

【DESCRIPTION】

【Invention Title】

ACCESS CONTROL SYSTEM IN NETWORK AND METHOD THEREFOR

5 **【Technical Field】**

The present disclosure relates to an access control system and method in a network, and more particularly, to an access control system for controlling access in a network including a plurality of in-home terminals located in different units, and a method thereof.

10 **【Background Art】**

Various functions are being added to wall pads installed in each unit in an apartment complex. As various functions such as cameras are installed in wall pads, the leakage of private information due to hacking of the wall pads has recently become a social problem. Accordingly, a function for controlling access
15 to wall pads of different units in the network of an apartment complex is required. In addition, there is a possibility that wall pads may be hacked through major network equipment such as closed circuit televisions (CCTVs) and parking management systems that always allow communication with the wall pads, and thus, there is a growing need to protect this network equipment from hacking such
20 as theft of Internet protocol (IP) addresses/media access control (MAC) addresses.

Typically, wall pads of the same building in an apartment complex network form a single subnet, and communication between the wall pads within the subnet

is performed through direct communication. In addition, communication between different wall pads is possible through the communication between the subnets. Therefore, in order to protect the wall pads from hacking, access from other subnets as well as access within the same subnet within the apartment complex should be controlled.

Conventionally, an access control list (ACL) or firewall functions provided by security devices such as switches or routers were used to control access between wall pads in an apartment complex network. An ACL technology is a technology that sets filters defined by a source IP address, a destination IP address, a protocol, an application port number, etc., and performs comparative inspection on in-bound or out-bound packets to allow or deny packets. The ACL technology operates to unconditionally deny or pass packets for devices not registered in a white list or a black list, which makes it difficult to manage policies according to changes in the network environment such as network configuration changes and new device registration. In addition, the ACL technology may deny communication between subnets of different buildings within an apartment complex, but it may be difficult to deny direct communication between wall pads within the same building. The communication between the wall pads within the same building belonging to one subnet is performed through an L2 switch belonging to the subnet, not an L3 switch. Therefore, the communication between the wall pads within the same building may not be denied by the ACL function configured in the L3 switch.

In addition, as the number of subnets and nodes configuring a network in

an apartment complex increases, that is, as the number of buildings and units in an apartment complex increases, policy management for access control between wall pads becomes more complicated, and the occurrence rate of failures increases accordingly. In addition, the number of security devices required to
5 configure the access control function also increases, which may cause problems such as increased costs and decreased security policy operation rate.

【Disclosure】

【Technical Problem】

The present disclosure attempts to provide an access control system and
10 method capable of controlling access to in-home terminals such as wall pads installed for each unit in an apartment complex.

【Technical Solution】

According to an exemplary embodiment of the present disclosure, an access control method in a network including a plurality of in-home terminals
15 located in different units may include: transmitting, by a management device, address resolution protocol (ARP) request packets to the plurality of in-home terminals; analyzing, by the management device, first ARP response packets received in response to the ARP request packets to acquire address information of the plurality of in-home terminals; generating, by the management device,
20 second ARP response packets in which a media access control (MAC) address is modified; and modifying, by the management device, the MAC address of each in-home terminal in an ARP table of the plurality of in-home terminals by transmitting the second ARP response packets to the plurality of in-home

terminals. The second ARP response packet may be an ARP response packet that includes an IP address of the in-home terminal whose MAC address is to be modulated in each ARP table and the modulated MAC address as source address information. The modulated MAC address may be an uncommunicable
5 MAC address.

The network may include a policy server that manages an access management policy including a virtual local area network (VLAN) bandwidth allocation policy and a communication permission policy for each of a plurality of subnets to which different network devices are connected, and a plurality of
10 network devices including the plurality of in-home terminals. The access control method may further include: transmitting, by the management device, a third ARP response packet with a modified MAC address to the plurality of network devices to modify the MAC address of a gateway in the ARP table of the plurality of network devices to the MAC address of the management device, receiving, by
15 the management device, a packet transmitted to the gateway from the plurality of network devices, and transmitting and discarding, by the management device, the received packet to the gateway based on the access management policy.

The transmitting or discarding of the received packet to the gateway may include: when the communication between the VLAN bandwidth to which a
20 destination IP address of the received packet belongs and the VLAN bandwidth to which a source IP address of the received packet belongs is prohibited in the communication permission policy, discarding the received packet.

The transmitting or discarding of the received packet to the gateway may

include: when the communication between the VLAN bandwidth to which the destination IP address of the received packet belongs and the VLAN bandwidth to which the source IP address of the received packet belongs is permitted in the communication permission policy, transmitting the received packet to the
5 gateway.

The transmitting or discarding of the received packet to the gateway may include: when the destination IP address of the received packet belongs to an external network of the network, transmitting the received packet to the gateway.

The communication permission policy may be set to prohibit
10 communication between subnets to which the plurality of in-home terminals belong.

The access control method may further include: acquiring, by the management device, address information of the network device that transmits a packet from the received packet; and detecting, by the management device, a
15 new network device by comparing address information acquired from the received packet with the address information managed by the policy server.

The access management policy may further include a policy for determining whether to authorize the new network device. The access control method may further include determining, by the policy server, whether to
20 authorize the new network device based on the access management policy or a control input that is input from a manager, and transmitting, by the management device, a fourth ARP request packet to the new network device for modifying a MAC address of another network device in the ARP table of the new network

device to the uncommunicable MAC address when the new network device is an unauthorized device.

The access control method may further include: transmitting, by the management device, a fifth ARP request packet to the new network device for
5 modifying the MAC address of the gateway in the ARP table of the new network device to the uncommunicable MAC address or the MAC address of the management device when the new network device is the unauthorized device.

The access management policy may further include a denying policy for an address spoofing device. The access control method may further include:
10 detecting, by the management device, an address spoofing device that has spoofed an address of another network device registered in the network by comparing the address information acquired from the received packet with the address information managed by the policy server, and denying, by the management device, the address spoofing device from the network based on the
15 denying policy.

The management device may be connected to an 802.1Q tagged port of an L3 switch.

According to another exemplary embodiment of the present disclosure, an access control system in a network including a plurality of in-home terminals
20 located in different units may include: a management device that transmits address resolution protocol (ARP) request packets to a plurality of in-home terminals, analyzes first ARP response packets received in response to the ARP request packets to acquire address information of the plurality of in-home

terminals, and transmits second ARP response packets with modified media access control (MAC) addresses to the plurality of in-home terminals to modify the MAC addresses of each in-home terminal registered in the ARP table of the plurality of in-home terminals and deny communication between the plurality of in-home terminals. The second ARP response packet may be an ARP response packet that includes an IP address of the in-home terminal whose MAC address is to be modulated in each ARP table and the modulated MAC address as source address information. The modulated MAC address may be an uncommunicable MAC address.

