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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
14 November 2013 (14.11.2013)

WIPO | PCT

(10) International Publication Number
WO 2013/168207 A1

(51) International Patent Classification:
H04L 12/701 (2013.01) *H04L 12/66* (2006.01)

(21) International Application Number:
PCT/JP2012/007592

(22) International Filing Date:
27 November 2012 (27.11.2012)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
2012-107596 9 May 2012 (09.05.2012) JP

(71) Applicant *(for all designated States except US)*: **NEC CORPORATION** [JP/JP]; 7-1, Shiba 5-chome, Minato-ku, Tokyo, 1088001 (JP).

(72) Inventor; and
(71) Applicant *(for US only)*: **MIBU, Ryota** [JP/JP]; c/o NEC CORPORATION, 7-1, Shiba 5-chome, Minato-ku, Tokyo, 1088001 (JP).

(74) Agent: **KATO, Asamichi**; c/o A. Kato & Associates, 20-12, Shin-Yokohama 3-chome, Kohoku-ku, Yokohama-shi, Kanagawa, 2220033 (JP).

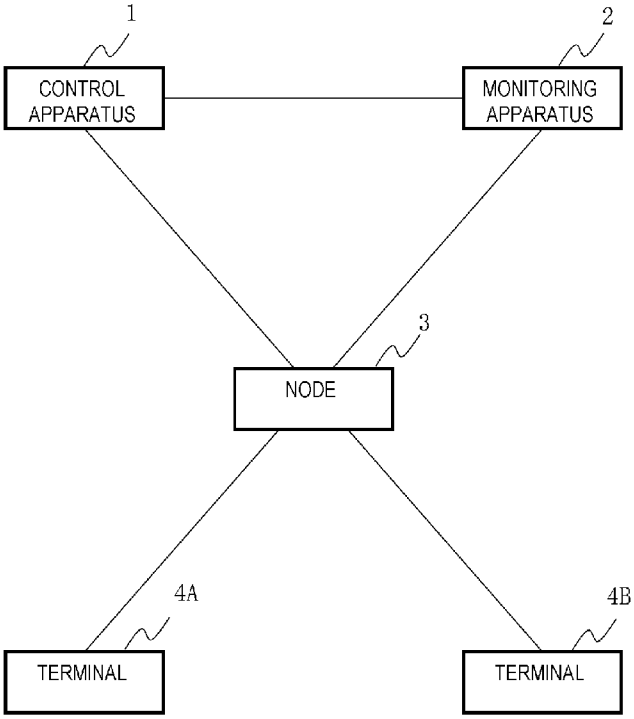
(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, 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, 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, ML, MR, NE, SN, TD, TG).

Published:

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

(54) **Title**: COMMUNICATION SYSTEM, COMMUNICATION METHOD, AND PROGRAM



(57) **Abstract**: The present invention provides a communication system, a communication method, and a program that are applicable to an OpenFlow-capable system or to a system similar to the system and that allow SPI or an equivalent function to be implemented. The communication system includes a control apparatus connected to a node via a network to control the node; and a monitoring apparatus that monitors a packet forwarded to the node arranged a between transmission source terminal and a transmission destination terminal of the packet. The control apparatus decides whether to or not to permit communication for a new packet, based on information collected by the monitoring apparatus and on a firewall rule. The control apparatus, in case of permitting communication, sets a forwarding rule, which includes a forwarding path from a transmission source terminal of a packet to a transmission destination terminal of the packet and a forwarding path of the packet from the transmission source terminal of the packet to the monitoring apparatus, in the node on the respective paths.

WO 2013/168207 A1

Description

Title of Invention: COMMUNICATION SYSTEM, COMMUNICATION METHOD, AND PROGRAM

Field

[0001] (CROSS-REFERENCE TO RELATED APPLICATIONS)

The present invention is based upon and claims the benefit of the priority of Japanese patent application No. 2012-107596, filed on May 09, 2012, the disclosure of which is incorporated herein in its entirety by reference thereto.

The present invention relates to a communication system, a communication method, and a program.

Background

[0002] The following describes a communication system that implements Stateful Packet Inspection (SPI) using the filtering function of OpenFlow. For OpenFlow, see Non Patent Literature 1 and Non Patent Literature 2.

[0003] As is well known, OpenFlow is a technology that identifies communications as end-to-end flows and performs the following on a per-flow basis.

. Path control

. Failure recovery

. Load balancing and

. Optimization

An OpenFlow switch, which functions as a forwarding node, operates according to a flow table (for example, 302 in FIG. 10) to which information is added, and whose contents are rewritten, according to an instruction from the OpenFlow controller.

[0004] In the flow table (302 in FIG. 10) of an OpenFlow switch, a set of the following three is defined for each flow as an entry (tuple).

. Rule (a rule against which the header information of a packet is matched)

. Action (an action that defines processing to be applied to a packet that matches the rule)

. Flow statistical information

This entry is called a "flow entry". The flow table in a node has flow entries each corresponding to a flow passing through the node.

[0005] The flow statistical information includes the following: number of active entries, number of packet lookups, and number of packest that match;

on a per flow basis, number of received packets, number of received bytes, and duration in which a flow is active;

on a per port basis, number of received packets, number of transmitted packets,

number of received bytes, number of transmitted bytes, number of receive drops, number of transmit drops, number of receive errors, number of transmit errors, number of receive frame alignment errors, number of receive overrun errors, number of receive Cyclic Redundancy Check (CRC) errors, and number of collisions.

[0006] The packet header (OpenFlow header) used on an OpenFlow network has the header format shown in FIG. 11.

. MAC DA (Media Access Control Destination Address) (Ethernet (registered trademark) transmission destination address: 48 bits),

. MAC SA (Media Access Control Source Address) (Ethernet (registered trademark) transmission source address: 48 bits),

. TPID (Type ID) (Ethernet (registered trademark) type: 16 bits),

. VLAN ID (Virtual Local Area Network ID) (16 bits),

. VLAN TYPE (16 bits),

. Ver (Version) (IP protocol version: 4 bits),

. IHL (Internet Header Length) (4 bits),

. Tos (Type of Services) (8 bits),

. Total Length (16bits: Size of whole packet in octet),

. Identification (16 bits),

. Flag/Flag Offset (16 bits),

. TTL (Time to Live: 8 bits),

. Protocol (Protocol: 8 bits) (Higher-level layer protocol: TCP (Transmission Control Protocol), UDP (User Datagram Protocol), ICMP (Internet Control Message Protocol), etc.),

. CheckSum (Header checksum: 16 bits),

. IP SA (Internet Protocol Source Address) (Transmission source IP address: for example, 32 bits),

. IP DA (Internet Protocol Destination Address) (Transmission destination IP address: for example, 32 bits),

. Source Port (TCP transmission source port: 16 bits),

. Destination Port (TCP transmission destination port: 16 bits),

. Sequence Number (Sequence number: 32 bits),

. Acknowledgement Number (Acknowledge number: 32 bits),

. Offset/Flags (Offset/Flag: 16 bits),

. Window Size (Window size: 16 bits),

. CheckSum (Checksum of data calculated by TCP: 16 bits), and

. Urgent Pointer (Urgent pointer: 16 bits).

The header is followed by the payload. Some of those header information items are used for comparison with a rule in a flow table.

[0007] On receipt of a packet, an OpenFlow switch searches the flow table (302 in FIG. 10) for an entry that matches the information in the OpenFlow header (see FIG. 11) of the received packet. That is, when a received packet is input, the OpenFlow switch searches the flow table in the OpenFlow switch to find a match between the header information of the packet and the rule. If a matching rule is found, the OpenFlow switch performs processing defined for an action corresponding to the rule (processing to be performed when the packet matches the rule).

[0008] An example of a rule included in a flow table includes a transmission destination (destination) IP address, a transmission source IP address, a transmission source port, and a destination port. An action to be performed in case this rule matches a packet is for example as follows. If a next OpenFlow switch to which the received packet is to be forwarded is specified, the received packet that matches the rule is forwarded to the OpenFlow switch specified in the action field. On the other hand, if a matching rule is not found as a result of searching the flow table, the OpenFlow switch forwards the received packet to the OpenFlow controller via the secure channel that is a link to the OpenFlow controller.

[0009] On receipt of the received packet from the OpenFlow switch, the OpenFlow controller uses the network topology information managed by the OpenFlow controller to determine a forwarding path of the received packet based on the transmission source/destination information included in the received packet and then performs flow setup.

[0010] Flow setup refers to the processing for setting up the flow tables in all OpenFlow switches on the determined forwarding path for implementing the determined forwarding path. Each of the OpenFlow switches adds a new flow entry, which includes a rule and an action that defines processing to be performed when a packet matches the rule, to the flow table thereof, based on the forwarding path information transferred to Each of the OpenFlow switches from the OpenFlow controller.

[0011] After flow setup is performed, the OpenFlow controller forwards the received packet, for example, to the OpenFlow switch that is located at the exit of the flow (OpenFlow switch connected to the transmission destination terminal) for transmitting the packet to the transmission destination terminal.

[0012] After that, the header information of a packet, which belongs to the same flow as that of the received packet described above, matches the rule in the flow table of each OpenFlow switch for which the flow setup has been performed. Therefore, the packet is forwarded via the OpenFlow switches on the forwarding path of the packet according to the flow tables (rule and action) that have been set up and is transmitted to the transmission destination terminal.

[0013] If a packet does not match a rule, as a result of the search by an OpenFlow switch in

the flow table thereof, that packet is a packet forwarded to the OpenFlow switch for the first time in a flow, in many cases. Such a packet is generically called a "first packet". Strictly speaking, in case a flow entry is deleted, a matching entry is sometimes not found for a packet that is not a packet forwarded for the first time. In such a case, a packet that is not a packet forwarded for the first time is also transferred to the OpenFlow controller.

[0014] The filtering function is implemented on an OpenFlow network such that the OpenFlow controller decides the permission of communication, based on a packet received from an OpenFlow switch and sets up only the permitted flows.

[0015] One method for deciding the permission/non-permission of communication on an OpenFlow network is that, with the OpenFlow header information, priority, and its communication permission/non-permission set in advance, the OpenFlow controller checks the permission of communication on a priority basis after packet-in (a packet is received).

[0016] An OpenFlow controller can acquire statistical information (for example, flow statistical information in the flow table) from an OpenFlow switch. The statistical information that can be acquired for each flow includes, for example, number of received packets, reception size, time-to-live, and so forth.

[0017] On the other hand, the Stateful Packet Inspection (SPI) technology is available that reads the data of a packet, which passes through a firewall, determines contents, and dynamically opens and closes a port, based on the contents. SPI reads the data of a packet that passes through a firewall, records the data in the communication log, references the communication log to determine whether the received packet is normal, and dynamically opens or closes a port. For SPI, see Patent Literature 1 and Patent Literature 2.

[0018] In general, the SPI processing in a firewall is implemented in such a way that SPI reads a packet that passes through the firewall, generates its communication status and stores it in a log and, when deciding whether to or not to pass a new packet, references the firewall rule and the communication status log (LINUX (registered trademark) Netfilter).

[0019] For use as the filtering condition, the connection state of a packet is set. The connection state of a packet is as follows.

. NEW (Newly connected packet)

. ESTABLISHED (continued packet)

. RELATED (related packet)

[0020] NEW indicates a communication state of a packet for which the ACK flag is not set or a connection state of a connection initiation packet such as an ICMP echo request.

[0021] ESTABLISHED indicates a communication state of a continued packet of an existing

connection for which the ACK flag is set.

[0022] RELATED indicates a communication state of a related packet related to an existing connection such as an ICMP error message. When indicating a packet whose connection state is none of NEW, ESTABLISHED, and RELATED, INVALID is set, for example.

[0023] In the SPI processing performed by a firewall, the above-described packet connection states are specified in advance in the firewall rule as the filtering condition. This filtering condition, as well as the communication status generated in the firewall, is used to decide whether to or not to pass a packet.

[0024] The information that is read from a packet differs according to the protocol. The following describes the information read from a packet with TCP and File Transfer Protocol (FTP) as an example. FTP is a file transfer protocol that uses UDP. The protocol such as TCP, UDP, or ICMP is set in the protocol field of the packet header.

