY device 100 is a first IC, the PHY memory 106 is a second IC, and the first IC and the second IC are formed as part of a SIP. In yet another implementation, the PHY device 100 is a first SIP, the PHY memory 106 is a second SIP, and the first SIP and the second SIP are integrally packaged using a package-on-package (POP) process. The second SIP may be stacked on the first SIP with a memory interface (e.g., the memory interface 148) between the SIPs to route signals between the first and second SIPs. The first SIP and the second SIP may be, for example, memory ball grid array (BGA) packages.

[0059] The PHY memory 106 may be used to buffer packets in case of congestion in one or more of the ingress modules 116 or egress modules 120. The PHY memory 106 may be used to store instructions, code, rules, tables, and/or packet data. The instructions, code, rules, and/or tables may be used by the central control module, the aggregation switch, and/or the modules 116-1, 120-1, 132, 134 when performing DPI and/or when controlling states of switches (e.g., switches in the fabric control module and/or the network interface 108). In one implementation, the instructions, code, rules, and/or tables are stored in the PHY memory 106 when, for example, there is not

available space in the bus memory 130. In another implementation, the instructions, code, rules, and/or tables are stored in the bus memory 130 when, for example, there is not available space in the PHY memory 106.

[0060] The bus memory 130 and the PHY memory 106 may be used to store: packets that are being inspected; copies of selected packets to be inspected; and/or packets that are to be forwarded, uplinked, and/or downlinked. The bus memory 130 and the PHY memory 106 may be used for packet buffering in case of temporary congestion at points in an access network (e.g., one of the access networks 10, 50). The bus memory 130 may be specific to a particular PHY module (e.g., the PHY module PHY_1), whereas the PHY memory 106 may be shared with each of the PHY modules 102. This minimizes the number of PHY memories used for a single PHY device 100.

[0061] In the example shown, the network interface 108 includes a first media access control (MAC) interface 140, a second MAC interface 142, a first quad-serial gigabit media independent interface (QSGMII) 144, and a second QSGMII 146. The MAC interfaces 140, 142 may be 10-gigabit Ethernet interfaces. The first and second MAC interfaces 140, 142 may each perform functions of a MAC and provide communication links to, for example, a fabric card via the access device 112. The first and second MAC interfaces 140 may have, for example, 10GE-KR interfaces for connecting the access device 112 over a back plane to enable low cost DPI via a modular access chassis (e.g., the access chassis 12 of FIG. 1). The first and second QSGMIIs 144, 146 may provide two parallel communication links to the access device 112.

[0062] During operation and as an example, each of the MDIs 114 may receive or transmit 1 gigabit of data per second (Gbps) while each of the interfaces 140, 142, 144, 146 may receive or transmit 10 Gbps. The MDIs 114 may be 1 Gbps Ethernet (GE) ports and the interfaces 140, 142, 144, 146 may have 10 GE ports. The PHY device 100 via the MDIs 114 and the network interface 108 may as a result provide dynamic binding of 1GE ports to 10GE interfaces 140, 142, 144, 146. This may include load balancing, interface redundancy, time division multiplexing scheduling for interleaved packets for an uplink, buffering of data in the PHY memory, and buffering data to the PHY memory to overcome or handle bursts of data. The load balancing may include transporting

equal amounts of data over two or more interfaces during the same time period. The interface redundancy may refer to the inclusion of two or more interfaces, where one or more of the interfaces are provided as a backup.

[0063] The PHY device 100, the PHY modules 102, and/or the first and second MAC interfaces 140, 142 may perform Institute of Electrical and Electronics Engineers (IEEE) 1588-2008 standard address network-based timing and synchronization. This may include the use of a precision time protocol (PTP) for synchronizing a clock of bus control modules (e.g., the bus control module 132) with a control module (e.g., the central control module 62) external to the PHY device 100. The PHY device 100, the PHY modules 102, and/or the first and second MAC interfaces 140, 142 may also provide MAC security (MACSec) support satisfying the IEEE 802.1AE-2006 security standard, which defines connectionless data confidentiality and integrity for media access independent protocols.

[0064] The PHY device 100 may also include a security cache module (SCM) 150. Packets and/or packet information may be transmitted between the parsing modules 116-2, 120-2 and/or the interface bus 118 and the security cache module 150. The security cache module 150 may store characters, data patterns, source addresses, destination addresses and/or other packet information to indicate a type of packet. The parsing modules 116-2, 120-2, of each of the PHY modules 102 may determine whether a packet is valid or invalid based on this packet information.

[0065] Referring now to FIGs. 1-4, the PHY devices 24, 44, 56, 100 and/or PHY modules 102 may perform as distributed sensors for detecting attacks along enforcement points on the perimeter of an access network. The central control modules 36, 62, when included, may collect information, such as packet information and attack information, from the distributed sensors. The attack information may include attack patterns, signatures, and/or other attack information disclosed herein. The central control modules 36, 62 may then apply rules and/or analyze the collected information to determine whether there is an attack and/or whether packets are valid and/or invalid. The type of the packets may be determined and the packets may be forwarded based on the result of this analysis. The results of this analysis may be provided from the central control modules 36, 62 to the distributed sensors for packet

forward determining purposes. The central control modules 36, 62 may instruct the distributed sensors of the packet types and how to handle packets of these types. This information may be collected, for example, in the PHY memory 106, in the bus memory 130, and/or in the security cache module 150 for future use.

[0066] Referring now also to FIG. 5, an ingress portion 170 of a PHY module (e.g., one of the PHY modules 102) providing multi-level security detection is shown. The ingress portion 170 includes an interframe finite state machine (FSM) module 172, which may be included in or separate from, for example, an ingress RegEx module (e.g., the ingress RegEx module 116-1). The ingress portion 170 may include the ingress (first) RegEx module 116-1, the ingress parsing module 116-2, the bus control module 132, the security cache module 150, and the bus (second) RegEx module 134.

[0067] The interframe FSM module 172 and the ingress RegEx module 116-1 provide a first level of security. The interframe FSM module 172 uses the ingress RegEx module 116-1 for pattern and signature lookup. The first level of security includes detecting zero-day RegEx attack patterns and signatures at a line rate (e.g., 1 Gbps in packets received by the interframe FSM module 172. The packets may be received from a MDI (e.g., MDI_0). The ingress RegEx module 116-1 is configured to monitor for predetermined patterns and signatures to detect packets prior to patches being installed in one of the central control modules 36, 62. The ingress RegEx module 116-1 may be programmable to allow a user to add or change signatures and patterns being monitored.

[0068] The ingress RegEx module 116-1 may perform RegEx parsing with anchors and wildcards. An anchor refers to an atomic zero-width assertion that causes a match to succeed or fail depending on a current position in a string of characters of a packet. An anchor does not cause the ingress RegEx module 116-1 to advance through the string or consume characters. A wildcard refers to a character that matches zero or more characters, which is used to efficiently detect a pattern or a signature.

[0069] The ingress RegEx module 116-1 may search headers and/or payloads of packets and sequential and/or non-sequential packets. The interframe FSM module 172 generates a first command signal 173 based on the comparisons and/or matches determined by the Ingress RegEx module 116-1.

[0070] The ingress parsing module 116-2 and the security cache module 150 provide a second level of security. The ingress parsing module 116-2 and/or the bus control module 132 may push off-loaded and validated data packets and/or indiscernible packets to the SCM 150. The ingress parsing module 116-2 and/or the security cache module 150 may then compare patterns of these packets to upcoming packets. As an example, the ingress parsing module 116-2 may not analyze a received packet having a pattern of an indiscernible packet type stored in the SCM 150. The ingress parsing module 116-2 may instead directly transfer the packet to a central control module for evaluation. This reduces RegEx processing time of the ingress parsing module 116-2.