The access control system may further include a policy server that manages an access management policy including a virtual local area network (VLAN) bandwidth allocation policy and a communication permission policy for each of a plurality of subnets constituting the network. The management device may transmit a third ARP response packet with a modified MAC address to the plurality of network devices registered in the network to modify the MAC address of a gateway registered in the ARP table of the plurality of network devices to the MAC address of the management device, and when a packet is received from the plurality of network devices, transmit or discard the received packet to the gateway based on the access management policy, and the plurality of network devices may include the plurality of in-home terminals.

When the communication between the VLAN bandwidth to which a destination IP address of the received packet belongs and the VLAN bandwidth to which a source IP address of the received packet belongs is prohibited in the

communication permission policy, the management device may discard the received packet.

When the communication permission policy prohibits communication between the VLAN bandwidth to which the destination IP address of the received packet belongs and the VLAN bandwidth to which the source IP address of the received packet belongs or the destination IP address of the received packet belongs to an external network of the network, the management device may transmit the received packet to the gateway.

The communication permission policy may be set to prohibit communication between different subnets to which the plurality of in-home terminals belong.

The policy server may manage address information of the plurality of network devices, and the management device may acquire address information of the network device that transmits the packet from the received packet, and detect a new network device by comparing the address information acquired from the received packet with the address information managed by the policy server.

The access management policy may further include a policy for determining whether to authorize the new network device. The policy server may determine whether to authorize the new network device based on the access management policy or a control input that is input from a manager. The management device may transmit a fourth ARP request packet to the new network device for modifying a MAC address of another network device in the ARP table of the new network device to the uncommunicable MAC address when

the new network device is an unauthorized device.

The management device may transmit a fifth ARP request packet to the new network device for modifying the MAC address of the gateway in the ARP table of the new network device to the uncommunicable MAC address or the MAC
5 address of the management device when the new network device is the unauthorized device.

The access management policy may further include a denying policy for an address spoofing device. The management device may detect the address spoofing device that has spoofed an address of another network device
10 registered in the network by comparing the address information acquired from the received packet with the address information managed by the policy server, and denies the address spoofing device from the network based on the denying policy.

The management device may be connected to an 802.1Q tagged port of an L3 switch.

15 **【Advantageous Effects】**

According to the present disclosure, it is possible to effectively deny illegal access to home terminals such as wall pads installed for each unit in an apartment complex.

【Description of the Drawings】

20 FIG. 1 is a diagram schematically illustrating a network in an apartment complex according to an exemplary embodiment.

FIG. 2 is a diagram schematically illustrating an access control system according to an exemplary embodiment.

FIG. 3 is a diagram schematically illustrating an access control method in a network according to an exemplary embodiment.

FIG. 4 is a diagram schematically illustrating a method for denying access by an address spoofing device in a network according to an exemplary
5 embodiment.

【Mode for Invention】

Hereafter, embodiments of the present disclosure will be described in detail with reference to the accompanying drawings and the same or similar components are given the same reference numerals and are not repeatedly
10 described. The suffix "module" and/or "unit" for components used in the following description is given or mixed in consideration of only the ease of writing of the specification, and therefore, do not have meanings or roles that distinguish from each other in themselves. In addition, when it is determined that a detailed description for the known art related to embodiments disclosed in the present
15 specification may obscure the gist of the embodiments disclosed in present specification, the detailed description will be omitted. Further, it should be understood that the accompanying drawings are provided only in order to allow exemplary embodiments of the present disclosure to be easily understood, and the spirit of the present disclosure is not limited by the accompanying drawings,
20 but includes all the modifications, equivalents, and substitutions included in the spirit and the scope of the present disclosure.

Terms including an ordinal number such as first, second, etc., may be used to describe various components, but the components are not limited to

these terms. The above terms are used solely for the purpose of distinguishing one component from another.

Singular forms are to include plural forms unless the context clearly indicates otherwise.

5 It will be further understood that terms "include" or "have" used in the present specification specify the presence of features, numerals, steps, operations, components, parts mentioned in the present specification, or combinations thereof, but do not preclude the presence or addition of one or more other features, numerals, steps, operations, components, parts, or combinations
10 thereof.

FIG. 1 is a diagram schematically illustrating a network in an apartment complex according to an exemplary embodiment.

Referring to FIG. 1, packets transmitted and received to and from an external network (Internet) in an apartment complex network 1 pass through a
15 firewall 11 and an L3 switch 12. The firewall 11 is responsible for the security of the network 1 and may perform the function of denying harmful traffic entering or leaving the network. The L3 switch 12 may operate as a backbone switch located at a center of nodes that want to connect to the Internet in the network 1. In this case, all packets transmitted and received between the network 1 and the
20 Internet pass through the L3 switch 12. The L3 switch 12 may also operate as a gateway of the network 1. The gateway may transmit packets between the Internet and the network 1, or between subnets that constitute the network 1, based on destination IP addresses included in each packet.

The network 1 may include at least one subnet 20.

In the network 1 within an apartment complex, each subnet 20 may include at least one L2 switch 21 that supports communication between in-home terminals 22 located in the same building and communication between the in-home terminals 22. The communication between the in-home terminals 22 belonging to the same subnet 20, that is, the in-home terminals 22 belonging to the same building, may correspond to direct communication via the L2 switch 21. The communication between the in-home terminals 22 belonging to different subnets 20, that is, the in-home terminals 22 belonging to different buildings, may correspond to the communication between subnets 20 via the gateway of the L3 switch 12. The in-home terminal 22 is a network device located within each unit, and may perform various functions such as providing information within the apartment complex/unit, controlling equipment within the apartment complex/unit, and calling. The in-home terminal 22 may include, for example, a video phone, a door phone, a wall pad, etc.

In addition to the in-home terminal 22, the network 1 may include various public systems (for example, CCTV 31, parking management system 32, complex entrance door 33, common front door 34, etc.) managed through the network 1 within the apartment complex. The network 1 may further include various servers located within the apartment complex, such as a complex server 41 and a call server 42.

In the network 1, the public systems (for example, CCTV 31, parking management system 32, complex entrance door 33, common front door 34, etc.)

and various servers (for example, complex server 41, call server 42, etc.) may form at least one of subnets 30 and 40. Each subnet 20, 30, and 40 in the network 1 may be divided into a virtual local area network (VLAN) band. That is, different VLAN bandwidths may be allocated to the subnets 20, 30, and 40.

