

CONNECTION POSITION SPECIFYING APPARATUS AND
CONNECTION POSITION SPECIFYING METHOD
FOR UNAUTHORIZED EQUIPMENTS

Field of the Invention

This invention relates to a method and apparatus for specifying a position of unauthorized equipment as improperly linked to any one of network
5 devices on a network.

BACKGROUND OF THE INVENTION

A prior known network topology creation method is disclosed, for example, in JP-A-2002-190819 (see paragraph "000023" and Fig. 2), which method uses
10 the correspondence relationship between terminals linked to respective ports of multiple stage-coupled switching hubs and respective ports of such terminals to create a form which indicates how these terminals and switching hubs are connected.

15

SUMMARY OF THE INVENTION

Unfortunately, the method as disclosed in JP-A-2002-190819 is incapable of detecting those ports which are interconnected between a plurality of
20 switching hubs residing at a lower level. This poses a problem as to the lack of an ability to specify a link port of equipment as improperly connected to a network device, such as a lower-level switching hub or the like.

This invention is made in order to avoid the problem faced with the prior art, and an object of this invention is to provide an unauthorized equipment connection position specifying method and apparatus
5 capable of specifying the link port of unauthorized equipment as improperly connected to any one of the network devices involved.

To attain the foregoing object, an unauthorized equipment connection position specifying
10 apparatus incorporating the principles of this invention is operatively associated with a network which is made up of a connection of multiple stages of remote management function-added network devices, for specifying a position of unauthorized equipment
15 improperly connected to any one of the remote management function-added network devices. The apparatus includes a storage unit and a processing unit for control of the storage unit. The processing unit is operable to perform, upon detection of unauthorized
20 connection of the equipment linked to the remote management function-added network device, bidirectional communications with the remote management function-added network device retaining therein a correspondence relationship between a physical address of the detected
25 equipment and a port relating thereto. Then, caused is the remote management function-added network device to store physical addresses and corresponding ports of the remote management function-added network device linked

to a far end of the port of each of the remote management function-added network devices and the connection position specifying apparatus. Thereafter, collected is in the storage unit a correspondence
5 relationship of the physical addresses and the ports held in each of the remote management function-added network devices.

In accordance with another aspect of this invention, an unauthorized equipment connection
10 position specifying method is provided, which specifies a position of equipment as improperly connected to a network configured by connection of a plurality of stages of switches each having a plurality of ports. The method includes the steps of storing information as
15 to each switch for identifying switches up to a terminate end connected to respective ports of the switches, and sequentially selecting, based in the stored information specifying the switches, those switches in which a port for connection to the
20 improperly linked equipment and a port linked to itself are different from each other with the switch linked to itself as a reference to thereby specify the position of the improperly linked equipment.

In the correspondence relationship between
25 the physical addresses and the ports as to the remote management function-added network devices as collected in the storage unit, retained are physical addresses of the improperly linked equipment and the connection

position specifying apparatus. Then, selected is more than one of the remote management function-added network devices with its port corresponding to each physical address being kept inconsistent. Next, 5 specified is a certain one of the remote management function-added network devices at a terminate end with the improperly linked equipment connected thereto along with the port thereof. Then, externally outputted is information concerning the specified remote management 10 function-added network device at the terminate end and the port thereof.

According to this invention, it is possible to accurately identify any remote management function-added network device with the unauthorized equipment 15 being linked thereto in the network and the port thereof.

BRIEF DESCRIPTION OF THE DRAWINGS

Fig. 1 is a block diagram showing an overall 20 system including an unauthorized equipment connection position specifying apparatus in accordance with an embodiment 1 of this invention.

Fig. 2 shows IP addresses and MAC addresses of devices including switches of Fig. 1.

25 Fig. 3 is a block diagram showing a configuration of the connection position specifying apparatus of Fig. 1.

Fig. 4 is a block showing an arrangement of a

switch of Fig. 1.

Fig. 5 is a block showing a configuration of a repeater hub of Fig. 1.

Fig. 6 shows an entire processing procedure of the connection position specifying apparatus of Fig. 1.

Fig. 7 shows one example of a switch address table of Fig. 3.

Fig. 8 shows one example of a repeater hub address table of Fig. 3.

Figs. 9A to 9C show FDB hold states of three switches of Fig. 1.

Figs. 10A to 10C show FDB hold states of three switches of Fig. 1 other than those of Figs. 9A to 9C.

Figs. 11A to 11B show address track hold states of repeater hubs of Fig. 1.

Fig. 12 shows a detailed processing procedure at step S500 of Fig. 6.

Figs. 13A to 13C show FDB hold states of three switches as retained at step S501 of Fig. 12.

Figs. 14A to 14C show FDB hold states of three switches other than those of Fig. 13A to 13C.

Fig. 15 shows a switch address table containing therein priority flags as set up at step S506 of Fig. 13.

Fig. 16 shows another switch address table including a priority flag as set at S506 of Fig. 13.

Fig. 17 is a block diagram showing an overall system including an unauthorized equipment connection position specifying apparatus in accordance with an embodiment 2 of this invention.

5 Figs. 18A to 18C show FDB hold states of three switches of Fig. 17.

 Figs. 19A to 19C show FDB hold states of three switches other than those of Figs. 18A to 18C.