[0071] The ingress parsing module 116-2 may perform packet parsing for off-loaded flows of data at a wire-speed (e.g., 1 Gbps). The ingress parsing module 116-2 (referred to as a hardware parser) may extract 5-tuple values from packets and scan the SCM 150 for matches. Values stored in the SCM 150 may be compared to the 5-tuple values. The 5-tuple values may be used to make up a transmission control protocol (TCP) or an Internet protocol (IP) and may include, for example, a source IP address, a destination IP address, a source port number, a destination port number, and a protocol ID. The SCM 150 may have interface specific entries for each of the interfaces 114. For example, a trusted interface may have permissions for the SCM 150 that are different than an untrusted interface. The comparisons performed by the ingress parsing module 116-2 may include a comparison of an identity of the interface associated with a received packet in determining whether certain values and/or 5-tuple values stored in the SCM 150 can be accessed in association with the interface. The ingress parsing module 116-2 generates a second command signal 175 based on the comparisons performed and the instructions stored in the SCM 150.

[0072] The bus control module 132 and/or the bus RegEx module 134 provide a third level of security. The bus control module 132 may inspect received data flows and either (i) forward the data flows, and/or (ii) tunnel and/or copy validated and/or unknown data flows (flows of indiscernible packets) to the central control module. As a result of packet inspection, the bus control module 132 may store additional patterns of previously unknown flows in the SCM 150 in order to instruct the ingress parsing

module 116-2 regarding actions to be taken upon receiving additional packets having the same patterns. The central control module may also or alternatively provide instructions to be stored in the SCM 150.

[0073] The bus memory 130 and/or the PHY memory 106 may store a hash table, which may be updated based on the provided instructions and recently learned data flows. The instructions may indicate actions (e.g., drop or forward) to be performed when the bus control module 132 detects a packet with a certain pattern. The RegEx modules 116-1, 120-1, 134 and the SCM 150 may be programmable to allow a user to add or change patterns, signatures and/or instructions stored. The instructions may be directed to determining a security level of the packets evaluated. The bus control module 132 may use the bus RegEx module 134 to detect patterns in received packets and then accordingly generate a third command signal 177. The bus control module 132 may continue to track non-validated flows of packets (flows of indiscernible packets) to detect an attack.

[0074] Although the multi-level security detection of FIG. 5 is shown for an ingress portion of a PHY module, the multi-level security detection may also be provided for an egress portion of the PHY module. As an example, the egress RegEx module 120-1 and the egress parsing module 120-2 may perform first and second levels of security as performed by the interframe FSM module 172, the ingress RegEx module 116-1, and the ingress parsing module 116-2. The bus control module 132 and the bus RegEx module 134 may provide the third level of security for egress purposes, as described above.

[0075] The command signals 173, 175, 177 for each of the security levels of the ingress portion are shown as drop-tunnel-local control module inspection-forward (DTLF) signals. The command signals are provided to a security level module 180. The security level module 180 determines a security level and generates a security level signal 182 based on the three command signals 173, 175, 177.

[0076] In the example, the security level module 180 includes an OR gate. Each of the command signals indicate a security level of the packet received as determined by a respective one of the security levels. The command signals may each indicate one of a first level and a second level. The first level indicates an invalid packet. The second

level indicates a valid packet. Each of the security levels may provide a command signal for each packet or for a series or selected group of packets.

[0077] As a first example, the command signals may be set to 1 when indicating that the packet is invalid or should be dropped. The command signals may be set to 0 when indicating that the packet is valid or should be forwarded. As a result, if any of the command signals indicate that the packet should be dropped, the packet is dropped. This is provided by an output of the security level module 180 or the OR gate.

[0078] As another example, four security levels may be used. The first level indicates an invalid or drop packet. The second level indicates a tunneling packet. The third level indicates a packet to be locally inspected by, for example, the bus control module 132 of the bus RegEx module 134. The fourth level indicates a valid or forwarding packet. In this implementation, the security level module 180 determines the lowest level indicated by the three command signals. The lowest level indicated may then be reported by the security level module 180 and used by, for example, the first transmit module 116-5 of FIG. 4 to determine whether to instruct the central control module to further inspect the packet. In one implementation, the lowest level may be reported when the lowest level is the second level or the third level and may not be reported when the lowest level is the first level or the fourth level. In another implementation, the lowest level is reported independent of the lowest level determined of the security level module 180.

[0079] Referring again to FIGs. 1-3, as one or more modules and/or devices of the PHY devices 24, 44, 56, 100 and/or PHY modules 102 may be programmable, a customized security platform may be provided that includes DPI at the edges of the access networks 10, 50.

[0080] In FIG. 6, a network interface 200 is shown. The network interface 200 may be used in the network interface 108 and/or in one of the PHY devices 24, 44, 56, 100 of FIGs. 1-3. The network interface 200 includes a first multiplexing module 202, a first QSGMII 204, a second multiplexing module 206, and a second QSGMII 208. The first and second multiplexing modules 202, 206 perform multiplexing and demultiplexing.

[0081] The first multiplexing module 202 may multiplex signals (e.g., 8 PHY module output signals) from a first set of PHY modules to multiplexed signals (e.g., 4

multiplexed signals) received by the first QSGMII 204. The second multiplexing module 206 may multiplex signals (e.g., 8 PHY device output signals) from a second set of PHY modules to multiplexed signals (e.g., 4 multiplexed signals) received by the second QSGMII 208. The first set of PHY modules may be the same or different than the second set of PHY modules. The first multiplexing module 202 may demultiplex output signals from the first QSGMII 204 to generate input signals received by the first set of PHY modules. The second multiplexing module 206 may demultiplex output signals from the second QSGMII 208 to generate input signals received by the second set of PHY modules. Outputs of the first and second QSGMII 204, 208 may be in communication with an aggregation switch and/or a central control module.

[0082] The network interface 200 allows ports of the PHY modules operating at a first speed to be connected to either the first QSGMII 204 or the second QSGMII 208, where each of the first QSGMII 204 and the second QSGMII 208 operate at a different speed than the MDIs. As an example, the first speed may be 1 Gbps and the second speed may be 10 Gbps. The multiplexing and demultiplexing performed by the multiplexing modules 202, 206 can eliminate a need for buffering of data signals at a network interface.

[0083] The access networks 10, 50 and the PHY devices 24, 44, 56, 100 described above may be operated using numerous methods, an example method is provided by the method of FIG. 7. In FIG. 7, a network access method including a security detection method is shown. Although the following tasks are primarily described with respect to the implementations of FIGs. 1-5, the tasks may be easily modified to apply to other implementations of the present disclosure. The tasks may be iteratively performed and/or performed in a different order. The method may begin at 300. Although the following tasks 302-322 are ingress tasks, the tasks may be performed similarly in reverse when performing egress tasks, such as the egress tasks performed by the egress modules 120. Also, although the following tasks are described with respect to a single packet, the tasks may be performed for multiple packets and/or a selected group of packets. The packets may be a sequential series of packets or non-sequential series of packets.

