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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
13 February 2014 (13.02.2014)

(10) International Publication Number
WO 2014/024481 A1

(51) International Patent Classification:
*H04L 12/46* (2006.01) *G06F 21/30* (2013.01)

(21) International Application Number:
PCT/JP2013/004756

(22) International Filing Date:
6 August 2013 (06.08.2013)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
2012-175120 7 August 2012 (07.08.2012) JP

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

(72) Inventors: **YAMATO, Junichi**; c/o NEC CORPORATION, 7-1, Shiba 5-chome, Minato-ku, Tokyo, 1088001 (JP). **SUGAWARA, Tomoyoshi**; c/o NEC CORPORATION, 7-1, Shiba 5-chome, Minato-ku, Tokyo, 1088001 (JP).

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

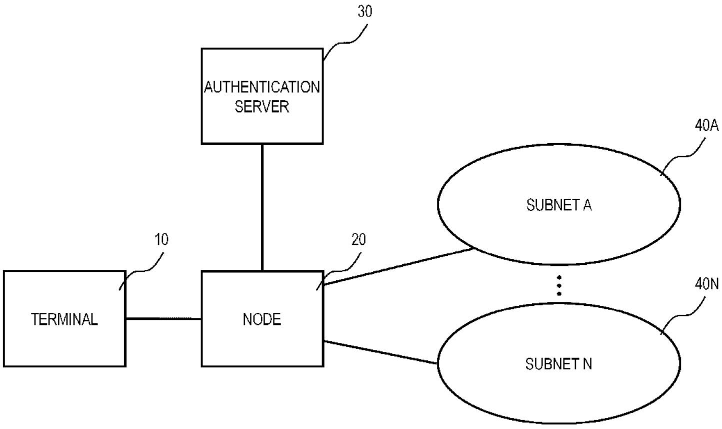
(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

**Published**:

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

(54) **Title**: NETWORK SYSTEM, AUTHENTICATION APPARATUS, SUBNET DECIDING METHOD AND PROGRAM



(57) **Abstract**: A network system in which a user may be subordinated to an appropriate one of a plural number of subnets is disclosed. The network system includes a node(s) connected to a plurality of subnets and an authentication apparatus. In response to a connection request from a terminal(s) via the node, the authentication apparatus decides on a subnet to be connected to the terminal(s), based upon the subnet(s) the terminal has the connection right to and upon the subnets connected to the node.

# Description

# Title of Invention: NETWORK SYSTEM, AUTHENTICATION APPARATUS, SUBNET DECIDING METHOD AND PROGRAM

## Field

[0001] (CROSS-REFERENCE TO RELATED APPLICATION)

The present application asserts priority rights upon JP Patent Application No. 2012-175120 filed in Japan on August 7, 2012. The total contents of disclosure of the Patent Application of the senior filing date are to be incorporated by reference into the present Application.

This invention relates to a network system, an authentication apparatus, a subnet deciding method and a program and, more particularly, to a network system including a plurality of subnets, an authentication apparatus, a subnet deciding method and a program. Note that a sub-network herein is expressed as a subnet.

## Background

[0002] In companies or educational organizations, such a network configuration comprised of a number of hierarchical subnets, which are in meeting with the constitutions of the organizations, is used. In such network configuration, there is known a method to decide on a subnet, a terminal is to belong to, using terminal authentication exploiting IEEE802.1x and RADIUS (Remote Authentication Dial In User Service), as an example.

[0003] In Non Patent Literatures 1 and 2, there is proposed a technology known as OpenFlow, which recognizes communication as an end-to-end flow and which manages path control, recovery from malfunctions, load distribution and optimization on the flow-by-flow basis. Example 2 of Non Patent Literature 1 shows constructing a virtual network, such as VLAN (Virtual Local Area Network) by combination of a plurality of OpenFlow switches and an OpenFlow controller, referred to below as 'controller', which exercises centralized control on the OpenFlow switches.

[0004] Patent Literature 1 discloses a system and a method for management according to which management contents are made to differ for a plurality of managed apparatuses in a network to reduce management loads.

[0005] Patent Literature 2 discloses a method and an apparatus for controlling user terminal connection whereby it is possible to limit the number of sessions connectible at the same time and to reduce forced session interruptions.

## Citation List

## Patent Literature

[0006] PTL 1: JP Patent Kokai Publication No. JP-A-2003-162510

PTL 2: JP Patent Kokai Publication No. JP-A-2006-148648

## Non Patent Literature

[0007] NPL 1: Nick McKeown and seven others, "OpenFlow: Enabling Innovation in Campus Networks", [online], [retrieved on July 13, Heisei24 (2012)], Internet <URL: http://www.openflow.org/documents/openflow-wp-latest.pdf>

NPL 2: "OpenFlow Switch Specification" Version1.1.0 Implemented (Wire Protocol 0x02), [online], [retrieved on July 13, Heisei24 (2012)], Internet <URL: http://www.openflow-spec-v1.1.0pdf>

## Summary

## Technical Problem

[0008] The following analysis is given by the present invention. In companies or organizations, it is customary that a user belongs to two or more organizations or groups. For example, a member of a company is an employee of the company and also belongs to a business division or to a section or department. A student of a school is a school pupil while being a member of a class or a department. As the case may be, he/she belongs to a laboratory, seminar, club or circle. If, in such case, as a manner for a user is to connect to a target subnet, it is customary that he/she accesses to a target subnet via a subnet he/she routinely uses or via a subnet of a lower most layer.

[0009] However, with the above access methods, it is necessary to pass through one or more subnets interposed between the user and the target subnet, thus incurring network costs, which offers a problem.

[0010] Although it may be contemplated that a user directly accesses to the target subnet each time he/she needs such access, the user in such case has to be authenticated at the target subnet. Moreover, the user may not, in such state, connect to other subnets, counted for a problem.

[0011] In short, in a system exploiting IEEE802.1x and RADIUS, the user is allocated to a sole subnet and allowed to access under such constraint. Under such configration, the user may not connect to an appropriate one of a plurality of subnets.

[0012] The same applies to Example 2 of Non Patent Literature 1, which simply sets out that a controller manages user authentication and that the user position information is used to tag the traffic.

[0013] Likewise, Patent Literatures 1, 2 lack in explicit disclosure or suggestion as to allowing a user to connect to the appropriate one among a plurality of subnets.

[0014] It is an object of the present invention to provide a network system, an authentication apparatus, a method for deciding on a subnet and a corresponding program, whereby it is possible to allow a user to connect to an appropriate one among a plurality of subnets.

## Solution

[0015] In a first aspect of the present invention, there is provided a network system which comprises a node(s) connected to a plurality of subnets, and an authentication apparatus that, in response to a connection request from a terminal(s) via the node, decides on a subnet(s) to be connected to the terminal(s), based upon subnet(s) the terminal(s) has a connection right to and upon subnet(s) the node is connected to.

[0016] In a second aspect of the present invention, there is provided an authentication apparatus, wherein the authentication apparatus is connected to a node(s) connected in turn to a plurality of subnets. The authentication apparatus decides, in response to a connection request from a terminal(s) via the node, on the subnet(s) to be connected to the terminal(s), based upon the subnet(s) the terminal(s) has a connection right to and upon the subnet(s) the node is connected to.

[0017] In a third aspect of the present invention, there is provided a method for deciding on a subnet(s). The method comprises a step of an authentication apparatus, connected to a node(s) connected in turn to a plurality of subnets, accepting, from a terminal(s), via the node, a connection request to the subnet(s) the terminal(s) has a connection right to, and a step of the authentication apparatus deciding on the subnet(s) to be connected to the terminal(s), in response to the connection request, based upon the subnet(s) the terminal has the connection right to and upon the subnet(s) the node is connected to.

[0018] In a fourth aspect of the present invention, there is provided a program which allows a computer configuring an authentication apparatus, connected to a node(s) which is connected to a plurality of subnets, to perform a processing of accepting, from a terminal(s), via the node, a connection request to the subnet(s) the terminal(s) has a connection right to, and a processing of deciding on the subnet(s) to be connected to the terminal(s), in response to the connection request, based upon the subnet(s) the terminal(s) has a connection right to and upon the subnets the node is connected to.

## Advantageous Effects of Invention

[0019] According to the present invention, it is possible to allow a user to be allocated to an appropriate one of a plurality of subnets.

## Brief Description of Drawings

[0020] [fig.1]Fig.1 is a schematic block diagram showing a configuration of exemplary embodiment 1 according to the present invention.

[fig.2]Fig.2 is a schematic block diagram showing a configuration of an authentication server of exemplary embodiment 1 of the present invention.

[fig.3]Fig.3 is a diagrammatic view showing example entries in a node database (node DB) of the authentication server of exemplary embodiment 1 of the present invention.

[fig.4]Fig.4(A), Fig.4(B), Fig.4(C) and Fig.4(D) are diagrammatic views showing example entries in an authentication database (authentication DB) of an authentication server according to exemplary embodiment 1 of the present invention.

[fig.5]Fig.5 is a sequence diagram showing the flow of authentication processing according to exemplary embodiment 1 of present invention.

[fig.6]Fig.6 is a flowchart showing the operation of the authentication server according to exemplary embodiment 1 of present invention.

[fig.7]Fig.7 is a block diagram showing a modification 1-2 of the authentication server according to exemplary embodiment 1 of the present invention.

[fig.8]Fig.8 is a diagrammatic view showing example entries in a connection number table of the authentication server of Fig.7.

[fig.9]Fig.9 is a block diagram showing a variant of exemplary embodiment 1 of the present invention.

[fig.10]Fig.10 is a block diagram showing a modification 2 of the authentication server of exemplary embodiment 1 of the present invention.

[fig.11]Fig.11 is a diagrammatic view showing example entries in a group database (group DB) of the authentication server of Fig.10.

[fig.12]Fig.12(A), Fig.12(B), Fig.12(C) and Fig.12(D) are diagrammatic views showing example entries in an authentication database (authentication DB) of the authentication server of Fig.10.

[fig.13]Fig.13 is a diagrammatic view showing example entries in a node database (node DB) of the authentication server of Fig.10.

[fig.14]Frig.14 is block diagram showing a configuration according to exemplary embodiment 2 of the present invention.

[fig.15]Fig.15 is a block diagram showing a configuration of an authentication server according to exemplary embodiment 2 of the present invention.

[fig.16]Fig.16(A), Fig.16(B), Fig.16(C) and Fig.16(D) are diagrammatic views showing example entries in an authentication database (automatic DB) of the authentication server according to exemplary embodiment 2 of the present invention.

[fig.17]Fig.17 is a diagrammatic view showing example entries in a connection terminal table of exemplary embodiment 2 of the present invention.

[fig.18]Fig.18 is a sequence diagram showing the flow of authentication processing according to exemplary embodiment 2 of the present invention.

[fig.19]Fig.19 is another sequence diagram showing the flow of authentication processing according to exemplary embodiment 2 of the present invention.

[fig.20]Fig.20 is a flowchart showing the operation of an authentication server according to exemplary embodiment 2 of the present invention.

[fig.21]Fig.21 is a block diagram showing a modification 1 of the authentication server according to exemplary embodiment 2 of the present invention.

[fig.22]Fig.22(A), Fig.22(B), Fig.22(C) and Fig.22(D) are diagrammatic views showing example entries in an authentication database (authentication DB) of the authentication server of Fig.21.

[fig.23]Fig.23 is a block diagram showing a modification 2 of the authentication server according to the exemplary embodiment 2 of the present invention.

[fig.24]Fig.24 is a diagrammatic view showing example entries in an account group database (account group DB) of the authentication server of Fig.23.

[fig.25]Fig.25 is a block diagram showing a modification 3 of the authentication server according to the exemplary embodiment 2 of the present invention.

[fig.26]Fig.26 is a block diagram showing a configuration of exemplary embodiment 3 of the present invention.

[fig.27]Fig.27 is a block diagram showing a configuration of an authentication server according to exemplary embodiment 3 of the present invention.

[fig.28]Fig.28(A), Fig.28(B), Fig.28(C) and Fig.28(D) are diagrammatic views showing example entries in an authentication database (authentication DB) of the authentication server according to exemplary embodiment 3 of the present invention.

[fig.29]Fig.29 is a diagrammatic view showing example entries in a node database (node DB) of the authentication server according to exemplary embodiment 3 of the present invention.

[fig.30]Fig.30 is a diagrammatic view showing example entries in a connection terminal table in the authentication server according to exemplary embodiment 3 of the present invention.

[fig.31]Fig.31 is a diagrammatic view showing other example entries in a connection terminal table in the authentication server according to exemplary embodiment 3 of the present invention.

[fig.32]Fig.32 is a sequence diagram showing a flow of authentication processing according to exemplary embodiment 3 of the present invention.

[fig.33]Fig.33 is a sequence diagram showing another flow of authentication processing according to exemplary embodiment 3 of the present invention.

[fig.34]Fig.34 is a flowchart showing the operation of an authentication server according to exemplary embodiment 3 of the present invention.

[fig.35]Fig.35 is a flowchart showing details of processing of deciding on an allocated subnet by the authentication server according to exemplary embodiment 3 of the present invention.

[fig.36]Fig.36 is a block diagram showing modification 1 of the authentication server according to exemplary embodiment 3 of the present invention.

[fig.37]Fig.37(A), Fig.37(B), Fig.37(C) and Fig.37(D) are diagrammatic views showing example entries in an authentication database (automatic DB) of the authentication server of Fig.36.

[fig.38]Fig.38 is a block diagram showing a configuration of exemplary embodiment 4 according to the present invention.

[fig.39]Fig.39 is a block diagram showing a configuration of an OpenFlow switch (OFS) of exemplary embodiment 4 of the present invention.

[fig.40]Fig.40 is a diagrammatic view showing flow entries held by the OpenFlow switch (OFS) of exemplary embodiment 4 of the present invention.

[fig.41]Fig.41 is a tabulated view showing examples of processing contents (actions) that may be set in instruction fields of a flow entry in Fig.40.

[fig.42]Fig.42 is a block diagram showing a configuration of an authentication server of exemplary embodiment 4 of the present invention.

[fig.43]Fig.43(A), Fig.43(B), Fig.43(C) and Fig.43(D) are diagrammatic views showing example entries in an authentication database (authentication DB) of the authentication server of exemplary embodiment 4 of the present invention.

[fig.44]Fig.44 is a block diagram showing a configuration of an OpenFlow controller (OFC) of exemplary embodiment 4 of the present invention.

[fig.45]Fig.45(A) and Fig.43(B) are diagrammatic views showing example entries in a topology database (topology DB) of the OpenFlow controller (OFC) of exemplary embodiment 4 of the present invention.

[fig.46]Fig.46 is a diagrammatic view showing example entries in a connection terminal memory of the OpenFlow controller (OFC) of exemplary embodiment 4 of the present invention.

[fig.47]Fig.47 is a diagrammatic view showing example entries in a subnet database (subnet DB) of the OpenFlow controller (OFC) of exemplary embodiment 4 of the present invention.

[fig.48]Fig.48(A), Fig.48(B) and Fig.43(C) are diagrammatic views showing example entries in the element information in the entries in a subnet database (subnet DB) of Fig.47.

[fig.49]Fig.49 is a sequence diagram showing a flow of authentication processing according to exemplary embodiment 4 of the present invention.

[fig.50]Fig.50 is a sequence diagram showing a flow of packet forwarding processing according to exemplary embodiment 4 of the present invention.

[fig.51]Fig.51 is a flowchart showing the operation of an OpenFlow switch (OFS) according to exemplary embodiment 4 of the present invention.

[fig.52]Fig.52 is a flowchart showing the operation of an OpenFlow controller (OFC) according to exemplary embodiment 4 of the present invention.

[fig.53]Fig.53 is a block diagram showing a modification of the OpenFlow controller (OFC) according to exemplary embodiment 4 of the present invention.

[fig.54]Fig.54 is a diagrammatic view showing example entries in a group database (group DB) of the OpenFlow controller (OFC) of Fig.53 according to exemplary embodiment 4 of the present invention.

[fig.55]Fig.55 is a diagrammatic view showing example entries in a connection terminal memory of the OpenFlow controller (OFC) shown in Fig.53.

[fig.56]Fig.56(A), Fig.56(B), Fig.56(C) and Fig.56(D) are diagrammatic views showing other example entries in an authentication database (authentication database) of the authentication server according to exemplary embodiment 4 of the present invention.

[fig.57]Fig.57 is a block diagram showing a first concrete mode of the present invention.

[fig.58]Fig.58 is a block diagram showing a second concrete mode of the present invention.

[fig.59]Fig.59 is a block diagram showing a configuration of an OpenFlow controller (OFC) of the second concrete mode of the present invention.

## Description of Embodiments

[0021] Initially, outline of an exemplary embodiment of the present invention will be described with reference to the drawings. It is noted that symbols for referring to the drawings are attached to the respective elements merely as examples to assist in the understanding and are not intended to limit the present invention to the illustrated modes.

[0022] In an exemplary embodiment of the present invention, the present invention may be implemented by a configuration comprising a node (corresponding to 20 of Fig.1) connected to a plurality of subnets, and an authentication apparatus (corresponding to an authentication server 30 of Fig.1) performing authentication processing in response to a connection request from a terminal (10 of Fig.1) via a node (20 of Fig.1). More specifically, the present authentication apparatus decides on a subnet to be connected to the terminal (10 of Fig.1) based upon the subnet(s) to which the terminal (10 of Fig.1) has a connection right, and upon the subnets the node (20 of Fig.1) is connected to. The subnet(s) to which the terminal (10 of Fig.1) has the connection right, may be acquired as a result of the authentication processing relative to the terminal (10 of Fig.1).

[0023] It is thus possible to have a terminal connected to an appropriate subnet(s) depending on the terminal's right to connection.

[0024] <Exemplary embodiment 1>

An exemplary embodiment 1 of the present invention will be explained in detail with reference to the drawings. Referring to Fig.1, there is shown a configuration including a terminal 10, a node 20 to which the terminal is connected, an authentication server 30 and two or more subnets 40A to 40N the node 20 is connected to. Although only one terminal 10 and only one node 20 are shown in Fig.1, a plurality each of the terminals and the nodes may also be used.

[0025] The terminal 10 is a device used by a user, such as a computer, a mobile device, a game machine or a mobile phone.