 Figs. 20A and 20B show address track hold
10 states of repeater hubs of Fig. 17.

Fig. 21 is a block diagram showing an overall system including an unauthorized equipment connection position specifying apparatus in accordance with an embodiment 3 of this invention.

15 Fig. 22 shows a data structure of a switch address table in the connection position specifying apparatus of Fig. 21.

 Figs. 23A to 23E show FDB hold states at switches of Fig. 21.

20 Fig. 24 shows a priority flag setup state in the switch address table of Fig. 22.

 Fig. 25 shows a priority flag setup state in the switch address table of Fig. 24.

25 DETAILED DESCRIPTION OF THE EMBODIMENTS

(Embodiment 1)

Fig. 1 is a block diagram showing an overall system including an unauthorized or "fraud" equipment

connection position specifying apparatus in accordance with an embodiment 1 of this invention.

In Fig. 1, the unauthorized equipment connection position specifying apparatus 10
5 (hereinafter referred to as "connect position specifier device") is connected to a port P1 of a switch module 21. The switch 21 is connected to a plurality of switches 22 and 23 placed at a lower level. The switches 21 to 23 have remote management functions (the
10 same goes with switches 24 to 26 to be later described). The remove management function as used herein refers to functionality for returning the information to be retained at a forwarding database (FDB) and/or address track in response to a request
15 from the connect position specifier device 10.

The switch 23 is connected via a switch 24 residing at a lower level to a multi-port repeater hub 41. The repeater hub 41 has a port P1, to which is linked an electronic equipment 5 such as a computer or
20 else. The repeater hub 41 has the above-noted remote management function (the same goes with a repeater hub 42 to be later described). The equipment 5 is an authorized network device with permission for connection.

25 The switch 23 is also connected through a plurality of switches 25 and 26 placed at a lower level to a repeater hub 42. The hub 42 has ports P1 and P2. A device 7 such as a computer is connected to the port

P1. An equipment 31 is connected to the port P2. The device 7 is authorized one like the device 5. The equipment 31 is an unauthorized one without having any permission for network connection, such as a personal computer (PC). Note that in Fig. 1, reference characters P1, P2, ..., P8 indicate port numbers. The devices 1 to 8 are authorized ones. In this way, a plurality of remote management function-added network devices, such as the switches (switching hubs) 21 to 26, are connected together to form multiple stages, thereby constituting a network as a whole.

Supposed is that every equipment on the network shown in Fig. 1, namely, the connect position specifier device 10, switches 21 to 26, repeater hubs 41 and 42 and devices 1 to 8 and 31, are assigned with an Internet protocol (IP) address (logical address) and a media access control (MAC) address (physical address) unique thereto.

A configuration of the connect position specifier device 10 is described.

Fig. 3 is a block diagram showing the configuration of the connect position specifier device. In Fig. 3, the connect position specifier 10 is a computer such as for example a PC, which includes a processing unit 110 connected on a bus 160, a communication interface (COM I/F) 120 for performing communications with other devices via the network, a storage unit 130, a display unit 140 and an input unit

150. These will be described in detail below.

The input unit 150 is a data entry device, such as a keyboard or a pointing device known as "mouse." The display unit 140 is a display device,
5 such as a computer display or else.

The storage unit 130 is a storage device such as a semiconductor memory, which stores a device address table 131, switch address table 132, repeater hub address table 133 and limit area information 134.
10 The device address table 131 is arranged so that the IP and MAC addresses of equipment (e.g., the devices 1 to 8) are stored therein.

The switch address table 132 is for storage of a correspondence relationship of the IP and MAC
15 addresses of the switches 21 to 26 shown in Fig. 1. The repeater hub address table 133 stores a correspondence relationship of the IP and MAC address of the repeater hubs 41 and 42 of Fig. 1. The arrangements of the switch address table 132 and
20 repeater hub address table 133 will be described later.

The limit area information 134 concerns (1) IP addresses or MAC addresses with permission for connection to the network or (2) IP or MAC addresses without permission for network connection. Supposed is
25 that network connection-prohibited IP addresses "192.162.1.31" to "192.168.1.39" are established. Any equipment having IP address included in the limit area information 134 is judged to be unauthorized equipment.

The processing unit 110 is a processor device, such as central processing unit (CPU), and has a remote collection unit 111, an equipment/device address detection unit 112, a connection/linkup monitor
5 unit 113, a communication unit 114, and an unauthorized equipment connection position specifying unit 115 (hereinafter referred to as "unauthorized linkup finder"). These respective units 111 to 115 are arranged to operate in accordance with a connection
10 position identification software program which is typically installed in the connect position specifying device 10, although details thereof will be set forth later. The connection position identification program may be prestored in a specified region of the storage
15 unit 130 or, alternatively, may be read out of a computer-readable recording media, such as a compact disc read only memory (CD-ROM).

The switches 21 to 26 are arranged in a way as follows.

20 Fig. 4 shows, in block diagram, a configuration of one switch 21. Although the switch 21 is discussed here, the remaining switches 22 to 26 are similar in configuration to the switch 21.

In Fig. 4, the switch 21 is equipped with a
25 processing unit (processor) 200, a storage unit (memory) 210, and a plurality of ports P1 to P8. The storage unit 210 stores a forwarding database (FDB) 211 for retaining a correspondence relationship between

port numbers and MAC addresses. The FDB 211 maintains the MAC address of a sender of a received frame as learned on a per-port basis.