[0025] In TCP or FTP, a session between a client and a server is started as follows. First, the client transmits a SYN packet (packet with the SYN flag on) to the server. In response to the SYN packet, the server transmits the SYN•ACK packet (packet with both SYN flag and the ACK flag on) to client the server to permit the client to carry out communication. Then, in response to the SYN•ACK packet, the client transmits the ACK packet to the server and starts a session with the server (ESTABLISHED). Therefore, when a client is a node that carries out communication for the first time, the client should transmit a SYN packet. In this case, if the client transmits a packet other than a SYN packet, the server determines that the packet is invalid. When the communication status is NEW, a packet other than the SYN packet is discarded.

[0026] When TCP is used, the packet information that is read during the SPI processing is as follows.

. Transmission source IP address (IP SA in FIG. 11),

. Transmission destination IP address (IP DA in FIG. 11),

. TCP transmission source port (Source Port in FIG. 11),

. TCP transmission destination port (Destination Port in FIG. 11), and

. TCP header flags (Flags in FIG. 11)

In FIG. 11, the 20-octet field, from the Source Port and Destination Port to CheckSum and Urgent Pointer, is the TCP header.

[0027] In the SPI processing, the control flags in the TCP header, such as SYN and ACK, are read from the packet and from the opposite-direction packet, whose transmission source and transmission destination are reversed, to confirm the establishment of the communication.

[0028] The SYN flag (1 bit) described above is set in the first connection-requesting packet

that is transmitted when a TCP connection is requested. The ACK flag (1 bit), when on, indicates that an effective acknowledgement number (ACK number) is included in the TCP header. The ACK number (32 bits), which is in the TCP response packet, corresponds to the sequence number of received data (incremented by one for each one byte of transmitted data) ("Position of received data + Sequence number + 1" is returned as the ACK number). When a packet with the SYN flag set is received, the ACK number is made to synchronize with the received sequence number. A packet with the SYN flag (SYN flag is on) indicates a communication status (NEW) in which a new communication is going to start. The packet is the first packet that is transmitted when the connection is not yet established.

[0029] After that, when a packet with the SYN flag and ACK flag (SYN ACK packet) is transmitted from the opposite direction and, in addition, a packet with the ACK flag is transmitted from the direction in which the first packet was transmitted, the communication is established (ESTABLISHED).

[0030] By keeping track of the communication status as described above, SPI performs an operation to release an established communication.

[0031] When FTP is used, SPI performs the following processing in addition to the processing performed when TCP is used. That is, SPI reads a TCP port number, which is used for data forwarding via FTP, from the payload of a packet belonging to the FTP control communication. SPI uses this port information to dynamically permit communication to a related port.

[0032] Patent Literature 1 discloses a packet passing control apparatus that reduces the SPI processing in the central processing unit. Patent Literature 2 discloses a gateway having a communication control apparatus that allows SPI to be applied to the communication from an out-of-site network client to an in-site network server. According to the technologies disclosed in Patent Literatures 1 and 2, the monitoring and control of communication required for the SPI processing is performed by one apparatus. In addition, the packets that are read include a packet for which communication is once permitted.

Citation List

Patent Literature

[0033] PTL 1: Japanese Patent Kokai Publication No. JP2007-221240A

PTL 2: Japanese Patent Kokai Publication No. JP2009-272659A

Non Patent Literature

[0034] NPL 1: Nick McKeown et al, "OpenFlow: Enabling Innovation in Campus Networks," ACM SIGCOMM Computer Communication Review-Volume 38, 2008, pp. 69-74

NPL 2: Openflow Switch Specification Version 1.0.0. (Wire Protocol 0x01),

December 31, 2009, [Searched on March 8, 2011], Internet <URL: http://www.openflow.org/documents/openflow-spec-v1.0.0.pdf>

Summary

Technical Problem

[0035] The following describes the analysis of related technologies.

[0036] The OpenFlow network disclosed and defined in Non Patent Literature 1 or Non Patent literature 2 is not configured to monitor packets after flow setup. This configuration makes it impossible to implement SPI. The following describes this problem.

[0037] The subsequent packets belonging to a flow, once permitted by the OpenFlow controller, are forwarded to a communication destination (terminal at a transmission destination) via only one or more OpenFlow switches on a path determined by the OpenFlow controller. This forwarding method makes it impossible for the OpenFlow controller to acquire usual conditions such as related communication or session termination. Therefore, SPI cannot be implemented.

[0038] The OpenFlow controller can acquire the statistical information from each OpenFlow switch. However, the OpenFlow controller can acquire only limited information as described above. The OpenFlow controller can acquire neither the flag information nor the related port information, included in the TCP header, for deciding the permission/non-permission of communication of related packets.

[0039] The following assumes and considers a system (example) in which a packet to be monitored is transmitted from an OpenFlow switch to the OpenFlow controller. In general, the communication band between an OpenFlow switch and the OpenFlow controller is narrow. Usually, one OpenFlow controller is connected to two or more OpenFlow switches. In the configuration in which all packets to be monitored are forwarded from the OpenFlow switches to the OpenFlow controller, congestion occurs in the OpenFlow controller. Therefore, the system configuration in this example (the configuration in which packets to be monitored are transmitted from OpenFlow switches to the OpenFlow controller) is not practical.

[0040] This means that SPI processing cannot be implemented in OpenFlow. That is, the configurations disclosed in Patent Literatures 1 and 2 cannot be installed in an OpenFlow-capable communication system.

[0041] In view of the foregoing, it is an object of the present invention to provide a communication system, a communication method, and a program that are applicable to an OpenFlow-capable system or a system similar to the system and that allow Stateful Packet Inspection (SPI) or an equivalent function to be implemented.

Solution to Problem

[0042] According to the present invention, there is provided a communication system comprising:

at least one node that forwards a packet in accordance with a forwarding rule set therein;

a transmission source terminal of the packet;

a transmission destination terminal of the packet;

a control apparatus that is connected to the node via a network and that controls the node; and

at least one monitoring apparatus that is connected to the node and to the control apparatus via networks, respectively, and that monitors a packet forwarded to the node arranged between the terminals, wherein

the control apparatus comprises:

communication permission decision means that decides whether to or not to permit communication for a packet transmitted from the node, based on information collected by the monitoring apparatus and on a firewall rule including a pre-defined filtering condition; and

forwarding rule setting means that, responsive to the decision to permit communication by communication permission decision means, sets a forwarding path of a packet from the transmission source terminal of the packet to the transmission destination terminal of the packet and a forwarding path of the packet from the transmission source terminal of the packet to the monitoring apparatus, in each node arranged on each of the forwarding paths, as the forwarding rule.

[0043] According to another aspect of the present invention, there is provided a control apparatus comprising:

communication permission decision means that decides whether to or not to permit communication for a packet forwarded from a node, based on information collected by at least one monitoring apparatus monitoring apparatus monitoring a packet forwarded to at least one node and on a firewall rule including a pre-defined filtering condition, the at least one node forwarding a packet in accordance with a forwarding rule set therein, the at least one node arranged between a transmission source terminal of the packet and a transmission destination terminal of the packet, and

forwarding rule setting means that, responsive to the decision to permit communication by communication permission decision means, sets a forwarding path of a packet from the transmission source terminal of the packet to the transmission destination terminal of the packet, and a forwarding path of the packet from the transmission source terminal of the packet to the monitoring apparatus, in each node on each of the forwarding paths, as the forwarding rule.

[0044] According to another aspect of the present invention, there is provided a monitoring

apparatus comprising:

packet analysis means that monitors a packet forwarded to at least one node arranged between a transmission source terminal of the packet and a transmission destination terminal of the packet and acquires a communication status; and

communication status holding means that holds the communication status acquired by the packet analysis means,

the monitoring apparatus transmitting the communication status to a control apparatus connected to the monitoring apparatus via a network,

the control apparatus deciding whether to or not to permit communication for a packet transmitted from the node, based on information collected by the monitoring apparatus and on a firewall rule including a pre-defined filtering condition,

the control apparatus, in case of the permission of communication being decided, setting a forwarding path of a packet from the transmission source terminal of the packet to the transmission destination terminal of the packet, and a forwarding path of the packet from the transmission source terminal of the packet to the monitoring apparatus, in each node on each of the forwarding paths, as a forwarding rule.

[0045] According to still another aspect of the present invention, there is provided a communication method comprising:

monitoring, by at least one monitoring apparatus, a packet forwarded to at least one node, the at least one node forwarding a packet in accordance with a forwarding rule, the at least one node arranged between a transmission source terminal of the packet and a transmission destination terminal of the packet,

upon reception of a packet forwarded from the node, deciding, by a control apparatus connected to the node, whether to or not to permit communication for the packet, based on information collected by the monitoring apparatus monitoring the packet and on a firewall rule including a pre-defined filtering condition; and

setting a forwarding path of a packet from the transmission source terminal of the packet to the transmission destination terminal of the packet, and a forwarding path of the packet from the transmission source terminal of the packet to the monitoring apparatus, in each node on each of the forwarding paths, as the forwarding rule, responsive to the decision of the permission of the communication.

[0046] According to still another aspect of the present invention, there is provided a node apparatus comprising:

a flow table that stores a rule including a forwarding rule, the node apparatus forwarding a packet in accordance with the forwarding rule; and

a communication processing unit that matches a received packet against the rule in the flow table,

the communication processing unit, in case a rule that matches the received packet is

not found in the flow table, forwarding the received packet to a control apparatus connected to the node apparatus, wherein the control apparatus decides whether to or not to permit communication for the received packet forwarded thereto from the node apparatus, based on information collected by a monitoring apparatus monitoring the packet and on a firewall rule including a pre-defined communication status specified as a filtering condition and the control apparatus, in case of the permission of communication being decided, sets a forwarding path of a packet from a transmission source terminal of the packet to a transmission destination terminal of the packet, and a forwarding path of the packet from the transmission source terminal of the packet to the monitoring apparatus, in each node on each of the forwarding paths, as the forwarding rule,

the communication processing unit receiving the forwarding rule from the control apparatus and setting the forwarding rule in the flow table, and

the communication processing unit forwarding a packet, which is received after the received packet and matches the forwarding rule set in the flow table, to the transmission destination terminal of the packet and to the monitoring apparatus.

[0047] According to still another aspect of the present invention, there is provided a program that causes a computer configuring a control apparatus connected to at least one node that forwards a packet in accordance with a forwarding rule, the program causing the computer to execute the processing of:

deciding whether to or not to permit communication for a packet transmitted from the node, based on information collected by at least one monitoring apparatus monitoring a packet forwarded to at least one node arranged between a transmission source terminal of the packet and a transmission destination terminal of the packet and on a firewall rule including a pre-defined filtering condition; and

setting a forwarding path of a packet from the transmission source terminal of the packet to the transmission destination terminal of the packet, and a forwarding path of the packet from the transmission source terminal of the packet to the monitoring apparatus, in each node on each of the forwarding paths, as the forwarding rule, responsive to the decision of the permission of the communication.

[0048] According to the present invention, there is provided a memory, a disk medium, a memory or disk unit in which the program described above is recorded.

Advantageous Effects of Invention

[0049] The communication system according to the present invention, applicable to an OpenFlow-capable system or to a system similar to the system, allows SPI or an equivalent function to be implemented.

Brief Description of Drawings

[0050] [fig.1]FIG. 1 is a diagram illustrating an example of the system configuration of a first exemplary embodiment of the present invention.
[fig.2]FIG. 2 is a diagram illustrating an example of the configuration of a control apparatus in the first exemplary embodiment of the present invention.
[fig.3]FIG. 3 is a diagram illustrating an example of the configuration of a monitoring apparatus in the first exemplary embodiment of the present invention.
[fig.4]FIG. 4 is a flowchart illustrating an example of the operation of the first exemplary embodiment of the present invention.
[fig.5]FIG. 5 is a diagram illustrating an example of the configuration of a control apparatus in a second exemplary embodiment of the present invention.
[fig.6]FIG. 6 is a diagram illustrating an example of the configuration of a monitoring apparatus in the second exemplary embodiment of the present invention.
[fig.7]FIG. 7 is a diagram illustrating an example of the configuration of a control apparatus in a third exemplary embodiment of the present invention.
[fig.8]FIG. 8 is a diagram illustrating an example of the configuration of a fifth exemplary embodiment of the present invention.
[fig.9]FIG. 9 is a diagram illustrating an example of the configuration of a seventh exemplary embodiment of the present invention.
[fig.10]FIG. 10 is a diagram illustrating an example of the configuration of a node apparatus in the first exemplary embodiment of the present invention.
[fig.11]FIG. 11 is a diagram showing the header information of an OpenFlow packet.

Description of Embodiments

[0051] Exemplary embodiments of the present invention are described in detail below with reference to the drawings.