5 Hereinafter, for convenience of description, the in-home terminal 22, public system (CCTV 31, parking management system 32, complex entrance door 33, common front door 34, etc.), and server (complex server 41, call server 42, etc.) belonging to the network 1 may be collectively referred to as 'network devices'.

10 The network 1 may further include a policy server 43 and a management device 13 to deny illegal access to the network devices belonging to the network 1.

FIG. 2 schematically illustrates an access control system for controlling access to a network device in the network 1 in an apartment complex according to an exemplary embodiment.

15 Referring to FIG. 2, the access control system 100 may include the L3 switch 12, the management device 13, and the policy server 43 of FIG. 1 described above.

 The management device 13 and the policy server 43 are connected to the L3 switch 12 and may communicate with each other through the L3 switch 12.

20 The policy server 43 may perform a function of setting and managing a policy (access management policy) for network access in the network 1 and the device information of network devices.

The policy server 43 may include a database 431 and a policy management unit 432.

The database 431 may store policy (access management policy) information for connection authentication, authorization, account operations, etc.,
5 for network access in the network 1. The access management policy may include a VLAN bandwidth (or subnet bandwidth) allocation policy, a communication permission policy (a communication permission policy for each VLAN bandwidth, a communication permission policy between VLAN bandwidths) for each subnet 20, 30, and 40 that constitutes the network 1. For example, the
10 communication permission policy may be set so that the communication is denied between different subnets 20 to which the in-home terminals 22 belong, and the communication is allowed between the subnet 20 to which the in-home terminals 22 belong and the subnet 30 to which the parking management system 32 belongs. The access management policy may further include a policy for
15 determining whether to authorize a network device attempting to newly connect to the network 1, a denying policy for devices that are not authorized by the network 1 or that have spoofed an address of another network device, etc.

The database 431 may further include the device information of each network device registered in the network 1. The device information may include
20 address information (IP address and MAC address), status information (online/offline), authentication information (authorized/unauthorized), and whether to deny, etc., of each network device.

The policy management unit 432 may set and manage policy information

stored in the database 431. The policy management unit 432 may set and manage policy information based on control input received from a manager.

The policy management unit 432 may also set and manage the device information stored in the database 431. The policy management unit 432 may
5 receive address information, status information, etc., of each network device from the management device 13, and set and manage the device information based on the received information.

When the detection of a new network device is notified by the management device 13, the policy management unit 432 may determine whether
10 to authorize the new network device based on the information of the new network device received from the management device 13. The policy management unit 432 may determine whether to authorize the new network device based on the policy information stored in the database 431. The policy management unit 432 may notify a manager of a detection of a new network device, and may determine
15 whether to authorize the network device based on the control input received from the manager thereafter.

The policy management unit 432 may also transmit the corresponding authorization information to the management device 13 when it is determined whether to authorize the new network device.

20 The management device 13 may control access to the network 1 using address resolution protocol (ARP) packet modulation and packet forwarding.

The management device 13 may include a storage unit 131, a transceiver unit 132, and a control unit 133.

The storage unit 131 may store various types of information, data, etc., processed by the management device 13. The storage unit 131 may store information (policy information, the device information, etc.) received from the policy server 43. The storage unit 131 may store address information, status
5 information, etc., of each network device acquired by the control unit 133 described later. The storage unit 131 may also temporarily store packets transmitted and received through the transceiver 132.

The transceiver 132 may transmit and receive information, packets, etc., between other devices belonging to the network 1 and the management device
10 13.

The transceiver 132 may receive the policy information, the device information, etc., from the policy server 43. The transceiver 132 may notify the policy server 43 of the occurrence of an event, and may also transmit the status information, the address information, etc., of the network device acquired by the
15 management device 13 to the policy server 43.

The transceiver 132 may collect packets (ARP packets, user datagram protocol (UDP)) packets, transmission control protocol (TCP) packets, etc.) transmitted through the L3 switch 12 within the network 1. The transceiver 132 may be connected to an 802.1Q tagged port (or trunk port) of the L3 switch 12.
20 The 802.1Q tagged port of the L3 switch 12 is a port through which the plurality of VLAN bandwidth traffic passes. As described above, different VLAN bandwidths may be allocated to each subnet 20, 30, and 40 of the network 1. Therefore, in order for the management device 13 to collect packets of all the

subnets 20, 30, and 40 transmitted through the L3 switch 12, it should be able to access all the VLAN bandwidths allocated to the subnets 20, 30, and 40, and for this purpose, the transceiver 132 may be connected to the 802.1Q tagged port of the L3 switch 12.

5 The transceiver 132 may also transmit and receive ARP packets (ARP request packets, ARP response packets, etc.) to and from each network device (e.g., in-home terminal 22) connected to the network 1.

 The transceiver 132 may also forward packets received from other network devices to the gateway (e.g., L3 switch 12 performing a gateway
10 function).

 The control unit 133 may control the overall operation of the management device 13.

 When the operation of the management device 13 is initiated, the control unit 133 may receive the policy information, the device information of network
15 devices, etc., from the policy server 43 and store the received policy information and device information in the storage unit 131.

 In addition, the control unit 133 may transmit an ARP request packet for each VLAN bandwidth (subnet band) to acquire information (address information, status information, etc.) of network devices connected to each VLAN bandwidth
20 (subnet bandwidth).

 The control unit 133 may broadcast an ARP request packet including the IP address of the network device for which the information is to be confirmed as destination address information to the subnet to which the network device

belongs. Then, the control unit 133 may determine the status information of the corresponding network device based on whether an ARP response packet is received for the transmitted ARP request packet. That is, when the control unit 133 does not receive the ARP response packet from the corresponding network device within a predetermined time after transmitting the ARP request packet at least once during a predetermined time, the control unit 133 may determine that the corresponding network device is in an offline state. When the control unit 133 receives the ARP response packet from the corresponding network device within a predetermined time after transmitting the ARP request packet, the control unit 133 may determine that the corresponding network device is in an online state. When the status of each network device is determined to be online or offline, the control unit 133 may set the status information of each network device based on the determined status and store the status information in the storage unit 131. Here, the online state may indicate a state in which the connection between the corresponding network device and the network 1 is activated, and the offline state may indicate a state in which the connection between the corresponding network device and the network 1 is deactivated.

When the control unit 133 acquires the status information, it may compare the status information with the previous status information of the corresponding network device to detect a status change event. Here, the previous status information of the corresponding network device may be acquired from the device information of the corresponding network device received from the policy server 43 or the previous status information of the corresponding network device stored

in the storage unit 131. When the control unit 133 detects that the network device has changed its status from the offline state to the online state or from the online state to the offline state, it may determine that the status change event has occurred for the corresponding network device. When the control unit 133
5 detects that the status change event has occurred in at least one network device, it may notify the policy server 43 of the occurrence of the status change event. In addition, the control unit 133 may transmit the updated status information to the policy server 43 so as to update the device information stored in the policy server 43.