An arrangement of repeater hubs 41 and 42 is
5 described below.

Fig. 5 depicts in block diagram a configuration of one repeater hub 41. The other repeater hub 42 is substantially the same in configuration as the hub 41.

10 In Fig. 5, the repeater hub 41 has a processing unit (processor) 400, storage unit (memory) 410, and multiple ports P1 to P4. A storage unit 410 stores an address track 411. Owing to the address track 411, the lastly per-port learned MAC address of a
15 sender that forwarded a received frame is retained.

An entire processing procedure of the connect position specifier device 10 is described.

Fig. 6 is a diagram showing an overall processing procedure of the connect position specifier
20 device. The following explanation assumes that the equipment 31 shown in Fig. 1 is connected to the port P2 of repeater hub 42 at a given timing.

The processor unit 110 of the connect position specifier device 10 shown in Fig. 3 transmits
25 an address resolution (AR) request to a logical address in its associated network (e.g., "192.168.1.0/24"), which address is any one of the logical addresses "192.168.1.1" to "192.168.1.254" other than its own

logical address "192.168.1.10," and then detects the IP and MAC addresses of a connection device that returns its reply. This detection is hereinafter referred to as the "address detection," which is performed at step 5 S100 of Fig. 6. The processor unit 110 at this time is called the "device address detector unit 112" shown in Fig. 3. Whereby, the connect position specifier 10 detects the IP and MAC addresses of connection device as to all the nodes concerned, including the devices 1 10 to 8, switches 21 to 26 and repeater hubs 41 and 42. The connect position specifier 10 then registers a correspondence relationship of the IP and MAC addresses of these linked devices in the equipment address table 131 of Fig. 3.

15 Subsequently the processor unit 110 requests by "SNMP Get" the FDB-retained information from the addresses on the address table 131 of Fig. 3, and then determines or "judges" that a reply-returned address is the address of a remote management function-added 20 switch. The processor unit 110 also requests by SNMP Get the address track-retained information from the address on the device address table 131 of Fig. 3, and judges a reply-returned address is the address of a remote management function-added repeater hub. In this 25 way, the addresses of remote management function-added switch and repeater hub are determined. Then, the processor unit 110 prepares the switch address table 132 and repeater hub address table 133 shown in Fig. 3,

at step S200 in Fig. 6. The processor unit 110 at this time also is called the "device address detector unit 112" shown in Fig. 3.

Additionally the term SNMP is an acronym of
5 simple network management protocol, which is a management protocol in network environments.

One example of the switch address table 132 at this time is shown in Fig. 7, and an example of the repeater hub address table 133 is shown in Fig. 8.

10 The switch address table 132 is first described. As shown in Fig. 7, the switch address table 132 stores therein IP addresses, MAC addresses, a priority flag and a referencing-completed flag in a manner that these are correlated together. Examples of
15 the stored contents are the IP addresses "192.168.1.21" to "192.168.1.26" and the MAC addresses "00:22:33:00:00:21" to "00:22:33:00:00:26" of the switches 21 to 26 shown in Fig. 1. The priority flag is a flag which indicates that upon specifying of a
20 connection position of unauthorized equipment, a switch on a record thereof is preferentially referred to. The referencing-completed flag is the one that indicates whether the record has already been referred to, although details will be stated later.

25 The repeater hub address table 133 is stated. As shown in Fig. 8, the table 133 stores the IP addresses "192.168.1.41" to "192.168.1.42" and MAC addresses "00:33:44:00:00:41" to "00:33:44:00:00:42" of

the repeater hubs 41 and 42 shown in Fig. 1.

Turning back to Fig. 6, at step S300, the processor unit 110 monitors the address resolution (AR) request protocol and performs linkup monitoring with
5 respect to a network linkage situation. The processor unit 110 at this time is called the "connection monitor unit 113" shown in Fig. 3. In this case, supposed is for example that the equipment 31 is connected to the repeater hub 42, which equipment 31 transmits an AR
10 request over broadcast. In this event, the processor unit 110 stores the IP address of such equipment 31 as acquired from the AR request along with its corresponding MAC address. The processor 110 judges that these addresses are unregistered to the device
15 address table 131 shown in Fig. 3, and thus judges that the equipment 31 is newly linked.

Due to the broadcast transmission, an address of the equipment 31 that is acquired from the AR request is expected to reach the switches 21 to 26.
20 Exemplary states of the FDBs 211 of switches 21 to 26 at this time are shown in Figs. 9A to 9C and 10A to 10C. Hold states of the address tracks 411 of the repeater hubs 41 and 42 in this event are shown in Figs. 11A and 11B.

25 The hold states of FDBs 211 of switches 21 to 26 are described. As shown by thick-line frame in Fig. 9A, there is held in the FDB 211 of switch 21 a correspondence relationship between the MAC address

"00:11:22:00:00:31" of the equipment 31 as retained in reply to the AR request from equipment 31 and its received port number "8." As shown in Fig. 9B, this correspondence relationship of the MAC address

5 "00:11:22:00:00:31" of equipment 31 as held in reply to the AR request from equipment 31 and its received port number "8" is also retained in the FDB 211 of switch 22 (see a thick-line frame in Fig. 9B). Additionally as shown by thick-line frame in Fig. 9C, the

10 correspondence relationship of the MAC address

"00:11:22:00:00:31" of the equipment 31 as retained by the AR request from equipment 31 and its received port number "7" is held in the FDB 211 of switch 23.