[0052] <First exemplary embodiment>
(System configuration)
FIG. 1 is a diagram illustrating an example of the general configuration of a communication system in a first exemplary embodiment. Referring to FIG. 1, this communication system includes a control apparatus 1, a monitoring apparatus 2, a node 3, and terminals 4A and 4B. When there is no need to distinguish between the two terminals, the terminals 4A and 4B are called a terminal 4 or simply a "terminal". The terminals 4A and 4B are connected to the node 3 to form a forwarding network over which user packets are forwarded.

[0053] The node 3 is an OpenFlow switch or a forwarding node similar to an OpenFlow switch.

[0054] In FIG. 1, the terminals 4A and 4B are connected to the node 3, and the path between the terminal 4A and the terminal 4B is a path that passes through the node 3.

[0055] The control apparatus 1, monitoring apparatus 2, and node 3 are interconnected to form a control network. The control network may be configured by a dedicated network. For example, in the OpenFlow network described above, the control network is configured by a dedicated network with a secure channel. In this exemplary embodiment, the control apparatus 1 maintains the communication status received from the monitoring apparatus 2.

[0056] (Control apparatus)

FIG. 2 is a diagram illustrating an example of the configuration of the control apparatus 1 in the first exemplary embodiment. Referring to FIG. 2, the control apparatus 1 includes communication permission decision means 101, forwarding rule setting means 102, communication status holding means 103, and a firewall rule 104 stored in a storage device in the control apparatus 1.

[0057] The communication permission decision means 101 analyzes a received packet (for example, a first packet) forwarded from the node (3 in FIG. 1) and extracts the flow information (flow of the packet from the transmission source to the transmission destination) and the information about the communication status (for example, flag information included in the TCP header). After that, the communication permission decision means 101 decides the permission of communication by referencing a prespecified firewall rule 104 and the communication status (communication status related to the flow) held in the communication status holding means 103. For example, if the communication status related to the flow, which is held in the communication status holding means 103, is NEW, the communication permission decision means 101 does not permit the communication of a packet, based on the rule that is set in the firewall rule 104, if the SYN flag of the TCP header of the received packet (first packet) forwarded from the node (3 in FIG. 1) is not on.

[0058] When the communication is not permitted, the communication permission decision means 101 discards the received packet. Once the control apparatus 1 discards a packet for which non -permission of communication is decided, a transmission error will be generated even if the transmission source terminal 4, which transmits the packet, retries the transmission (The processing (procedure) to be performed in this case depends on the installed protocol of the higher-level layer).

[0059] The communication status holding means 103 includes storage means (not shown), such as a semiconductor memory or a magnetic disc, and access means (not shown) that writes (updates) and reads (references) information to and from the storage means. The communication status holding means 103 stores therein the communication status, related to each flow, in association with the flow. In this exemplary embodiment, the monitoring apparatus 2 writes (updates) communication information in the communication status holding means 103, and the communication permission decision means

101 reads (references) or writes (updates) communication information from or to the communication status holding means 103.

[0060] A rule such as a filtering condition is set in the firewall rule 104 using a predefined, predetermined command received from input means (not shown) of the control apparatus 1. An example of a rule that is set in the firewall rule 104 is that, when the communication status is NEW, the communication is permitted if a received packet (first packet) is a SYN packet.

[0061] The forwarding rule setting means 102 carries out path calculation based on the network topology information, managed by the control apparatus 1, and sets a forwarding rule in the node 3 on the path. In this exemplary embodiment, in case the communication permission decision means 101 decides that communication is permitted for a packet (for example, first packet) forwarded from the node 3, the forwarding rule setting means 102 sets, in each node (3 in FIG. 1) on the forwarding path, as a forwarding rule (flow setup),

. Packet forwarding path from the packet transmission source terminal (for example, 4A in FIG. 1) to the transmission destination terminal (for example, 4B in FIG. 1), and

. Forwarding path from the transmission source terminal (for example, 4A in FIG. 1) to the monitoring apparatus (2 in FIG. 1)

[0062] The flow setup, when performed, causes the forwarding rule transmitted from the control apparatus 1 to be set and held in the rule field and the action field (if a packet matches the rule, an action is performed to forward the packet to the forwarding path) of the flow table (302 in FIG. 10) of each node (3 in FIG. 1) on the forwarding path. After the packet (first packet) is forwarded, the subsequent packets forwarded from the transmission source terminal (for example, 4A in FIG. 1) are forwarded from the node (3 in FIG. 1) on the forwarding node to the packet forwarding path to the transmission destination terminal (for example, 4B in FIG. 1) and to the packet forwarding path to the monitoring apparatus (2 in FIG. 1) according to the content that is set in the flow table (302 in FIG. 10).

[0063] As described above, when a received packet (first packet, etc.) is received from the node 3, the OpenFlow controller in the related art uses the network topology information to determine a path for a packet based on the transmission source/destination information included in the received packet and then performs flow setup. On the other hand, the control apparatus 1 in this exemplary embodiment decides the permission of the received packet based on the firewall rule 104 and the communication status (history) held in the communication status holding means 103. In case it is decided to permit the communication, the control apparatus 1 generates the packet forwarding path information, which indicates forwarding not only to the transmission destination terminal but also to the monitoring apparatus, and sets the packet forwarding path in-

formation in the flow tables of the nodes on the transfer path during flow setup.

[0064] (Monitoring apparatus)

FIG. 3 is a diagram illustrating an example of the configuration of the monitoring apparatus 2 in the first exemplary embodiment. Referring to FIG. 3, the monitoring apparatus 2 includes packet analysis means 201. The monitoring apparatus 2 may also be arranged in the node 3 as the monitoring unit (or monitoring module) of the node 3. The packet analysis means 201 monitors a packet that is forwarded from a node (3 in FIG. 1) in which a forwarding rule is set in its flow table during flow setup performed by the control apparatus 1.

[0065] The information monitored by the packet analysis means 201 includes at least one of the OpenFlow header information, the higher-level layer header, the port number of related communication in the payload, and so forth.

[0066] (Node)

FIG. 10 is a diagram showing the configuration of the node 3. The node 3 includes a communication processing unit 301 and a flow table 302. The communication processing unit 301 transmits and receives a packet between the terminal 4A and the terminal 4B (transmission of a packet to the next OpenFlow switch), forwards a packet (for example, first packet) to the control apparatus 1, and forwards a packet to the monitoring apparatus 2. The flow table 302 includes the above-described rule, action, and statistical information on each flow. The monitoring apparatus 2 and the node 3 are connected to forward a user packet.

[0067] (System operation)

FIG. 4 is a flowchart showing the operation of the system in the first exemplary embodiment. In the first exemplary embodiment shown in FIG. 1, the node 3 has the configuration and the function conforming to the above-described OpenFlow switch as shown in FIG. 10. The control apparatus 1 has the configuration and the function complying with the OpenFlow controller, as described with reference to FIG. 2.

[0068] First, terminal A (4A in FIG. 1) transmits a packet destined to terminal B (4B in FIG. 1), to the node (3 in FIG. 1) (step S1).

[0069] The node (3 in FIG. 1) searches the flow table (302 in FIG. 10) in the node for a rule that matches the information (for example, header information) of the packet received from terminal A (step S2). Although the present invention is not limited thereto, each entry of the flow table includes two fields, a rule field and an action field. The rule field includes information on a destination IP address, a transmission source IP address, a transmission source port, and a destination port, and the action field includes forwarding destinations to which a received packet is to be forwarded when the header information of the received packet matches the rule. If a flow entry is found whose rule matches the destination IP address, transmission source IP address, transmission source

port, and destination port included in the received packet's header information used in OpenFlow, the received packet is forwarded to the packet forwarding destinations specified in the action field of the flow entry (in this exemplary embodiment, to the next forwarding destination (terminal 4B) of the received packet and to the monitoring apparatus 2).

[0070] If a flow entry that matches the header information of the received packet is not found in the node (3 in FIG. 1) (No in step S3), the node (3 in FIG. 1) forwards the packet to the control apparatus (1 in FIG. 1; OpenFlow controller) via the secure channel (step S4).

[0071] The communication permission decision means (101 in FIG. 2) of the control apparatus (1 in FIG. 1) decides whether permission is given to the flow to which the packet forwarded from the node (3 in FIG. 1) belongs (step S5). In this case, the communication permission decision means (101 in FIG. 2) analyzes the packet to acquire the flow information (a path corresponding to the flow between the transmission source terminal and the transmission destination terminal) and the information on the communication status (for example, flag information (Flags) in the TCP header, "Flags" in FIG. 11).

[0072] The communication permission decision means (101 in FIG. 2) references the firewall rule 104 set in advance, references the communication status held in the communication status holding means (103 in FIG. 2) to reference the communication status log information related to the flow, and decides whether to or not to permit the communication (whether to or not to pass the packet which is forwarded via this flow).

[0073] As the communication status, the flow information ("Flags" information in FIG. 11), similar to that in the header used in OpenFlow, as well as NEW, ESTABLISHED, RELATED and so forth described above are held. Note that the communication status is not limited to above described NEW, ESTABLISHED, and RELATED.

[0074] In case the communication permission decision means (101 in FIG. 2) does not permit communication, the packet is discarded (step S7).

[0075] In case the communication permission decision means (101 in FIG. 2) permits communication, the forwarding rule setting means (102 in FIG. 2) of the control apparatus (1 in FIG. 1) sets the forwarding rule (forwarding destination), in which it is specified that the flow to which the packet belongs is forwarded to terminal B (4B in FIG. 1) and to the monitoring apparatus (2 in FIG. 1), in the node (3 in FIG. 1) that forwarded the packet to the control apparatus (that is, flow setup is performed) (step S8). This flow setup causes the forwarding rule to be set in the rule and action fields in the flow table (302 in FIG. 10) of the node (3 in FIG. 1) that belongs to the flow.

[0076] Next, the control apparatus (1 in FIG. 1) forwards the packet to terminal B (4B in FIG. 1) via the node (3 in FIG. 1) (step S9). Because the control apparatus (1 in FIG. 1)

already has done analysis of the packet, the packet is not forwarded to the monitoring apparatus (2 in FIG. 1). Each of the subsequent packets that will be forwarded is matched against the forwarding rule, which is set in the flow table, in the node (3 in FIG. 1) and, if the packet matches the forwarding rule, is forwarded to the monitoring apparatus (2 in FIG. 1) that is one of the forwarding destinations specified in the action field.

[0077] The control apparatus (1 in FIG. 1) updates the communication status of the flow (step S10). That is, the control apparatus (1 in FIG. 1) updates the communication status held in the communication status holding means (103 in FIG. 2).

[0078] When a flow entry, which contains a rule that matches the received packet, is found in the node (3 in FIG. 1), the node forwards the packet to terminal B (4B in FIG. 1) and to the monitoring apparatus (2 in FIG. 1) according to the action defined by the rule (forwarding rule) that matches the packet (step S11).

[0079] The monitoring apparatus (2 in FIG. 1) analyzes the packet, forwarded from the node (3 in FIG. 1), via the packet analysis means (201 in FIG. 3) and extracts the information, necessary for grasping the communication status, from the packet (step S12). The information extracted by the packet analysis means (201 in FIG. 3) includes at least one of the OpenFlow header information, the upper- layer header, a port number for related communication in the data, and so forth.

[0080] The monitoring apparatus (2 in FIG. 1) checks the information, extracted from the packet, to decide whether or not the packet is such a packet that makes it necessary for the control apparatus (1 in FIG. 1) to update the communication status (for example, whether or not the packet of the protocol that requires the update of the communication status) (step S13). If the monitoring apparatus (2 in FIG. 1) decides that the communication status must be updated, the communication status is transmitted to the control apparatus (1 in FIG. 1). Then, the communication status holding means (103 in FIG. 2) updates the communication status, which is held therein, based on the communication status transmitted from the monitoring apparatus (2 in FIG. 1).

[0081] The updated communication status is referenced when the control apparatus (1 in FIG. 1) receives a new received packet from the node (3 in FIG. 1) and the communication permission decision means 101 decides whether to or not to permit communication.

[0082] In order to implement a stricter firewall operation, the decision of the permission of communication may be executed when the communication status is updated. In case the existing communication is not permitted as a result of the decision, the forwarding rule corresponding to this communication (flow for which the existing communication is not permitted) may be deleted.

[0083] (Effect)

According to the first exemplary embodiment, the communication permission decision means 101 of the control apparatus 1 references the communication status. Therefore, whether to or not to permit communication may be decided according to the communication status. That is, the SPI processing can be performed.