10 The control unit 133 may analyze the received ARP response packet after transmitting the ARP request packet to the network devices and, when the ARP response packet is received, acquire the address information (IP address and MAC address) of each network device. The network device that has confirmed its IP address from the destination address information of the ARP request packet
15 transmitted from the management device 13 may transmit the ARP response packet that includes its IP address and MAC address as the source address information. Accordingly, when the control unit 133 receives the ARP response packet, it may acquire the address information (IP address and MAC address) of the corresponding network device from the source address information (source
20 IP address and source MAC address) included in the response packet.

The control unit 133 may collect the status information and the address information of the in-home terminals 22 installed in each unit in the apartment complex in the above-described manner, and may also confirm which subnet 20

(VLAN band) each in-home terminal 22 belongs to.

The control unit 133 may identify the in-home terminals 22 connected to each subnet 20 based on the information collected in the above-described manner, and deny the communication between the in-home terminals 22 of different units belonging to the same subnet 20 by using the ARP packet modulation.

The control unit 133 may generate the modulated ARP response packets for modulating the MAC addresses in the ARP table of each in-home terminal 22 based on the address information of each in-home terminal 22. Each modulated ARP response packet may include the IP address of the in-home terminal 22 that is the target of the MAC address modulation and the modulated MAC address as the source address information. The modulated MAC address may be a meaningless MAC address that is not suitable for communication.

When the modulated ARP response packet is generated, the control unit 133 may transmit the generated ARP response packet to the subnet 20 to which the in-home terminal 22 that is the target of the MAC address modulation belongs. Accordingly, other in-home terminals 22 in the same subnet 20 that receive the modified ARP response packet may update their stored ARP tables based on the source address information included in the received ARP response packet. That is, each in-home terminal 22 that receives the modified ARP response packet may acquire the source IP address and the source MAC address from the received ARP response packet, and change the MAC address corresponding to the source IP address in its ARP table to the source MAC address.

The ARP table of each network device may include the address information (IP address and MAC address) of the network devices belonging to the same broadcast domain (e.g., subnet) as the network device and the address information (IP address and MAC address) of the gateway to which the network device is connected. Each in-home terminal 22 refers to the address information of the other in-home terminal 22 stored in this ARP table in order to communicate with other in-home terminals 22 belonging to the same subnet 20. Therefore, when the MAC addresses of the ARP table that the home terminals 22 belonging to the same subnet 20 is referenced to communicate with other home terminals 22 are modified to the uncommunicable MAC addresses, the home terminals 22 may not know the correct MAC addresses of other home terminals 22 belonging to the same subnet 20, so the direct communication with other home terminals 22 becomes impossible.

The control unit 133 may also control the access between the network devices belonging to different subnets by using the ARP packet modification and packet forwarding.

The control unit 133 may generate the modified ARP response packet to modify the MAC address of the gateway (e.g., L3 switch 12) to the MAC address of the management device 13 for each subnet requiring the access control, and transmit the modified ARP response packet to each subnet. The modified ARP response packet may include the IP address of the gateway (L3 switch 12) and the MAC address of the management device 13 as the source address information. Each network device that receives the MAC address may update

the MAC address of the gateway to the MAC address of the management device 13 in the ARP table stored in the network device. Accordingly, when a specific network device transmits a packet destined for the outside of its subnet (an external network of another subnet or network 1), it may be transmitted to the management device 13 rather than the gateway of the L3 switch 12. That is, when each network device transmits a packet to the outside of the subnet (the Internet or another subnet) to which it belongs, the control unit 133 may receive the transmitted packet instead of the gateway.

When the control unit 133 receives a packet instead of the gateway, it may confirm the source subnet and destination subnet of the received packet based on the source IP address and destination IP address of the received packet. In addition, the control unit 133 may confirm whether the access from the source subnet to the destination subnet is permitted based on the policy information (communication permission policy between VLAN bandwidths (or subnet bandwidths)) received from the policy server 43. When the access from the source subnet to the destination subnet is prohibited in the communication permission policy, the control unit 133 may deny the access by discarding the packet without forwarding the packet. For example, this case applies when the in-home terminal 22 transmits a packet to access the in-home terminal 22 belonging to a different building (different subnet 20), and in this case, the packet transmitted from the in-home terminal 22 may be discarded and may be denied from being transmitted. The control unit 133 may forward the packet to the gateway (L3 switch 12) so that the packet is normally transmitted to the

destination when the access from the source subnet to the destination subnet is permitted in the communication permission policy. For example, this case applies when the home terminal 22 transmits the packet to access the network device commonly used in the apartment complex (e.g., CCTV 31, parking management system 32, complex entrance door 33, common front door 34, etc.). In this case, the packet transmitted from the home terminal 22 is forwarded to the gateway so that it is normally transmitted to the destination.

The control unit 133 may forward the packet to the gateway (L3 switch 12) so that the packet is normally transmitted even if the received packet is the packet transmitted to an external network of the network 1.

When the packet is forwarded from the management device 13, the gateway (L3 switch 12) may confirm the destination address of the forwarded packet and transmit the packet to the destination subnet or the external network.

The control unit 133 may continuously analyze the packets received from network devices and update the status information of each network device. When the packet is received, the control unit 133 may confirm whether the network device that has transmitted the corresponding packet is the network device previously registered in the policy server 43 based on the source address information of the received packet. When the network device that has transmitted the packet is the previously registered network device, the control unit 133 may confirm that the network device is in the online state. In addition, when the control unit 133 identifies a network device, which has not transmitted a packet for a predetermined period of time, among the network devices (i.e.,

network devices whose address information is registered in the device information of the policy server 43) registered in the policy server 43, the control unit 133 may confirm the status of the network device using the ARP packet as described above. That is, the control unit 133 may transmit the ARP request
5 packet to confirm the status of the corresponding network device, and confirm the status of the corresponding network device based on whether the ARP response packet thereto is received.

The control unit 133 may continuously analyze the packets received from network devices to detect new network devices attempting to newly connect to
10 the network 1. When the packet is received from the network device, the control unit 133 may acquire the source address information (source IP address and source MAC address) from the received packet and compare the source address information with the address information of the previously registered network devices to determine whether the network device that has transmitted the packet
15 is a new device. When the control unit 133 does not search for the same address information as the source address information acquired from the received packet among the address information of the previously registered network devices, the control unit 133 may determine that the network device that has transmitted the packet is a new device newly connected to the network 1.
20 When the control unit 133 determines that the network device that has transmitted the packet is a new device, it may notify the policy server 43 of the occurrence of a new device detection event and transmit the address information (IP address and MAC address) of the network device to the policy server 43.