Similarly, the correspondence relationship of the MAC
15 address "00:11:22:00:00:31" of the equipment 31 held by the AR request from equipment 31 and its received port number is held in the FDB 211 of any one of the other switches 24 to 26 as shown by thick-line frames in Figs. 10A to 10C.

20 A hold state of the address track 411 of the repeater hubs 41 and 42 is described. As shown in Fig. 11A, there is retained in the address track 411 of repeater hub 41 a correspondence relationship of the MAC address "00:11:22:00:00:05" of the device 5 shown
25 in Fig. 1 and its received port number "1." On the contrary, as shown by thick-line frame in Fig. 11B, a correspondence relationship of the MAC address "00:11:22:00:00:31" of the equipment 31 as retained by

the AR request from equipment 31 and its received port number "2" is held in the address track 411 of repeater hub 41.

Although in Fig. 11B the MAC addresses
5 corresponding to two port numbers "1" and "2" are retained, the MAC address as received at the port "1" is rewritten and replaced with MAC address of another remote management function-added network device being linked to the same port in cases where this network
10 device is connected to the port "1" via a repeater hub or else. This is because the address track 411 is the one that stores therein the lastly received sender MAC address of the frame.

Again returning to Fig. 6, at step S400, the
15 processor unit 110 determines whether the IP address "192.168.1.31" of equipment 31 that is acquired based on the AR request from the equipment 31 linked during execution of the connection monitoring at step S300 is contained in the limit area information 134 shown in
20 Fig. 3. In this example the IP address is contained, and the processor 110 detects it as unauthorized equipment, i.e., "YES" at step S400. In this case, it proceeds to step S500.

At step S500, the processor unit 110 uses the
25 IP address "192.168.1.31" and MAC address "00:11:22:00:00:31" of the equipment 31, which is detected as unauthorized equipment at step S400, to specify the connection position of equipment 31. In

the step S500, the processor unit 110 at this time is called the "unauthorized linkup finder 115" shown in Fig. 3. As for this specifying processing, a detailed explanation is given with reference to Fig. 12.

5 Fig. 12 shows in greater detail a procedure of the processing at step S500 of Fig. 6.

 The processor unit 110 shown in Fig. 3 performs, for example, "SNMP Get" requesting against all of the switches 21 to 26 and repeater hubs 41 and 42 at step S501. The processor unit 110 at this time is called the "communication unit 114" shown in Fig. 3. Due to this SNMP Get request, each of the switches 21 to 26 and repeater hubs 41 and 42 shown in Fig. 1 is expected to return its reply responding to the request toward the connect position specifier device 10, resulting in the FDBs 211 of switches 21 to 26 in mid course storing therein the sender MAC addresses of the responding frame capable of being received on a per-port basis. Hold states of the FDBs 211 of switches 21 to 26 in this event are shown in Figs. 13A to 13C and 14A to 14C, respectively.

 As shown in Fig. 13A, the FDB 211 of switch 21 retains on a per-port basis the MAC addresses, such as for example "00:22:33:00:00:23" of the switch 23 shown in Fig. 1. Similarly the FDBs 211 of switches 22 and 23 hold MAC addresses in units of ports as shown in Figs. 13B and 13C.

 Furthermore, the MAC addresses are held in

FDBs 211 of the other switches 24 to 26 in units of ports, as shown in Figs. 14A to 14C.

Although at step S501, the SNMP Get request is used, other types of communications may be performed
5 as far as bidirectional or two-way communicabilities are available relative to the switches 21 to 26 and repeater hubs 41 and 42. Examples thereof include, but not limited to, address resolution protocol (ARP) requesting/responding and Internet control message
10 protocol (ICMP) echo communications.

The two-way communications are performed at specific time intervals having a length shorter than the expiration of a retention time period of the MAC addresses and ports held in the FDBs 211 of switches 21
15 to 26 (i.e., prior to the time-up of an aging timer).

Turning back to Fig. 12, at step S502, the processor unit 110 makes reference to the switch address table 132 shown in Fig. 7 and collects together the storage data of the FDB 21 of switch 21 by using
20 the IP and MAC addresses of the switch 21 shown in Fig. 1, for example (see the top row of Fig. 7). This data collection is performed in reply to an SNMP request (network management request) for example (the processor unit 110 at this time is called the "remote
25 collection unit 111" shown in Fig. 3). Whereby, the processor unit 110 collects the storage data of FDB 211 of switch 21 shown in Fig. 13A and then stores the data in a specified region of the storage unit 130 shown in

Fig. 3.

At step S503, the processor unit 110 determines, from the FDB 211 of switch 21 of Fig. 13A as collected by the SNMP request performed at S502, whether a port corresponding to the MAC address of the equipment 31 that is detected and stored at S300 is present or absent. As a port "8" which corresponds to the MAC address "00:11:22:00:00:31" of equipment 31 is present in the table of Fig. 13A, the processor unit 110 judges that such corresponding port exists (in case of "YES" at step S503). Then, it proceeds to the next step S504, which determines whether the MAC address "00:11:22:00:00:10" of the connect position specifier device 10 is present or not at the same port as the port "8" which is judged to be present at step S503.