[0084] At 302, the ingress RegEx module 116-1 receives a packet from the MDI_0. The packet may be received from a network device (e.g., one of the network devices 18) that is in communication with the PHY module PHY_1 via the network 14. The ingress RegEx module 116-1 may perform an initial inspection of the packet to quickly determine whether to drop or forward the packet. The ingress RegEx module 116-1 may generate the first command signal and/or a first packet information signal based on results of the initial inspection. The first command signal may indicate a first estimate of the security level of the packet. The first estimate may be one of the four above-described security levels. The first packet information signal may include packet information as described above and/or indicate whether the interface bus 118 and/or bus control module 132 should inspect the packet. The packet information may include source and destination addresses, a protocol ID, packet length, a packet descriptor, etc. The initial inspection may include dropping or forwarding the packet. The packet when forwarded is provided to the ingress parsing module 116-2.

[0085] At 304, the ingress parsing module 116-2 may perform a second packet inspection based on information stored in the security cache module 150, the first command signal, and/or the first packet information signal and generate a second command signal. The second packet inspection may include dropping or forwarding the packet. The packet when forwarded may be provided to the first receive module 116-3 and/or to the interface bus 118. The ingress parsing module 116-2 may generate the second command signal and/or a second packet information signal based on results of the second packet inspection. The second command signal may indicate a second estimate of the security level of the packet. The second estimate may be one of the four above-described security levels and may be based on the first estimate. The second packet information signal may include packet information as described above and/or indicate whether the interface bus 118 and/or bus control module 132 should inspect the packet.

[0086] At 305, the RegEx module 116-1 determines whether the packet has an unsecure pattern and/or belongs to a secure data flow (e.g., has a corresponding "allow" entry in a table of the SCM 150). If the packet does not have an unsecure pattern and/or the packet belongs to a secure data flow, then localized inspection of

the packet is skipped and task 314 can be performed to have the packet safely forwarded. Localized inspection may be performed when the packet belongs to an unkown data flow and/or set by the RegEx module 116-1 and/or the SCM 150 to be further inspected. If the packet: has an unsecure (or dangerous) pattern; a corresponding SCM entry of the packet indicates that the packet is unsafe; and/or does not belong to a secure data flow, task 306 may be performed to have the packet tunneled to a central control module or dropped.

[0087] At 306, the first receive module 116-3 may store the packet and other information in the bus memory 130 and/or the PHY memory 106. The other information may include the packet descriptor, the first and second command signals and/or the first and second packet information signals.

[0088] At 308, the interface bus 118 performs a third inspection of the packet based on the first command signal, the second command signal, the first packet information signal, and/or the second packet information signal. The bus control module 132 and/or the bus RegEx module 134 may perform the third packet inspection. The third packet inspection may be performed using one or more TCAMs. The bus control module 132 may generate a third command signal and a third packet information signal based on results of the third inspection of the packet.

[0089] The third command signal may indicate a third estimate of the security level of the packet. The third estimate may be one of the four above-described security levels and may be based on the first estimate and/or the second estimate. As an alternative or in addition to generating the third estimate, the security level module 180 may generate the security level signal. The security level signal may be generated based on the first command signal, the second command signal, and the third command signal. The third packet information signal may include packet information as described above and/or indicate whether the central control module 36 or 62 should inspect the packet. The central control module 36, 62 may be instructed to inspect the packet when the interface bus 118 and/or the bus control module 132 is unable to determine whether to: drop the packet; or forward the packet from the PHY module PHY_1 (first PHY module) to another (second) PHY module (e.g., PHY $module_m$) or to a network device separate from the PHY device 100.

[0090] The inspections performed at 302, 304, and 308 may be performed periodically, randomly, subsequent to receiving a predetermined number of packets, subsequent to receiving a predetermined number of bytes, subsequent to receiving a predetermined number of valid and/or invalid packets, and/or at predetermined time intervals. One or more of the inspections described at 302, 304, and 308 may be performed and the others may not be performed. At each of tasks 302, 304, and 308 some or all of the packets received may be inspected. Also, packets inspected at one of 302, 304 and 308 may not be inspected at one or more of the other one of tasks 302, 304, 308.

[0091] At 310, the packet may be stored in the receive FIFO module 116-4 when forwarded to the central control module 36, 62, the second PHY device and/or the network device separate from the PHY device 100. At 312, the packet and other information may then be provided to the first transmit module 116-5. The other information may include, for example, the first, second, and/or third command signals, the security level signal, and/or other packet information described above. At 314, the first transmit module 116-5 determines whether the packet is to be forwarded to the second PHY module and/or to the network device separate from the PHY device 100. This determination may be based on the third command signal, the security level signal, and/or other information provided at 312. Task 316 may be performed when the packet is forwarded, otherwise task 315 may be performed.

[0092] A packet may be forwarded at 316 as described below and sent to the central control module for further inspection, as described with respect to task 322. When the packet is both forwarded at 316 and inspected at 322, the packet may be duplicated as to provide the packet to multiple destinations (e.g., the original destination and the central control module).

[0093] At 315, the first transmit module 116-5 determines whether the packet is to be further inspected by the central control module 36, 62. This determination may be based on the third command signal, the security level signal and/or other information provided at 312. Task 322 may be performed when the packet is to be further inspected, otherwise task 330 may be performed.

[0094] At 316, the packet may be forwarded from the first PHY module PHY_1 to an expected and/or originally selected destination. Ingress packets may be forwarded, for example, from the network 14, to the access device 112, one of the aggregation switches 26, 38, one of the fabric cards 20, 32, and/or the central network device 60. Egress packets may be forwarded, for example, from the access device 112, one of the aggregation switches 26, 38, one of the fabric cards 20, 32, and/or the central network device 60 to the network 14. The method may end at 320.

[0095] At 322, the packet may be tunneled to the central control module 36, 62 via the network interface 108. A MAC header with a MAC address of the PHY device 100 may be added to the packet (first packet) to form a second packet. The second packet is forwarded to the central control module 36, 62 via the network interface 108. At 324, the central control module 36, 62 may perform a fourth packet inspection of the packet. The central control module 36, 62 may perform an inspection periodically, randomly, subsequent to receiving a predetermined number of packets, subsequent to receiving a predetermined number of bytes, subsequent to receiving a predetermined number of valid and/or invalid packets, and/or at predetermined time intervals. The packets may be forwarded to the central control module 36, 62 independent of the security level determined by the PHY device 100.

[0096] At 326, the central control module 36, 62 instructs the first PHY module PHY_1 to drop and/or not to forward packets similar to the first packet. The method may end at 320 subsequent to performing task 326. Task 330 is performed when the packet is dropped, otherwise task 316 is performed.

[0097] At 330, the packet is deleted from the bus memory 130, the PHY memory 106 and/or other memory, module and/or device of the PHY device 100. This may include deleting the packet from one or more PHY modules and corresponding memories, modules, and devices. The method may end at 320 subsequent to task 330.

[0098] The above-described tasks are meant to be illustrative examples; the tasks may be performed sequentially, synchronously, simultaneously, continuously, during overlapping time periods or in a different order depending upon the application. Also, any of the tasks may not be performed or skipped depending on the implementation and/or sequence of events.

[0099] In addition to the above-described features, the implementations disclosed herein provide packet inspection at an edge of an access network that is performed via multiple PHY modules. This allows inspection of packets to be distributed to multiple PHY modules and to be performed as the packets are received and at rates at which the packets are received. This off-loads inspection processing from a central control module to multiple devices and/or modules within multiple PHY devices.

[00100] The foregoing description is merely illustrative in nature and is in no way intended to limit the disclosure, its application, or uses. The broad teachings of the disclosure can be implemented in a variety of forms. Therefore, while this disclosure includes particular examples, the true scope of the disclosure should not be so limited since other modifications will become apparent upon a study of the drawings, the specification, and the following claims. For purposes of clarity, the same reference numbers will be used in the drawings to identify similar elements. As used herein, the phrase at least one of A, B, and C should be construed to mean a logical (A or B or C), using a non-exclusive logical OR. It should be understood that one or more steps within a method may be executed in different order (or concurrently) without altering the principles of the present disclosure.