When the detection of the new network device is notified from the management device 13, the policy server 43 may determine whether to authorize the new network device based on the access management policy or the control input received from the manager. When the new network device is authorized,
5 the policy server 43 may register the new network device in the network 1 and include the address information of the new network device in the device information in the database 431. In addition, the policy server 43 may transmit the information indicating whether the new network device is authorized to the management device 13.

10 When the control unit 133 receives the authorization information (authorized/unauthorized) for the new network device from the policy server 43, it may deny the access of the new network device to the network 1 depending on whether the new network device is authorized. When the new network device is the unauthorized device, the control unit 133 may use the modified ARP
15 response packet to modify the MAC address of the network devices belonging to the same subnet as the unauthorized network device to a meaningless MAC address that is impossible to communicate with in the ARP table of the unauthorized network device. That is, the control unit 133 may generate the modified ARP response packet for modifying the MAC addresses of each network
20 device belonging to the same subnet as the unauthorized network device to meaningless addresses, and transmit the modified ARP response packet to the subnet to which the unauthorized network device belongs. The unauthorized network device that receives the modified ARP response packet updates its ARP

table based on the address information acquired from the modified ARP response packet, so the unauthorized network device may not confirm the correct MAC address of the network device.

The control unit 133 may also deny the unauthorized network device from
5 accessing the network device outside the subnet to which it belongs by modifying the MAC address of the gateway to the meaningless address in the ARP table of the unauthorized network device. That is, the control unit 133 may transmit the ARP response packet for changing the MAC address of the gateway (e.g., L3 switch 12) to the meaningless MAC address, thereby modifying the MAC address
10 of the gateway to the meaningless MAC address in the ARP table of the unauthorized network device. Accordingly, the unauthorized network device may be denied from communicating not only with other network devices in the subnet to which it belongs, but also with network devices in other subnets that should be accessed through the gateway.

15 The control unit 133 may also deny the unauthorized network devices from accessing other network devices by using the packet forwarding method described above. When the unauthorized network device is detected, the control unit 133 may transmit the ARP response packet for modifying the MAC address of the gateway to the MAC address of the management device 13 in the
20 ARP table of the unauthorized network device to the subnet to which the unauthorized network device belongs. Accordingly, the MAC address of the gateway in the ARP table in the unauthorized network device is modified to the MAC address of the management device 13, and the packets transmitted by the

unauthorized network device may be transmitted to the management device 13 instead of the gateway. Since the management device 13 already knows that the network device is the unauthorized device, when the packet is received from the unauthorized network device, it may discard the packet and deny the communication of the unauthorized network device.

The control unit 133 may also analyze the received packets to confirm whether the address of the network device has been spoofing (IP address spoofing, MAC address spoofing, IP address and MAC address spoofing).

When the packet is received, the control unit 133 may compare the source address information of the received packet with the address information of devices registered in the policy server 43 to detect the network device that has spoofed the IP address or the MAC address. The control unit 133 may determine that the network device that has transmitted the packet has spoofed the IP address when the source address information extracted from the collected packet has the same IP address as the network device previously registered in the policy server 43 but has different MAC addresses. In addition, the control unit 133 may determine that the network device that has transmitted the packet has spoofed the MAC address when the source address information extracted from the collected packet has the same MAC address as the network device previously registered in the policy server 43 but has different IP addresses.

The control unit 133 may also detect the network devices that have spoofed the IP and MAC addresses by analyzing ARP probe packets transmitted from each network device.

In RFC 5227 which is a proposed standard for IPv4 address conflict detection, the ARP probe packets are specified. In ACD, the ARP probe packet is a packet used when a host confirms whether its IP address is already in use within the network to which it belongs, and is used for the purpose of preventing the IP conflict. The host sets an ARP Opcode to 1 to broadcast the ARP probe packet set as an ARP request within the network to which it belongs, and waits for the reception of the response packet (packet with an ARP Opcode of 2). When transmitting the ARP probe packet (ARP request), the host may set a source MAC address of a header to its own MAC address and set a source IP address to 0.0.0.0. In addition, the host may set the destination MAC address of the ARP probe packet header to 00:00:00:00:00:00 and the destination IP address to its own IP address. This ARP probe packet does not update the ARP tables of other hosts belonging to the same network to prevent the IP address conflicts.

In the network 1, each network device (host) operates to repeatedly broadcast the ARP probe packets when its IP address changes. Therefore, the spoofing device that copies address data of another network device and changes its own IP address and MAC address broadcasts the ARP probe packets within the network to which the copied IP address belongs. As described above, the ARP probe packet (ARP request) transmitted from each network device (host) may include the IP address and MAC address of the network device that has transmitted it. Therefore, when the control unit 133 receives the ARP probe packet transmitted as the ARP request from the network device, the control unit

133 may detect the IP address and MAC address of the corresponding network device from the received ARP probe packet. In addition, the control unit 133 may compare the detected IP address and MAC address with the address information registered in the policy server 43 to determine whether the device is
5 the spoofing device that copies and uses the IP address and MAC address of another network device.

In addition to when the IP address changes, each network device may also transmit the ARP probe packet in situations such as when the network interface switches from an inactive state to an active state, when the network
10 device returns from a power-saving mode to a normal mode, when the change occurs in the link status with the network 1 (e.g., connection status of an Ethernet cable), or when an 802.11 wireless interface is related to a new base station. In other words, the normal network device, not the spoofing device, may also repeatedly broadcast the ARP probe packet when its connection to the network
15 switches from the offline state to the online state.

Therefore, the control unit 133 may additionally confirm the status information of the network device that has transmitted the ARP probe packet in order to prevent the normal network device from being mistakenly recognized as the spoofing device. When the control unit 133 has previously registered the
20 same address information as the newly collected address information through the ARP probe packet in the policy server 43, the control unit 133 may additionally confirm the status information before receiving the ARP probe packet of the corresponding network device to make a final decision on whether the address

has been spoofed. That is, when the status information of the corresponding network device indicates the offline state before receiving the ARP probe packet, the control unit 133 may determine that the received ARP probe packet was received from the normal device whose connection status with the network 1 has
5 been switched to the online state, and may finally determine the corresponding network device as the normal network device instead of the spoofing device.

As described above, when the control unit 133 confirms that the device has spoofed address information of another network device, the control unit 133 may notify the policy server 43 of the occurrence of an address spoofing event.