[0026] The node 20 is a network device, such as a network switch, a router or a radio access point. The node 20 refers to e.g., a table in which destinations of connection of ports, such as terminals 10 or subnets 40A to 40N, are stored, in order to accomplish communication between the terminal 10 and the subnets 40A to 40N. It should be noted that, in the above table, the terminal 10 can be identified by a MAC address, as an example. The information concerning which of the subnets are connected to each of the ports may be configured beforehand in the node 20 or may be notified to the node 20 from e.g., a management server (not shown) or the like, at the time of booting or changing the configuration of the network system.

[0027] The authentication server 30 is a device for authentication of a user or terminal, such as a RADIUS server, a DIAMETER server operating in accordance with a DIAMETER protocol or a LADP server operating in accordance with Lightweight Directory Access Protocol, etc.

[0028] The subnets 40A to 40N may each be a network, such as Ethernet (registered trademark), VLAN (Virtual Local Area Network) or VPN (Virtual Private Network). It may also be a circuit, such as an optical network, ADSL (Asymmetric Digital Subscriber Line), ISDN (Integrated Services Digital Network), a 3G network, LTE (UMTS Long Term Evolution), a PHS (Personal Handy-phone System) network, wireless LAN or WiMAX (Worldwide Interoperability for Microwave Access), etc.

[0029] Meanwhile, the node 20 and the authentication server 30 may be interconnected directly or via either a subnet or a devoted network.

[0030] Fig.2 depicts a block diagram showing a configuration of an authentication server according to exemplary embodiment 1 of the present invention. Referring to Fig.2, the authentication server 30 of the present exemplary embodiment includes a node database (DB) 31, an authentication DB 32, a subordination (allocation) decision unit 33, an authentication processing unit 34 and an authentication result notification unit 35.

[0031] The node DB 31 is a database in which to store entries that record the subnets each of the nodes 20 is connected to. Fig.3 depicts a diagrammatic view showing example entries in the node DB 31. Node ID is an identifier uniquely identifying a node, and Subnet ID is an identifier uniquely identifying a subnet. For example, if the node 20 is connected to a plural number of subnets, among the subnets 40A to 40N, subnet IDs of these subnets connected to the node 20 are recorded as entries for the node 20.

[0032] The authentication DB 32 is a database in which to store entries that correlate the information to authenticate a terminal to a list of the subnets to which an authenticated terminal can be connected. The information to authenticate a terminal may be exemplified by an ID/ user name/ account name/ terminal ID/ MAC address, password/ passphrase and a certificate. Fig.4(A), Fig.4(B), Fig.4(C) and Fig.4(D) depict diagrammatic views showing example entries in the authentication DB 32. User ID in Fig.4(A) is an identifier for a user, and may be a user name. Password in Fig.4(A) is a character string used for user authentication. Terminal ID in Fig.4(B) is an identifier uniquely identifying the terminal 10. MAC address in Fig.4(C) is a MAC address of the terminal 10. Certificate in Fig.4(D) is a certificate, such as PKI (Public Key Infrastructure) registered in the terminal, etc. Subnet ID is similar to the subnet ID in the node DB 31, with each entry having one or more subnet IDs.

[0033] The operation of the present exemplary embodiment will now be described with reference to the drawings. Fig.5 depicts a sequence diagram showing a flow of authentication processing according to exemplary embodiment 1 of the present invention. Referring to Fig.5, the terminal 10 initially transmits an authentication request to the node 20 (S01).

[0034] The node 20 forwards the authentication request to the authentication server 30 (S02). The authentication server performs authentication. In case of success in the authentication, the authentication server performs a processing to decide on a subnet to which the terminal belongs (is allocated) and transmits an authentication response to the terminal 10 via the node 20 (S03, S04).

[0035] Based upon the authentication response from the authentication server 30, the node 20 causes the relation of correspondence between the subnet and the terminal 10 (or a port the terminal 10 is connected to) to be stored in its inner table, The node then transmits a packet from the terminal 10 to the relevant subnet.

[0036] In an Example of Fig.5 (of forwarding and returning), authentication is completed by a sole message exchange operation. It is however also possible to perform the message exchange operation a plural number of times depending on the authentication scheme used.

[0037] The sequence for the authentication server 30 to decide on the subnet in Fig.5 will now be described. Fig.6 depicts a flowchart showing the operation of the authentication server according to exemplary embodiment 1 of the present invention. Referring to Fig.6, on receipt of an authentication request from the terminal 10, the authentication processing unit 34 of the authentication server 30 refers to the authentication DB 32 to perform authentication processing (step S101).

[0038] If, as a result of the authentication processing, the authentication is successful (Yes in step A102), the subordination (allocation) decision unit 33 acquires, from the node DB

31, a list of subnets the node 20 as the source of the request for authentication is connected to (step S103).

[0039] The subordination (allocation) decision unit 33 then collates the list of subnets acquired in step S103 to the information on the subnets the authentication processing unit 34 has acquired from the authentication DB 32. The subnets in the information thus acquired are those the terminal has a connection right to (step S104).

[0040] The authentication result notification unit 35 transmits a response of success in authentication via the node 20 to the terminal 10 (step S105). The response transmitted has appended thereto the information on the subnets decided on in the step S104.

[0041] If, as a result of authentication processing of step S101, the authentication failed (No at step S102), the authentication result notification unit 35 transmits a authentication failure response via the node 20 to the terminal 10 (step S106).

[0042] If, in step S104, there are a large number of subnets the terminal 10 should belong to, such a method selecting one or more out of the subnets by using a random number(s), as an example, may be used.

[0043] According to the present exemplary embodiment, it is possible to cause the terminal 10 to belong (be allocated) to a plurality of subnets just by performing the processing of authentication.

[0044] <Modifications of exemplary embodiment >

Several modifications of the above described exemplary embodiment 1 will now be illustrated.

<Modification 1-1 (using priority level)>

Such a modification may be thought of which consists in donating the priority level to the subnet ID from one terminal 10 of the authentication DB 32 of the authentication server 30 to another. By such modification, in the processing of deciding on the subnet in step S104 of Fig.6, it is possible for the authentication server 30 to select the subnet(s) having a higher priority levels out of the subnets connected to the node 20. In donating the priority levels to the subnet IDs, there is, in addition to a method of adding a priority information field to respective fields, such a method of arraying the subnet IDs of the respective entries in the (descending) order of the priority levels. By so doing, the terminals may be connected to the subnets as the priority level set in each terminal is taken into consideration.

[0045] <Exemplary embodiment 1-2 (number of terminals connected is taken into consideration)>

Fig.7 is a block diagram showing another modification of the authentication server of the exemplary embodiment 1 of the present invention. The present modification differs from the configuration of the authentication server shown in Fig.2 in that a connection number table 36 is added so that the subordination (allocation) decision unit may additionally refer to the connection number table 36 in order to decide on the subnet(s) the terminal 10 should belong to.

[0046] Fig.8 is a diagrammatic view showing example entries in the connection number table 36 of an authentication server 30A of Fig.7. Referring to Fig.8, the connection number table 36 is a table that manages the number of the connected terminals from one subnet to another.

[0047] In step S104 of Fig.6, the authentication server 30A of Fig.7 gets, from the connection number table 36, the number(s) of the terminals connected to the subnet(s), insofar as the information on the subnets acquired in step S103 coincides with the information on the subnets which the authentication processing unit 34 has acquired from the authentication DB 32 and which the terminal has the connection right to. The authentication server 30A decides on the subnet(s), the terminal 10 should belong to, out of the coincident subnets, taking into consideration the number of the terminals connected to the subnet(s). If once a subnet(s), the terminal 10 should belong to, is decided on, the authentication server 30A increments the number of the terminals connected to the relevant subnet(s) in the connection number table 36 by one. In case the terminal 10 has become detached from the node 20, the authentication server 30A decrements the number of the terminals connected to the relevant subnet(s) in the connection number table 36 by one.

[0048] In selecting the subnet(s) taking the number of the terminals connected into consideration, such a method may be used, as a selection rule, in which such a subnet(s) having the least number of the connected terminals is selected. By so doing, it is possible to average out (or balance) the numbers of the connected terminals among (/between) the subnets 40A to 40N.

[0049] <Modification 1-3 (subnet load is taken into consideration)>

Fig.9 depicts a block diagram showing a further modification of the exemplary embodiment 1. The present modification differs from the global configuration shown in Fig.1 in that a load measurement unit 50 is connected to an authentication server 30B.

[0050] The load measurement unit (or apparatus) 50 of Fig.9 measures volume of packets per unit time, or packet use rate, for each of the subnets 40A to 40N.

[0051] Based upon the results of the measurement by the load measurement unit 50, the authentication server 30B of Fig.9 in step S104 of Fig.6 selects such one(s) of the subnets 40A to 40N, connected to the node 20, which are least in the number of packets or lowest in the packet use rate and to which the terminal 10 is connectable. In this case, load balancing may be achieved among the subnets 40A to 40N.

[0052] <Modification 1-4 (introducing subnet grouping)>

Fig.10 is a block diagram showing a further modification of an authentication server of exemplary embodiment 1 of the present invention. The present modification differs from the configuration of the authentication server shown in Fig.2 in that a group DB 37 to manage subnets in units of groups is added and referred to in authentication processing or in decision on a subordination subnet(s).

[0053] Fig.11 shows example entries in the group DB 37 of Fig.10. Referring to Fig.11, the entries are configured to correlate a group ID, uniquely identifying a group, to subnet IDs of subnets belonging to the group.

[0054] In case such group DB 37 is provided, it is possible to simplify the authentication DB 32 and the node DB 31 of Fig.2 as follows: Fig.12(A), Fig.12(B), Fig.12(C) and Fig.12(D) show example entries in the authentication DB 32 in which, in place of one or more subnet IDs, a group ID of subnets, the terminal 10 and/or the user has the right of connection to, are/is entered. Fig.13 shows example entries in the node DB 31. It is seen that, in place of one or more subnet IDs, a group ID of the subnet connected to the node in question is entered for use for correlation.

[0055] The authentication server 30C in the present configuration uses the authentication DB 32, node DB 31 and the group DB 37 to select, among the groups of the subnets 40A to 40N connected to the node 20, such group of the subnets to which the terminal 10 is connectable. By so doing, the labor on the part of a management operator in correlating the node, terminal and the subnets may be relieved. In the example of Fig.10, the group DB 37 is shared between the node DB 31 and the authentication DB 32. Alternatively, the group DB may be used only by one of the node DB and the authentication DB. Still alternatively, different group DBs may be provided and separately used, respectively.

[0056] Exemplary embodiment 1 and its modifications have been shown and described above. It is noted that the respective modifications may be combined together. For example, the modifications 1-2, 1-3 and 1-4 may be combined together to decide on the subordination subnet(s) such as to take the number of terminals or the load in units of the subnet groups into consideration.

[0057] <Exemplary embodiment 2>

An exemplary embodiment 2 of the present invention, in which it is presupposed that the priority levels in the connection to the subnets are already set among the terminals, will now be described. Fig.14 depicts a block diagram showing a configuration of the exemplary embodiment 2 of the present invention. Referring to Fig.14, the present exemplary embodiment 2 includes two or more terminals 10A to 10M, a node 20, the terminals 10A to 10M are connected to, an authentication server 60 and two or more subnets 40A to 40N to which, the node 20 is connected. The node 20 and the subnets 40A to 40N are similar to the corresponding units in exemplary embodiment 1 and hence the corresponding explanation is here dispensed with. The terminals 10A to 10M are also similar to the terminal in the exemplary embodiment 1 except that the present exemplary embodiment has a plurality of the terminals. The following explanation is centered about the difference of the present exemplary embodiment from exemplary embodiment 1.

[0058] Fig.15 depicts a block diagram showing a configuration of an authentication server of exemplary embodiment 2. Referring to Fig.15, the authentication server includes a node DB 31, an authentication DB 32, a subordination (allocation) decision unit 33, an authentication processing unit 34, an authentication result notification unit 35, a connection terminal table 38 and a connection cancel notification unit 35-2.

[0059] The node DB 31 is similar to the node DB 31 of the authentication server 30 of exemplary embodiment 1.

[0060] The authentication DB 32 is approximately the same as the authentication DB 32 of the authentication server 30 of exemplary embodiment 1, with the exception that the connection priority level for each terminal or each user is already added in each entry. Fig.16(A), Fig.16(B), Fig.16(C) and Fig.16(D) show entries in the authentication DB 32 of the authentication server 60 of the present exemplary embodiment. In Fig.16(A) through to Fig.16(D), a 'connection priority (level) field is added as the entry in the authentication DB 32 of the authentication server 30 of the exemplary embodiment 1 shown in Fig.4(A) through to Fig.4(D).

[0061] The 'connection priority (level)' will now be explained. The connection priority (level) is a value indicating the priority level when a subject (terminal/ user) authenticated by each entry of the authentication DB 32 uses the subnets 40A to 40N. In case a pre-set number of users are already connected to a subnet, and a user with a high priority level subsequently has requested connection to the subnet, the authentication server 60 of the present exemplary embodiment selects out a user with a low priority level, out of the pre-connected users, to cancel the connection of the user with the low priority level.

[0062] The connection terminal table 38 is a table that records the terminals 10A to 10M connected to each of the subnets 40A to 40N. Fig.17 shows example entries in the connection terminal table 38. In the example of Fig.17, a subnet ID is correlated to the connection terminal information concerning the total of the terminals connected to the subnet in question. Each of the connection terminal information contains a node ID specifying the node a terminal of interest is connected to, the terminal information of the terminal of interest, such as MAC address, certificate, username or a port for connection, and the connection priority (level).

[0063] By having the node ID, terminal information and the connection priority (level) thus recorded in the connection terminal information, the processing of retrieving the terminal connection priority (level), terminal information and the node ID at the time of decision on the subnet(s) may be dispensed with. Hence, enhancement the processing speed is expectable.

[0064] It is assumed that, in the present exemplary embodiment, an upper limit of the number of terminals that can be connected at the same time is already set in each of the subnets 40A to 40N. It is also assumed that the authentication server 60 already knows the upper limit of the number of the terminals from a field for the upper limit value of the number of the connected terminals provided in the connection terminal table 38.

[0065] The operation of the present exemplary embodiment will now be described in detail with reference to the drawings. Fig.18 and Fig.19 depict sequence diagrams representing the flow of authentication processing according to exemplary embodiment 2. Fig.18 is a sequence diagram for a case where the number of connected terminals is less than an upper limit of the number of the connected terminals, and the basic flow is similar to exemplary embodiment 1 shown in Fig.5. Hence, the description of the sequence diagram is here dispensed with.

[0066] Fig.19 is a sequence diagram for a case where, on receipt of the request for authentication for the terminal 10A, the number of the connections of the subnet, decided as a destination, to the terminals has reached the upper limit. Specifically, on accepting a request for authentication from the terminal 10A via the node 20 (S11, S12), the authentication server 60 decides on the terminal whose connection is to be canceled (it is assumed herein to be the terminal 10B). The authentication server accordingly cancels the connection for the terminal 10B via the node 20 (S13, S14). On the other hand, the authentication server 60 transmits an authentication response to the terminal 10A via the node 20 (S15, S16).

[0067] An authentication request is sent from the terminal 10 the connection for which has been canceled (S17, S18). Since the number of the terminals connected to the subnet of interest remains at the upper limit value, the authentication server 60 determines that the requesting terminal is to be subordinated (allocated) to another subnet. The authentication server accordingly transmits an authentication response to the terminal (S19, S20).

[0068] The operation of the node 20 in forwarding the authentication response and in forwarding a packet following the authentication is the same as that of the node 20 of exemplary embodiment 1. On receipt of the connection cancel from the authentication server 60, the node 20 wipes out the information concerning the terminal of interest to handle that the terminal as non-authenticated terminal.

[0069] The transmission of the connection cancel notification to the terminal 10B from the authentication server 60 of S14 of Fig.19 may be dispensed with. In such case, the node 20 discontinues packet forwarding to the terminal 10B. In case the connection cancel is notified from the node 20 to the terminal 10B, as shown in Fig.19, the terminal 10B, the connection for which has been canceled, is able to promptly request authentication, thus reducing the time until re-commencing the communication.

[0070] The sequence of operations in deciding on the subnet by the authentication server 60 of Fig.18, Fig.19 will now be explained. Fig.20 depicts a flowchart showing the operation of the authentication server 60 according to exemplary embodiment 2. Referring to Fig.20, on receipt of a request for authentication from the terminal 10, the authentication processing unit 34 of the authentication server 60 refers to the authentication DB 32 to perform processing for authentication (step S201). It is noted that a terminal is sometimes referred to as a terminal 10 if there is no particular necessity to distinguish among the terminals 10A to 10M.

[0071] If, as a result of the processing for authentication in step S201, the authentication failed (No at step S202), the authentication result notification unit 35 transmits a response of failed authentication via the node 20 to the terminal 10 (step S203).

[0072] If, as a result of the processing for authentication, the authentication is successful (Yes at step S202), the subordination (allocation) decision unit 33 acquires, from the node DB 31, a list of the subnets, the node 20 of the source of the request for authentication is connected to, and the connection priority (step S204).

[0073] Next, the subordination (allocation) decision unit 33 collates a list of subnets acquired in step S204 to the information concerning the subnets acquired by the authentication processing unit 34 from the authentication DB 32. It is noted that the right of connection to the subnets contained in the information is owned by the terminal of interest. The subordination (allocation) decision unit thus decides, from the subnets, as found upon the collation to be coincident, the subnet(s) to which the terminal 10 is to be subordinated (step S205).

[0074] The subordination (allocation) decision unit 33 then acquires, from the connection terminal table 38, a group of the connection terminal information of the subnet(s) decided on as described above (step S206) to check whether or not the decided number of the terminals connected to the subnet(s) is less than an upper limit value (step S207).

[0075] If, as a result of the above check, the decided number of the terminals connected to the subnet(s) is less than an upper limit value (Yes at step S207), the subordination (allocation) decision unit 33 adds the information on the terminal, which has won success in the outstanding authentication, to the connection terminals for the subnet(s) of interest in the connection terminal table 38 (step S211). The authentication result notification unit 35 transmits a response of success in authentication, along with the appended information concerning the subnet(s) as decided on in step S205, via the node 20 to the terminal 10 (step S212).