[00101] Although the terms first, second, third, etc. may be used herein to describe various devices, modules, signals, elements, and/or components, these items should not be limited by these terms. These terms may be only used to distinguish one item from another item. Terms such as “first,” “second,” and other numerical terms when used herein do not imply a sequence or order unless clearly indicated by the context. Thus, a first item discussed below could be termed a second item without departing from the teachings of the example implementations.

[00102] In addition, in the following description various variable labels and values are disclosed. The variable labels and values are provided as examples only. The variable labels are arbitrarily provided and may each be used to identify or refer to different items. For example, the variable label n may be used to refer to a number of modules or to a number of devices. The values are also arbitrarily provided and may vary per application.

[0100] As used herein, the term module may refer to, be part of, or include an Application Specific Integrated Circuit (ASIC); an electronic circuit; a combinational logic circuit; a field programmable gate array (FPGA); a processor (shared, dedicated, or group) that executes code; other suitable hardware components that provide the described functionality; or a combination of some or all of the above, such as in a system-on-chip. The term module may include memory (shared, dedicated, or group) that stores code executed by the processor.

[0101] The term code, as used above, may include software, firmware, and/or microcode, and may refer to programs, routines, functions, classes, and/or objects. The term shared, as used above, means that some or all code from multiple modules may be executed using a single (shared) processor. In addition, some or all code from multiple modules may be stored by a single (shared) memory. The term group, as used above, means that some or all code from a single module may be executed using a group of processors. In addition, some or all code from a single module may be stored using a group of memories.

[0102] The apparatuses and methods described herein may be implemented by one or more computer programs executed by one or more processors. The computer programs include processor-executable instructions that are stored on a non-transitory tangible computer readable medium. The computer programs may also include stored data. Non-limiting examples of the non-transitory tangible computer readable medium are nonvolatile memory, magnetic storage, and optical storage.

CLAIMS

What is claimed is:

1. A physical layer device comprising:

memory;

a memory control module configured to control access to the memory;

a physical layer module configured to store packets in the memory via the memory control module, the physical layer module comprising

at least one interface configured to receive the packets from a network device via a network, and

an interface bus comprising at least one of a control module and a regular expression module, wherein the at least one of the control module and the regular expression module is configured to inspect the packets to determine a security level of the packets; and

a network interface configured to, based on the security level, provide the packets to a device separate from the physical layer device.

2. The physical layer device of claim 1, wherein the memory comprises a double data rate memory and is accessible via a memory interface connected between the physical layer module and the memory.

3. The physical layer device of claim 1, wherein:

the physical layer device is implemented in a first system-in-a-package;

the memory is implemented in a second system-in-a-package; and

the first system-in-a-package and the second system-in-a-package are stacked.

4. The physical layer device of claim 1, wherein the at least one of the control module and the regular expression module is configured to determine the security level of each of the packets to be one of:

valid;

a packet to be further inspected via the at least one of the control module and the regular expression module;

a packet to be tunneled to a central control module for further inspection, wherein the central control module is separate from the physical layer device; and

invalid.

5. The physical layer device of claim 4, wherein:

each of the packets having a security level of valid is forwarded from the physical layer device to the device separate from the physical layer module; and

each of the packets have a security level of invalid is dropped.

6. The physical layer device of claim 1, wherein:

the device separate from the physical layer device is an aggregation switch of a fabric card; and

the physical layer module is implemented in a line card and is in communication with the fabric card.

7. The physical layer device of claim 1, wherein:

the network interface is configured to provide selected ones of the packets to a central control module;

the central control module is separate from the physical layer device; and

the network interface is configured to forward packets other than the selected ones of the packets based on the inspection of the selected ones of the packets performed by the central control module.

8. The physical layer device of claim 1, further comprising a ternary content addressable memory, wherein the at least one of the control module and the regular expression module are configured to inspect the packets to determine the security level of the packets using the ternary content addressable memory.

9. The physical layer device of claim 1, wherein:

the memory is a first memory;

the interface bus comprises a second memory;

the at least one of the control module and the regular expression module is configured to determine whether to store the packets and corresponding packet information in at least one of the first memory and the second memory; and

the packet information comprises the security level of the packets.

10. The physical layer device of claim 1, wherein:

the physical layer module is a first physical layer module;

the physical layer device further comprises a second physical layer module; and

the second physical layer module shares the memory with the first physical layer module.

11. The physical layer device of claim 1, further comprising:

a security cache module configured to store at least one of rules and tables; and

an ingress parsing module configured to inspect the packets based on the rules and tables.

12. The physical layer device of claim 11, wherein the control module is configured to inspect the packets to generate inspection results and update the security cache module based on the results.

13. The physical layer device of claim 1, wherein the physical layer module further comprises:

a first module configured to inspect the packets to generate a first command signal;

a second module configured to inspect the packets to generate a second command signal,

wherein the at least one of the control module and the regular expression module is configured to inspect the packets and generate a third command signal; and

a security level module configured to generate a security level signal based on the first command signal, the second command signal, and the third command signal,

wherein the network interface, based on the security level signal, provides the packets to the device separate from the physical layer device.

14. The physical layer device of claim 1, wherein:

the physical layer module comprises a plurality of modules;

each of the plurality of modules is configured to inspect the packets and generate a plurality of security level estimates;

a security level module configured to generate a security level signal based on the plurality of security level estimates; and

based on the security level signal, the network interface is configured to provide the packets to the device separate from the physical layer device.

15. The physical layer device of claim 1, wherein:

the network interface is configured to provide selected ones of the packets to a central control module for inspection;

the central control module is separate from the physical layer device; and

the physical layer module is configured to receive an instruction signal from the central control module based on the inspection performed at the central control module and forward packets other than the selected ones of the packets based on the instruction signal.

16. An access chassis comprising:

a plurality of line cards configured to receive the packets from the network device and transmit the packets to the device separate from the physical layer device, wherein a first line card of the plurality of line cards comprises the physical layer device of claim 1; and

at least one fabric card configured to provide switch connections between the first line card and a second line card of the plurality of line cards and forward the packets from the first line card to the second line card.

17. The access chassis of claim 16, wherein:

the at least one fabric card comprises a central control module;

one of an ingress module and an egress module of the physical layer module is configured to determine whether selected ones of the packets are to be inspected by the central control module; and

the central control module is configured to inspect the selected ones of the packets based on the determination of whether the selected ones of the packets are to be inspected by the central control module.

18. The access chassis of claim 17, wherein:

the central control module is configured to generate an instruction signal indicating whether to drop or forward packets having a similar format as the selected ones of the packets; and

based on the instruction signal, the physical layer device is configured to drop or forward the packets having a similar format as the selected ones of the packets.

19. A method comprising:

receiving packets from a network device via a network at an interface of a physical layer module;

transferring the packets from a physical layer device to a memory control module to store the packets in a memory, wherein the physical layer device comprises the physical layer module, and wherein the physical layer module comprises an interface bus;

inspecting the packets to determine a security level of the packets via at least one of a control module and a regular expression module, wherein the interface bus comprises the at least one of the control module and the regular expression module; and

based on the security level, provide the packets via a physical layer interface to a device separate from the physical layer device.