10 In addition, based on the policy information received from the policy server 43, it is possible to deny the access of the detected spoofing device to the network 1. For example, when the spoofing device is detected, the control unit 133 may deny the network use of the spoofing device by transmitting the network use denying packet (ARP probe packet response packet (ARP probe reply packet)).

15 In the case of the public systems such as the CCTV 31 and the parking management systems 32, they are usually maintained in the online state for 24 hours a day, 365 days a year, and permits the communication with the home terminal 22 and the server in the apartment complex is always permitted. Therefore, when someone spoofs the address of such a public system for
20 malicious purposes, illegal access to other network devices may be possible. In the network 1, the management device 13 detects such illegal address spoofing and denies the spoofing device from accessing other network devices in advance, thereby denying attempts to infiltrate the network 1 by spoofing the address of

the public system.

Hereinafter, with reference to FIGS. 3 and 4, an access control method in a network 1 within an apartment complex will be described.

FIG. 3 schematically illustrates a method for controlling access between
5 network devices in the network 1 according to an exemplary embodiment. The method of FIG. 3 may be performed by an access control system 100 described with reference to FIG. 2.

Referring to FIG. 3, when the management device 13 starts an operation, the management device 13 may acquire the status information and address
10 information of each network device registered in the network 1 (S11).

In step S11, the management device 13 may acquire the status information and address information of each network device by transmitting the ARP request packet. The management device 13 may generate the ARP request packet including the IP address of the corresponding network device as
15 the destination address information for each network device, and transmit the ARP request packet to the subnet to which the corresponding network device belongs. Then, the control unit 133 may determine the status information of the corresponding network device based on whether an ARP response packet is received for the transmitted ARP request packet. In addition, when the
20 management device 13 transmits the ARP request packet to the network devices and the ARP response packet is received, the management device 13 may acquire the address information (IP address and MAC address) of each network device from the source address information of the received ARP response packet.

When the status information and address information of each network device are confirmed, the management device 13 may use the ARP packet to modify the MAC addresses of the network device and gateway that require the access control in the ARP table of each network device (S12).

5 In step S12, the management device 13 may modify the MAC address of another in-home terminal 22 in the ARP table of each in-home terminal 22 to the meaningless address in order to deny the communication between the in-home terminals 22. To this end, the management device 13 may generate the modified ARP response packet for modifying the MAC address of each in-home
10 terminal 22 in the ARP table. Each modified ARP response packet may include the IP address of the corresponding in-home terminal 22 and the modified MAC address (MAC address unsuitable for communication) as the source address information. The management device 13 may transmit the ARP response packet thus generated to the subnet 20 to which the corresponding in-home
15 terminal 22 belongs. Accordingly, the corresponding MAC address in the ARP table of the in-home terminals 22 belonging to the corresponding subnet 20 may be modified to the MAC address that is incapable of communication, so that access by other in-home terminals to the corresponding in-home terminal 22 may be denied. In this way, the management device 13 may deny all direct
20 communication between the in-home terminals 22 by changing all the MAC addresses of other in-home terminals to addresses that are incapable of the communication in the ARP table of each in-home terminal 22.

In step S12, the management device 13 may modify the MAC address of

the gateway in the ARP table of each network device 22 to the MAC address of the management device 13 in order to restrict the access between different subnets 20, 30, and 40. To this end, the management device 13 may transmit the modified ARP response packet including the IP address of the actual gateway
5 (IP address of the L3 switch 12) and the MAC address of the management device 13 as the source address information to the subnet to which each network device belongs. Accordingly, the MAC address of the gateway in the ARP table of each network device may be modified to the MAC address of the management device 13. Accordingly, when each network device wants to transmit the packet outside
10 the subnet to which it belongs, it transmits the packet by referencing the MAC address of the management device 13 instead of the gateway, and the transmitted packet may be received by the management device 13 instead of the gateway.

After modifying the MAC address of the gateway in the ARP table, the
15 management device 13 may receive the packets transmitted by network devices belonging to each subnet to another network (e.g., another subnet) instead of the gateway (S13).

When the packet is received, the management device 13 may analyze the packet to determine whether the network device that has transmitted the
20 packet, i.e., the source of the packet, is a new network device (S14).

In step S14, the management device 13 may acquire the source address information (source IP address and source MAC address) from the received packet and compare the source address information with the address information

of the network devices previously registered in the policy server 43. When the same address information as the source address information acquired from the received packet is not detected among the address information of the registered network devices, the management device 13 may determine that the source of the packet is a new device newly connected to the network 1. When the management device 13 searches for the same address information as the source address information acquired from the received packet among the address information of the previously registered network devices, the management device 13 may determine that the source of the packet is the network device previously registered in the network 1.

When the management device 13 confirms through step S14 that the packet source is the network device previously registered in the network 1, the management device 13 may determine whether to deny the received packet based on the access management policy received from the policy server 43 (S15).

In step S15, the management device 13 may extract the source IP address and the destination IP address from the received packet, and confirm whether the communication permission policy between the VLAN bandwidths (or subnet bandwidths) is set to allow the communication between the subnet to which the source IP address belongs and the subnet to which the destination IP address belongs. When the communication permission policy prohibits the communication between the VLAN bandwidth (subnet bandwidth) to which the source IP address belongs and the VLAN bandwidth (subnet bandwidth) to which the destination IP address belongs (for example, when the home terminal 22

attempts to connect to the home terminal 22 belonging to a different building (different subnet 20)), the management device 13 may determine that the packet needs to be denied. On the other hand, when the management device 13 allows the communication between the VLAN bandwidth (subnet bandwidth) to which the source IP address belongs and the VLAN bandwidth (subnet bandwidth) to which the destination IP address belongs in the communication permission policy (for example, when the home terminal 22 attempts to connect to the network device commonly used in the apartment complex (for example, CCTV 31, parking management system 32, complex entrance door 33, common front door 34, etc.), the management device 13 may determine that there is no need to deny the packet.

When the management device 13 requires the denying of the packet by the policy (S16), the management device 13 may discard the packet to deny the communication (S17). On the other hand, when the management device 13 does not require the denying of the packet (S16), it may forward the packet to an actual gateway (for example, L3 switch 12) (S18) so that the packet is normally transmitted to the destination.

When the management device 13 determines that the source of the packet received in step S14 is a new network device, it may transmit the address information of the new network device to the policy server 43 to notify the detection of the detected new network device. The policy server 43 that has been notified of the detection of the new network device from the management device 13 may determine whether to authorize the new network device based on

the control input that is input from the policy or manager (S19). When the new network device is an authorized device (S20), the policy server 43 may register the new network device in the network 1 (S21) and include the address information of the new network device in the device information of the database

5 431.