In Fig. 13A, the MAC address "00:11:22:00:00:10" of the connect position specifier device 10 is present at a port "1" that is different from the port "8" so that it is determined at step S504 that the MAC address of connect position specifier 10 is absent at the same port as the port "8" that is judged to be present at step S503 (when "NO" at S504). Then, it goes to step S505.

At S505, the MAC addresses "00:22:33:00:00:23" to "00:22:33:00:00:26" of switches 23 to 26 are registered to the port "8" in the FDB 211 of the switch 21 shown in Fig. 13A so that the processor unit 110 determines that the MAC address of

the switch is present at the same port as the port "8" that is judged to be present at S503 (when "YES" at S505); thus, it goes to the next step S506. In S506, the processor unit 110 sets up priority flags of the switches 23 to 36 that are each judged to have the MAC address at S505 in the switch address table 132 shown in Fig. 7 in a manner as shown in Fig. 15 (see "Priority" in Fig. 15), while setting up a referencing-completed flag of switch 21 (see "Completed" in Fig. 15). In this way, the switches 23 to 26 are selected, which are used as a communication pathway of the equipment 31 shown in Fig. 1.

The processor unit 110 proceeds to step S507 and determines that the switches 22 to 26 without setup of the Reference-Completed flag, i.e., not-referenced switches, are present in the switch address table 132 shown in Fig. 15 (in the case of "YES" at S507); then, it returns to S502.

At S502, the processor unit 110 makes reference to the switch address table 132 shown in Fig. 15 and then collects together the storage data of the FDB 221 of switch 24 shown in Fig. 14A by use of the IP address "192.162.1.24" and MAC address "00:22:33:00:00:24" of the not-referenced switch 24 with the priority flag added thereto, by way of example. The port "8" corresponding to the MAC address of the improperly linked equipment 31 exists in the FDB 221 of switch 24 shown in Fig. 14A. Simultaneously, at

the port "8," the MAC address of the connect position specifier device 10 is found. Thus, the processor unit 110 proceeds to "YES" of step S503 and thereafter goes to YES at the next step S504, and then goes to S507.

- 5 The processor 110 determines that unprocessed switches 22-23 and 25-26 are present in the switch address table 132 shown in Fig. 15 (in the case of YES at S507), and then returns to S502.

At the next step S502, the processor unit 110
10 refers to the switch address table 132 shown in Fig. 15 and collects together the storage data of the FDB 221 of switch 25 shown in Fig. 14B by using the IP address "192.162.1.25" and MAC address "00:22:33:00:00:25" of the not-referenced switch 25 with the priority flag
15 added thereto, for example. Although a port "7" which corresponds to the MAC address of the improperly linked equipment 31 is found in the FDB 221 of switch 25 shown in Fig. 14B, such port "7" lacks the MAC address of connect position specifier device 10. Thus the
20 processor unit 110 proceeds to "YES" of S503 and thereafter goes to "NO" at the next step S504 and then goes to S505.

At step S505, the processor unit 110
determines that the MAC address "00:22:33:00:00:26" of
25 switch 26 exists at the port "7" that is judged at step S503 to be present in the FDB 221 of switch 25 shown in Fig. 14B (in the case of YES at S505) and then proceeds to the next step S506, YES of S507 and S502 in this

order of sequence. At S506, as shown in Fig. 16, update setup is done to validate the priority flag of switch 26 of the MAC address that is judged to be present at S504.

5 At the next step S504, the processor unit 110 refers to the switch address table 132 shown in Fig. 16 and collects together the storage data of the FDB 221 of switch 26 shown in Fig. 14C by use of the IP address "192.162.1.26" and MAC address "00:22:33:00:00:26" of
10 the not-referenced switch 26 with the priority flag added thereto, for example. Although the port "7" corresponding to the MAC address of equipment 31 as linked within the limit area exists in the FDB 221 of switch 26 shown in Fig. 14C, the port "7" lacks the MAC
15 address of connect position specifier device 10. Thus the processor unit 110 proceeds to "YES" of S503 and thereafter goes to "NO" at the next step S504 and then goes to S505.

 At step S505, the processor unit 110
20 determines the MAC address of the switch is absent at the port "7" which is judged at S503 to be present in the FDB 221 of switch 26 shown in Fig. 14C (in the case of "NO" at S505), and then proceeds to the next step S508.

25 At S508, the MAC address "00:22:33:00:00:42" of repeater hub 42 is present at the port "7" that is judged at S503 to be present in the FDB 221 of switch 26 shown in Fig. 14C, and proceed to "YES" of S508 and

then go to S509.

Additionally if "NO" at S508, then the processor unit 110 goes to the next step S508 for switch/port identification, and then goes to S511 as
5 will be discussed later.

At step S509, the processor unit 110 refers to the repeater hub address table 133 shown in Fig. 8 and, upon receipt of SNMP request, collects the storage data of the address track 411 of repeater hub 42 shown
10 in Fig. 11B by using the IP address "192.162.1.42" and MAC address "00:33:44:00:00:42" of repeater hub 42 as detected at S508. A port "2" that corresponds to the MAC address "00:11:22:00:00:31" of the improperly linked equipment 31 is present in the address track 411
15 of repeater hub 42 shown in Fig. 11B, so the processor 110 proceeds to YES of S509 and then goes to S510.