[0076] If conversely the result of the above check indicates that the decided number of the terminals connected to the subnet(s) has reached the upper limit value (No at step S207), the subordination (allocation) decision unit 33 checks to see if there is any terminal(s) among the connected terminals, acquired in step S206, which has a lower priority level than the terminal which has won success in the outstanding authentication (step S208). Should there be no pertinent terminal, processing reverts to step S205 to select another subnet (No at step S208).

[0077] If conversely there is any terminal(s) among the terminals connected to the subnet(s), which has a lower priority level than the terminal which has won success in the outstanding authentication, the subordination (allocation) decision unit 33 selects, out of the terminal(s), such terminal whose connection is to be canceled (step S209). The subordination (allocation) decision unit notifies to the node 20 that connection of such terminal is to be canceled (step S210). The operation that ensues is the same as that in case the number of the terminals connected to the subnet(s) is less than the upper limit value (steps S211, S212). It is noted that, in step S211, the terminal whose connection has been canceled, and the terminal, decided to be newly connected, are interchanged.

[0078] If there are a large number of subnets to which the terminal 10 should be subordinated, such a method of selecting one or more out of the subnets by using a random number(s), as an example, may be used, as in exemplary embodiment 1 shown above.

[0079] In the present exemplary embodiment, described above, the subnet(s), the terminal should belong to, can be decided on taking the terminal-based connection priority level into consideration, thus adding to the advantageous effect of exemplary embodiment 1. It is noted that, in the present exemplary embodiment, the upper limit is set to the number of the terminals connectible to each subnet. Hence, there may be cases wherein connection of a terminal to the subnet(s) is not possible even though the terminal has won success in authentication.

[0080] <Modifications of exemplary embodiment 2>

Several modifications of the above described exemplary embodiment 2 will now be described.

<Modification 2-1 (introducing a subnet group)>

Fig.21 depicts a block diagram showing a modification of the authentication server of exemplary embodiment 2 according to the present invention. The present modification differs from the configuration of the authentication server 60 shown in Fig.15 in that a group DB 37 which manages the subnets on the group basis (units) is added and referred to during the time of processing of authentication or decision on the subordination subnet(s).

[0081] The group DB 37 and a node DB 31 are similar to the group DB 37 and the node DB 31 of modification 1-4 of the exemplary embodiment 1 described above (see Fig.11 and Fig.13).

[0082] Fig.22 shows example entries in the authentication DB 32, in which, in place of one or more subnet IDs, a group ID to which a terminal 10 or a user has the right of connection, is entered and used for correlation.

[0083] As in modification 1-4 of the exemplary embodiment 1, described above, an authentication server 60A selects, using the authentication DB 32, node DB 31 and the group DB 37, a group of subnets, the terminal 10 can be connected to, from among the subnets 40A to 40N, which are connected to the node 20 and which form a group of the entire subnets. By so doing, the labor on the part of a management operator in correlating the node, terminal and the subnets may be relieved. In the example of Fig.21, the group DB 37 is shared between the node DB 31 and the authentication DB 32. Alternatively, the group DB may be used by only one of the node DB and the authentication DB. Still alternatively, different group DBs may be provided and separately used by the node DB and the authentication DB, respectively

[0084] <Modification 2-2 (management based upon the connection priority level group)>

Fig.23 depicts a block diagram showing another modification of the authentication server of the exemplary embodiment 2 of the present invention. In the authentication server 60B of Fig.23, there is no 'connection priority (level)' field in the authentication DB 32. The authentication server 60B includes an account group DB 39 which manages the connection priority level of the terminals 10 on the terminal group basis.

[0085] Fig.24 shows example entries in the account group DB 39. The Example of Fig.24 shows entries that correlate, from one account group to another, the connection priority (level) and accounts belonging to the account group. The accounts used may be usernames of the authentication DB 32, terminal names, MAC addresses or the main key information of the entries, etc.

[0086] The authentication server 60B in the present configuration acquires, from the account group DB 39, the connection priority level of the terminal 10 which has won success in the authentication. In this case, it is unnecessary to set the connection priority level on the account basis, thus simplifying the management.

[0087] <Modification 2-3 (combining the modifications 2-1 and 2-2)>

Fig.25 depicts a block diagram showing a further modification of the authentication server of the exemplary embodiment 2 according to the present invention. An authentication server 60C of Fig.25 shows a configuration that includes both the group DB 37 and the account group DB 39.

[0088] In such formulation, both the subnet management and the connection priority level management may be simplified, as in the modifications 2-1 and 2-2 described above.

[0089] <Exemplary embodiment 3>

Next, exemplary embodiment 3 of the present invention, in which the priority (level) is given to each subnet and used in conjunction with the connection priority (level) on the part of a user to decide on the subnet, the user should belong to, will now be described. Fig.26 shows a configuration of exemplary embodiment 3 of the present invention. Referring to Fig.26, the present exemplary embodiment includes two or more terminals 10A to 10M, a node 20 the terminals 10A to 10M are connected to, an authentication server 70, and two or more subnets 40A to 40N the node 20 is connected to. The terminals 10A to 10M, node 20 and the subnets 40A to 40N are similar to the corresponding components of the exemplary embodiment 2 and hence the corresponding description is dispensed with. The following explanation is centered on the difference of the present exemplary embodiment from exemplary embodiment 2.

[0090] Fig.27 depicts a block diagram showing a configuration of the authentication server 70 of the present exemplary embodiment 3. Referring to Fig.27, the authentication server includes a node DB 31, an authentication DB 32, a subordination (allocation) decision unit 33, an authentication processing unit 34, an authentication result notification unit 35, a connection terminal table 38 and a connection cancel notification unit 35-2. In the present exemplary embodiment, the basic configuration is similar to the configuration of the authentication server 60 of exemplary embodiment 2 shown in Fig.15. However, the configuration of the present exemplary embodiment differs from the configuration of Fig.15 as to entry configurations in the node DB 31, authentication DB 32 and the connection terminal table 38 and as to the operation of the subordination (allocation) decision unit 33. These different parts will now be discussed in detail.

[0091] Fig.28(A), Fig.28(B), Fig.28(C) and Fig.28(D) show example entries in the authentication DB 32 of the authentication server 70. These example entries correspond to those of the authentication DB 32 of the authentication server 60 of exemplary embodiment 2 shown in Fig.15 provided that the subnet IDs are omitted.

[0092] Fig.29 shows entry examples in the node DB 31 of the authentication server 70 of the present exemplary embodiment. In distinction from the entries in the node DB 31 of the exemplary embodiments 1 and 2, shown in Fig.3, not only the subnet IDs but also the connection order as well as the permission priority level from each node to each subnet can be stored.

[0093] The 'connection order' herein means the level of priority in using the subnet from each node, and is determined from the throughput, response time, stability and so on of the subnet(s). The higher the connection order, the higher is the quality of the subnet as the network. The 'permission priority (level)' is a value for comparison to the connection priority level of each entry of the authentication DB 32. In case the connection priority level is lower than the permission priority level, a terminal in question is controlled so as not to be connectible to a relevant subnet.

[0094] The connection order and the permission priority level may be set at the time of setting a node, booting or changing its configuration. The network management operator may, of course, modify them in response to the state of load on the subnets.

[0095] The connection terminal table 38 is a table that records the terminals 10A to 10M connected to the subnets 40A to 40N. As shown in Fig.30, the basic configuration of the connection terminal table is the same as that of the connection terminal table 38 of exemplary embodiment 2 shown in Fig.17.

[0096] In the present exemplary embodiment, the connection terminal table 38 may be configured on the node-by-node basis (i.e. per node units). Fig.31 shows example entries for such case. By so doing, it becomes possible to improve the retrieving performance of the connection state on the node-by-node basis.

[0097] It is also assumed that, in the present exemplary embodiment, an upper limit of the number of terminals that can be connected at the same time is already set in each of the subnets 40A to 40N. It is also assumed that the authentication server 70 already knows the upper limit of the number of the terminals from e.g., a field for the upper limit value of the number of the connected terminals which is provided in the connection terminal table 38.

[0098] The operation of the present exemplary embodiment will now be explained in detail with reference to the drawings. Fig.32 and Fig.33 depict sequence diagrams showing the flow of a processing for authentication according to exemplary embodiment 3 of the present invention. The sequence diagram of Fig.32 is for a case where the number of the terminals connected is less than the upper limit value of the number of the terminals connected. Since the basic flow is similar to that of exemplary embodiment 1 shown in Fig.5, the corresponding explanation for such case is dispensed with for simplicity.

[0099] Fig.33 depicts a sequence diagram for a case in which, as a result of accepting a request for authentication from the terminal 10A, the number of the connections of the terminals to the subnet, decided on as the destination of connection, has reached the upper limit value. Specifically, on receiving a request for authentication from the terminal 10A via the node 20 (S11, S12), the authentication server 70 decides on the terminal, whose connection is to be canceled, here assumed to be the terminal 10B, and proceeds to cancel the connection for the terminal 10B via the node 20 (S13, S14). On the other hand, the authentication server 70 transmits an authentication response to the terminal 10A via the node 20 (S15, S16).

[0100] If a request for authentication is received from the terminal 10B, whose connection has been canceled (S17, S18), a decision is made that the terminal is to be subordinated to another subnet because the number of the terminals connected to the former subnet has reached and is remaining at the upper limit value. The authentication server 70 accordingly transmits an authentication response (S19, S20).

[0101] The operations of the node 20 in transmitting the authentication response and in forwarding a packet following the authentication are similar to those of the node 20 in the exemplary embodiments 1, 2. On receipt of a notification to cancel the connection from the authentication server 70, the node 20 wipes out the information concerning the terminal in question from its memory to handle the terminal as unauthenticated terminal.

[0102] The present exemplary embodiment is similar to exemplary embodiment 2 in that it is possible to omit transmission of connection cancel notification from the authentication server 70 in step S14 of Fig.33 to the terminal 10B.

[0103] The sequence of the operations of the authentication server 70 deciding on the subnet in Fig.32, Fig.33 will now be explained. Fig.34 depicts a flowchart showing the operation of the authentication server 70 of the present exemplary embodiment 3. Referring to Fig.34, on receipt of an authentication request from the terminal 10 (terminal 10A or 10B), the authentication processing unit 34 of the authentication server 70 refers to the authentication DB 32 to perform the processing for authentication (step S301).

[0104] If, as a result of the processing for authentication in step S301, the authentication failed (No at step S302), the connection cancel notification unit 35 transmits an authentication failure response to the terminal 10 via the node 20 (step S303).

[0105] If conversely the processing for authentication has won success (Yes at step S302), the subordination (allocation) decision unit 33 gets, from the node DB 31, a list of the information on a subnet(s) the node 20 of the source of the request for authentication is connected to. The list also includes the connection priority level (step S304).

[0106] The subordination (allocation) decision unit 33 then decides on the subnet, the terminal 10 is to be subordinated to, from the list of the subnet information acquired in the step S304, the connection priority level of the terminal the authentication processing unit 34 acquired from the authentication DB 32, and from the status of each subnet acquired from the connection terminal table 38 (step S305).

[0107] The subordination (allocation) decision unit 33 then checks to see whether or not the number of the terminals connected to the subnet, thus decided on, is less than the upper limit value (step S306).

[0108] If, as a result of the above check, the number of the terminals connected to the subnet, thus decided on, is less than the upper limit value (No in the step S306), the subordination (allocation) decision unit 33 adds the information on the terminal, which has won success in the outstanding authentication, to the terminals in the connection terminal table 38 connected to the relevant subnet(s) (step S309). The connection cancel notification unit 35 transmits the authentication success response, added by the subnet information, as decided on in step S305, to the terminal 10 via the node 20 (step

S310).

[0109] If, as a result of the above check, the number of the terminals connected to the subnet, thus decided on, has reached the upper limit value (Yes AT step S306), the subordination (allocation) decision unit 33 selects, out of the connected terminals as acquired in step S304, the terminal whose connection is to be canceled (step S307). The subordination (allocation) decision unit 33 then notifies the node 20 about the connection cancellation for the terminal in question (step S308). The ensuing operation is the same as that when the number of the terminals connected to the subnet decided on is less than the upper limit value (steps S309, S310). It is noted that, in step S309, the terminal, whose connection has been canceled, and the terminal newly connected, are interchanged.

[0110] The method in step S305 of Fig.34 to decide on the subnet, the terminal 10 is to be subordinated to, will now be explained in more detail. Fig.35 depicts a flowchart showing the processing for the authentication server of exemplary embodiment 3 to decide on the subnet the terminal 10 is to be subordinated to. Referring to Fig.35, the subordination (allocation) decision unit 33 selects, out of the subnets connected to the node 20, such subnets whose permission priority level is not higher than the connection priority level of the terminal 10 (step S401).

[0111] The subordination (allocation) decision unit 33 sorts the subnets, selected in step S401, in the sequence of the descending order of connection (step S402), and selects the subnet which ranks highest in the connection order as a subject (step S403).

[0112] If the number of the terminals, connected to the subnet, selected as the subject, has not reached the upper limit value (Yes at a step S404), the subordination (allocation) decision unit 33 decides on the subject subnet as a subnet to be connected (step S405).

[0113] If conversely the number of the terminals, connected to the subnet, selected as the subject, has reached the upper limit value (No at step S404), the subordination (allocation) decision unit 33 checks to see whether or not there is any terminal, among the terminals connected to the subject subnet, having the connection priority level lower than the connection priority level of the terminal 10. Viz., the subordination (allocation) decision unit checks whether or not, in the selected subject subnet, terminal interchanging is possible (step S406). If there is no terminal, among the terminals connected to the subject subnet, having the connection priority level less than the connection priority level of the terminal 10 (No at step S406), the subordination (allocation) decision unit 33 selects, out of the subnets sorted in the step S402, a subnet which ranks second highest (next) in the connection order (step S407). The subordination (allocation) decision unit then performs the processing following step S404.

[0114] If, among the terminals connected to the subnet, selected as the subject, there is such terminal having the connection priority level lower than the connection priority level of the terminal 10 (Yes at step S406), the subordination (allocation) decision unit 33 decides on the terminal, having the connection priority level lower than the connection priority level of the terminal 10, as a target terminal whose connection is to be canceled. The subordination (allocation) decision unit 33 also decides on the subnet, as selected in step S403 or S407, as a subnet for connection (step S408).

[0115] In the present exemplary embodiment, described above, it becomes possible to decide on the subnet, a terminal is to be subordinated to, in consideration of the connection order of the subnets and the connection priority level of the terminals, thus adding to the advantageous effect of exemplary embodiment 1. It should be noted that, since there is the upper limit to the number of the terminals connectible to each subnet, there may be cases where a successfully authenticated terminal is unable to connect to the subnet.

[0116] <Modification of exemplary embodiment 3>

A modification of exemplary embodiment 3, described above, will now be described.

[0117] <Modification 3-1 (management of connection priority by groups)>

Fig.36 depicts a block diagram showing a modification of an authentication server according to exemplary embodiment 3 of the present invention. In an authentication server 70A of Fig.36, there is no 'connection priority (level)' field in the authentication DB 32, as in the modification 2-2 of exemplary embodiment 2 described above. The authentication server includes an account group DB 39 which manages the connection priority level of the terminals 10 on the terminal group basis.

[0118] Fig.37(A), 37(B), 37(C) and Fif.37(D) show example entries in the authentication DB 32 in the present modification. In the Example of Fig.37(A) to Fig.37(D), just the information for authentication is stored in the authentication DB 32, such that any other account-based information is to be acquired from the account group DB 39 shown as an example in Fig.24.

[0119] The authentication server 70A in the present configuration acquires the connection priority level of the terminal 10, which has won success in the authentication, from the account group DB 39. By so doing, it is unnecessary to set the connection priority level on the account basis, as in the above described modification 2-2 of exemplary embodiment 2, thus simplifying the management.

[0120] <Exemplary embodiment 4>

Exemplary embodiment 4 of the present invention, in which an appropriate subnet may be selected using the OpenFlow shown in Non Patent Literatures 1 and 2, will now be described. Fig.38 depicts a schematic block diagram showing a configuration of exemplary embodiment 4 of the present invention. Referring to Fig.38, the exemplary embodiment 4 includes a terminal 10, an OpenFlow switch (OFS) 20A to which the terminal 10 is connected, an authentication server 81, an OpenFlow controller (OFC) 82, and two or more subnets 40A to 40N connected to the OFS 20A. In the Example of Fig.38, a host apparatus 83, a communication counterpart for the terminal 10, is connected to the subnet 40A among the subnets 40A to 40N.

[0121] The terminal 10 is similar to the terminal 10 of exemplary embodiment 1.

[0122] The OFS 20A is an OpenFlow switch shown in Non Patent Literature 1. Fig.39 depicts a block diagram showing a configuration of the OFS 20A. Referring to Fig.39, the OFS 20A includes a flow entry memory 22 and a packet processor 21 that refers to the flow entries to process a received packet. The flow entry memory holds flow entries configured by the OFC 82.

[0123] Fig.40 shows example flow entries. These flow entries are comprised of a set of fields for rules (matching conditions) against which a packet header is to be matched, a field for flow statistic information (Counters), updated each time a packet matched to the rules (matching conditions) is received, and a field for instructions (Instructions). In the field for instructions, there are stored actions (Actions) to apply to packets matched to the rules (matching conditions). The entries in these fields are coordinated to one another.

[0124] Fig.41 shows, in a tabulated form, several action names and several example contents of the actions as defined in Non Patent Literature 2. OUTPUT is an action to output a received packet at a specified port (interface). SET_VLAN_VID through to SET_TP_DST are actions to modify relevant fields of the packet header.

[0125] The authentication server 81 is an apparatus that authenticates the terminal 10. Fig.42 depicts a block diagram showing a configuration of the authentication server 81. The authentication server 81 includes an authentication DB 811, an authentication processing unit 812 and an authentication result notification unit 813, which are respectively corresponding to the authentication DB 32, authentication processing unit 34 and the authentication result notification unit 35 of the exemplary embodiments 1 to 3. The authentication server 81 is simplified in configuration as compared to the authentication server of the exemplary embodiment 1, 2 or 3 because the OFC 82 that has received the result of authentication from the authentication result notification unit 813 executes next following processing operations.

[0126] Fig.43(A), Fig.43(B), Fig.43(C), Fig.43(D) show example entries in the authentication DB 811. These example entries are equivalent to the entries in the authentication DB 32 of the authentication server 30 of the exemplary embodiment 1 shown in Fig.4(A), Fig.4(B), Fig.4(C), Fig.4(D).