When the policy server 43 determines whether to authorize the new network device, it may transmit information on whether to authorize to the management device 13. When a new network device is an unauthorized device (S20), the management device 13 that has received this information may deny
10 the access of the unauthorized device to the network 1 (S22).

In step S22, the management device 13 may use the modified ARP response packet to modify the MAC address of the network devices belonging to the same subnet as the unauthorized network device to the meaningless MAC address that is impossible to communicate with in the ARP table of the
15 unauthorized network device. Accordingly, the unauthorized network device may not verify the correct MAC address of the other network devices belonging to the same subnet as itself, and thus the communication with other network devices is denied.

In step S22, the management device 13 may also use the modified ARP
20 response packet to modify the MAC address of the gateway to the meaningless address in the ARP table of the unauthorized network device. Accordingly, the unauthorized network device may be denied from communicating not only with other network devices in the subnet to which it belongs, but also with network

devices in other subnets that should be accessed through the gateway.

In step S22, the management device 13 may also use the ARP packet modification and packet forwarding method to deny the unauthorized network device from accessing other network devices. When the unauthorized network device is detected, the management device 13 may transmit the ARP response packet to the subnet to which the unauthorized network device belongs in order to modify the MAC address of the gateway in the ARP table of the unauthorized network device to the MAC address of the management device 13. Accordingly, the packets transmitted by the unauthorized network device are transmitted to the management device 13 rather than the gateway, and since the management device 13 already knows that the network device is the unauthorized device, the management device 13 may discard the packets received from the unauthorized network device.

FIG. 4 schematically illustrates a method for denying access by an address spoofing device in the network 1 according to an exemplary embodiment. The method of FIG. 4 may be performed by an access control system 100 described with reference to FIG. 2.

Referring to FIG. 4, when the packets are collected from the network devices (S31), the management device 13 may analyze each packet to determine whether the network devices that have transmitted the packets have spoofed their addresses (S32).

In step S32, the management device 13 may detect the network device that has spoofed the IP address or MAC address by comparing the source

address information of the collected packet with the address information of the devices registered in the policy server 43. The management device 13 may determine that the network device that has transmitted the packet has spoofed the IP address when the source address information extracted from the collected
5 packet has the same IP address as the network device already registered in the policy server 43 but has different MAC addresses. In addition, the management device 13 may determine that the network device that has transmitted the packet has spoofed the MAC address when the source address information extracted from the collected packet has the same MAC address as the network device
10 already registered in the policy server 43 but has different IP addresses.

In step S32, the management device 13 may also detect the network device that has spoofed the IP and MAC address by analyzing the ARP probe packets transmitted from each network device. The management device 13 may detect the IP address and MAC address of the corresponding network device
15 from the ARP probe packet transmitted as the ARP request from the network device. Then, the management device 13 may compare the detected IP address and MAC address with the address information registered in the policy server 43 to determine whether the device is the spoofing device that copies and uses the IP address and MAC address of another network device. In this case,
20 the management device 13 may additionally confirm the status information of the network device that has transmitted the ARP probe packet in order to prevent the normal network device from being mistakenly recognized as the spoofing device. When the status information of the corresponding network device indicates the

offline state before receiving the ARP probe packet, the management device 13 may determine that the received ARP probe packet was received from the normal device whose connection status with the network 1 has been switched to the online state, and may finally determine the corresponding network device as the
5 normal network device instead of the spoofing device.

When the network device is confirmed as the address spoofing device through step S32 (S33), the management device 13 may notify the policy server 43 that the address spoofing device has been detected (S34). In addition, based on the policy information received from the policy server 43, the access of the
10 detected address spoofing device to the network 1 may be denied (S35). For example, when the control unit 133 detects the address spoofing device, the control unit may transmit a network use denying packet (a response packet to an ARP probe packet) to deny the spoofing device from using the network.

When the management device 13 confirms that the network device is not
15 the address spoofing device through step S32 (S33), the management device may process the packets received from the network device according to the set policy (S36). For example, the packets may be processed through steps S14 to S22 of FIG. 3.

According to the above-described exemplary embodiment, the access
20 control system 100 may effectively deny the direct communication between the in-home terminals 22 registered in the same subnet 20 by modifying the MAC address of another in-home terminal 22 owned by each in-home terminal 22 to the uncommunicable address using the modified ARP packet.

In addition, the access control system 100 may also effectively deny the access between the subnets (for example, subnets 20 where in-home terminals 22 of different consents are connected) that are not allowed to communicate with each other by modifying the MAC address of the gateway owned by each network device to the MAC address of the management device 13, so that the management device 13 receives the packets instead of the gateway and discards or forwards the packets according to the policy.

In addition, the management device 13 of the access control system 100 may analyze the collected packets to detect and deny the access by the unauthorized network devices or the address spoofing devices in advance.

The above-described exemplary embodiment may be implemented as computer-readable code on a medium in which a program is recorded. The computer-readable media includes all types of recording apparatus that store data that may be read by a computer system. An example of the computer readable medium may include a hard disk drive (HDD), a solid state disk (SSD), a silicon disk drive (SDD), a read only memory (ROM), a random access memory (RAM), a compact disk read only memory (CD-ROM), a magnetic tape, a floppy disk, an optical data storage, and the like, and also include a medium implemented in a form of a carrier wave (for example, transmission through the Internet). In addition, the computer may include a terminal control unit. Therefore, the above-described detailed description is to be interpreted as being illustrative rather than being restrictive in all aspects. The scope of the present disclosure is to be determined by reasonable interpretation of the claims, and all

modifications within an equivalent range of the present disclosure fall in the scope of the present disclosure

【CLAIMS】

【Claim 1】

An access control method in a network including a plurality of in-home terminals located in different units, comprising:

5 transmitting, by a management device, address resolution protocol (ARP) request packets to the plurality of in-home terminals;

analyzing, by the management device, first ARP response packets received in response to the ARP request packets to acquire address information of the plurality of in-home terminals;

10 generating, by the management device, second ARP response packets in which a media access control (MAC) address is modified; and

modifying, by the management device, the MAC address of each in-home terminal in an ARP table of the plurality of in-home terminals by transmitting the second ARP response packets to the plurality of in-home terminals,

15 wherein the second ARP response packet is an ARP response packet that includes an IP address of the in-home terminal whose MAC address is to be modulated in each ARP table and the modulated MAC address as source address information, and

the modulated MAC address is an uncommunicable MAC address.