At step S510, the processor unit 110 specifies the repeater hub 42 and the port "2" and, at the next step S511, externally outputs the information
20 indicative of such content, that is, the port "2" of repeater hub 42, to the display unit 140, which displays it on its screen. In this displaying, it is also permissible to display the IP and MAC addresses of repeater hub 42.

25 Additionally, if "NO" at step S509, then the processor unit 110 specifies only the reaper hub (at S509A) and then displays such information at the display unit 140.

In this way, it becomes possible for users to affirm the repeater hub 42 with the equipment 31 being linked thereto and its port "2." For example, it is possible to specify by the connection port the position of the improperly linked equipment 31 without executing the MAC-address/port correspondence relationship collection with respect to all the network devices in a way irrespective of the topology relating to the fact that the equipment is linked at which position of the upper and lower levels of a switch. Thus it becomes possible to rapidly specify the exact connection position of the unauthorized equipment 31, thereby making it possible to take corrective measures in such a way as to avoid any unauthorized connection to the network.

(Embodiment 2)

Fig. 17 is a block diagram showing an overall system including an unauthorized equipment connection position specifying apparatus in accordance with an embodiment 2 of this invention. The same parts or components as those of the above-noted embodiment 1 are indicated by the same reference numerals, with repetitive explanations eliminated herein.

In Fig. 17, an incompatible repeater hub 51 having no remote management functions is connected at a low level of the remote management function-added repeater hub 42 shown in Fig. 1. The above-stated unauthorized equipment 31 is connected to the

incompatible repeater hub 51. The other arrangements are almost similar to those of the embodiment 1, so explanations thereof are omitted.

In this case, in the connection position
5 specifier device 10 shown in Fig. 17, the FDBs 211 of the switches 21 to 23 shown in Fig. 17 are set in retention states such as shown in Figs. 18A to 18C at the step S501 shown in Fig. 12. The FDBs 211 of switches 24 to 26 shown in Fig. 17 are set in hold
10 states as shown in Figs. 19A to 19C. The address tracks 411 of remote management function-added repeater hubs 41 and 42 shown in Fig. 17 are set in hold states shown in Figs. 20A and 20B. The processor unit 110 of connect position specifier 10 executes the processing
15 tasks of from step S502 up to S510 shown in Fig. 12 whereby the port "2" of repeater hub 42 shown in Fig. 17 is displayed at the display unit 140.

More specifically, the processor unit 110 retains the physical addresses of the improperly linked
20 equipment 31 and connect position specifier 10 and selects those switches 21, 23, 25 and 26 and repeater hub 42 with inconsistent ports corresponding to respective physical addresses in such a way as to come closer to a port corresponding to the MAC address of
25 unauthorized equipment 31 to thereby specify and externally output the port "2" of remote management function-added repeater hub 42 at an upper level as connected to the incompatible repeater hub 51, to which

the equipment 31 is linked. This advantageously makes it possible for users to ascertain the repeater hub 42 to which the unauthorized equipment 31 is connected at a terminate end and the port "2" thereof.

5 Even when the MAC address as held at the port "2" of the upper-level repeater hub 42 having the remote management functionality is rewritten from that of the equipment 31, it is possible to specify up to the repeater hub 42 with the unauthorized equipment 31
10 linked thereto, even although the port per se is kept unknown. This is advantageous.

(Embodiment 3)

Fig. 21 is a block diagram showing an entire system including an unauthorized equipment connection
15 position specifying device in accordance with an embodiment 3 of this invention. The same components as those of the afore-said embodiments 1 and 2 are denoted by the same reference numerals, with duplicative explanations eliminated herein.

20 In Fig. 21, an incompatible repeater hub 52 is connected between the switches 23 and 26 as shown in Fig. 1, with the above-noted unauthorized equipment 31 being linked to the switch 26 at its port "2." The incompatible repeater hub 52 has no remote management
25 functions. The other arrangements are substantially the same as those of the embodiment 1, and the explanation is eliminated herein.

In this case, the connection position

specifier device 10 creates the switch address table 132 at the step S200 shown in Fig. 6. Thereafter, at S501 shown in Fig. 12, the FDBs 211 of the switches 21 to 24 shown in Fig. 21 are set in the hold states such as shown in Figs. 23A to 23E. The processor unit 110 of the connect position specifier 10 executes the processing of from the S502 to S510 whereby the switch address table 132 shown in Fig. 22 is updated in the order of Fig. 24 and Fig. 25.

10 Finally the processor unit 110 causes the port "2" of switch 26 shown in Fig. 21 to be visually displayed at the display unit 140.

 More specifically, the processor unit 110 retains the physical addresses of the improperly linked equipment 31 and connect position specifier device 10 and then attempts to select the switches 21, 23 and 26 with inconsistency of those ports corresponding to such respective physical addresses in such a way as to come closer to a port corresponding to the MAC address of unauthorized equipment 31 to thereby specify and externally output the port number "2" of the switch 26 with the equipment 31 linked thereto. Thus it becomes possible for users or subscribers to confirm the terminate-end switch 26 with the equipment 31 linked thereto and the port "2" thereof.