[0127] The OFC 82 corresponds to the OpenFlow controller of Non Patent Literature 2 added by the function to decide on the subnet to which the terminal is to be subordinated. It is assumed that, in the present exemplary embodiment, each of the subnets 40A to 40N includes OFSes each of which corresponds to the OFS 20A. Under such assumption, the OFC 82 is able to exercise path control for the network as a whole. Of course, it is not necessarily needed that the OFSes are contained in the subnets 40A to 40N. In case the OFS is not contained in the subnets 40A to 40N, just the subnet not having the OFS is not subject to path control from the OFC 82.

[0128] Fig.44 depicts a block diagram showing a configuration of the OFC 82 of the present exemplary embodiment. Referring to Fig.44, the OFC 82 includes a subordination (allocation) decision unit 821, a connection terminal memory 822, a topology DB 823, a subnet DB 824, a packet processor 825, a path calculation unit 826 and a flow setting unit 827. The subordination (allocation) decision unit 821 corresponds to the subordination (allocation) decision unit 33 of the authentication server of exemplary embodiments 1 to 3.

[0129] The topology DB 823 is a database in which there is recorded the connection information of the total of the subnets. Fig.45(A), Fig.45(B) show the configurations of entries in the topology DB 823. Fig.45(A) represents the form of a case where links interconnect the OFSes 20A. In this case, the entries are comprised of DPIDs (DataPathIDs), as identifiers of the OFSes 20A, and port numbers, each forming a pair with the DPID. Fig.45(B) represents the form of a case where an apparatus, such as a terminal or a host apparatus or the like, is connected at a remote side of the port. In this case, the entries are comprised of a DPID (DataPathID), as an identifier of the OFS 20A, a port number and a MAC address of the apparatus or the like connected. The connection relationship of the entire subnets may be represented by combinations of these entries.

[0130] The connection terminal memory 822 corresponds to the node DB 31 of the authentication server of the exemplary embodiments 1 to 3. The subnets to which a terminal 10 connected to the OFS 20A is connectible may be saved in the connection terminal memory 822.

[0131] Fig.46 shows example entries in the connection terminal memory 822. In the Example of Fig.46, the DPID and the port number of the OFS 20A, the terminal 10 is connected to, the terminal information, subnet ID of the selected subnet (main subnet ID) and the subnet ID of the subnet to which the terminal is connectible, are correlated one with another. As the terminal information of Fig.46, a MAC address may be used as an example.

[0132] The subnet DB 824 is a database in which there are recorded elements proper to the subnets 40A to 40N. Fig.47 shows example entries in the subnet DB 824. In the Example of Fig.47, the entries are formed of a subnet ID identifying a subnet and the element information.

[0133] Fig.48(A), Fig.48(B) and Fig.48(C) show examples of the element information. As shown in these figures, the element information is described by a set of the DPID of the OFS connected to the subnet and its port numbers, by a MAC address of an apparatus belonging to the subnet or by a set of the DPID of the OFS connected to the subnet (VLAN), its port number and VLAN tag, or the like.

[0134] If a packet requesting setting a flow entry is received from the OFS 20A, the packet processor 825 outputs it to a subordination (allocation) decision unit 821. If a response is returned from the subordination (allocation) decision unit 821, a packet processor 825 outputs to a path calculation unit 826 the packet and a response from the subordination (allocation) decision unit 821 concerning the subordination subnet.

[0135] The subordination (allocation) decision unit 821 refers to a topology DB 823, connection terminal memory 822 and the subnet DB to decide on the subnet the terminal 10 as a source of the input packet should belong to, in such a manner as to respond to the packet processor.

[0136] The path calculation unit 826 refers to the topology DB 823 and the connection terminal memory 822 to calculate a path of forwarding the packets next following the packet requesting setting the flow entry (flow), based upon the packet requesting the flow entry setting and upon the subordination subnet decided on by the subordination (allocation) decision unit 821. The Dijkstra's algorithm may be used as a method for path calculation by the path calculation unit 826.

[0137] The flow setting unit 827 generates, in each OFS on the path as calculated by the path calculation unit 826, a flow entry to allow forwarding the packets along the path, and sets the flow entry in each OFS. In setting the flow entry in each OFS, a FLOW MOD message shown in Non Patent Literature 2 may be used.

[0138] The operation of the present exemplary embodiment will now be described in depth by referring to the drawings. Fig.49 depicts a sequence diagram representing the flow of authentication processing according to exemplary embodiment 4 of the present invention. Referring to Fig.49, initially an authentication request related packet is sent from the terminal 10 (step S21). The OFS 20A then forwards the authentication request related packet to the OFC 82 (step S22). The OFC 82 forwards the authentication request related packet to the authentication server 81 (step S23).

[0139] When the authentication processing has come to a close, the authentication server 81 sends the result as an authentication response packet to the OFC 82 (step S24). The OFC 82 forwards the authentication response packet to the OFS 20A, which then transmits the packet to the terminal 10 (steps S25, S26).

[0140] The basic flow is similar to that of exemplary embodiment 1 shown in Fig.5, except that the OFC 82 and the authentication server 81 are used in the present exemplary embodiment in place of the authentication server 30.

[0141] Fig.50 depicts a sequence diagram representing the flow of communication processing between the terminal 10 and the host apparatus 83 following the authentication processing. Referring to Fig.50, when the terminal 10 has sent a communication packet, addressed to the host apparatus, to the OFS 20A (step S31), the OFS transfers the communication packet to the OFC 82 (step S32). The OFC 82 calculates, based upon the result of the authentication processing, the path to transmit the communication packet to the host apparatus 83 via the subnet 40A, and sets the flow entries on the OFS 20A and on the OFSes disposed in the subnet 40A (steps S33, S34). The OFC transmits the first communication packet, addressed to the host apparatus 83, to the OFSes of the subnet 40A to forward the packet to the host apparatus (steps S35, S36).

[0142] The packet addressed to the host apparatus, which was transmitted from the terminal 10 to the host apparatus, is forwarded by the flow entries, as set in the steps S33, S34, via the OFS 20A and the OFSes on the path in the subnet 40A to the host apparatus 83 (steps S31-2, S32-2, S36-2).

[0143] The operation of the OFS 20A in Fig.49, Fig.50 will now be explained in detail with reference to the drawings. Fig.51 depicts a flowchart representing the operation of the OFS 20A at the time of receipt of a packet in the exemplary embodiment 4 of the present invention. Referring to Fig.51, when the packet is received, the OFS 20A searches, from the flow entry memory 22, a flow entry including a rule (matching condition) that matches to the received packet (step S501).

[0144] If, as a result of the search, no flow entry having the rule (matching condition) that matches to the received packet is found (No at the step S502), the OFS 20A forwards the received packet to the OFC 82 to request generating (setting) the flow entry (step S503). This operation corresponds to packet forwarding from the OFS 20A to the OFC 82 in the step S22 of Fig.49 or in the step S32 of Fig.50.

[0145] If, as the result of the search, a flow entry having the rule (matching condition) that matches to the received packet is found (Yes at step S502), the OFS 20A executes the processing contents (action) stated in the instruction field of the flow entry (step S504). This operation corresponds to the packet transfer from the OFS 20A to the OFC 82 in step S22 of Fig.49 and in step S32 of Fig.50. This operation also corresponds to the packet transfer from the OFS 20A to the subnet 40A in step S32-2 of Fig.50.

[0146] The operation of the authentication server 81 which has received from the OFC 82 an authentication request related packet, in step S23 of Fig.49, will now be described. On receipt of the authentication request related packet, the authentication server 81 search in the authentication DB 811 by the authentication processing unit 812 to perform the authentication processing. Specifically, the authentication server retrieves among the entries shown in Fig.43(A) to Fig.43(D) such entries matching to the source of the authentication request related packet.

[0147] If, as a result of the above mentioned authentication processing, no entries matched to the source of the authentication request related packet, are found, such that authentication failure, the authentication server 81 sends an authentication failed response to the OFC 82 from the authentication result notification unit 813. If, on the contrary, the authentication is successful, the authentication server 81 transmits an authentication success response to the OFC 82, from the authentication result notification unit 813, at the same time as a subnet ID list of the relevant account, included in the retrieved entry, is appended to the response transmitted.

[0148] The operation of the OFC 82 in Fig.49, Fig.50 will now be described in depth with reference to the drawings. Fig.52 depicts a flowchart representing the operation of the OFC 82 of exemplary embodiment 4 according to the present invention. Referring to Fig.52, the OFC 82 on receipt of a packet checks to see whether or not the packet received is the authentication request related packet (step S601). If the packet received is the authentication request related packet (Yes at the step S601), the OFC 82 forwards the packet received to the authentication server 81. This operation corresponds to the packet forwarding from the OFC 82 to the authentication server 81 in step S23 of Fig.49.

[0149] If the packet received is not the authentication request related packet (No at step S601), the OFC 82 checks to see whether or not the packet received is a packet that is sent from the authentication server 81 and that is an authentication response related packet (step S603). In case the packet received is the authentication response related packet from the authentication server 81, the OFC 82 further checks to see whether or not the contents of the authentication response are for authentication success (step S604). If the contents of the authentication response are for authentication failure, the processing of the steps S605 to S607 is skipped.

[0150] In case the contents of the authentication response are for authentication success, the OFC 82 refers to the topology DB 823 and the subnet DB 824 to find out the subnets connectible from the OFS 20A the terminal 10 is connected to. The OFC collates the subnets, thus found out, to the subnet ID list that is annexed to the authentication response and that shows subnet(s) the terminal 10 is connectible to (step S605). The OFC thus finds out a group of the subnets the terminal 10 is connectible to (step S605).

[0151] As the subnets connectible from the OFSes, those subnets containing coincident DPIDs of the element information in the entries in the subnet DBS 824 or those subnets in which, by tracing the links from the topology DB 823, the DPIDs of the connectible OFSes are found to be recorded as the element information in the entries in the subnet DBS 824, may be selected.

[0152] The OFC 82 then decides, among the subnets of the subnet group, thus found out, the subnet(s) the terminal 10 is to be subordinated to (step S606). The OFC 82 then saves, in the connection terminal memory 822, the DPID and the port number of the OFS

20A, the terminal is connected to, the terminal information (MAC address), a main subnet ID (subnet ID of the subordination subnet decided on as described above) and a list of subnets the terminal is connectible to (step S607).

[0153] If the results of the authentication processing, as described above, are obtained, the OFC 82 forwards to the terminal 10 the authentication response via the OFS 20A (step S608).

[0154] If the packet received is neither the authentication request related packet nor the authentication response related packet from the authentication server 81 (No at the step S603), the OFC 82 searches, from the connection terminal memory 822, the entries of the terminal of the source of transmission, that is, the entries having the DPID of the OFS 20A as the source of the received packet, In Port of the packet header, and the source MAC address (step S609).

[0155] If, as a result of the search, there are coincident entries, that is, if the subnet, the terminal is subordinated to, is already defined, the OFC 82 performs path calculations, using the topology DB 823, transmission source MAC address of the packet header of the received packet, destination MAC address, source IP address and the destination IP address (step S611).

[0156] If, as a result of the above search, there are no coincident entries, the OFC 82 calculates the path, using the topology DB 823, destination MAC address, source IP address and the destination IP address. The path calculations are performed using one or more of the ports of the OFS 20A belonging to the subnet, the terminal 10 is connectible to, as start point(s) (step S612).

[0157] The OFC 82 then selects, out of the results of the path calculations, having the respective ports as start points, the path calculation result with the lowest network costs, as a path (step S613). The path with the lowest network cost may be calculated using the number of hops or the response time lengths. Of course, the load states of the respective subnets may be taken into consideration.

[0158] When the path calculations have come to a close, the OFC 82 calculates, in its flow setting unit 827, the flow entry to be set in each OFS on the calculated path (step S614).

[0159] The OFC 82 then configures, in the flow entry memory 22 of each OFS, the flow entries calculated as described above (step S615). This operation corresponds to the flow entry setting processing of the steps S33, S34 of Fig.50.

[0160] Finally, the OFC 82 transmits the received packet to the OFS at the trailing end of the path calculated to instruct sending the received packet to the destination host apparatus 83 from the port connected to the destination of the received packet (step S615). This operation corresponds to an instruction to output a packet of step S35 of Fig.50.

[0161] If, in the above step S605, there are a plurality of subnets, the terminal 10 is to be subordinated to, selection may be made out of those subnets by a method that uses random numbers. If the arraying order of subnets in the subnet list is the order of priority levels, the terminal may be connected to subnet(s) of the higher priority level(s).

[0162] In the flowchart of Fig.52, the subnets, the OFSes are connectible to, are calculated in the step S605. It is however also possible to search for links with respect to the respective OFSes in advance to calculate the subnets that are connectible. Doing so may speed up the processing.

[0163] In the present exemplary embodiment, described above, it is possible not only to decide on the subordination subnets but also to manage end-to-end path control.

[0164] <Modification of exemplary embodiment 4]

Certain modifications of exemplary embodiment 4 will now be described.

[0165] <Modification 4-1 (introducing a subnet group)>

Fig.53 depicts a block diagram showing a modification of an OFC according to exemplary embodiment 4 of the present invention. In an OFC 82A of Fig.53, as in modification 1-4 of the exemplary embodiment 1, a group DB 828 is added to manage the subnets on the group basis, and is referred to in deciding on the subordination subnet.

[0166] Fig.54 shows example entries in the group DB 828. Referring to Fig.54, the group ID as an identifier uniquely indicating a group is correlated to subnet IDs of subnets belonging to the group.

[0167] In the present modification, the entries in the connection terminal memory 822 are simplified as will be shown below. Fig.55 shows example entries in the connection terminal memory 822 of Fig.53. In the example of Fig.55, the group ID is shown correlated in place of the group of the subnet IDs of the subnets the terminal is connectible to.

[0168] In the present modification, the entries in the authentication DB 811 of the authentication server 81 are also simplified as will be shown below. Fig.56(A), Fig.56(B), Fig.56(C) and Fig.56(D) show example entries in the authentication DB 811 of the authentication server 81 in case the group DB 828 has been added to the OFC 82A. In the example of Fig.56, the group ID is shown correlated in place of the group of the subnet IDs the terminal is connectible to.

[0169] In the present configuration, the group of the subnets, the terminal 10 is connectible to, is selected from the group of the subnets 40A to 40N connected to the OFS 20A, using the group DB 828. Doing so may relieve the labor of a management operator involved in correlating the node, terminal and the subnets.

[0170] <Modification 4-2 (integration of the authentication server and the OFC>

In the above described exemplary embodiment 4, it is presupposed that the authentication server 81 and the OFC 82 are provided independently of each other. Alternatively, the function of authentication may be owned by the OFC 82. In this case, processing may be speeded up because no communication is needed for authentication. Of course, the advantageous effect of the invention of exemplary embodiment 4 is intact.

[0171] Several additional modifications of the present invention will now be described.

<Modification 5-1 (the node having the authentication function>

In the exemplary embodiments 1 to 3, it is the authentication servers 30, 60 or 70 that take charge of authentication. However, such a configuration may be used in which a node 20C has the authentication function (authentication unit 201) equivalent to the authentication server 30, as shown in Fig.57. In this configuration, it may be contemplated that, when the values of the DBs are modified at the time of installation, configuration modification or booting, the information updated as a result of the modifications may be acquired or set at a pre-set time interval.

[0172] In this case, communication is unneeded for authentication, so that an accelerated processing is expectable, at the same time as the authentication server does not prove a bottleneck. Moreover, authentication may be performed even in case the communication to the authentication server is interrupted. Of course, the advantageous effect of the invention of exemplary embodiment 4 is kept intact.

[0173] <Modification 5-2 (median form between the modification 5-1 and the exemplary embodiments 1 to 3)>

In case communication with the authentication servers 30, 60 and 70 is possible, authentication may be done by the authentication servers 30, 60 and 70. In case of interruption, a configuration in which a node executes authentication may be used. If, in this configuration, communication with the authentication server is possible, the connection destination may be decided on based upon much newest information. If communication with the authentication server has come to be unable, it is still possible to decide on the connection destination.

[0174] <Modification 5-3 (implementing an authentication function using OFS and OFC)>

Such a configuration that uses an OFS and an OFC in place of the nodes of the exemplary embodiment 1 to 3, inclusive of those nodes having the authentication function, may also be used. Fig.58 shows a configuration in which an OFS and an OFC are used in place of the nodes of the exemplary embodiment 1 to 3 inclusive of those having the authentication function.

[0175] Fig.59 shows a detailed configuration of the OFC in the configuration of Fig.58. In the example of Fig.59, an OFC 82B includes a connection terminal memory 822 that records a MAC address of an authenticated terminal and a packet processor 825. If a packet has arrived from the OFS, and the packet is not an authentication related packet but is a communication packet, the packet processor 825 of Fig.59 does not process the packet, except in case the source MAC address or the destination MAC address in the packet header is an authenticated MAC address. In this case, it is possible to implement the function equivalent to that performed by the node 20C having the authentication function as shown in the modification 5-1.

[0176] <Another concrete form 6-1 (concrete form of the exemplary embodiment 2)>

In case of application of the configuration of exemplary embodiment 2 to the organization having a hierarchical structure, such as enterprises or universities, there may be occasions where a network usable on the entire company scale or on the entire university scale, a network for an upper order branch and a network for an ordinary branch, are installed. In such environment, there may be occasions where the ordinary branch network is installed only for a local area of the branch, or the upper order branch network is installed only for a local area where there is a lower order branch.

[0177] A user owns a right to connection to the branch, he/she belongs to, the upper order branch and the company network, with the right becoming weaker in this order. The order of the merit of connection will fall in the reverse order.

[0178] If it is possible that, if user connection may be made, based upon the user priority, to a network more readily connectible in light of the local area/ site of the switch for connection or the access point, user friendliness may be improved.

[0179] If there is a network for guests or for roaming, such network needs to be isolated from other networks. It is thus desirable that a user is able to select a subnet by a node.

[0180] <Another concrete form 6-2 (concrete form of the exemplary embodiment 3)>

In exemplary embodiment 3, there are occasions where the node 20 that acts an access point or a switch is connected to a plurality of subnets having respective different properties, such as 3G, WiMAX, PHS or optical subnets. The order of connection to the subnets and, for the user, connection priority, may be determined based upon the throughput, response time or stability of the subnets.

[0181] Based upon the connection priority level for the user and upon the order of subnet connection priority, it is determined automatically which of the subnets a user is allowed to use.