20

【Claim 2】

The access control method of claim 1, wherein:

the network includes a policy server that manages an access

management policy including a virtual local area network (VLAN) bandwidth allocation policy and a communication permission policy for each of a plurality of subnets to which different network devices are connected, and a plurality of network devices including the plurality of in-home terminals, and

5 the access control method further includes:

transmitting, by the management device, a third ARP response packet with a modified MAC address to the plurality of network devices to modify the MAC address of a gateway in the ARP table of the plurality of network devices to the MAC address of the management device,

10 receiving, by the management device, a packet transmitted to the gateway from the plurality of network devices, and

transmitting and discarding, by the management device, the received packet to the gateway based on the access management policy.

15 **【Claim 3】**

The access control method of claim 2, wherein:

the transmitting or discarding of the received packet to the gateway includes:

20 when the communication between the VLAN bandwidth to which a destination IP address of the received packet belongs and the VLAN bandwidth to which a source IP address of the received packet belongs is prohibited in the communication permission policy, discarding the received packet.

【Claim 4】

The access control method of claim 2, wherein:

the transmitting or discarding of the received packet to the gateway includes:

5 when the communication between the VLAN bandwidth to which the destination IP address of the received packet belongs and the VLAN bandwidth to which the source IP address of the received packet belongs is permitted in the communication permission policy, transmitting the received packet to the gateway.

10

【Claim 5】

The access control method of claim 2, wherein:

the transmitting or discarding of the received packet to the gateway includes:

15 when the destination IP address of the received packet belongs to an external network of the network, transmitting the received packet to the gateway.

【Claim 6】

The access control method of claim 2, wherein:

20 the communication permission policy is set to prohibit communication between subnets to which the plurality of in-home terminals belong.

【Claim 7】

The access control method of claim 2, further comprising:

acquiring, by the management device, address information of the network device that transmits a packet from the received packet; and

detecting, by the management device, a new network device by
5 comparing address information acquired from the received packet with the address information managed by the policy server.

【Claim 8】

The access control method of claim 7, further comprising:

10 determining, by the policy server, whether to authorize the new network device based on the access management policy or a control input that is input from a manager; and

transmitting, by the management device, a fourth ARP request packet to the new network device for modifying a MAC address of another network device
15 in the ARP table of the new network device to the uncommunicable MAC address when the new network device is an unauthorized device,

wherein the access management policy further includes a policy for determining whether to authorize the new network device,

20 【Claim 9】

The access control method of claim 8, further comprising:

transmitting, by the management device, a fifth ARP request packet to the new network device for modifying the MAC address of the gateway in the ARP

table of the new network device to the uncommunicable MAC address or the MAC address of the management device when the new network device is the unauthorized device.

5 **【Claim 10】**

 The access control method of claim 2, further comprising:

 detecting, by the management device, an address spoofing device that has spoofed an address of another network device registered in the network by comparing the address information acquired from the received packet with the
10 address information managed by the policy server; and

 denying, by the management device, the address spoofing device from the network based on the denying policy,

 wherein the access management policy further includes a denying policy for an address spoofing device, and
15

【Claim 11】

 The access control method of claim 1, wherein:

 the management device is connected to an 802.1Q tagged port of an L3 switch.
20

【Claim 12】

 An access control system in a network including a plurality of in-home terminals located in different units, comprising:

a management device that transmits address resolution protocol (ARP) request packets to a plurality of in-home terminals, analyzes first ARP response packets received in response to the ARP request packets to acquire address information of the plurality of in-home terminals, and transmits second ARP
5 response packets with modified media access control (MAC) addresses to the plurality of in-home terminals to modify the MAC addresses of each in-home terminal registered in the ARP table of the plurality of in-home terminals and deny communication between the plurality of in-home terminals,

wherein the second ARP response packet is an ARP response packet
10 that includes an IP address of the in-home terminal whose MAC address is to be modulated in each ARP table and the modulated MAC address as source address information, and

the modulated MAC address is an uncommunicable MAC address.

15 **【Claim 13】**

The access control system of claim 12, further comprising:

a policy server that manages an access management policy including a virtual local area network (VLAN) bandwidth allocation policy and a communication permission policy for each of a plurality of subnets constituting
20 the network,

wherein the management device transmits a third ARP response packet with a modified MAC address to the plurality of network devices registered in the network to modify the MAC address of a gateway registered in the ARP table of

the plurality of network devices to the MAC address of the management device, and when a packet is received from the plurality of network devices, transmits or discards the received packet to the gateway based on the access management policy, and

5 the plurality of network devices include the plurality of in-home terminals.

【Claim 14】

The access control system of claim 13, wherein:

10 when the communication between the VLAN bandwidth to which a destination IP address of the received packet belongs and the VLAN bandwidth to which a source IP address of the received packet belongs is prohibited in the communication permission policy, the management device discards the received packet.

15 **【Claim 15】**

The access control system of claim 13, wherein:

20 when the communication permission policy prohibits communication between the VLAN bandwidth to which the destination IP address of the received packet belongs and the VLAN bandwidth to which the source IP address of the received packet belongs or the destination IP address of the received packet belongs to an external network of the network, the management device transmits the received packet to the gateway.

【Claim 16】

The access control system of claim 13, wherein:

the communication permission policy is set to prohibit communication between different subnets to which the plurality of in-home terminals belong.

5

【Claim 17】

The access control system of claim 13, wherein:

the policy server manages address information of the plurality of network devices, and

10

the management device acquires address information of the network device that transmits the packet from the received packet, and detects a new network device by comparing the address information acquired from the received packet with the address information managed by the policy server.

15

【Claim 18】

The access control system of claim 17, wherein:

the access management policy further includes a policy for determining whether to authorize the new network device,

20

the policy server determines whether to authorize the new network device based on the access management policy or a control input that is input from a manager, and

the management device transmits a fourth ARP request packet to the new network device for modifying a MAC address of another network device in the

ARP table of the new network device to the uncommunicable MAC address when the new network device is an unauthorized device.

【Claim 19】

5 The access control system of claim 18, wherein:

 the management device transmits a fifth ARP request packet to the new network device for modifying the MAC address of the gateway in the ARP table of the new network device to the uncommunicable MAC address or the MAC address of the management device when the new network device is the
10 unauthorized device.

【Claim 20】

 The access control system of claim 13, wherein:

 the access management policy further includes a denying policy for an
15 address spoofing device, and

 the management device detects the address spoofing device that has spoofed an address of another network device registered in the network by comparing the address information acquired from the received packet with the address information managed by the policy server, and denies the address
20 spoofing device from the network based on the denying policy.

【Claim 21】

 The access control system of claim 12, wherein:

the management device is connected to an 802.1Q tagged port of an L3 switch.