 This invention should not exclusively be limited to the illustrative embodiments stated supra. The number of the switches is changeable by prior known

techniques. The switches are combinable in various ways for establishment of the network, without departing from the scope and coverage of the invention.

The configuration of the connect position specifier device 10 and the program processing procedure are modifiable in a variety of forms by known techniques. For example, although at the steps S502 to S507 of Fig. 12 the explanation is given as to the case where the FDBs 211 of those switches registered to the switch address table 132 are sequentially collected together for later reference of their contents, the FDBs 211 of all the switches involved may alternatively be collected at a time, the contents of which are referred to in adequate events.

CLAIMS:

1. An unauthorized equipment connection position specifying apparatus for use in a network configured from a connection of multiple stages of remote management function-added network devices each having a plurality of ports linkable to the network and a forwarding database ("FDB") for learning and holding therein a plurality of sender physical addresses of frames as received in units of ports and also having remote management functionality for passing contents of the FDB to a requester in reply to a request from a remote device, said apparatus being operative to specify a position of unauthorized equipment as improperly connected to any one of the remote management function-added network devices, said apparatus comprising:

a storage unit and a processing unit for controlling the storage unit; and

the processing unit performing, upon detection of unauthorized connection of the equipment linked to the remote management function-added network device, bidirectional communications with the remote management function-added network device retaining therein a correspondence relationship between a physical address of the detected equipment and a port relating thereto, and then causing the remote management function-added network device to store physical addresses and corresponding ports of the

remote management function-added network device linked to a far end of the port of each of the remote management function-added network devices and the connection position specifying apparatus,

collecting in the storage unit a correspondence relationship of the physical addresses and the ports held in each of the remote management function-added network devices,

in the correspondence relationship between the physical addresses and the ports as to the remote management function-added network devices as collected in the storage unit, holding physical addresses of the improperly linked equipment and the connection position specifying apparatus, selecting more than one of the remote management function-added network devices with the port corresponding to each physical address being kept inconsistent, and specifying a certain one of the remote management function-added network devices at a terminate end with the improperly linked equipment being connected thereto along with the port thereof, and

externally outputting information concerning the specified remote management function-added network device at the terminate end and the port thereof.

2. The connection position specifying apparatus according to claim 1, wherein when a port with storage of the physical address of the improperly linked equipment and also with storage of a physical address

of another network device but without storage of the physical address of the connection position specifying apparatus is present in a certain physical address to port correspondence relationship, the processing unit determines as the port with the improperly linked equipment connected thereto a port with storage of the physical address of the improperly linked equipment at a network device wherein the network device having the physical address in port correspondence relationship is connected to the improperly linked equipment.

3. The connection position specifying apparatus according to claim 1, wherein when a port with storage of the physical address of the improperly linked equipment and also with storage of a physical address of another network device but without storage of the physical address of the connection position specifying apparatus is found in a certain physical address to port correspondence relationship, the processing unit selects a next one while taking priority of a network device as held at the port with storage of the physical address of the improperly linked equipment.

4. The connection position specifying apparatus according to claim 1, wherein the processing unit performs bidirectional communications between the connection position specifying apparatus and the remote management function-added network devices at a time interval in which a hold time limit of the physical address to port correspondence relationship held in

each of the remote management function-added network devices is not expired.

5. The connection position specifying apparatus according to claim 1, wherein the processing unit is responsive to receipt of an address resolution request for detecting a physical address and a logical address of a remote management function-added network device other than that linked to itself and for using the physical address and the logical address thus detected to issue a network management request to the remote management function-added network device.

6. The connection position specifying apparatus according to claim 1, wherein the storage unit has in advance a table of logical addresses or physical addresses with permission for connection to the network or logical addresses or physical addresses with imprecision of connection, and

 when the physical address or logical address of the equipment as detected in response to the address resolution request is out of a permissible addresses or is an impermissible address, the processing unit determines it as an unauthorized connection.

7. The connection position specifying apparatus according to claim 1, wherein in case a network is configured by connecting an incompatible network device without having remote management functionality at a lower level of the remote management function-added network device, when an equipment is improperly linked

to the incompatible network device,

the processing unit performs bidirectional communications at least with respect to the remote management function-added network device holding the correspondence relationship between a physical address of the detected equipment and the port, and causes each of the remote management function-added network devices to hold physical addresses and corresponding ports as to the remote management function-added network device linked to a far end of the port of each the remote management function-added network device and the connection position specifying apparatus,

collects in the storage unit a physical address to port correspondence relationship as held in each the remote management function-added network device,

in the physical address to port correspondence relationship as to each the remote management function-added network device, holds physical addresses of the improperly linked equipment and the connection position specifying apparatus, and selects more than one remote management function-added network device with the port corresponding to each physical address being kept inconsistent, and

externally outputs information concerning a specified port of remote management function-added network device as linked at an upper level of the incompatible network device.