[0084] According to the first exemplary embodiment, only Packet-In from the node 3, as well as a communication status update from the monitoring apparatus 2, are transmitted to the control apparatus 1. This configuration therefore reduces the amount of data forwarding to the control apparatus 1 and the amount of packet analysis in the control apparatus 1 as compared with those in the configuration in which packets for entire communications are forwarded to the control apparatus 1 for monitoring.

[0085] Although FIG. 1 shows an example of a typical configuration in which one node, node 3, is included, two or more nodes 3 may be arranged between the terminals 4A and 4B as shown in the exemplary embodiments below.

[0086] The control and processing of each means provided in the control apparatus 1 and the monitoring apparatus 2 shown in FIG. 2 and FIG. 3 may be implemented by a program executed in each computer forming the control apparatus 1 and the monitoring apparatus 2. In this case, the program is stored in a storage medium or a storage apparatus, such as a memory, and a magnetic/optical disc, from which the computer reads the program for execution. The same is true of the exemplary embodiments described below.

[0087] <Secondary exemplary embodiment>

In the second exemplary embodiment, the communication status is held in a monitoring apparatus 2. A control apparatus 1 inquires of the monitoring apparatus 2 about the communication status and controls a node 3. The system configuration of the second exemplary embodiment is described below with reference to FIG. 1, FIG. 5, and FIG. 6. The general configuration of the system in the second exemplary embodiment is as shown in FIG. 1. This configuration is the same as that in the first exemplary embodiment.

[0088] (Control apparatus)

FIG. 5 is a diagram illustrating an example of the configuration of the control apparatus 1 in the second exemplary embodiment. Referring to FIG. 5, the control apparatus 1 includes communication permission decision means 101, forwarding rule setting means 102, a firewall rule 104, and communication status collection means 105. In this exemplary embodiment, the control apparatus 1 does not include the communication status holding means 103 shown in FIG. 2.

[0089] (Monitoring apparatus)

FIG. 6 is a diagram illustrating an example of the configuration of the monitoring apparatus 2 in the second exemplary embodiment. Referring to FIG. 6, the monitoring

apparatus 2 includes packet analysis means 201, communication status holding means 202, and communication status response means 203. The monitoring apparatus 2 monitors the communication status and responds to an inquiry from the control apparatus 1. The monitoring apparatus 2 may also be arranged in the node 3 as the monitoring unit (monitoring module) of the node 3.

[0090] (System operation)

In this exemplary embodiment, the communication permission decision step (S6 in FIG. 4) and the communication status update step (S10 in FIG. 4) are different from those of the first exemplary embodiment in FIG. 4. The other steps in FIG. 4 are the same as those in the first exemplary embodiment.

[0091] In this exemplary embodiment, the communication permission decision means 101 of the control apparatus 1 decides in the communication permission decision step (S6 in FIG. 4) whether to or not to permit the communication of the flow, to which a packet belongs. In this case, the communication permission decision means 101 first analyzes the packet to obtain the flow information and the information on the communication status.

[0092] Next, the communication permission decision means 101 decides whether to or not to permit the communication based on the pre-set firewall rule 104 and the communication status collected related to the flow.

[0093] To acquire the communication status related to the flow, the communication status collection means 105 of the control apparatus 1 inquires of the monitoring apparatus 2 about the communication status. In response to this inquiry from the control apparatus 1, the communication status response means 203 of the monitoring apparatus 2 obtains the related communication status from the communication status holding means 202 and returns the obtained communication status to the control apparatus 1.

[0094] A communication status update is made to the communication status holding means 202 of the monitoring apparatus 2.

[0095] For a received packet whose header does not match a flow entry in the node 3, the update information on the communication status is forwarded from the monitoring apparatus 2 to the control apparatus 1. Instead of this, the node 3 may forward the packet directly to the monitoring apparatus 2 to allow the monitoring apparatus 2 to analyze the packet and update the communication status as if a matching flow entry was found.

[0096] With regard to the communication status of bi-directional communication between the terminal 4A and the terminal 4B, the communication status of a packet forwarded in the direction opposite to that of the packet described above is referenced to update and hold the communication status.

[0097] (Effect)

According to the second exemplary embodiment, the communication status is updated in the monitoring apparatus 2 and, only when the decision of the permission of communication is made, the communication status is transmitted from the monitoring apparatus 2 to the control apparatus 1. The operation in the second exemplary embodiment achieves an effect similar to that in the first exemplary embodiment and, in addition, reduces the frequency of transmissions from the monitoring apparatus 2 to the control apparatus 1 and the amount of data transmitted.

[0098] <Third exemplary embodiment>

In a third exemplary embodiment, the communication status is held by both a control apparatus 1 and a monitoring apparatus 2. The system configuration of this exemplary embodiment is basically the same as that in FIG. 1 referenced in the description of the first and second exemplary embodiments. The configuration of the monitoring apparatus 2 is basically the same as that shown in FIG. 6. The monitoring apparatus 2 includes a communication status holding means 202.

[0099] (Control apparatus)

FIG. 7 is a diagram showing the configuration of the control apparatus 1. Referring to FIG. 7, the control apparatus 1 includes communication permission decision means 101, forwarding rule setting means 102, communication status holding means 103, a firewall rule 104, and communication status collection means 105.

[0100] The communication status holding means 103 and 202 is provided in the control apparatus 1 and the monitoring apparatus 2 respectively.

[0101] The communication status holding means 103 of the control apparatus 1 holds a communication status extracted from a packet that is forwarded to the control apparatus 1 as a first packet.

[0102] (System operation)

In this exemplary embodiment, the communication permission decision step (S6 in FIG. 4) and the communication status update step (S13 in FIG. 4) are different from those of the first and second exemplary embodiments. The other steps in FIG. 4 are the same as those in the first and second exemplary embodiments.

[0103] The communication status is updated by the communication status holding means 103 of the control apparatus 1 or by the communication status holding means 202 of the monitoring apparatus 2.

[0104] In case an entry corresponding to a rule, which matches the header information of a received packet, is not found in the node 3 (for example, if the packet is a first packet), the packet is forwarded from the node 3 to the control apparatus 1 that decides whether to or not to permit the communication. After that, the extracted information on the communication status is passed to the communication status holding means 103 of the control apparatus 1.

[0105] In case a rule (forwarding rule), which matches a received packet, is found in the flow table of the node 3, the received packet is forwarded from the node 3 to the monitoring apparatus 2 where the packet analysis means 201 of the monitoring apparatus 2 analyzes the received packet. After that, the extracted information on the communication status is passed to the communication status holding means 202.

[0106] The communication permission decision means 101 of the control apparatus 1 inquires of the communication status collection means 105 of the control apparatus 1 about the communication status related to the flow in which the packet is forwarded.

[0107] The communication status collection means 105 of the control apparatus 1 acquires the communication status, related to the packet (flow), from the communication status holding means 103 of the control apparatus 1 and the communication status holding means 202 of the monitoring apparatus 2. In this case, the values held in the communication status holding means 103 and the communication status holding means 202 sometimes differ. In such a case, based on the communication status acquired from the communication status holding means 103 of the control apparatus 1 and from the communication status holding means 202 of the monitoring apparatus 2, the communication status collection means 105 generates a new communication status related to the packet (flow) and returns the generated communication status to the communication permission decision means 101. The communication permission decision means 101 decides whether to pass the received packet based on the communication status generated by the communication status collection means 105 and the pre-set firewall rule 104.

[0108] For example, if the forward direction path (from transmission source terminal to transmission destination terminal) and the backward direction path (from transmission destination terminal to transmission source terminal) are different in a bi-directional communication between the terminal 4A and the terminal 4B (for example, the path is changed due to flow aggregation), the backward direction communication status is sometimes held in the communication status holding means of some other apparatus with the result that the communication status can be neither referenced nor updated directly. For example, assume that the communication status of the forward direction path in a bi-directional communication between the terminal 4A and the terminal 4B is held in the communication status holding means 103 of the control apparatus 1 and that the communication status of the backward direction path is held in the communication status holding means 202 of the monitoring apparatus 2. In this case, the communication status of the backward direction/forward direction path cannot be referenced to decide the communication permission of the forward direction/backward direction path. Nor can the communication status of the forward direction/backward direction path be updated by the communication status of the backward direction/forward

direction path. In such a case, it is possible for the communication status holding means 202 of the monitoring apparatus 2 to hold, not the communication status, but other information such as the packet information (header information, or IP address or port information in the payload) and the time (packet reception time). The communication status collection means 105 of the control apparatus 1 generates the communication status of the flow based on the information in the communication status holding means 103 of the control apparatus 1 and the information (packet information, reception time) from the communication status holding means 202 of the monitoring apparatus 2.

[0109] (Effect)

According to the third exemplary embodiment, the update processing of the communication status is confined in the control apparatus 1 and the monitoring apparatus 2 that analyze a packet. Therefore, the third exemplary embodiment reduces the communication between the control apparatus 1 and the monitoring apparatus during the update of the communication status as compared with the first and second exemplary embodiments.

[0110] <Fourth exemplary embodiment>

In a fourth exemplary embodiment, a control apparatus 1 instructs a monitoring apparatus 2 which communication (packet) is to be monitored. The control apparatus 1 decides whether or not monitoring is required for each flow based on a firewall rule and the type of communication and sets a rule, which specifies that the flow is to be forwarded to the monitoring apparatus, in a node.

[0111] Although not limited thereto, the condition under which monitoring is required are as follows:

. a firewall rule 104 that specifies a state is present;

. the communication is one carried out under transmission control such as TCP and so forth; or

. the communication is one that controls other communications such as FTP control and so forth.

[0112] In addition, the node 3 may be extended to allow, in addition to the above-described OpenFlow header information, TCP flags and so forth to be specified in a rule of an entry of the flow table in the node 3 to narrow down the packets to be monitored. Although not limited thereto, this operation may be performed during the flow setup of a flow. The operation may also be performed when a firewall rule is changed.

[0113] (Effect)

According to this exemplary embodiment, the monitoring apparatus 2 monitors only a communication specified by the control apparatus 1. Therefore, this exemplary embodiment achieves an effect similar to that in the first exemplary embodiment to the

third exemplary embodiment and, in addition, reduces analysis processing of un-necessary communications.

[0114] <Fifth exemplary embodiment>

A fifth exemplary embodiment is configured by multiple nodes and one monitoring apparatus. FIG. 8 is a diagram illustrating an example of the general configuration of a system in the fifth exemplary embodiment. Referring to FIG. 8, the system includes a control apparatus 1, a monitoring apparatus 2, a node 3A, a node 3B, a terminal 4A, and a terminal 4B. There is one monitoring apparatus 2 while there are multiple nodes 3 and terminals 4 (not limited to two). When there are multiple nodes 3, each of all nodes 3 is connected to one or more of the other nodes to form a forwarding network of user packets. When there is no need to distinguish between the nodes and between the terminals in the description below, the node 3A and node 3B are called a node and the terminal 4A and terminal 4B are called a terminal.

[0115] A network is connected between the node 3A and the node 3B, between the node 3A and the terminal 4A, and between the node 3B and the terminal 4B. Each network forms a user packet forwarding network.

[0116] The terminal 4A is connected to the node 3A and the terminal 4B is connected to the node 3B, respectively, and the path between the terminal 4A and the terminal 4B is a path that passes through the node 3A and the node 3B. User packets other than a first packet are forwarded along this path. Each of the nodes 3A and 3B is connected to the control apparatus 1 and the monitoring apparatus 2 to form the control network described above. Such an arrangement is possible in which a part of the multiple nodes 3 are connected to the monitoring apparatus 2. For example, a node, which relays between the nodes 3, may not be connected to the monitoring apparatus 2.

[0117] A packet may be forwarded from the node 3 to the monitoring apparatus 2 from any one of the nodes on a path.

[0118] Therefore, a method for forwarding a packet from the node 3 to the monitoring apparatus 2 is as follows. For example, the node 3A or the node 3B (edge node), connected to the terminal 4A and the terminal 4B respectively, forwards a packet, received from the terminal 4A or terminal 4B, to the control apparatus 1.

[0119] Another arrangement is also possible in which a specific node is determined as a forwarding node in advance and, if this specific forwarding node is not on a path of a flow, a packet-forwarding rule defining that a packet be forwarded from a node on the path of the flow to this specific forwarding node is set. This arrangement causes a packet to be forwarded to the communication destination terminal and to the monitoring apparatus in accordance with the forwarding rule in each node.

