【CLAIMS】

【Claim 1】

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

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, 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,

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,

wherein the modulated MAC address is an uncommunicable MAC address,

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

wherein 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,

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.

【Claim 2】

The access control method of claim 1, wherein:

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

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 3】

The access control method of claim 1, wherein:

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

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.

【Claim 4】

The access control method of claim 1, wherein:

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

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 5】

The access control method of claim 1, wherein:

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

【Claim 6】

The access control method of claim 1, 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 comparing address information acquired from the received packet with the address information managed by the policy server.

【Claim 7】

The access control method of claim 6, further comprising:

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 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,

【Claim 8】

The access control method of claim 7, 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.

【Claim 9】

The access control method of claim 1, 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 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

【Claim 10】

The access control method of claim 1, wherein:

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

【Claim 11】

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 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; and

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,

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,

wherein the modulated MAC address is an uncommunicable MAC address,

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

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

【Claim 12】

The access control system of claim 12, wherein:

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.

【Claim 13】

The access control system of claim 12, wherein:

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 14】

The access control system of claim 12, wherein:

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

【Claim 15】

The access control system of claim 12, wherein:

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

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.

【Claim 16】

The access control system of claim 15, wherein:

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

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 17】

The access control system of claim 16, 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 unauthorized device.

【Claim 18】

The access control system of claim 12, wherein:

the access management policy further includes a denying policy for an 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 spoofing device from the network based on the denying policy.

【Claim 19】

The access control system of claim 12, wherein:

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