8. The connection position specifying apparatus according to claim 1, wherein when in the network devices an incompatible network device without having the remote management functionality is further linked between an upper-level remote management function-added network device and a lower-level remote management function-added network device to thereby make up a network with an unauthorized equipment being improperly linked to the lower-level remote management function-added network device,

 the processing unit performs bidirectional communications at least with respect to the remote management function-added network device holding the correspondence relationship between a physical address of the detected equipment and the port, and causes each of the remote management function-added network devices to hold physical addresses and corresponding ports as to the remote management function-added network device linked to a far end of the port of each the remote management function-added network device and the connection position specifying apparatus,

 collects in the storage unit a physical address to port correspondence relationship as held in each the remote management function-added network device,

 in the physical address to port correspondence relationship as to each the remote management function-added network device, holds

physical addresses of the improperly linked equipment and the connection position specifying apparatus, and selects more than one of the remote management function-added network devices with the port corresponding to each physical address being kept inconsistent, and

specifies and externally outputs information concerning a port of a remote management function-added network device with the unauthorized equipment being linked thereto at a lower level.

9. The connection position specifying apparatus according to claim 1, wherein a remote management function-added repeater hub having a plurality of network-linkable ports and an address track for holding therein only one sender physical address of a lastly received frame of frames as received in units of ports and also having remote management functionality for providing contents of the address track to a requester in reply to a request from a remote device is connected at a lower level of the remote management function-added network devices to thereby make up a network, and when an unauthorized equipment is improperly linked to the remote management function-added repeater hub,

the processing unit performs bidirectional communications at least with respect to the remote management function-added network device holding the correspondence relationship between a physical address of the detected equipment and the port, and causes each

of the remote management function-added network devices to hold physical addresses and corresponding ports as to the remote management function-added network device linked to a far end of the port of each the remote management function-added network device and the connection position specifying apparatus,

collects in the storage unit a physical address to port correspondence relationship as held in each the remote management function-added network device,

in the physical address to port correspondence relationship as to each the remote management function-added network device, holds physical addresses of the improperly linked equipment and the connection position specifying apparatus, and selects more than one of the remote management function-added network devices with the port corresponding to each physical address being kept inconsistent, and

specifies and externally outputs information concerning a remote management function-added repeater hub with the unauthorized equipment being linked thereto or the remote management function-added repeater hub to which the unauthorized equipment is connected, and a port thereof.

10. An unauthorized equipment connection position specifying apparatus for specifying a position of equipment as improperly connected to a network

configured by connection of a plurality of stages of switches each having a plurality of ports, said apparatus comprising storage means for storing therein information as to each said switch for identifying switches up to a terminate end connected to respective ports of the switches, and a processing unit for sequentially selecting, based on the stored information specifying the switches, those switches in which a port for connection to the improperly linked equipment and a port linked to itself are different from each other with the switch linked to itself being as a reference to thereby specify the position of the improperly linked equipment.

11. A connection position specifying method for use in an unauthorized equipment connection position specifying apparatus for use in a network configured from a connection of multiple stages of remote management function-added network devices each having a plurality of ports linkable to the network and a forwarding database ("FDB") for learning and holding therein a plurality of sender physical addresses of frames as received in units of ports and also having remote management functionality for passing contents of the FDB to a requester in reply to a request from a remote device, said apparatus being operative to specify a position of unauthorized equipment as improperly connected to any one of the remote management function-added network devices and having a

storage unit and a processing unit for control of the storage unit, said method comprising the steps of:

causing the processor unit to perform, upon detection of unauthorized connection of the equipment linked to the remote management function-added network device, bidirectional communications with the remote management function-added network device retaining therein a correspondence relationship between a physical address of the detected equipment and a port relating thereto;

causing the remote management function-added network device to store physical addresses and corresponding ports of the remote management function-added network device linked to a far end of the port of each of the remote management function-added network devices and the connection position specifying apparatus;

collecting in the storage unit a correspondence relationship of the physical addresses and the ports held in each of the remote management function-added network devices;

in the correspondence relationship between the physical addresses and the ports as to the remote management function-added network devices as collected in the storage unit, holding physical addresses of the improperly linked equipment and the connection position specifying apparatus;

selecting more than one of the remote

management function-added network devices with its port corresponding to each physical address being kept inconsistent;

specifying a certain one of the remote management function-added network devices at a terminate end with the improperly linked equipment being connected thereto along with the port thereof; and

externally outputting information concerning the specified remote management function-added network device at the terminate end and the port thereof.

12. The connection position specifying method according to claim 11, wherein when a port with storage of the physical address of the improperly linked equipment and also with storage of a physical address of another network device but without storage of the physical address of the connection position specifying apparatus is present in a certain physical address to port correspondence relationship, the processing unit determines as the port with the improperly linked equipment connected thereto a port with storage of the physical address of the improperly linked equipment at a network device wherein the network device having the physical address to port correspondence relationship is connected to the improperly linked equipment.

13. The connection position specifying method according to claim 11, wherein when a port with storage of the physical address of the improperly linked

equipment and also with storage of a physical address of another network device but without storage of the physical address of the connection position specifying apparatus is found in a certain physical address to port correspondence relationship, the processing unit selects a next one while taking priority of a network device as held at the port with storage of the physical address of the improperly linked equipment.

14. An unauthorized equipment connection position specifying method for specifying a position of equipment as improperly connected to a network configured by connection of a plurality of stages of switches each having a plurality of ports, said method comprising the steps of:

storing information as to each said switch for identifying switches up to a terminate end connected to respective ports of the switches; and

sequentially selecting, based on the stored information specifying the switches, those switches in which a port for connection to the improperly linked equipment and a port linked to itself are different from each other with the switch linked to itself being as a reference to thereby specify the position of the improperly linked equipment.