[0120] In this exemplary embodiment, the communication status holding means 202 in the monitoring apparatus 2 or the communication status holding means 103 in control

apparatus 1 is used in a configuration in which multiple nodes are present. In addition, the control apparatus 1 references the communication status holding means 103 to decide whether to or not to permit the communication in the same manner as in the first to fourth exemplary embodiments.

[0121] (Effect)

This exemplary embodiment achieves an effect similar to that in the first to the fourth exemplary embodiments in a configuration in which there are multiple nodes.

[0122] <Sixth exemplary embodiment>

The system configuration in a sixth exemplary embodiment includes multiple nodes and one monitoring apparatus as in the fifth exemplary embodiment described with reference to FIG. 8. The sixth exemplary embodiment has a configuration in which the load is balanced.

[0123] In FIG. 8, a control apparatus 1 determines from which node 3 a packet is to be forwarded to a monitoring apparatus 2 in each flow. More specifically, in this exemplary embodiment, each time flow setup is performed, the control apparatus 1 determines from which node 3 a packet is to be forwarded to the monitoring apparatus 2, in consideration of the load of the node 3 based on the flow table of the node 3 on a forwarding path or the information similar to it, and sets the forwarding rule.

[0124] (Effect)

This exemplary embodiment performs the operation described above to achieve an effect similar to that in the first to the fifth exemplary embodiments and, in addition, balances the load of the nodes for forwarding a packet to the monitoring apparatus 2.

[0125] <Seventh exemplary embodiment>

A seventh exemplary embodiment includes multiple nodes and multiple monitoring apparatuses. FIG. 9 is a diagram showing the system configuration of this exemplary embodiment.

[0126] Referring to FIG. 9, the system in this exemplary embodiment includes a control apparatus 1, multiple monitoring apparatuses 2, multiple nodes 3A and 3B, and multiple terminals 4A and 4B. In this exemplary embodiment, the description of the configuration and the operation is omitted because the control apparatus 1 and each of the monitoring apparatuses 2 are the same the control apparatus 1 and the monitoring apparatus 2 in the third exemplary embodiment described with reference to FIG. 6 and FIG. 7 respectively.

[0127] This exemplary embodiment achieves an effect similar to that in the third exemplary embodiment and, in addition, provides multiple monitoring apparatuses 2 to distribute the loads of the packet analysis means 201 and the communication status holding means 202 of the monitoring apparatus 2 among the multiple monitoring apparatuses 2. This configuration leads to an increase in the processing performance of the

monitoring apparatus 2 and the processing performance of the entire system.

[0128] While the third exemplary embodiment to the seventh exemplary embodiment are described while comparing them with the second exemplary embodiment, such an embodiment is also possible in which the above described exemplary embodiments are combined as necessary.

[0129] Although a network to which OpenFlow is applied is described in the above exemplary embodiments, the present invention is not limited to this type of network. The present invention is applicable to a network other than an OpenFlow network in which a control server performs integral control of the network.

[0130] The function of the control apparatus in the above exemplary embodiments may be implemented by hardware or by a computer and a program executed on the computer. The program is recorded in a recording medium, such as a magnetic disk or a semiconductor memory, for distribution and is read by a computer when it is started. The operation of the computer is controlled in this way to allow it to function as the control apparatus in each exemplary embodiment for performing the processing described above.

[0131] In addition, a part or an entirety of the above exemplary embodiments may be described in, but are not limited to, the following supplementary notes.

[0132] (Supplementary note 1)

A communication system comprising:

at least one node that forwards a packet in accordance with a forwarding rule set therein;

a transmission source terminal of the packet;

a transmission destination terminal of the packet;

a control apparatus that is connected to the node via a network and that controls the node; and

at least one monitoring apparatus that is connected to the node and to the control apparatus via networks, respectively, and that monitors a packet forwarded to the node arranged between the terminals, wherein

the control apparatus comprises:

communication permission decision means that decides whether to or not to permit communication for a packet transmitted from the node, based on information collected by the monitoring apparatus and on a firewall rule including a pre-defined filtering condition; and

forwarding rule setting means that, responsive to the decision to permit communication by communication permission decision means, sets a forwarding path of a packet from the transmission source terminal of the packet to the transmission destination terminal of the packet and a forwarding path of the packet from the

transmission source terminal of the packet to the monitoring apparatus, in each node arranged on each of the forwarding paths, as the forwarding rule.

[0133] (Supplementary note 2)

The communication system according to supplementary note 1, wherein the control apparatus and/or the monitoring apparatus comprises communication status holding means that holds a communication status.

[0134] (Supplementary note 3)

The communication system according to supplementary note 1 or 2, wherein the monitoring apparatus comprises:

packet analysis means that extracts information on a packet, forwarded from the node, and acquires a communication status; and

communication status holding means that holds the communication status,

the control apparatus comprises:

communication status holding means that holds a communication status that the monitoring apparatus has acquired for the packet; and/or

communication status collection means that inquires of the monitoring apparatus about a communication status, and

the monitoring apparatus transmits the communication status to the control apparatus.

[0135] (Supplementary note 4)

The communication system according to supplementary note 3 wherein each of the control apparatus and the monitoring apparatus has communication status holding means that holds a communication status, and

the communication status collection means generates a communication status of a corresponding flow based on the communication status acquired from the communication status holding means of the control apparatus and the monitoring apparatus.

[0136] (Supplementary note 5)

The communication system according to supplementary note 4 wherein the monitoring apparatus holds information on, and a reception time of, a packet instead of acquiring a communication status from the node for the packet.

[0137] (Supplementary note 6)

The communication system according to one of supplementary notes 1-3, wherein the control apparatus instructs the monitoring apparatus which communication is to be monitored.

[0138] (Supplementary note 7)

The communication system according to one of supplementary notes 1-3, including a plurality of the nodes, wherein one or more predetermined nodes of the plurality of the nodes transmit a packet to the monitoring apparatus.

[0139] (Supplementary note 8)

The communication system according to one of supplementary notes 1-7, wherein the control apparatus determines at least one of the plurality of nodes as a node that transmits a packet to the monitoring apparatus.

[0140] (Supplementary note 9)

The communication system according to one of supplementary notes 1-8, including a plurality of the monitoring apparatuses.

[0141] (Supplementary note 10)

A control apparatus comprising:

communication permission decision means that decides whether to or not to permit communication for a packet forwarded from a node, based on information collected by at least one monitoring apparatus monitoring apparatus monitoring a packet forwarded to at least one node and on a firewall rule including a pre-defined filtering condition, the at least one node forwarding a packet in accordance with a forwarding rule set therein, the at least one node arranged between a transmission source terminal of the packet and a transmission destination terminal of the packet, and

forwarding rule setting means that, responsive to the decision to permit communication by communication permission decision means, sets a forwarding path of a packet from the transmission source terminal of the packet to the transmission destination terminal of the packet, and a forwarding path of the packet from the transmission source terminal of the packet to the monitoring apparatus, in each node on each of the forwarding paths, as the forwarding rule.

[0142] (Supplementary note 11)

The control apparatus according to supplementary note 10, further comprising communication status holding means that holds a communication status acquired by the monitoring apparatus.

[0143] (Supplementary note 12)

The control apparatus according to supplementary note 10 or 11, further comprising:

communication status holding means that holds a communication status acquired by the monitoring apparatus for the packet; and/or

communication status collection means that inquires of the monitoring apparatus about a communication status.

[0144] (Supplementary note 13)

The control apparatus according to supplementary note 10 or 11 wherein the control apparatus instructs the monitoring apparatus which communication is to be monitored.

[0145] (Supplementary note 14)

The control apparatus according to any one of supplementary notes 10-13 wherein the control apparatus determines at least one node out of the plurality of nodes as a

node that transmits a packet to the monitoring apparatus.

[0146] (Supplementary note 15)

A monitoring apparatus comprising:

packet analysis means that monitors a packet forwarded to at least one node arranged between a transmission source terminal of the packet and a transmission destination terminal of the packet and acquires a communication status; and

communication status holding means that holds the communication status acquired by the packet analysis means,

the monitoring apparatus transmitting the communication status to a control apparatus connected to the monitoring apparatus via a network,

the control apparatus deciding whether to or not to permit communication for a packet transmitted from the node, based on information collected by the monitoring apparatus and on a firewall rule including a pre-defined filtering condition,

the control apparatus, in case of the permission of communication being decided, setting a forwarding path of a packet from the transmission source terminal of the packet to the transmission destination terminal of the packet, and a forwarding path of the packet from the transmission source terminal of the packet to the monitoring apparatus, in each node on each of the forwarding paths, as a forwarding rule.

[0147] (Supplementary note 16)

The monitoring apparatus according to supplementary note 15 wherein the control apparatus and the monitoring apparatus include communication status holding means that holds the communication status, and hold information on, and a reception time of, a packet instead of acquiring the communication status from the node for the packet.

[0148] (Supplementary note 17)

A communication method comprising:

monitoring, by at least one monitoring apparatus, a packet forwarded to at least one node, the at least one node forwarding a packet in accordance with a forwarding rule, the at least one node arranged between a transmission source terminal of the packet and a transmission destination terminal of the packet,

upon reception of a packet forwarded from the node, deciding, by a control apparatus connected to the node, whether to or not to permit communication for the packet, based on information collected by the monitoring apparatus monitoring the packet and on a firewall rule including a pre-defined filtering condition; and

setting a forwarding path of a packet from the transmission source terminal of the packet to the transmission destination terminal of the packet, and a forwarding path of the packet from the transmission source terminal of the packet to the monitoring apparatus, in each node on each of the forwarding paths, as the forwarding rule, responsive to the decision of the permission of the communication.

[0149] (Supplementary note 18)

The communication method according to supplementary note 17, further comprising holding, by the control apparatus and/or the monitoring apparatus, a communication status.

[0150] (Supplementary note 19)

The communication method according to supplementary note 17 or 18, wherein the monitoring apparatus holds a communication status by extracting information on a packet forwarded from the node, the communication method further comprising:

inquiring, by the control apparatus, of the monitoring apparatus about a communication status; and

transmitting, by the monitoring apparatus, a communication status to the control apparatus in response to the inquiry from the control apparatus.

[0151] (Supplementary note 20)

The communication method according to supplementary note 17, further comprising:

holding, by the control apparatus and the monitoring apparatus, a communication status; and

generating, by the control apparatus, a communication status of a corresponding flow based on the communication status held in the control apparatus and the monitoring apparatus.

[0152] (Supplementary note 21)

The communication method according to supplementary note 20, wherein the monitoring apparatus holds information on, and a reception time of, a packet instead of acquiring a communication status from the node for the packet.

[0153] (Supplementary note 22)

The communication method according to supplementary note 17 or 18, wherein the control apparatus instructs the monitoring apparatus which communication is to be monitored.

[0154] (Supplementary note 23)

The communication method according to any one of supplementary notes 17-19, wherein a plurality of nodes are provided and a predetermined node of the plurality of nodes transmits a packet to the monitoring apparatus.

[0155] (Supplementary note 24)

The communication method according to any one of supplementary notes 17-23, wherein the control apparatus determines at least one node out of the plurality of nodes as a node that transmits a packet to the monitoring apparatus.

[0156] (Supplementary note 25)

A program that causes a computer forming a control apparatus connected to at least one node that forwards a packet in accordance with a forwarding rule, the program

causing the computer to execute processing of:

deciding whether to or not to permit communication for a packet transmitted from the node, based on information collected by at least one monitoring apparatus monitoring a packet forwarded to at least one node arranged between a transmission source terminal of the packet and a transmission destination terminal of the packet and on a firewall rule including a pre-defined filtering condition; and

setting a forwarding path of a packet from the transmission source terminal of the packet to the transmission destination terminal of the packet, and a forwarding path of the packet from the transmission source terminal of the packet to the monitoring apparatus, in each node on each of the forwarding paths, as the forwarding rule, responsive to the decision of the permission of the communication.

[0157] (Supplementary note 26)

The program according to supplementary note 25, further causing the computer to cause the control apparatus to instruct the monitoring apparatus which communication is to be monitored.