[0182] It is assumed that, for example, users are grouped into personnel of local administrative offices, personnel of fire stations and general users, and that the priority rank for the general users is set at the lowest level.

[0183] In such setting, control may be exercised in which communication is allowed for the general users only in case of no emergent communication. In case of emergent communication, connection to the general users, if any, is canceled (disconnected), such that connection is allowed using a path having a lower rank in the connection priority. Or, connection may be inhibited.

[0184] <Another concrete form 6-3 (concrete form of the exemplary embodiment 4)>

In case of application of the configuration of exemplary embodiment 4 to an organization having a hierarchical structure, such as enterprises or universities, there may be occasions where a network usable on the entire company scale or on the entire university scale, a network for an upper ordinate branch and a network for ordinary branch, are present. If, in such environment, the OFS 20A is connectible to branch networks and to the entire company network, and the user prefers connection to a branch network, the user is connected to the branch network.

[0185] If the user accesses of the entire company services, communication occurs via several routers in case the start point is the branch network. However, the entire company network is also usable. It is thus also possible that all possible paths are calculated first so that the entire company network will be directly used provided that the network cost is low.

[0186] It should be noted that all parts (processing means) of the authentication server or the OFC, shown in the above exemplary embodiments, may also be implemented by the hardware of a computer composing these parts (or means) using a computer program that will allow execution of the above mentioned processing.

[0187] Although the description has been made of preferred exemplary embodiments of the present invention, such exemplary embodiments are not intended to limit the scope of the present invention. That is, further modifications, substitutions or adjustments may be made without departing from the basic technical concept of the present invention. For example, the network configuration or the number of the nodes (OFSes) as well as terminals or subnets, indicated in each of the exemplary embodiments, set out above, are given only by way of illustration, such that no limitations should be imposed on the configuration or numbers.

[0188] In the above described exemplary embodiments, the group of the subnets, for which the terminal has the right to connection, is acquired from the authentication DB 32 of the authentication server, as an example. It is however also possible that the role information owned by a terminal or its user is acquired as a result of the authentication processing with the terminal, such that a group of subnets, the terminal has the connection right to, may be acquired as a result of this role information.

[0189] Certain preferred modes of the present invention will now be set out.

<Mode 1>

(See the network system according to the above mentioned first aspect).

<Mode 2>

A network system according to mode 1, wherein,

the authentication apparatus performs authentication processing with the terminal to decide on the subnet the terminal has the connection right to.

<Mode 3>

The network system according to mode 1 or 2, wherein,
connection priority is set in the terminal(s);
the authentication apparatus deciding on the subnet to be connected to the terminal based upon the connection priority of the terminal.

<Mode 4>

The network system according to mode 3, wherein,
a connection order is set in each of the subnet(s);
the authentication apparatus deciding on the subnet(s) so that a terminal having a higher connection priority will be connected to a subnet higher in connection order.

<Mode 5>

The network system according to mode 3 or 4, wherein.
the automatic apparatus removes, from connection candidates of terminals having a connection priority not higher than a pre-set level, the subnets having a in connection order not lower than a pre-set level.

<Mode 6>

The network system according to any one of mode 3 to 5, wherein,
in each of the subnets, an upper limit of number of the terminals for connection is set; and wherein,
if, in a state where the number of terminal(s) connected to a given one of the subnets has reached an upper limit, the authentication apparatus has received a connection request from a terminal having a higher connection priority, the authentication apparatus cancels a connection of the subnet with a terminal having low connection priority and connects the terminal having a higher connection priority.

<Mode 7>

The network system according to any one of modes 1 to 6, wherein,
the authentication apparatus decides on the subnet to be connected to the terminal so that the terminal will perform communication using the subnet having low network cost incurred in communication with a communication destination.

<Mode 8>

The network system according to any one of modes 1 to 7, further comprising
a load measurement unit that measures load state of each of the subnets;
the authentication apparatus excluding a the subnet, which is in a high load state, from subjects of connection.

<Mode 9>

The network system according to any one of modes 1 to 8, wherein,
the connection priority is set from one account to another;

the authentication apparatus deciding on the subnet to be connected to the terminal based upon connection priority according to the account at the time of authentication of the terminal.

<Mode 10>

The network system according to any one of modes 1 to 9, wherein,

the subnets are grouped;

the authentication apparatus deciding on the subnet(s) to be connected to the terminal(s) based upon a group of the subnets the terminal(s) has the connection right to and a group of the subnets the node is connected to.

<Mode 11>

The network system according to any one of modes 1 to 10, wherein,

the node has a function of authentication; and wherein,

the subnet(s) the terminal has the connection right to is decided on based upon the result of authentication by the node.

<Mode 12>

(See the authentication apparatus according to the second aspect)

<Mode 13>

(See the method for deciding on a subnet(s) according to the third aspect)

<Mode 14>

(See the program according to the fourth aspect)

[0190] The disclosure of the aforementioned Patent Literatures and Non Patent Literatures are incorporated by reference herein. The particular exemplary embodiments or examples may be modified or adjusted within the scope of the entire disclosure of the present invention, inclusive of claims, based on the fundamental technical concept of the invention. Further, a variety of combinations or selection of elements disclosed herein may be made within the context of the claims. Viz., the present invention may encompass a wide variety of modifications or corrections that may occur to those skilled in the art in accordance with the entire disclosure of the present invention, inclusive of claim and the technical concept of the invention.

## Symbols

[0191] 10, 10A to 10M terminals

20 node

20A OFS

21 packet processor

22 flow entry memory

20A OFS

20C node having the authentication function

30, 30A, 30B, 60, 60A, 60B, 60C, 70, 70A, 81 authentication servers

| | |
|---|---|
| 31 | node database (node DB) |
| 32, 811 | authentication databases (authentication DBs) |
| 33 | terminal subordination (allocation) decision unit |
| 34, 812 | authentication processing units |
| 35, 813 | authentication result notification units |
| 35-2 | connection cancel notification unit |
| 36 | connection number table |
| 37, 828 | group database (group DB) |
| 38 | connection terminal table |
| 39 | account group database (account group DB) |
| 40A to 40N | subnets |
| 50 | load measurement unit |
| 81 | authentication server |
| 82, 82A, 82B | OFCs |
| 83 | host apparatus |
| 90 | authentication information server |
| 201 | authentication unit |
| 821 | terminal subordination (allocation) decision unit |
| 822 | connection terminal memory |
| 823 | topology database (topology DB) |
| 824 | subnet database (subnet DB) |
| 825 | packet processor |
| 826 | path calculation unit |
| 827 | flow setting unit |

# Claims

[Claim 1] A network system, comprising:
a node(s) connected to a plurality of subnets; and
an authentication apparatus that, in response to a connection request from a terminal(s) via the node, decides on a subnet(s) to be connected to the terminal(s), based upon subnet(s) the terminal(s) has a connection right to and upon subnet(s) the node is connected to.

[Claim 2] The network system according to claim 1, wherein,
the authentication apparatus performs authentication processing with the terminal to decide on the subnet(s) the terminal has the connection right to.

[Claim 3] The network system according to claim 1 or 2, wherein.
connection priority is set in the terminal(s);
the authentication apparatus deciding on the subnet(s) to be connected to the terminal based upon the connection priority of the terminal.

[Claim 4] The network system according to claim 3, wherein,
a connection order is set in each of the subnets;
the authentication apparatus deciding on the subnet(s) so that a terminal having a higher connection priority will be connected to a subnet having a higher connection order.

[Claim 5] The network system according to claim 3 or 4, wherein.
the authentication apparatus removes, from connection candidates of terminals having a connection priority not higher than a pre-set level, the subnet(s) having a in connection order not lower than a pre-set level.

[Claim 6] The network system according to any one of claims 3 to 5, wherein,
in each of the subnets, an upper limit of number of the terminals for connection is set; and wherein,
if, in a state where the number of terminal(s) connected to a given one of the subnets has reached an upper limit, the authentication apparatus has received a connection request from a terminal having a higher connection priority, the authentication apparatus cancels a connection of a subnet with a terminal having a low connection priority and connects the terminal having the higher connection priority.

[Claim 7] The network system according to any one of claims 1 to 6, wherein,
the authentication apparatus decides on the subnet(s) to be connected to the terminal so that the terminal will perform communication using the

subnet(s) having low network cost incurred in communication with a communication destination.

[Claim 8] The network system according to any one of claims 1 to 7, further comprising:
a load measurement unit that measures load state of each of the subnets;
the authentication apparatus excluding a subnet, which is in a high load state, from subjects of connection.

[Claim 9] The network system according to any one of claims 1 to 8, wherein,
the connection priority is set from one account to another;
the authentication apparatus deciding on the subnet(s) to be connected to the terminal based upon connection priority according to the account at the time of authentication of the terminal.

[Claim 10] The network system according to any one of claims 1 to 9, wherein,
the subnets are grouped;
the authentication apparatus deciding on the subnet(s) to be connected to the terminal(s) based upon a group of the subnets the terminal(s) has the connection right to and a group of the subnets the node is connected to.

[Claim 11] The network system according to any one of claims 1 to 10, wherein,
the node has a function of authentication; and wherein,
the subnet(s) the terminal has the connection right to is decided on based upon the result of authentication by the node.

[Claim 12] An authentication apparatus, wherein
the authentication apparatus is connected to a node(s) which is connected to a plurality of subnets;
the authentication apparatus deciding, in response to a connection request from a terminal(s) via the node, on the subnet(s) to be connected to the terminal(s), based upon the subnet(s) the terminal(s) has a connection right to and upon the subnets the node is connected to.

[Claim 13] A method for deciding on a subnet(s), comprising:
a step of an authentication apparatus, connected to a node(s) which is connected to a plurality of subnets, accepting, from a terminal(s), via the node, a connection request to the subnet(s) the terminal(s) has a connection right to; and
a step of the authentication apparatus deciding on the subnet(s) to be connected to the terminal(s), in response to the connection request, based upon the subnet(s) the terminal(s) has the connection right to and

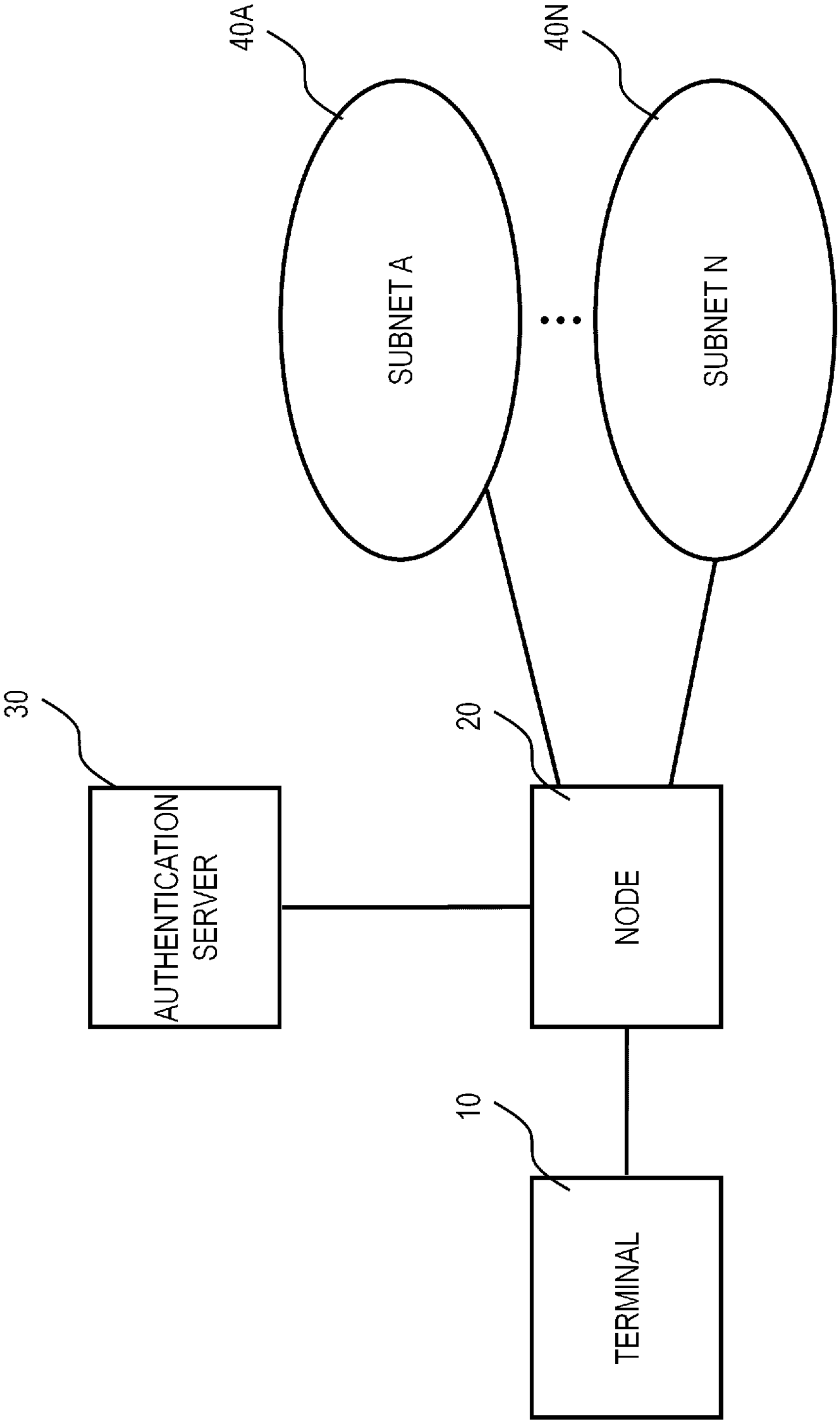
upon the subnets the node is connected to.

[Claim 14] A program that allows a computer configuring an authentication apparatus connected to a node which is connected to a plurality of subnets, to perform

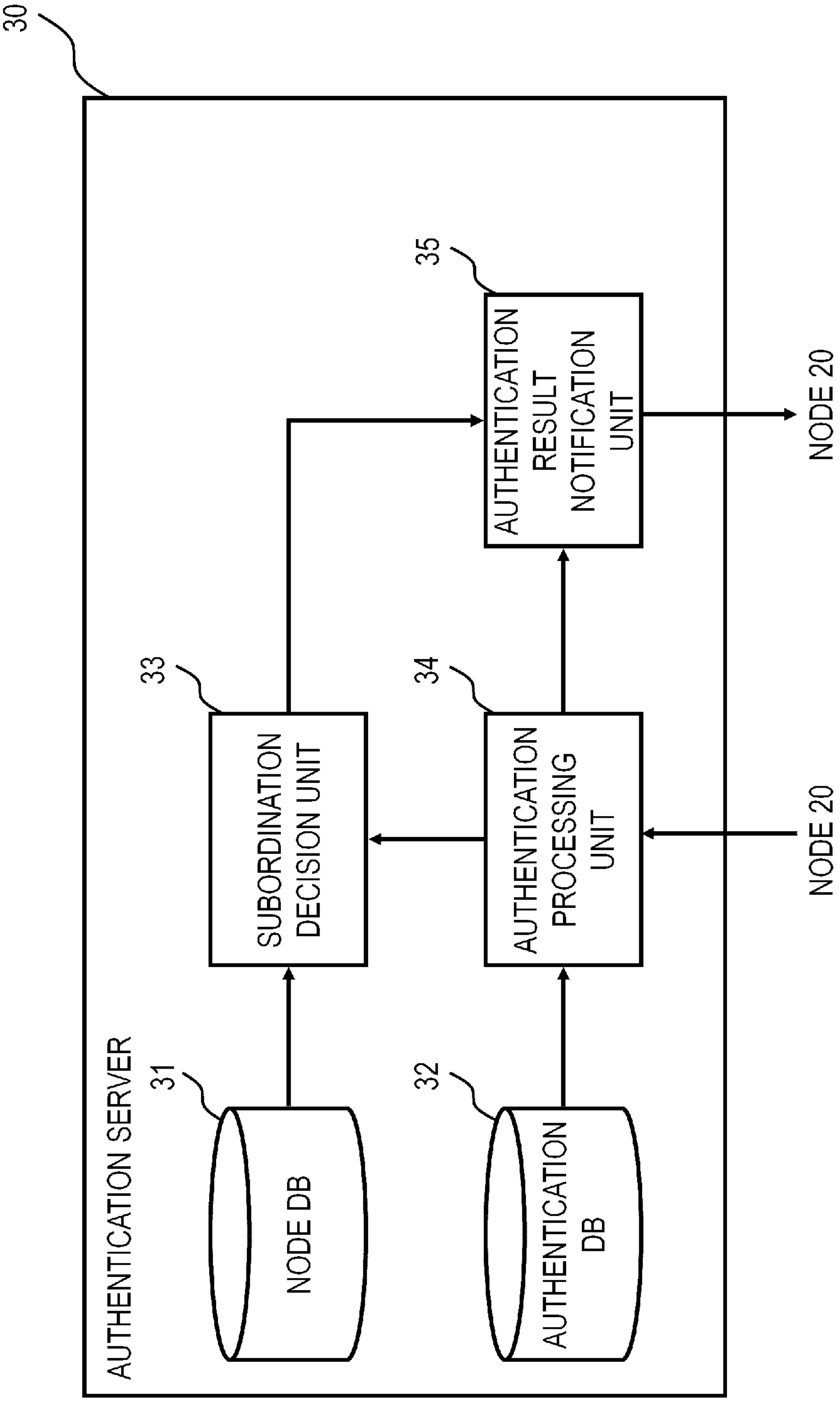
a processing of accepting, from a terminal(s), via the node, a connection request to the subnet(s) the terminal(s) has a connection right to; and

a processing of deciding on the subnet(s) to be connected to the terminal(s), in response to the connection request, based upon the subnet(s) the terminal(s) has the connection right to and upon the subnet(s) the node is connected to.