20. The method of claim 19, further comprising:

inspecting the packets to generate a first command signal via a first module;

inspecting the packets to generate a second command signal via a second module;

inspecting the packets via the at least one of the control module and the regular expression module to generate a third command signal;

generating a security level signal based on the first command signal, the second command signal, and the third command signal; and

based on the security level signal, providing the packets to the device separate from the physical layer device.

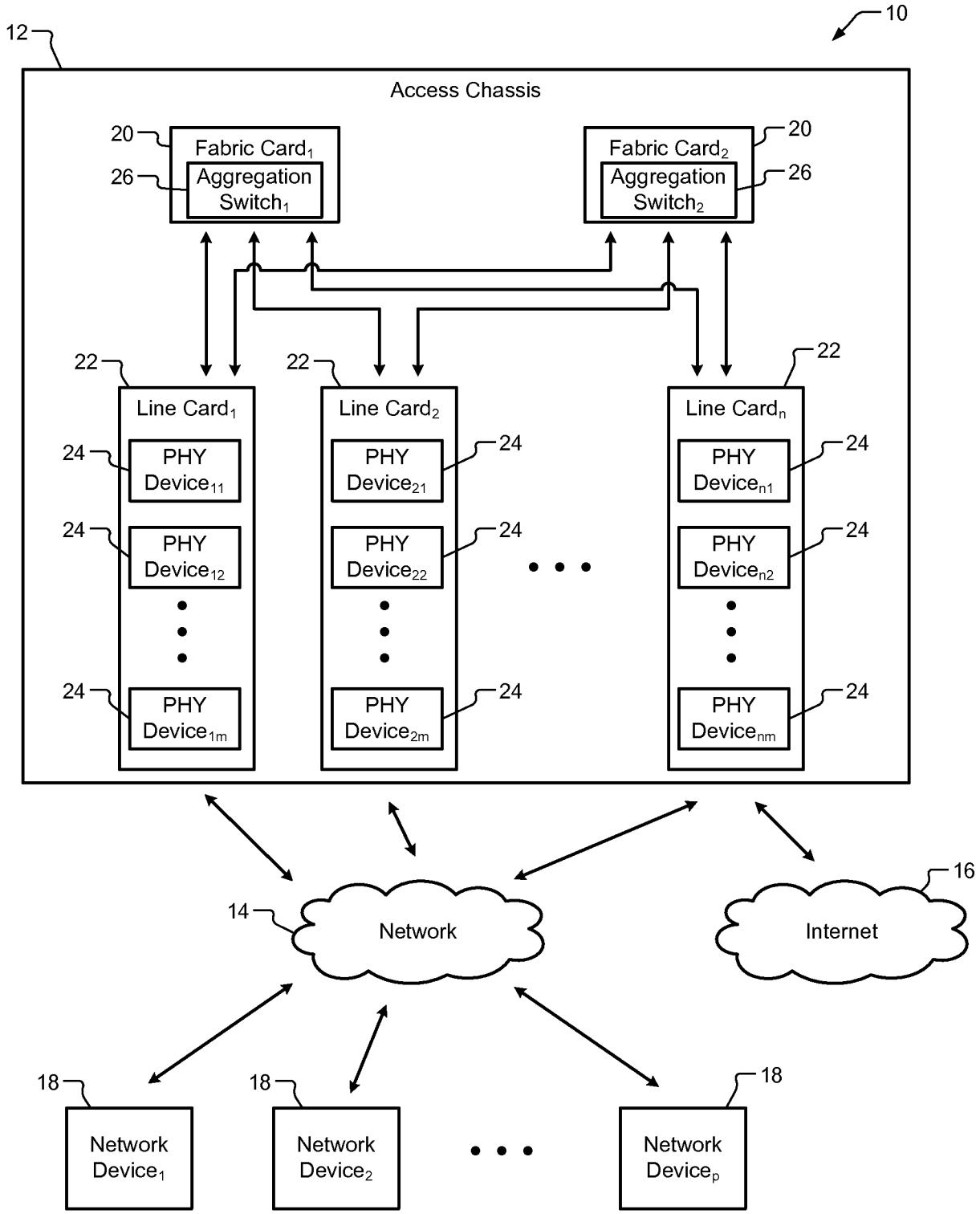
10
12
Access Chassis
20
Fabric Card1
26
Aggregation Switch1
Fabric Card2
Aggregation Switch2
22
Line Card1
Line Card2
Line Cardn
24
PHY Device11
PHY Device12
PHY Device1m
PHY Device21
PHY Device22
PHY Device2m
PHY Devicen1
PHY Devicen2
PHY Devicenm
14
Network
16
Internet
18
Network Device1
Network Device2
Network Devicep

FIG. 1

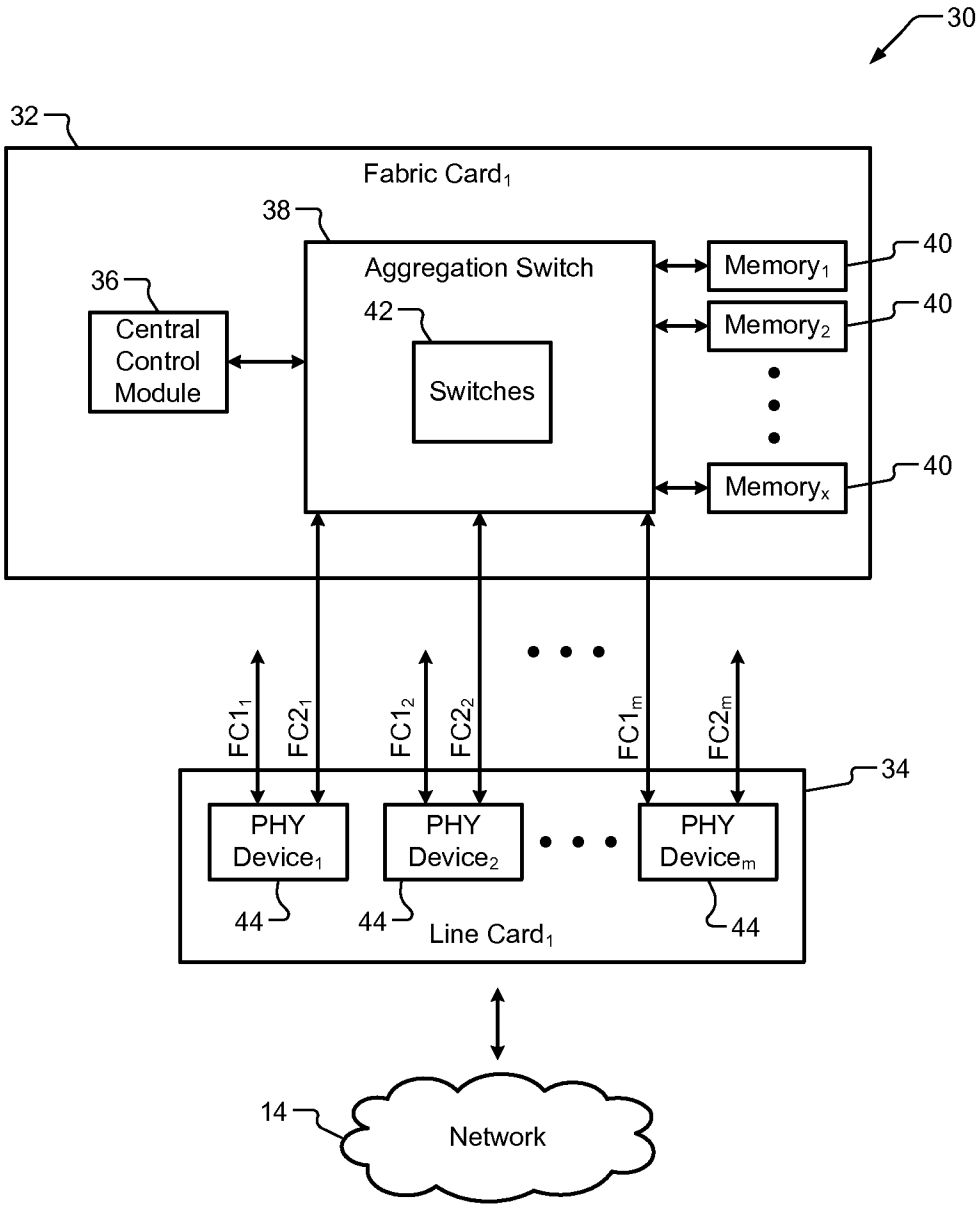
30
32
Fabric Card1
38
Aggregation Switch
36
Central Control Module
42
Switches
Memory1
Memory2
Memoryx
40
40
40
FC11
FC21
FC12
FC22
FC1m
FC2m
34
PHY Device1
PHY Device2
PHY Devicem
44
44
44
Line Card1
14
Network