[0158] (Supplementary note 27)

A node apparatus comprising:

a flow table in which a rule is set, the rule including a forwarding rule of a packet; and

a communication processing unit that matches a received packet against the rule in the flow table,

the communication processing unit, in case a rule that matches the received packet is not found in the flow table, forwarding the received packet to a control apparatus connected to the node apparatus, wherein the control apparatus decides whether to or not to permit communication for the received packet forwarded thereto from the node apparatus, based on information collected by a monitoring apparatus monitoring the packet and on a firewall rule including a pre-defined communication status specified as a filtering condition and the control apparatus, in case of the permission of communication being decided, sets a forwarding path of a packet from a transmission source terminal of the packet to a transmission destination terminal of the packet, and a forwarding path of the packet from the transmission source terminal of the packet to the monitoring apparatus, in each node on each of the forwarding paths, as the forwarding rule,

the communication processing unit receiving the forwarding rule from the control apparatus and setting the forwarding rule in the flow table, and

the communication processing unit forwarding a packet, which is received after the received packet and matches the forwarding rule set in the flow table, to the transmission destination terminal of the packet and to the monitoring apparatus.

[0159] (Supplementary note 28)

The node apparatus according to supplementary note 27 wherein the monitoring apparatus is provided.

[0160] (Supplementary note 29)

A terminal connected to the node of the communication system according to supplementary notes 1-9.

[0161] The disclosure of Patent Literatures and Non Patent Literatures given above is hereby incorporated by reference into this specification. The exemplary embodiments may be changed and adjusted in the scope of the entire disclosure (including claims) of the present invention and based on the basic technological concept. In the scope of the claims of the present invention, various disclosed elements (including the elements of the supplementary notes, the elements of the exemplary embodiments, and the elements of the drawings) may be combined and selected in a variety of ways. That is, it is apparent that the present invention includes various modifications and changes that may be made by those skilled in the art according to the entire disclosure, including claims, and technological concepts thereof.

Reference Signs List

[0162] 1,1A,1B Control apparatus

2,2A,2B Monitoring apparatus

3,3A,3B Node

4,4A,4B Terminal

101 Communication permission decision means

102 Forwarding rule setting means

103 Communication status holding means

104 Firewall rule

105 Communication state collection means

201 Packet analysis means

202 Communication status holding means

203 Communication state response means

301 Communication processing unit

302 Flow table

Claims

[Claim 1] A communication system comprising:
at least one node that forwards a packet in accordance with a forwarding rule set therein;
a transmission source terminal of the packet;
a transmission destination terminal of the packet;
a control apparatus that is connected to the node via a network and that controls the node; and
at least one monitoring apparatus that is connected to the node and to the control apparatus via networks, respectively, and that monitors a packet forwarded to the node arranged between the terminals, wherein
the control apparatus comprises:
communication permission decision means that decides whether to or not to permit communication for a packet transmitted from the node, based on information collected by the monitoring apparatus and on a firewall rule including a pre-defined filtering condition; and
forwarding rule setting means that, responsive to the decision to permit communication by communication permission decision means, sets a forwarding path of a packet from the transmission source terminal of the packet to the transmission destination terminal of the packet and a forwarding path of the packet from the transmission source terminal of the packet to the monitoring apparatus, in each node arranged on each of the forwarding paths, as the forwarding rule.

[Claim 2] The communication system according to claim 1, wherein at least one of the control apparatus and the monitoring apparatus comprises
communication status holding means that holds a communication status acquired by the monitoring apparatus monitoring the packet.

[Claim 3] The communication system according to claim 1, wherein the monitoring apparatus comprises:
packet analysis means that extracts information on a packet, forwarded thereto from the node, and acquires a communication status; and
communication status holding means that holds the communication status acquired by the packet analysis means, and wherein
the control apparatus comprises:
communication status holding means that holds a communication status acquired by the monitoring apparatus monitoring the packet; and/or
communication status collection means that inquires of the monitoring

apparatus about a communication status,
the monitoring apparatus transmitting the communication status to the control apparatus.

[Claim 4] The communication system according to claim 1 or 2, wherein the control apparatus instructs the monitoring apparatus which communication is to be monitored.

[Claim 5] The communication system according to any one of claims 1 to 3, including a plurality of the nodes, at least one predetermined node out of the plurality of the nodes transmitting a packet to the monitoring apparatus.

[Claim 6] A control apparatus comprising:
communication permission decision means that decides whether to or not to permit communication for a packet forwarded from a node, based on information collected by at least one monitoring apparatus monitoring apparatus monitoring a packet forwarded to at least one node and on a firewall rule including a pre-defined filtering condition, the at least one node forwarding a packet in accordance with a forwarding rule set therein, the at least one node arranged between a transmission source terminal of the packet and a transmission destination terminal of the packet, and
forwarding rule setting means that, responsive to the decision to permit communication by communication permission decision means, sets a forwarding path of a packet from the transmission source terminal of the packet to the transmission destination terminal of the packet, and a forwarding path of the packet from the transmission source terminal of the packet to the monitoring apparatus, in each node on each of the forwarding paths, as the forwarding rule.

[Claim 7] A monitoring apparatus comprising:
packet analysis means that monitors a packet forwarded to at least one node arranged between a transmission source terminal of the packet and a transmission destination terminal of the packet and acquires a communication status; and
communication status holding means that holds the communication status acquired by the packet analysis means,
the monitoring apparatus transmitting the communication status to a control apparatus connected to the monitoring apparatus via a network,
the control apparatus deciding whether to or not to permit communication for a packet transmitted from the node, based on information

collected by the monitoring apparatus and on a firewall rule including a pre-defined filtering condition,
the control apparatus, in case of the permission of communication being decided, setting a forwarding path of a packet from the transmission source terminal of the packet to the transmission destination terminal of the packet, and a forwarding path of the packet from the transmission source terminal of the packet to the monitoring apparatus, in each node on each of the forwarding paths, as a forwarding rule.

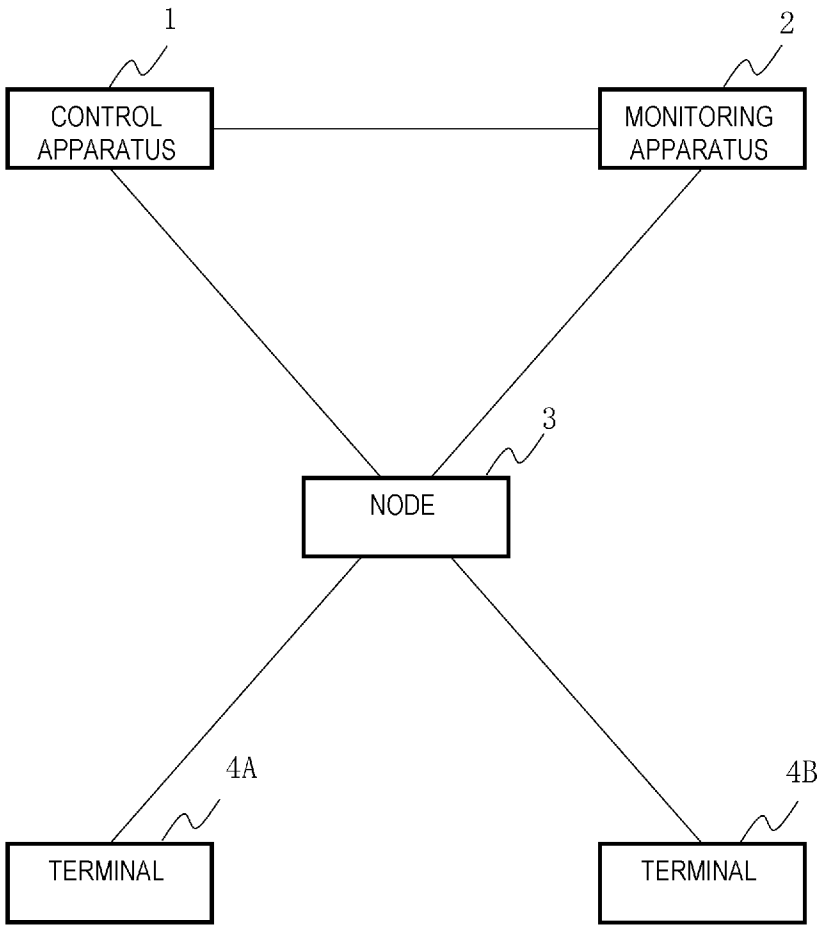
[Claim 8] A node apparatus comprising:
a flow table that stores a rule including a forwarding rule, the node apparatus forwarding a packet in accordance with the forwarding rule; and
a communication processing unit that matches a received packet against the rule in the flow table,
the communication processing unit, in case a rule that matches the received packet is not found in the flow table, forwarding the received packet to a control apparatus connected to the node apparatus, wherein the control apparatus decides whether to or not to permit communication for the received packet forwarded thereto from the node apparatus, based on information collected by a monitoring apparatus monitoring the packet and on a firewall rule including a pre-defined communication status specified as a filtering condition and the control apparatus, in case of the permission of communication being decided, sets a forwarding path of a packet from a transmission source terminal of the packet to a transmission destination terminal of the packet, and a forwarding path of the packet from the transmission source terminal of the packet to the monitoring apparatus, in each node on each of the forwarding paths, as the forwarding rule,
the communication processing unit receiving the forwarding rule from the control apparatus and setting the forwarding rule in the flow table, and
the communication processing unit forwarding a packet, which is received after the received packet and matches the forwarding rule set in the flow table, to the transmission destination terminal of the packet and to the monitoring apparatus.

[Claim 9] A communication method comprising:
monitoring, by at least one monitoring apparatus, a packet forwarded to

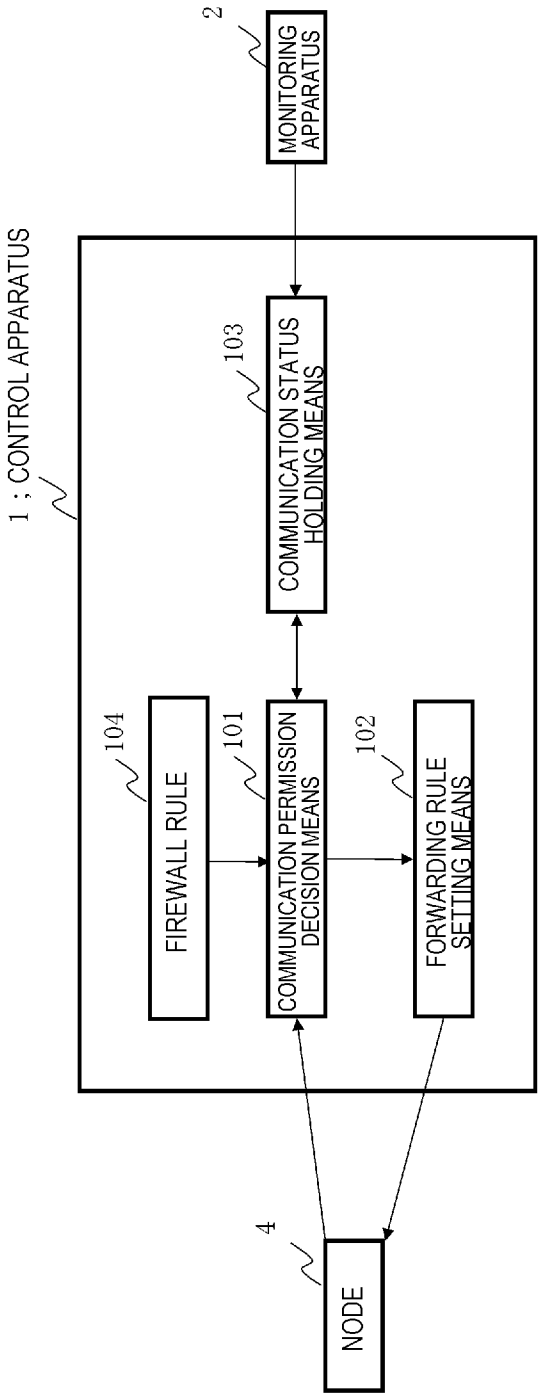
at least one node, the at least one node forwarding a packet in accordance with a forwarding rule, the at least one node arranged between a transmission source terminal of the packet and a transmission destination terminal of the packet,
upon reception of a packet forwarded from the node, deciding, by a control apparatus connected to the node, whether to or not to permit communication for the packet, based on information collected by the monitoring apparatus monitoring the packet and on a firewall rule including a pre-defined filtering condition; and
setting a forwarding path of a packet from the transmission source terminal of the packet to the transmission destination terminal of the packet, and a forwarding path of the packet from the transmission source terminal of the packet to the monitoring apparatus, in each node on each of the forwarding paths, as the forwarding rule, responsive to the decision of the permission of the communication.