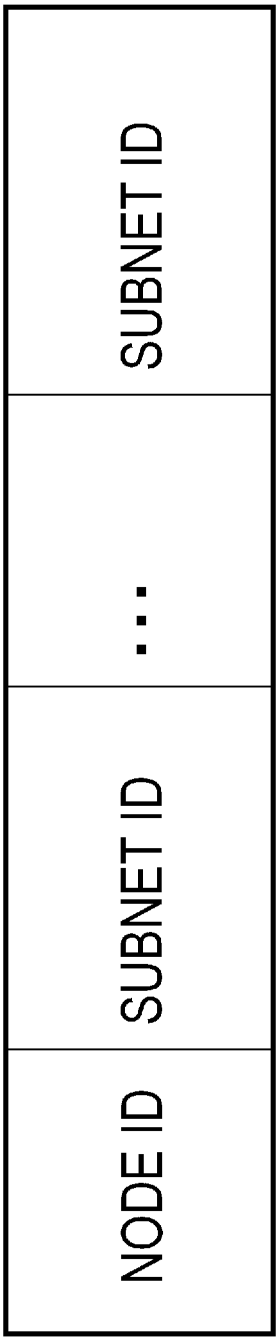
[Fig. 1]


40A
40N
SUBNET A
SUBNET N
30
20
AUTHENTICATION SERVER
NODE
10
TERMINAL

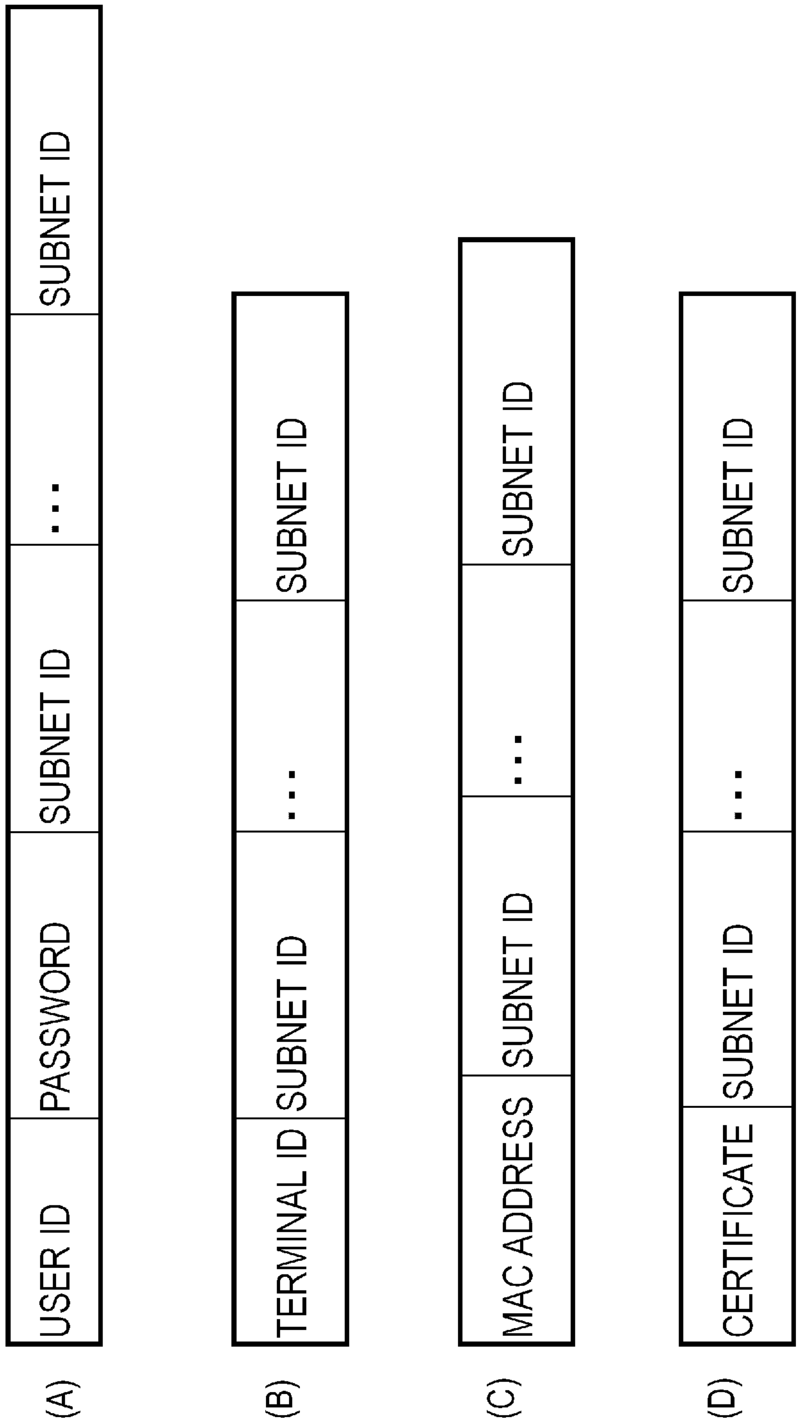
[Fig. 2]


30
AUTHENTICATION SERVER
31
NODE DB
32
AUTHENTICATION DB
33
SUBORDINATION DECISION UNIT
34
AUTHENTICATION PROCESSING UNIT
35
AUTHENTICATION RESULT NOTIFICATION UNIT
NODE 20
NODE 20

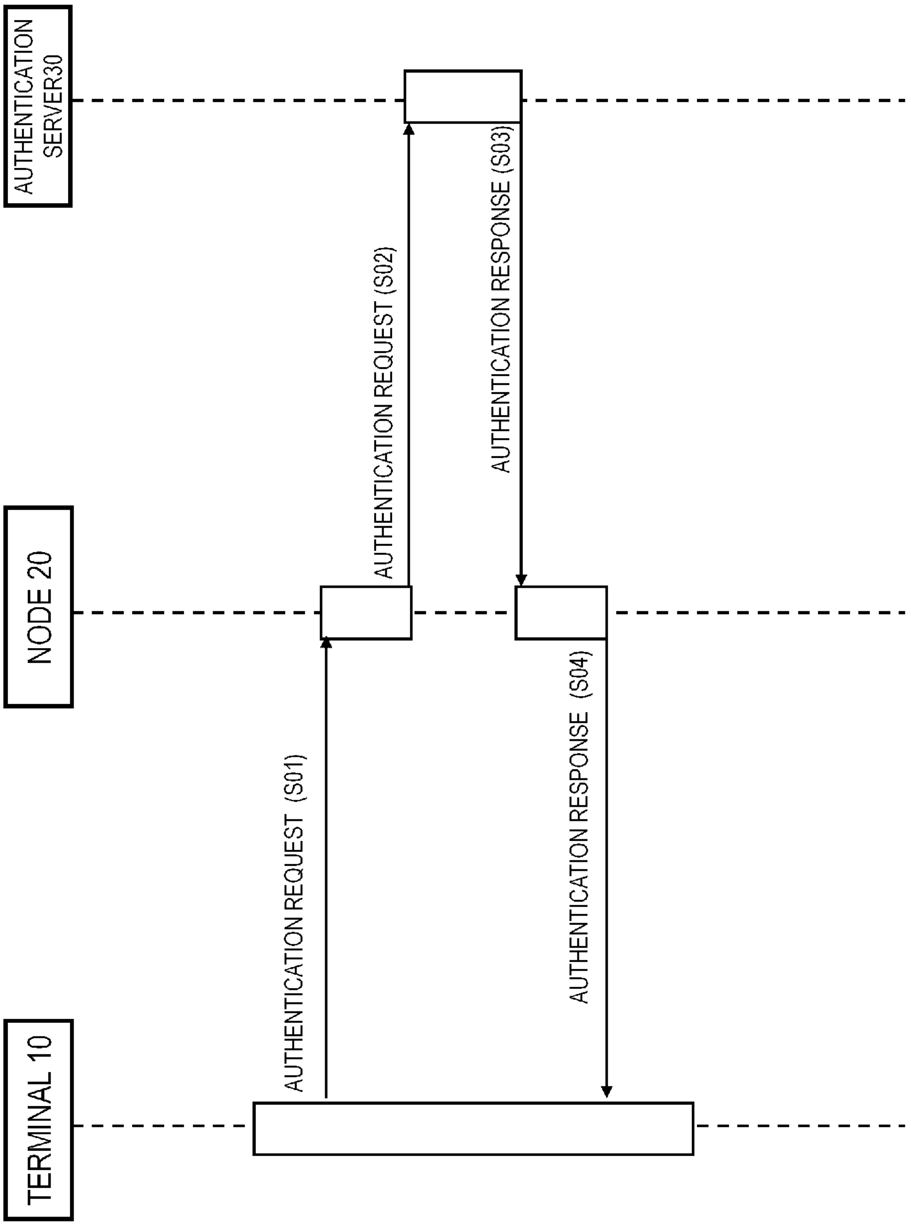
[Fig. 3]



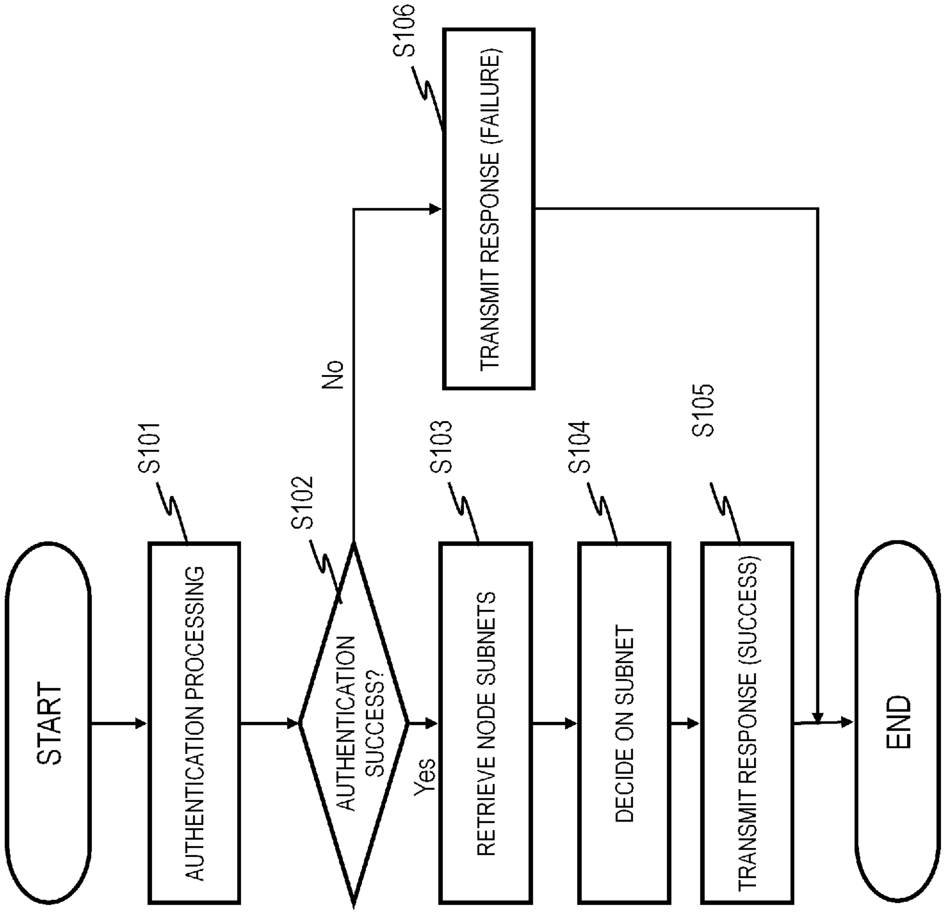
[Fig. 4]


(A)
USER ID
PASSWORD
SUBNET ID
...
SUBNET ID
(B)
TERMINAL ID
SUBNET ID
...
SUBNET ID
(C)
MAC ADDRESS
SUBNET ID
...
SUBNET ID
(D)
CERTIFICATE
SUBNET ID
...
SUBNET ID

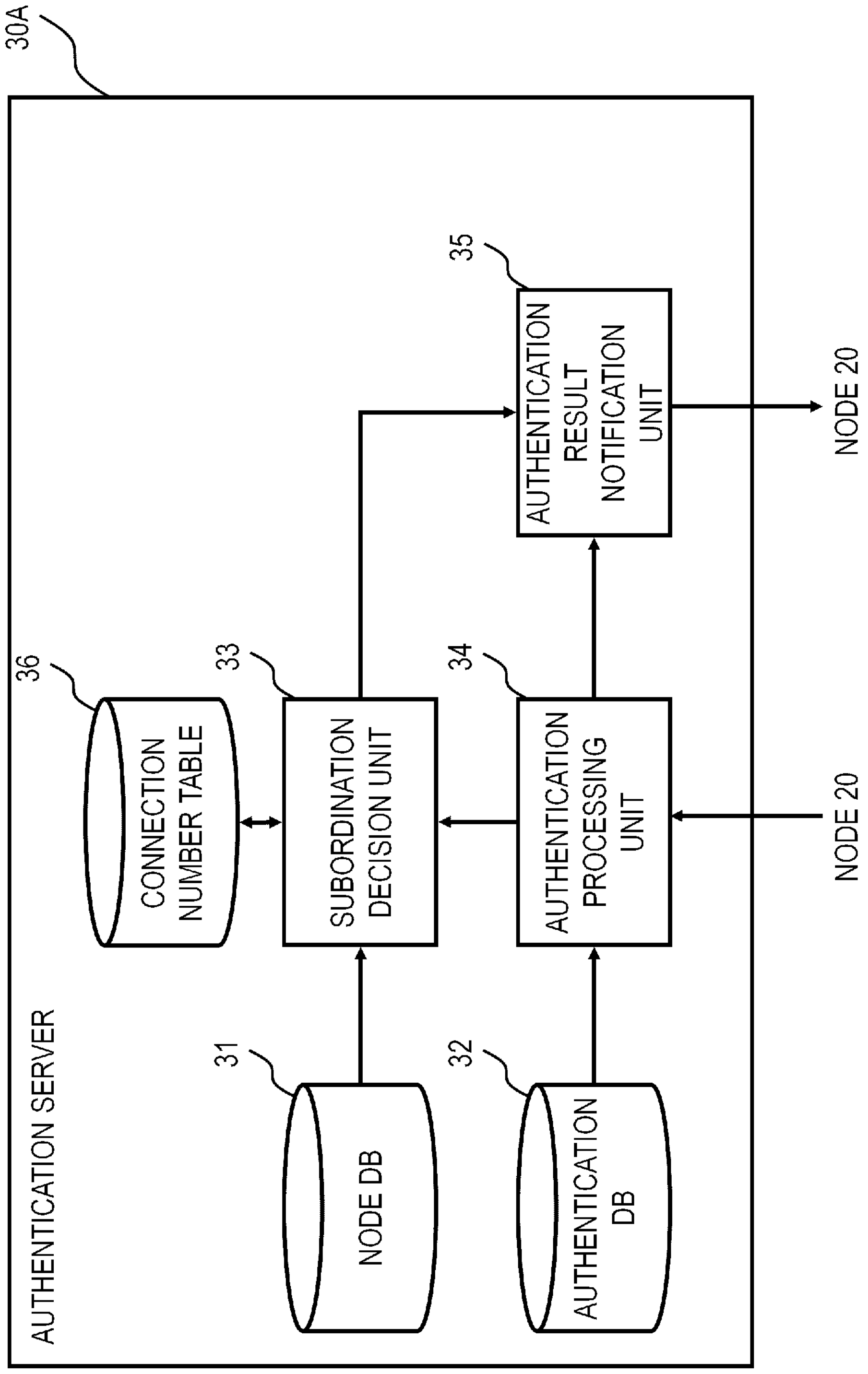
[Fig. 5]


AUTHENTICATION SERVER30
NODE 20
TERMINAL 10
AUTHENTICATION REQUEST (S01)
AUTHENTICATION REQUEST (S02)
AUTHENTICATION RESPONSE (S03)
AUTHENTICATION RESPONSE (S04)

[Fig. 6]


START
AUTHENTICATION PROCESSING
S101
AUTHENTICATION SUCCESS?
S102
No
Yes
TRANSMIT RESPONSE (FAILURE)
S106
RETRIEVE NODE SUBNETS
S103
DECIDE ON SUBNET
S104
TRANSMIT RESPONSE (SUCCESS)
S105
END

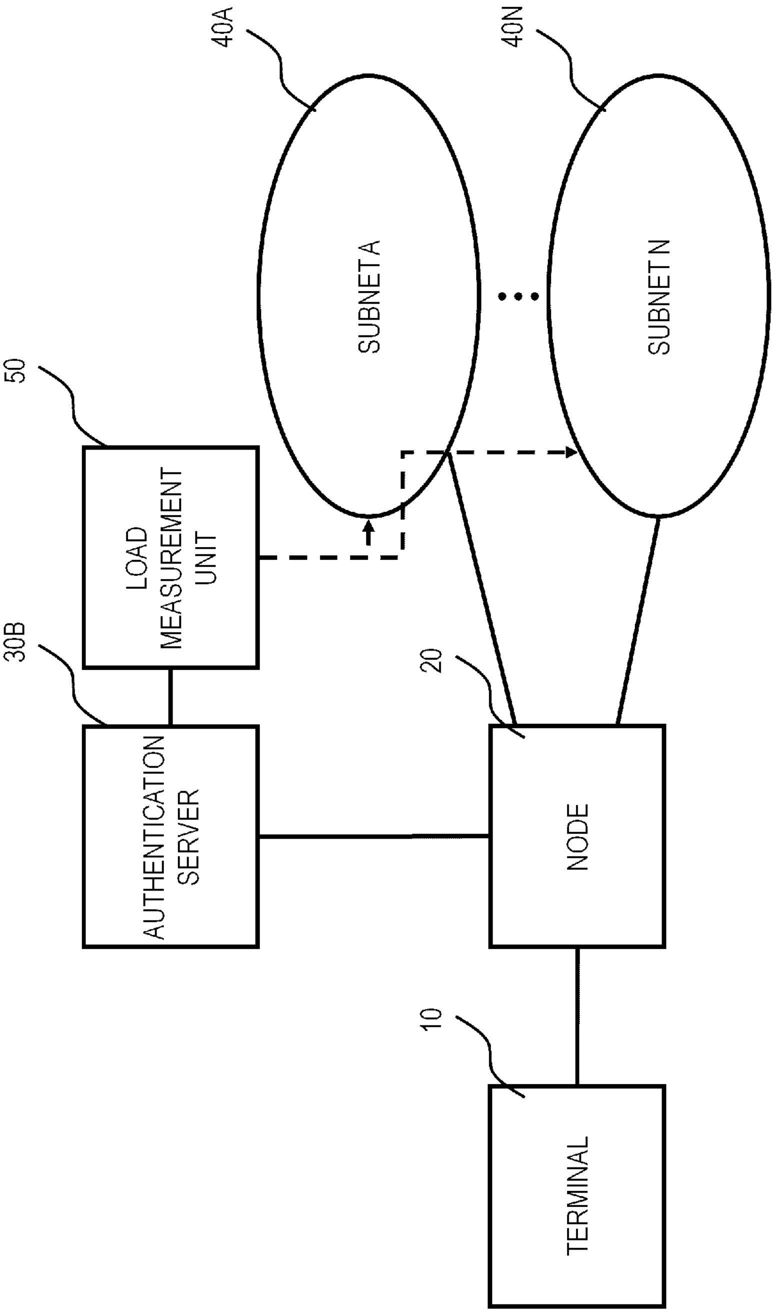
[Fig. 7]