FIG. 2

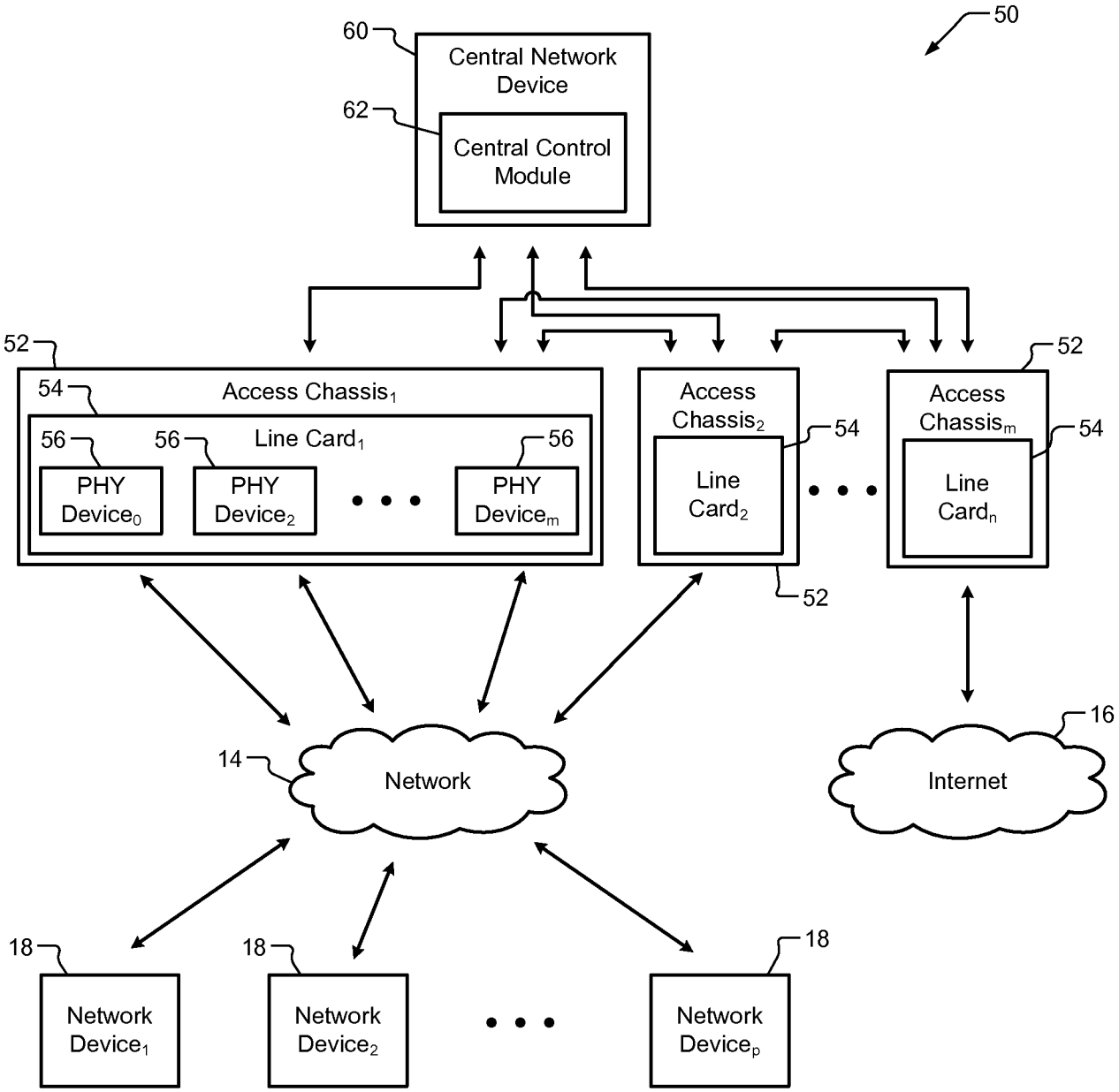
50
60
Central Network Device
62
Central Control Module
52
54
Access Chassis1
56
Line Card1
PHY Device0
PHY Device2
PHY Devicem
Access Chassis2
Line Card2
Access Chassism
Line Cardn
14
Network
16
Internet
18
Network Device1
Network Device2
Network Devicep