[Claim 10] A program that causes a computer forming a control apparatus connected to at least one node that forwards a packet in accordance with a forwarding rule, the program causing the computer to execute processing of:
deciding whether to or not to permit communication for a packet transmitted from the node, based on information collected by at least one monitoring apparatus monitoring a packet forwarded to at least one node arranged between a transmission source terminal of the packet and a transmission destination terminal of the packet and on a firewall rule including a pre-defined filtering condition; and
setting a forwarding path of a packet from the transmission source terminal of the packet to the transmission destination terminal of the packet, and a forwarding path of the packet from the transmission source terminal of the packet to the monitoring apparatus, in each node on each of the forwarding paths, as the forwarding rule, responsive to the decision of the permission of the communication.

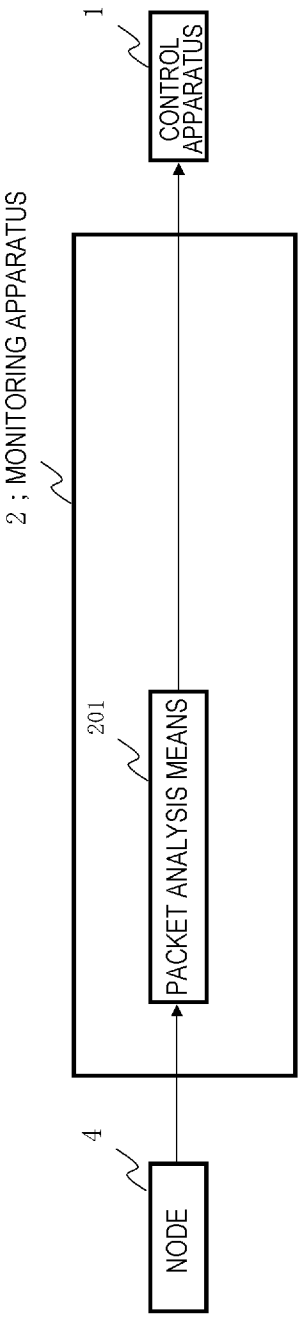
[Fig. 1]


1
2
CONTROL APPARATUS
MONITORING APPARATUS
3
NODE
4A
4B
TERMINAL
TERMINAL

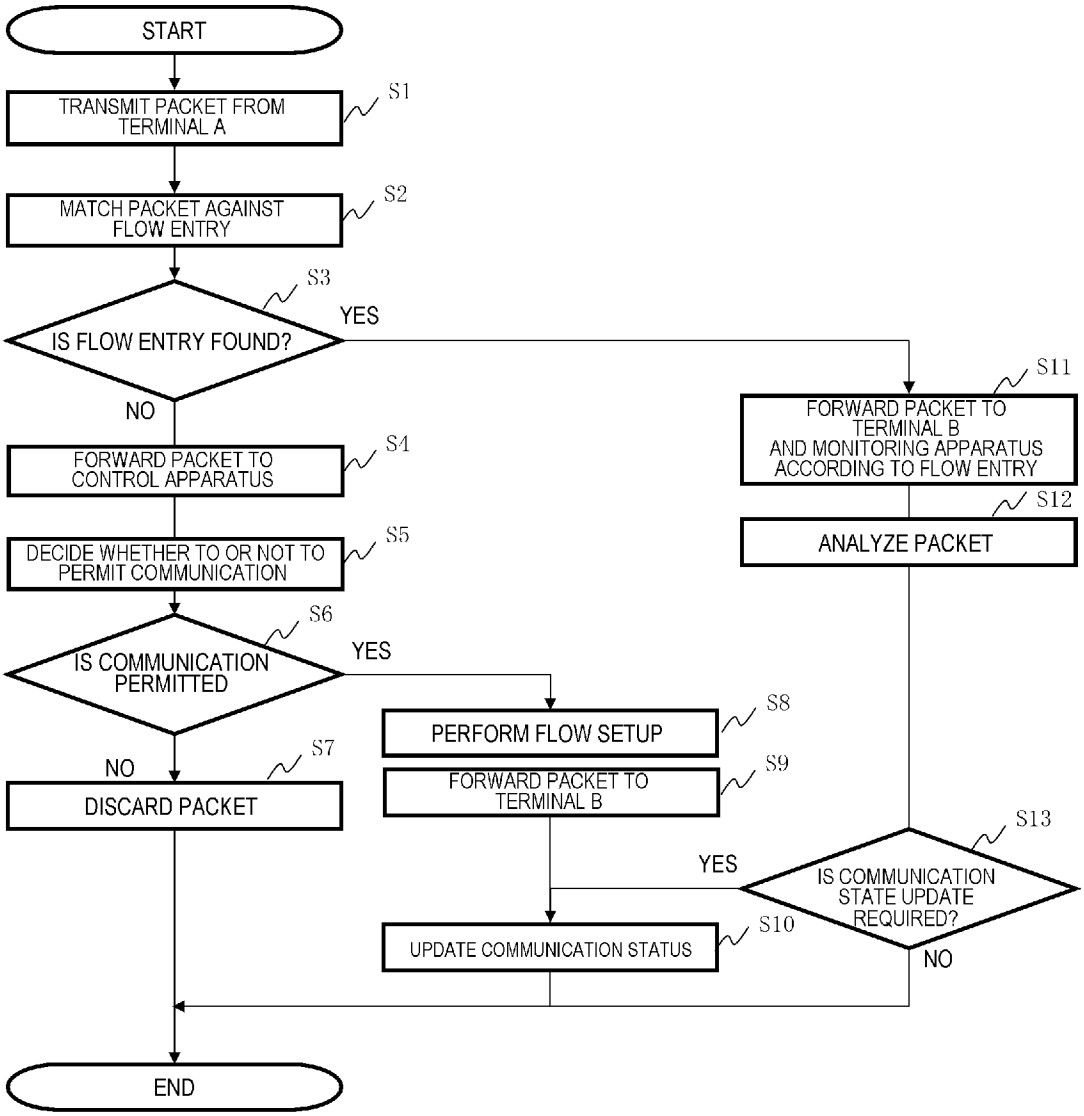
[Fig. 2]


2
MONITORING APPARATUS
1 ; CONTROL APPARATUS
103
COMMUNICATION STATUS HOLDING MEANS
104
FIREWALL RULE
101
COMMUNICATION PERMISSION DECISION MEANS
102
FORWARDING RULE SETTING MEANS
4
NODE

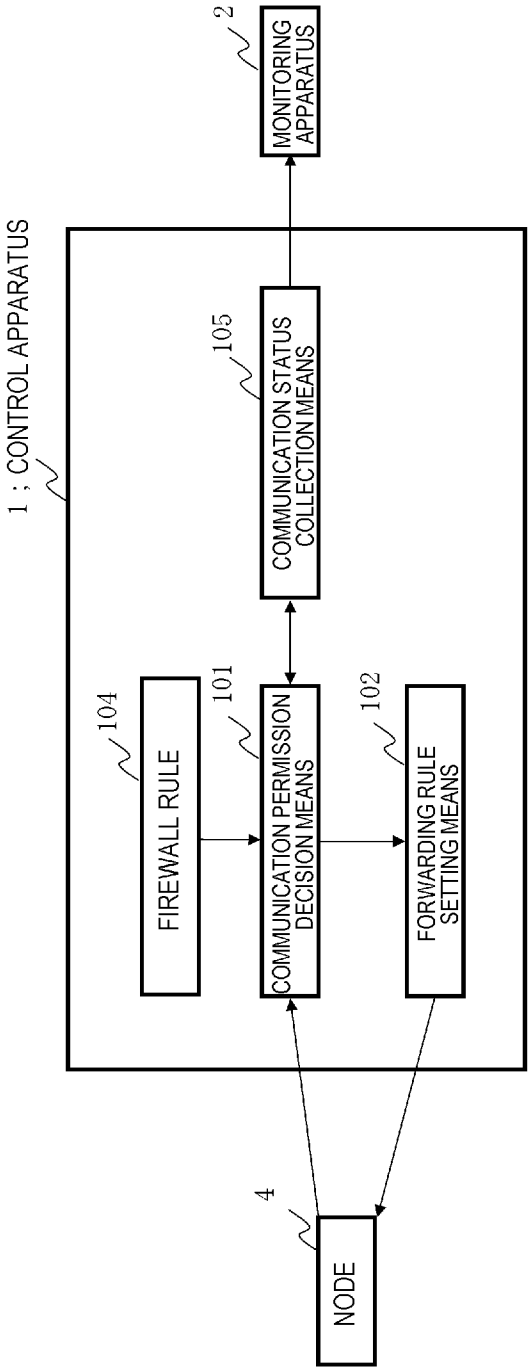
[Fig. 3]


1
CONTROL APPARATUS
2 ; MONITORING APPARATUS
201
PACKET ANALYSIS MEANS
4
NODE

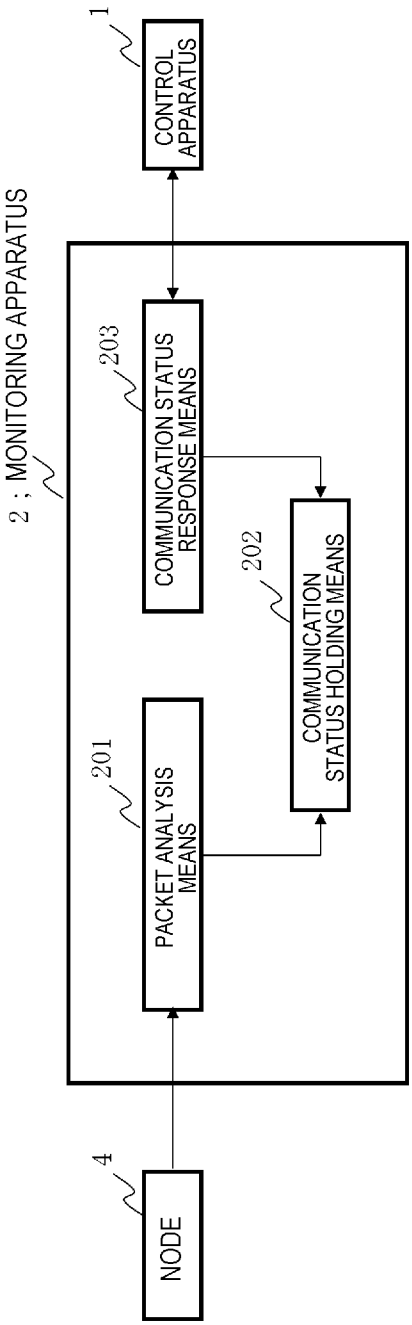
[Fig. 4]


START
TRANSMIT PACKET FROM TERMINAL A
S1
MATCH PACKET AGAINST FLOW ENTRY
S2
IS FLOW ENTRY FOUND?
S3
YES
NO
FORWARD PACKET TO CONTROL APPARATUS
S4
DECIDE WHETHER TO OR NOT TO PERMIT COMMUNICATION
S5
IS COMMUNICATION PERMITTED
S6
YES
NO
DISCARD PACKET
S7
PERFORM FLOW SETUP
S8
FORWARD PACKET TO TERMINAL B
S9
UPDATE COMMUNICATION STATUS
S10
FORWARD PACKET TO TERMINAL B AND MONITORING APPARATUS ACCORDING TO FLOW ENTRY
S11
ANALYZE PACKET
S12
IS COMMUNICATION STATE UPDATE REQUIRED?
S13
YES
NO
END