30A
AUTHENTICATION SERVER
31
NODE DB
32
AUTHENTICATION DB
36
CONNECTION NUMBER TABLE
33
SUBORDINATION DECISION UNIT
34
AUTHENTICATION PROCESSING UNIT
35
AUTHENTICATION RESULT NOTIFICATION UNIT
NODE 20
NODE 20

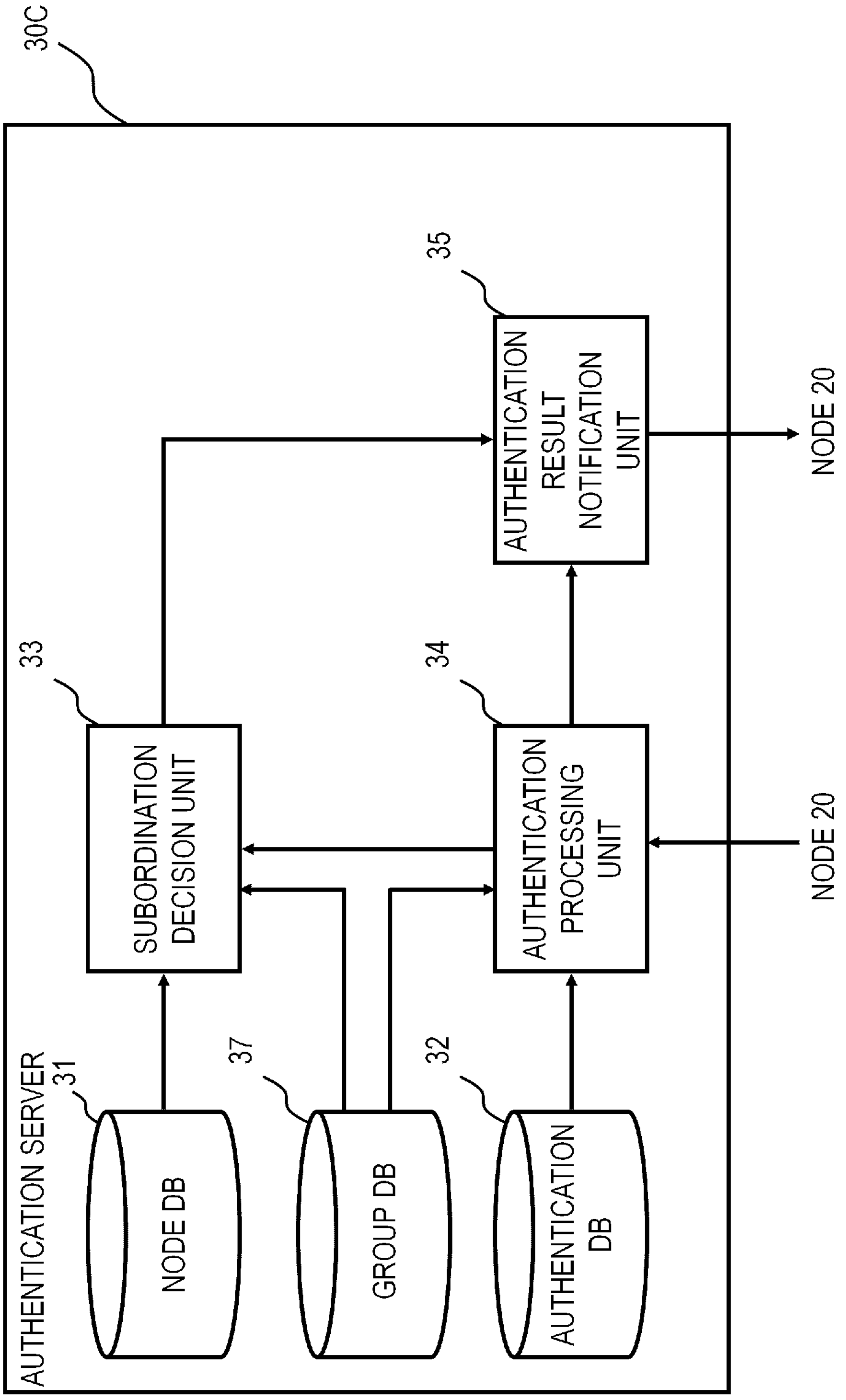
[Fig. 8]

| SUBNET ID | NUMBER OF TERMINALS CONNECTED |
|---|---|

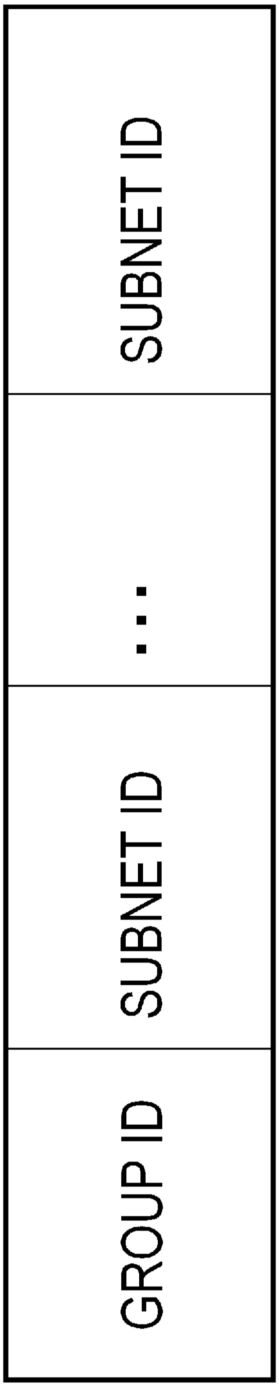
[Fig. 9]


40A
40N
SUBNET A
SUBNET N
50
LOAD MEASUREMENT UNIT
30B
AUTHENTICATION SERVER
20
NODE
10
TERMINAL

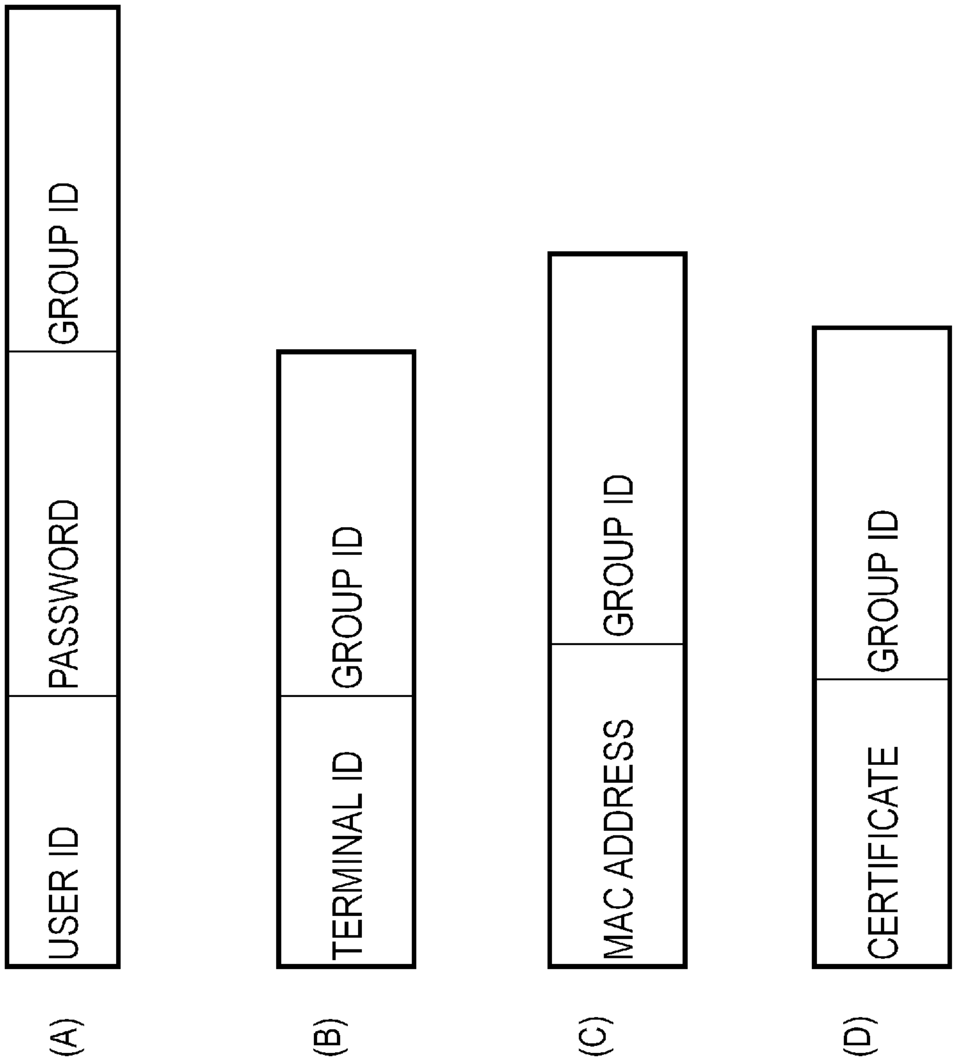
[Fig. 10]


30C
AUTHENTICATION SERVER
31
NODE DB
37
GROUP DB
32
AUTHENTICATION DB
33
SUBORDINATION DECISION UNIT
34
AUTHENTICATION PROCESSING UNIT
35
AUTHENTICATION RESULT NOTIFICATION UNIT
NODE 20
NODE 20

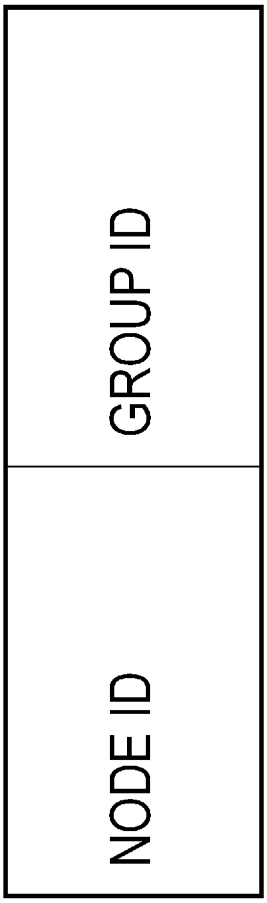
[Fig. 11]



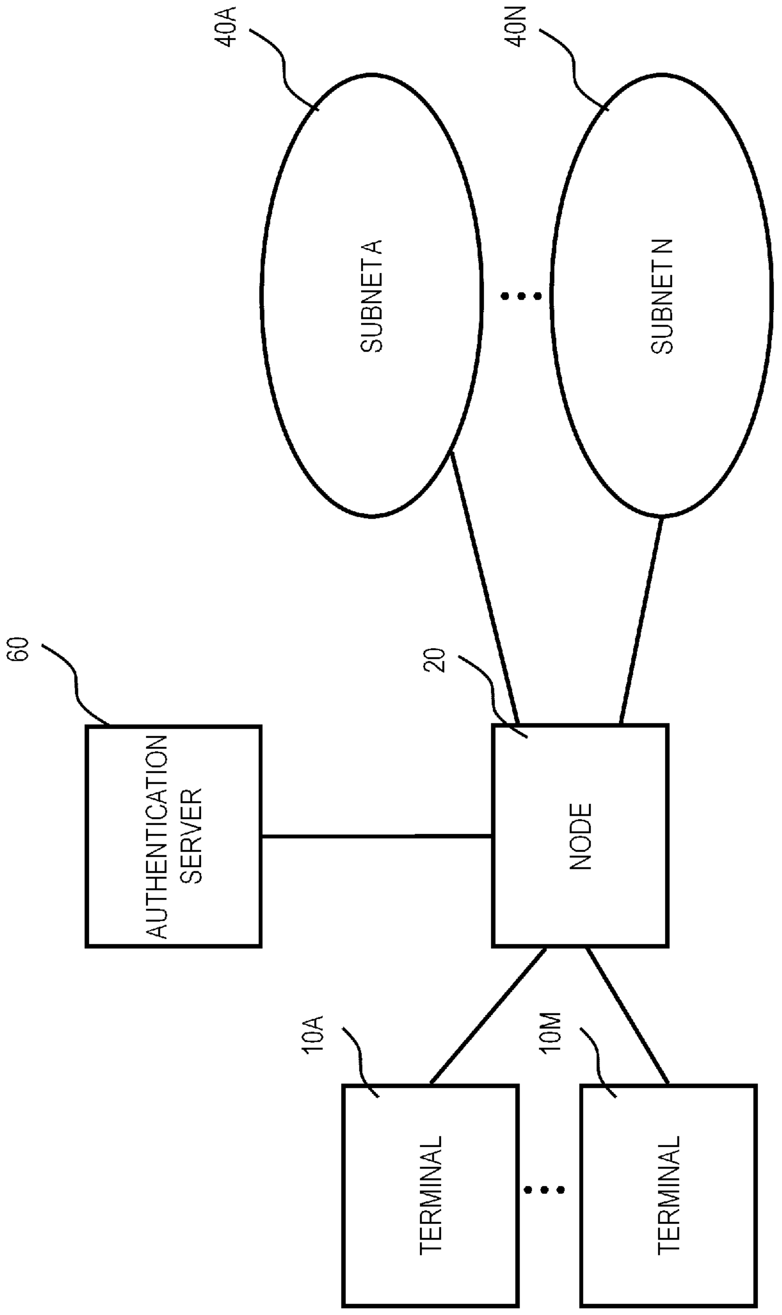
[Fig. 12]


(A)
USER ID
PASSWORD
GROUP ID
(B)
TERMINAL ID
GROUP ID
(C)
MAC ADDRESS
GROUP ID
(D)
CERTIFICATE
GROUP ID

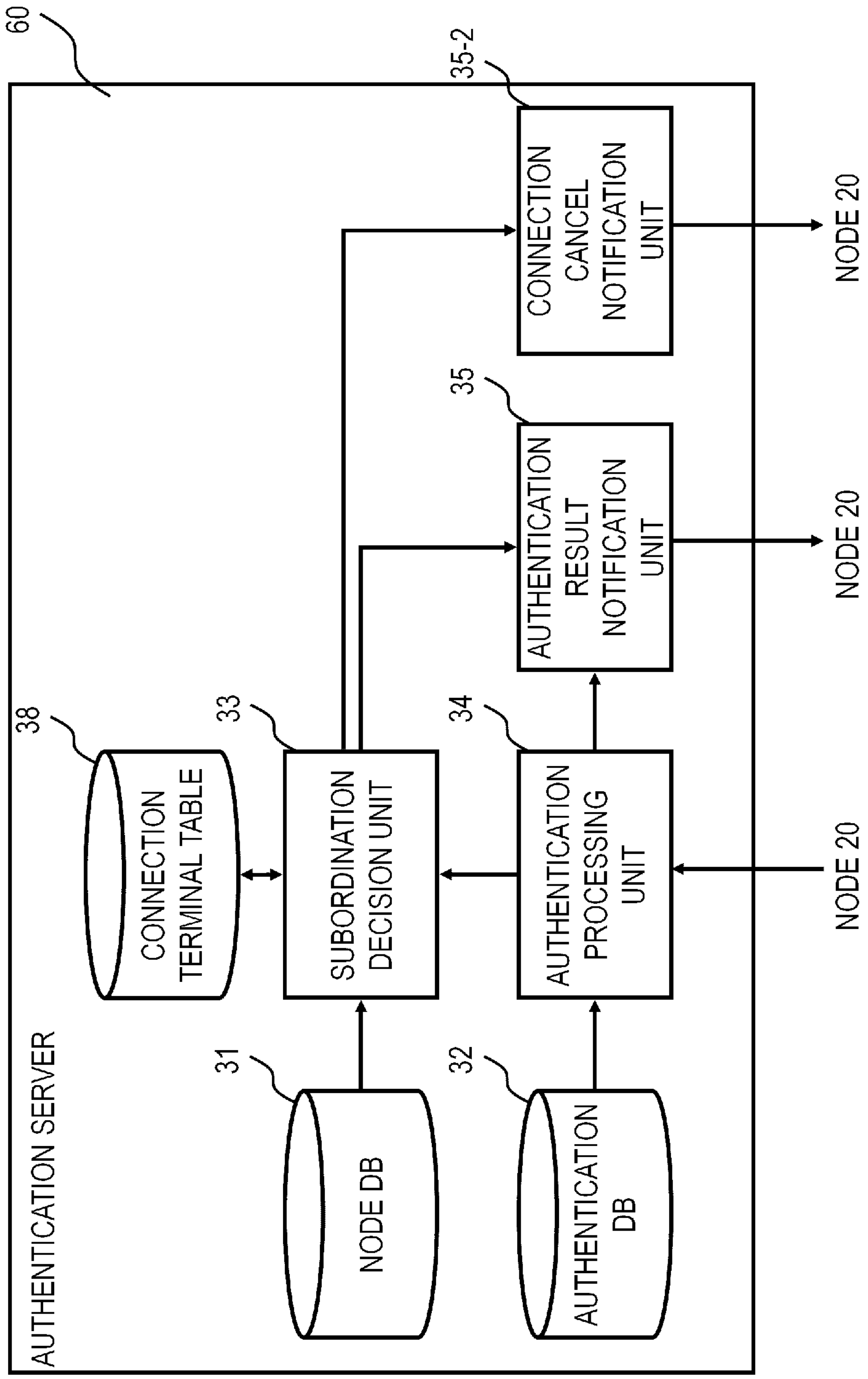
[Fig. 13]