FIG. 3

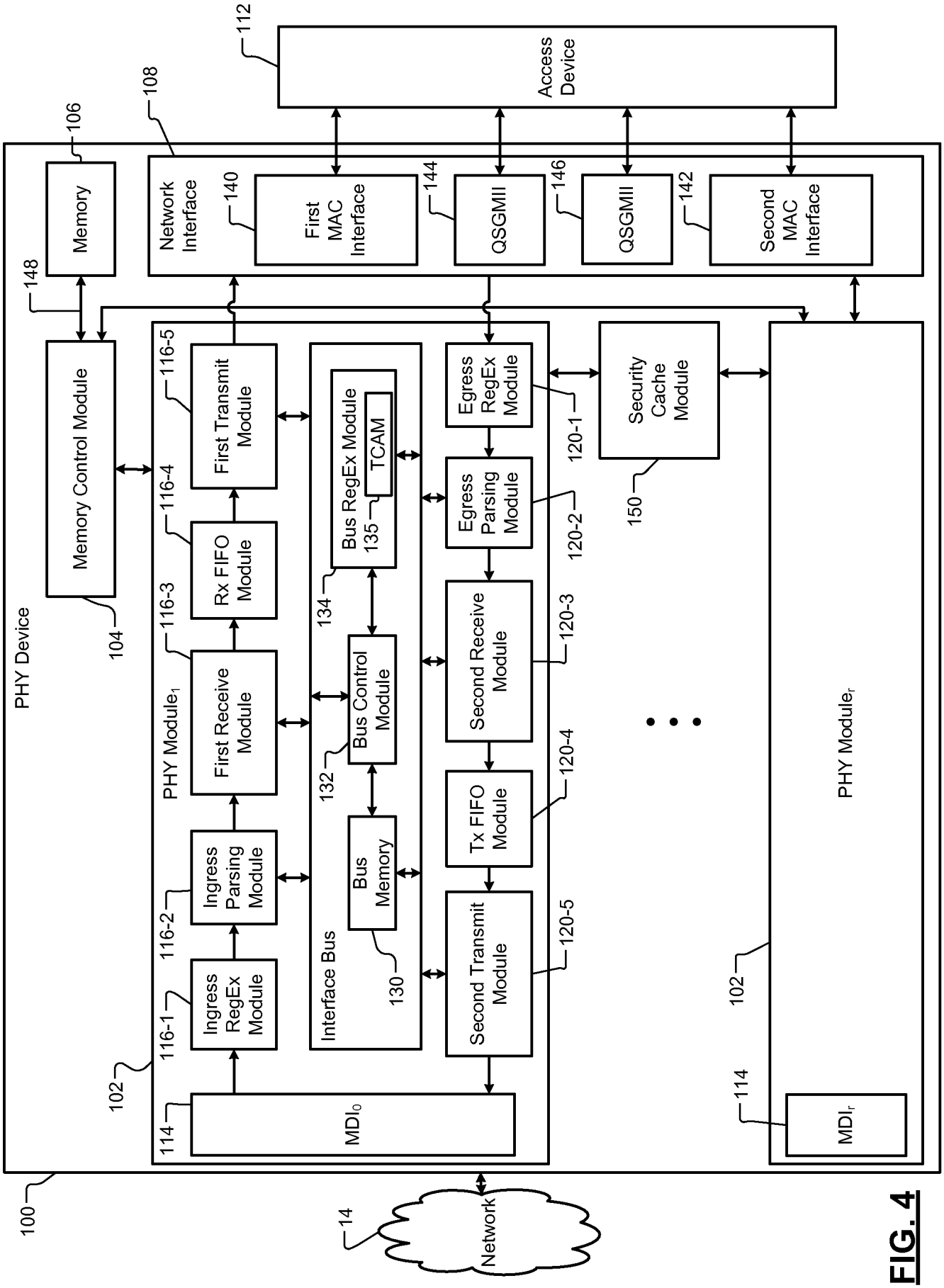
Access Device
112
108
106
Memory
Network Interface
140
First MAC Interface
144
QSGMII
146
QSGMII
142
Second MAC Interface
148
Memory Control Module
104
PHY Device
116-5
First Transmit Module
116-4
Rx FIFO Module
116-3
First Receive Module
PHY Module1
116-2
Ingress Parsing Module
116-1
Ingress RegEx Module
102
114
MDI0
Bus RegEx Module
TCAM
135
134
Bus Control Module
132
Bus Memory
130
Interface Bus
Egress RegEx Module
120-1
Egress Parsing Module
120-2
Second Receive Module
120-3
Tx FIFO Module
120-4
Second Transmit Module
120-5
Security Cache Module
150
PHY Modulen
102
114
MDIn
100
14
Network

FIG. 4

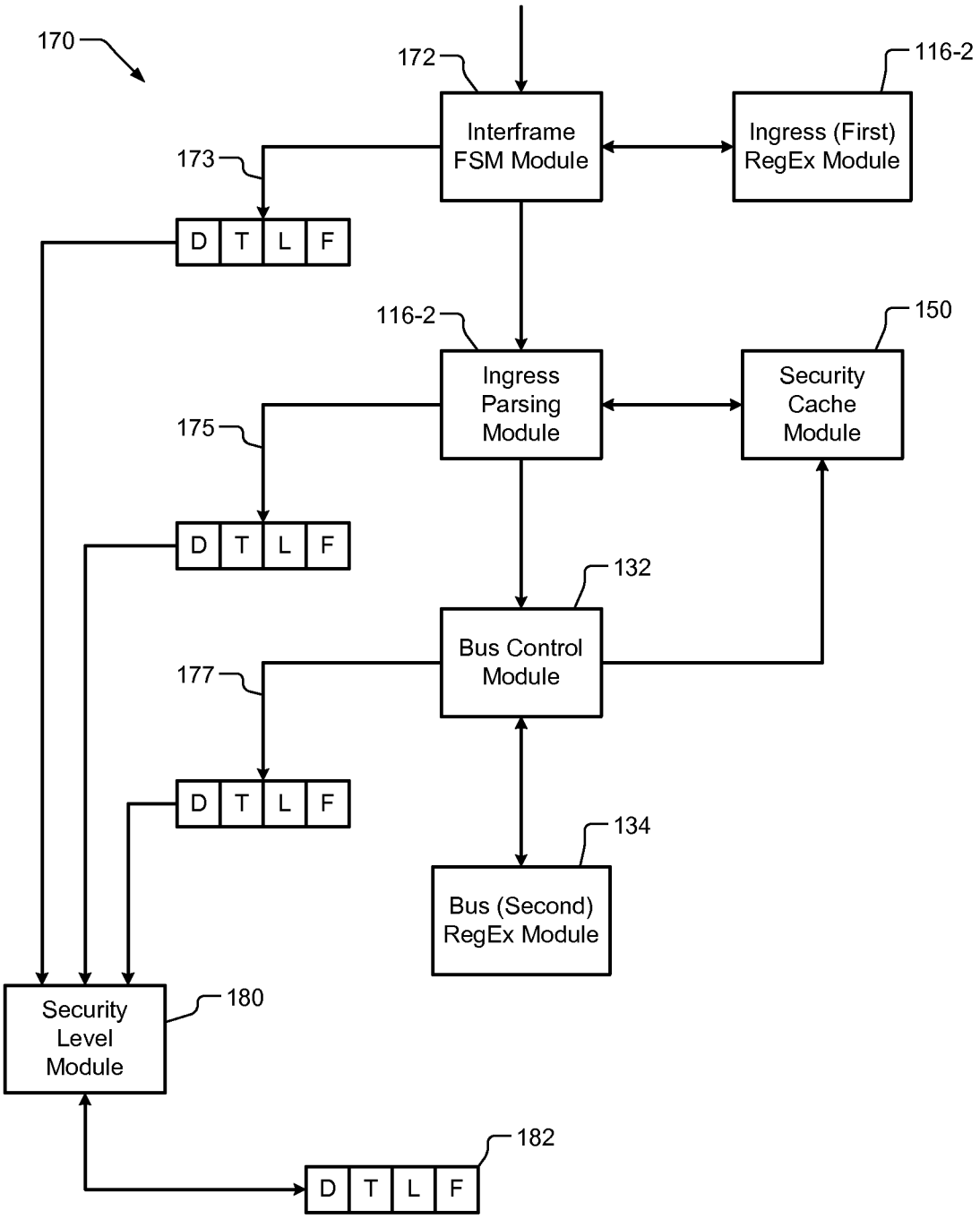
170
172
116-2
Interframe FSM Module
Ingress (First) RegEx Module
173
D T L F
116-2
150
Ingress Parsing Module
Security Cache Module
175
D T L F
132
Bus Control Module
177
D T L F
134
Bus (Second) RegEx Module
Security Level Module
180
182
D T L F