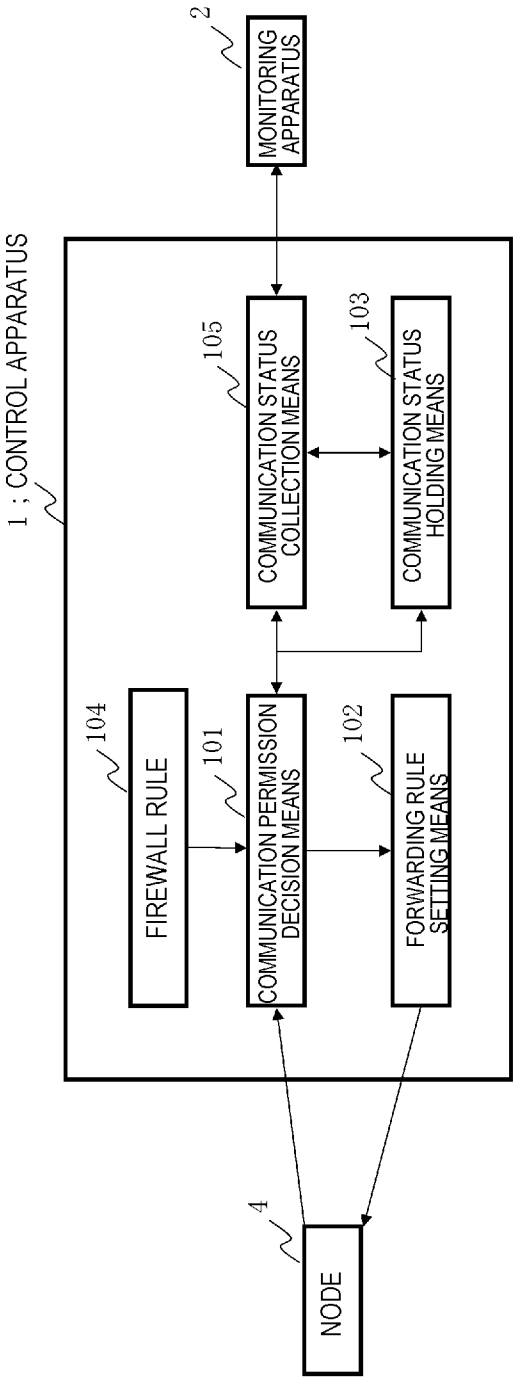
[Fig. 5]


2
MONITORING APPARATUS
1 ; CONTROL APPARATUS
105
COMMUNICATION STATUS COLLECTION MEANS
104
FIREWALL RULE
101
COMMUNICATION PERMISSION DECISION MEANS
102
FORWARDING RULE SETTING MEANS
4
NODE

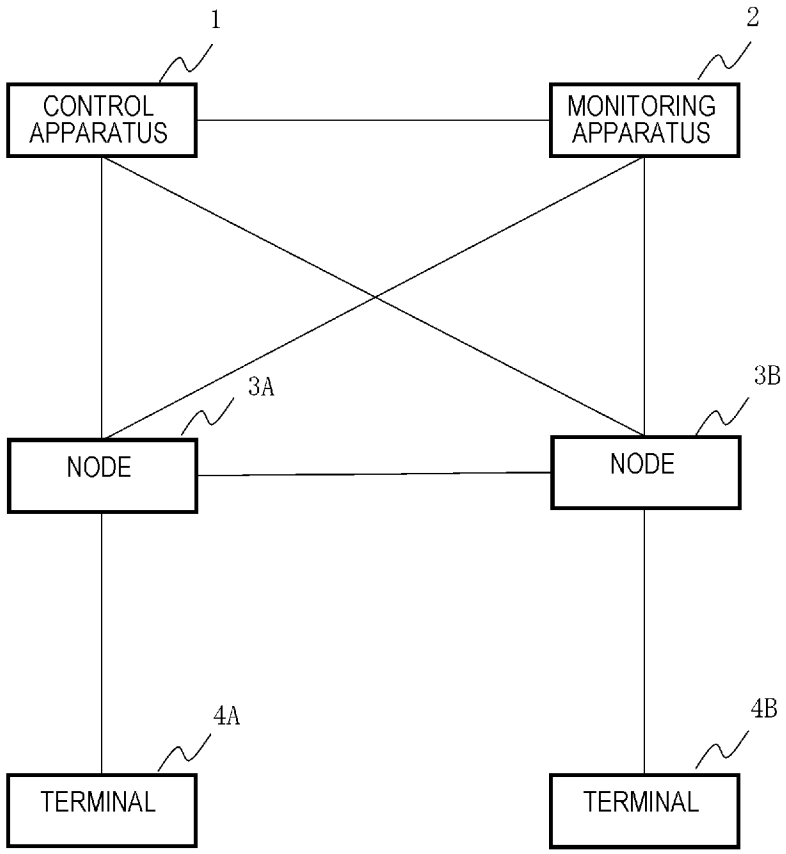
[Fig. 6]


1
CONTROL APPARATUS
2 ; MONITORING APPARATUS
203
COMMUNICATION STATUS RESPONSE MEANS
202
COMMUNICATION STATUS HOLDING MEANS
201
PACKET ANALYSIS MEANS
4
NODE

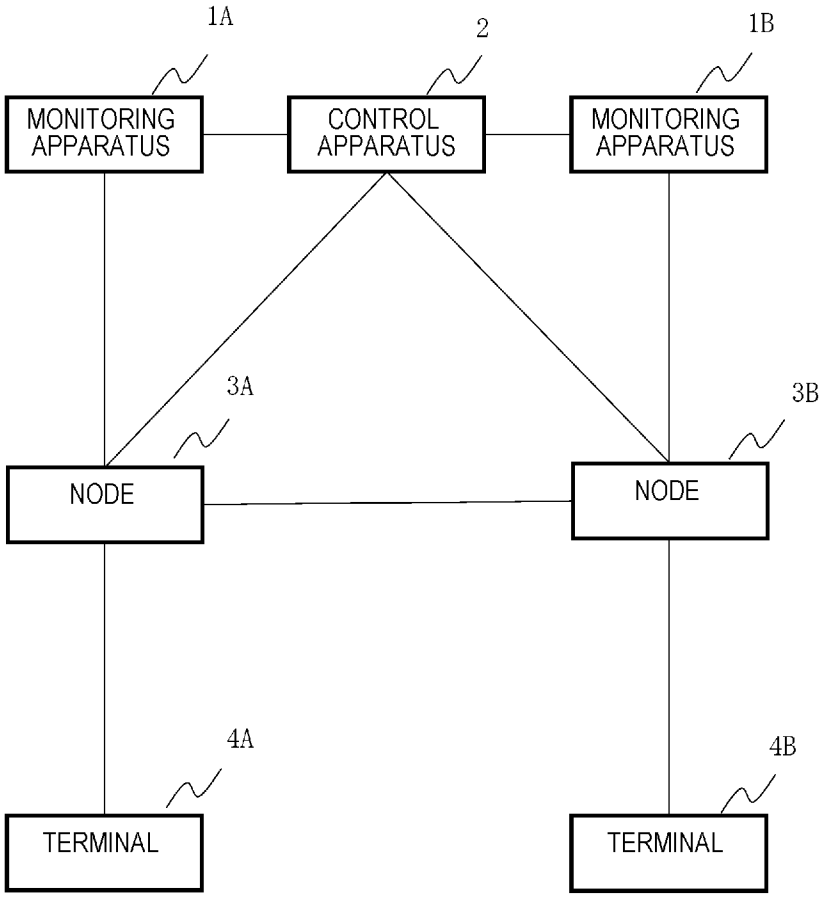
[Fig. 7]


2
MONITORING APPARATUS
1 ; CONTROL APPARATUS
105
COMMUNICATION STATUS COLLECTION MEANS
103
COMMUNICATION STATUS HOLDING MEANS
104
FIREWALL RULE
101
COMMUNICATION PERMISSION DECISION MEANS
102
FORWARDING RULE SETTING MEANS
4
NODE

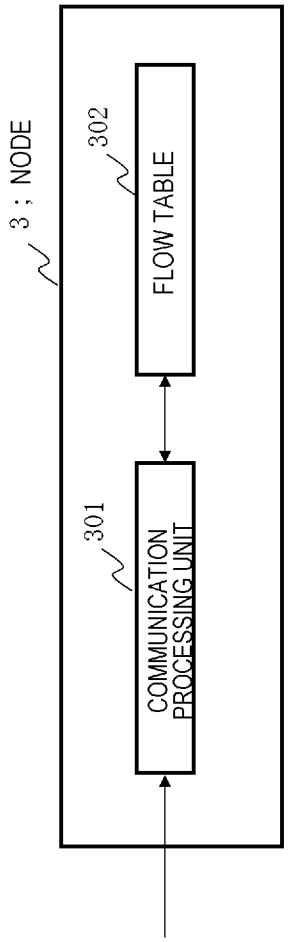
[Fig. 8]


1
2
CONTROL APPARATUS
MONITORING APPARATUS
3A
3B
NODE
NODE
4A
4B
TERMINAL
TERMINAL

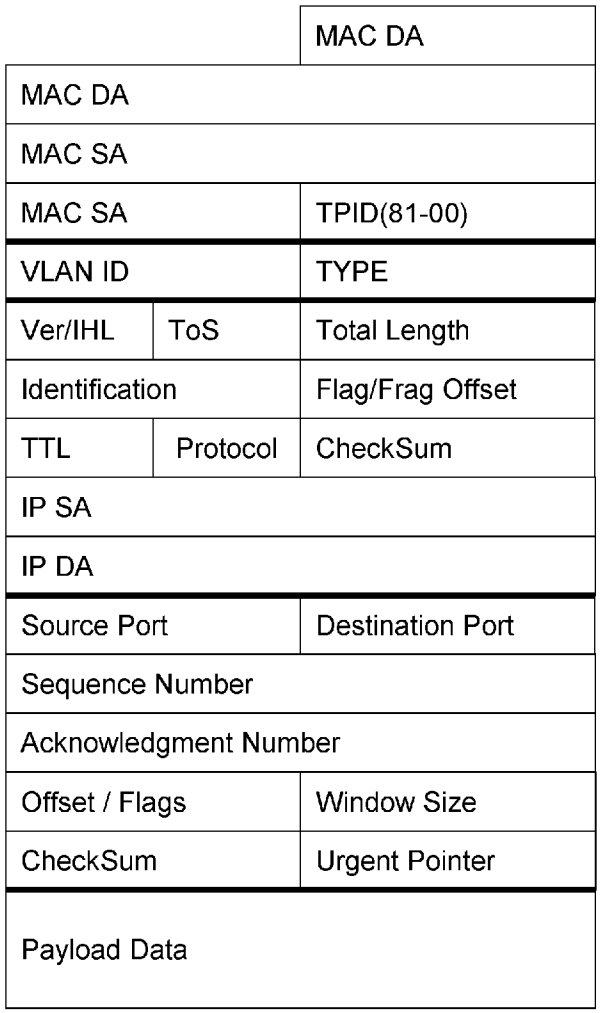
[Fig. 9]


1A
2
1B
MONITORING APPARATUS
CONTROL APPARATUS
MONITORING APPARATUS
3A
3B
NODE
NODE
4A
4B
TERMINAL
TERMINAL

[Fig. 10]



[Fig. 11]


MAC DA
MAC DA
MAC SA
MAC SA
TPID(81-00)
VLAN ID
TYPE
Ver/IHL
ToS
Total Length
Identification
Flag/Frag Offset
TTL
Protocol
CheckSum
IP SA
IP DA
Source Port
Destination Port
Sequence Number
Acknowledgment Number
Offset / Flags
Window Size
CheckSum
Urgent Pointer
Payload Data

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2012/007592

A. CLASSIFICATION OF SUBJECT MATTER

Int.Cl. H04L12/701(2013.01)i, H04L12/66(2006.01)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)

Int.Cl. H04L12/56, H04L12/66

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

Published examined utility model applications of Japan 1922-1996
Published unexamined utility model applications of Japan 1971-2012
Registered utility model specifications of Japan 1996-2012
Published registered utility model applications of Japan 1994-2012

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

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	WO 2011/155510 A1 (NEC CORPORATION) 2011.12.15, [0021]-[0053], figs. 1-8 (family:none)	1-10
Y	WO 2011/065227 A1 (NEC CORPORATION) 2011.06.03, [0034] (family:none)	1-10
A	Aaron Gember, at al., OpenSAFE: Hardware-Based Network Monitoring Using Software Control, opensafe-usenix2011.pdf, [online] University of Wisconsin-Madison, 2011.01.12, [retrieved on 2012-12-17] Retrieved from the Internet: <URL: http://pages.cs.wisc.edu/~bpkroth/papers/>	1-10
A	WO 2012/049960 A1 (NEC CORPORATION) 2012.04.19, [0039], [0130]-[0131] (family:none)	1-10

☑ 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
18.12.2012	25.12.2012

Name and mailing address of the ISA/JP	Authorized officer
Japan Patent Office 3-4-3, Kasumigaseki, Chiyoda-ku, Tokyo 100-8915, Japan	Yuta HAYAMI 5X 3365 Telephone No. +81-3-3581-1101 Ext. 3596

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2012/007592

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP 2010-541426 A (NICIRA NETWORKS) 2010.12.24, [0070] & US 2009/0138577 A1 & EP 2193630 A & WO 2009/042919 A2 & AU 2008304243 A & CA 2700866 A & CN 102217228 A	1-10