FIG. 5

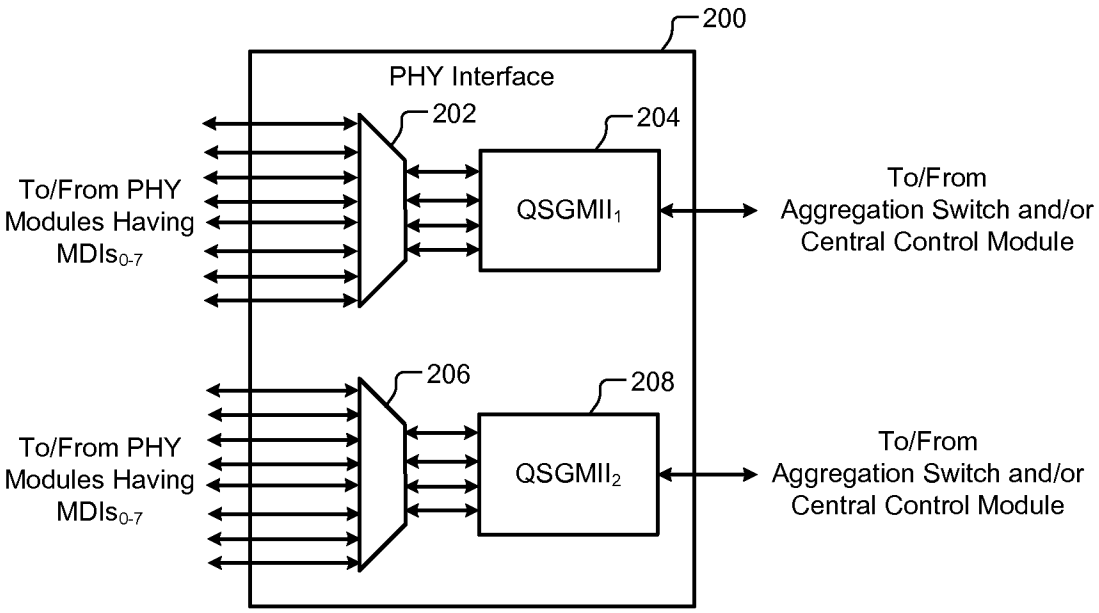
200
PHY Interface
202
204
To/From PHY Modules Having MDIs0-7
QSGMII1
To/From Aggregation Switch and/or Central Control Module
206
208
To/From PHY Modules Having MDIs0-7
QSGMII2
To/From Aggregation Switch and/or Central Control Module

FIG. 6

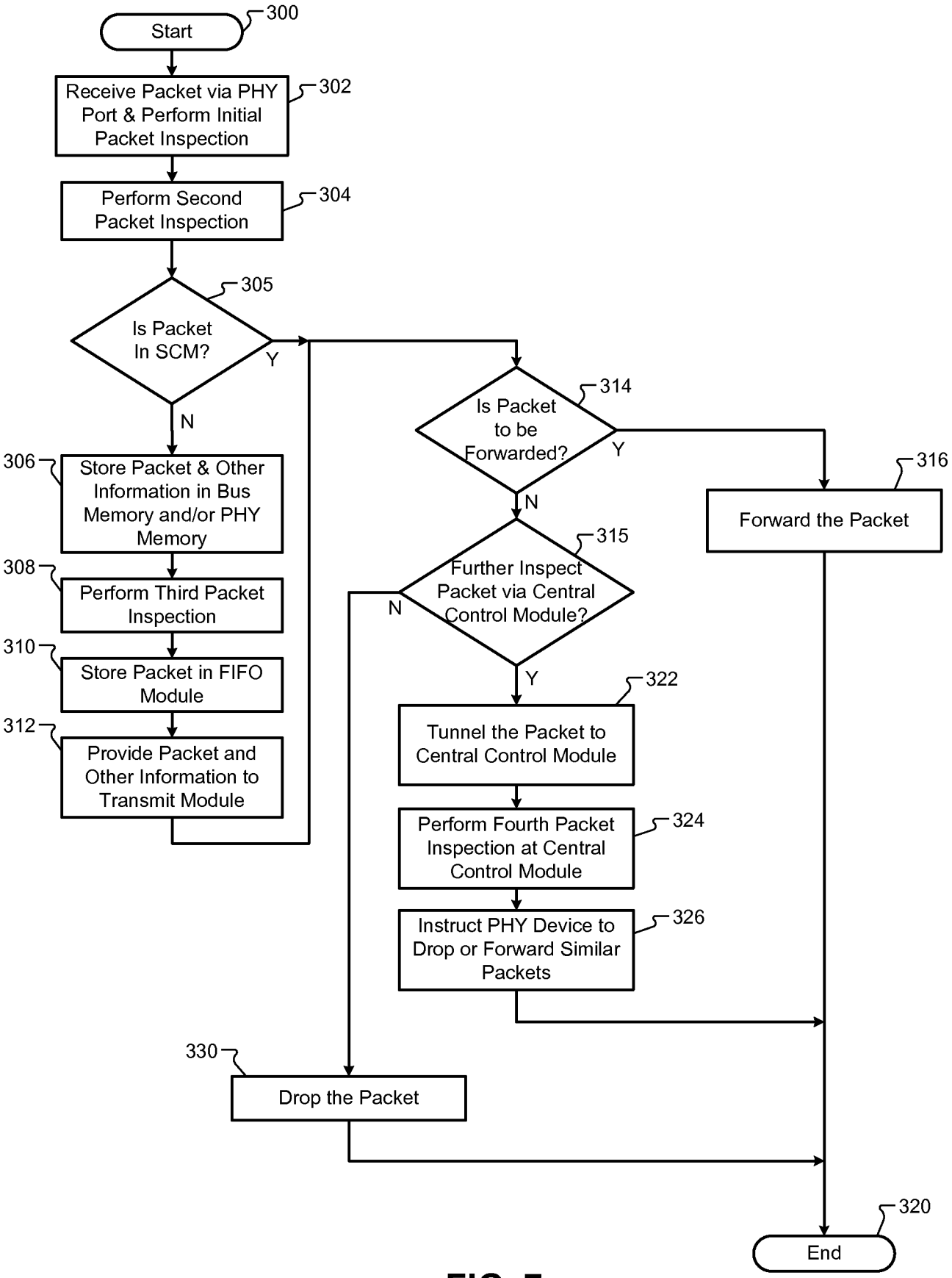
Start
300
Receive Packet via PHY Port & Perform Initial Packet Inspection
302
Perform Second Packet Inspection
304
Is Packet In SCM?
305
Y
N
306
Store Packet & Other Information in Bus Memory and/or PHY Memory
308
Perform Third Packet Inspection
310
Store Packet in FIFO Module
312
Provide Packet and Other Information to Transmit Module
Is Packet to be Forwarded?
314
Y
N
Forward the Packet
316
Further Inspect Packet via Central Control Module?
315
N
Y
Tunnel the Packet to Central Control Module
322
Perform Fourth Packet Inspection at Central Control Module
324
Instruct PHY Device to Drop or Forward Similar Packets
326
330
Drop the Packet
End
320

FIG. 7

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2012/050373

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04L12/28 H04L29/06
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.
A	US 2011/035580 A1 (WANG DAVID WEI [US] ET AL) 10 February 2011 (2011-02-10) abstract page 1, paragraph 1 - page 3, paragraph 32 page 4, paragraph 39 page 6, paragraph 61 - paragraph 64; claims 1-20; figures 1-3 -----	1-20
A	US 2007/157306 A1 (ELROD CRAIG T [US] ET AL) 5 July 2007 (2007-07-05) the whole document -----	1-20
A	US 2006/206936 A1 (LIANG YUNG-CHANG [US] ET AL) 14 September 2006 (2006-09-14) the whole document -----	1-20
A	US 2007/261112 A1 (TODD JOHN [CA] ET AL) 8 November 2007 (2007-11-08) the whole document -----	1-20

☐ 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	Date of mailing of the international search report
10 December 2012	17/12/2012

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	Jimenez Hernandez, P

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/US2012/050373

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2011035580 A1	10-02-2011	NONE	
US 2007157306 A1	05-07-2007	US 2007157306 A1	05-07-2007
		US 2012311664 A1	06-12-2012
US 2006206936 A1	14-09-2006	US 2006206936 A1	14-09-2006
		WO 2006098900 A2	21-09-2006
US 2007261112 A1	08-11-2007	NONE	