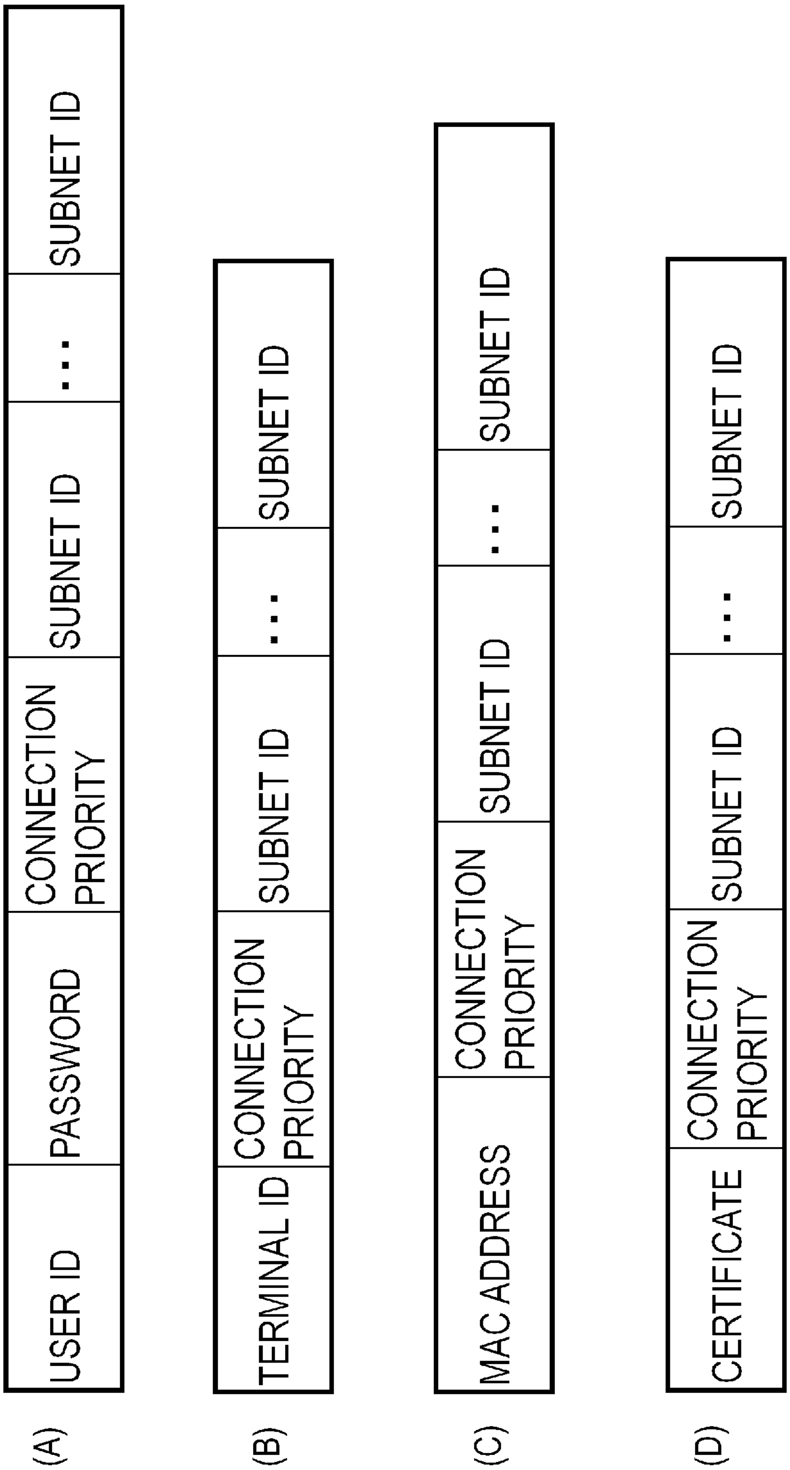
[Fig. 14]


40A
40N
SUBNET A
SUBNET N
60
AUTHENTICATION SERVER
20
NODE
10A
10M
TERMINAL
TERMINAL

[Fig. 15]


60
AUTHENTICATION SERVER
31
NODE DB
32
AUTHENTICATION DB
38
CONNECTION TERMINAL TABLE
33
SUBORDINATION DECISION UNIT
34
AUTHENTICATION PROCESSING UNIT
NODE 20
35
AUTHENTICATION RESULT NOTIFICATION UNIT
NODE 20
35-2
CONNECTION CANCEL NOTIFICATION UNIT
NODE 20

[Fig. 16]



(A)

| | | | | | |
|---|---|---|---|---|---|
| USER ID | PASSWORD | CONNECTION PRIORITY | SUBNET ID | ... | SUBNET ID |

(B)

| | | | | | |
|---|---|---|---|---|---|
| TERMINAL ID | CONNECTION PRIORITY | SUBNET ID | ... | SUBNET ID |

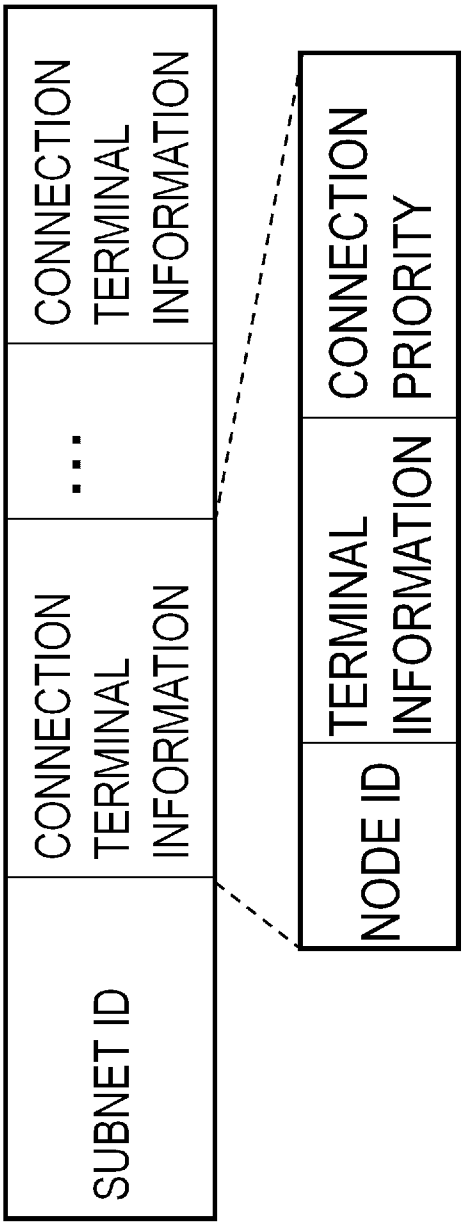
(C)

| | | | | |
|---|---|---|---|---|
| MAC ADDRESS | CONNECTION PRIORITY | SUBNET ID | ... | SUBNET ID |

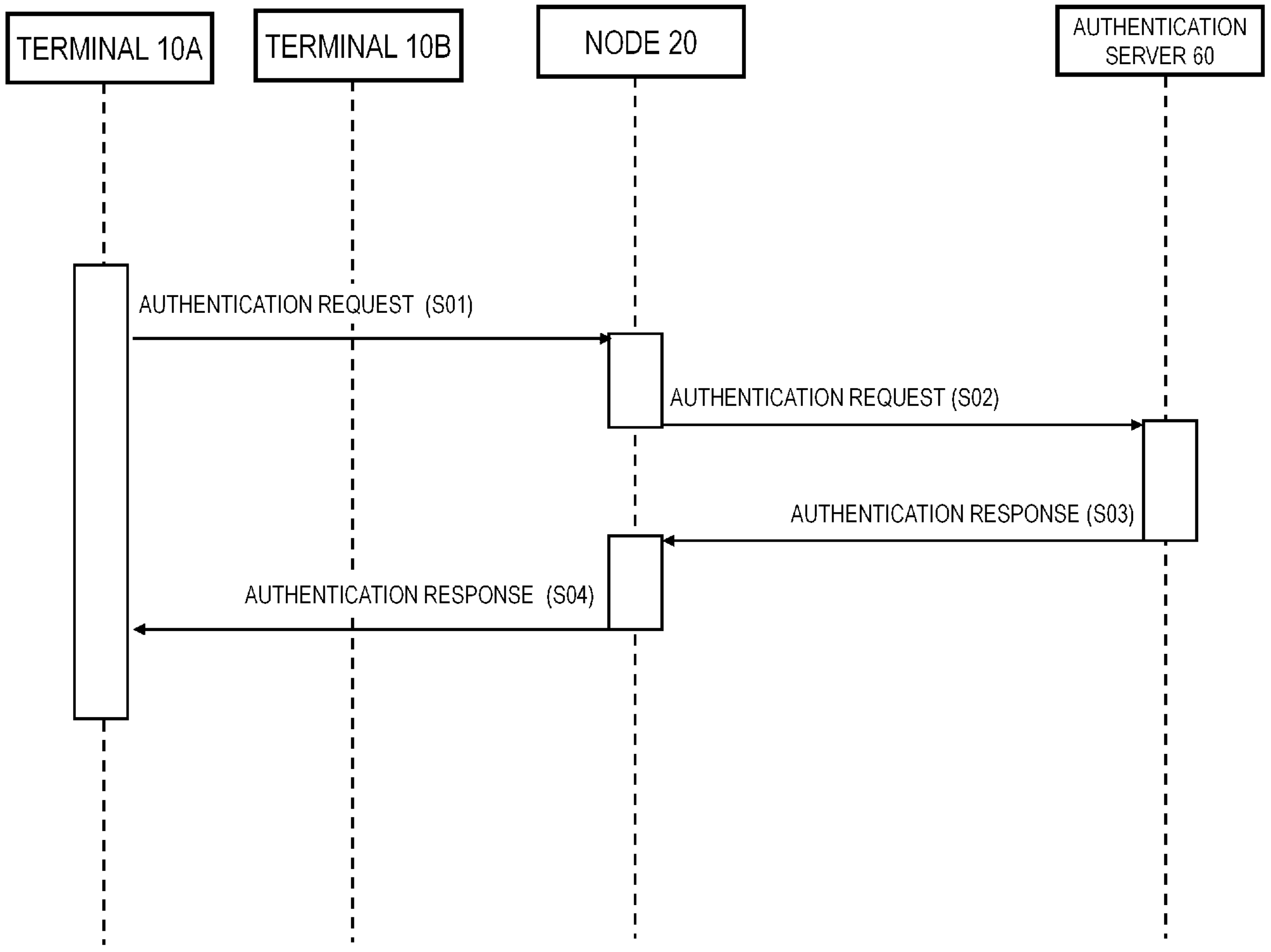
(D)

| | | | | |
|---|---|---|---|---|
| CERTIFICATE | CONNECTION PRIORITY | SUBNET ID | ... | SUBNET ID |

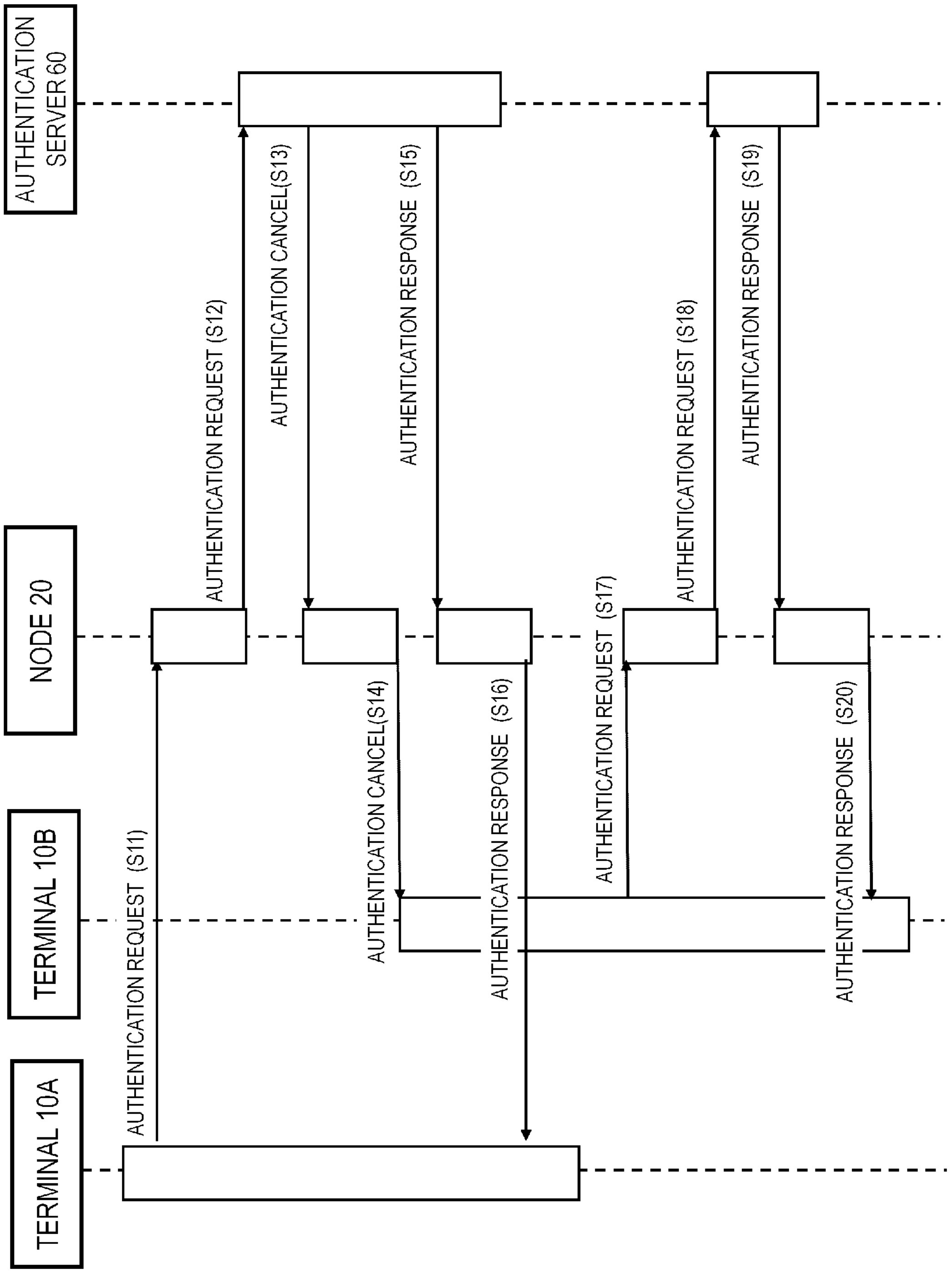
[Fig. 17]


SUBNET ID
CONNECTION TERMINAL INFORMATION
...
CONNECTION TERMINAL INFORMATION
NODE ID
TERMINAL INFORMATION
CONNECTION PRIORITY

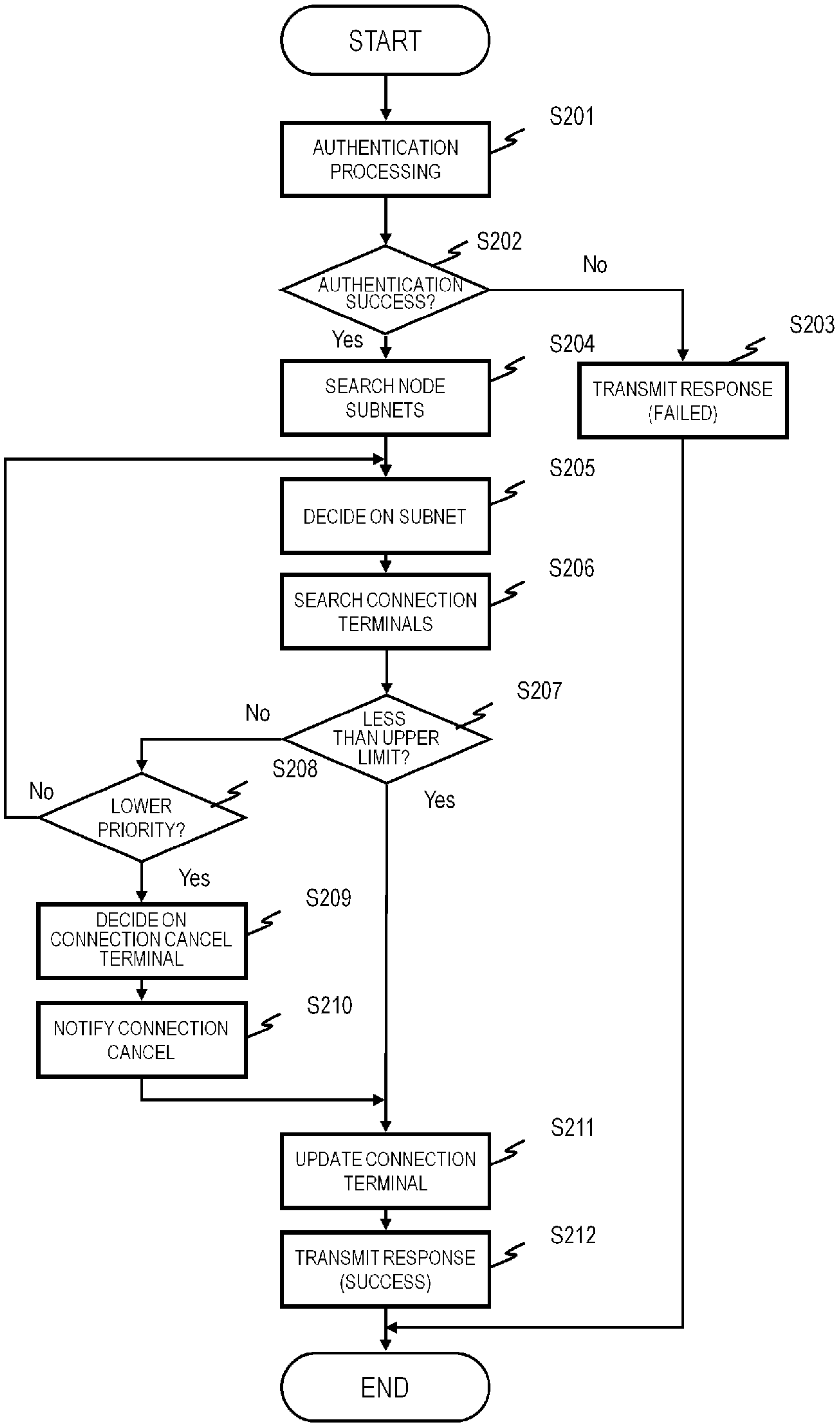
[Fig. 18]


TERMINAL 10A
TERMINAL 10B
NODE 20
AUTHENTICATION SERVER 60
AUTHENTICATION REQUEST (S01)
AUTHENTICATION REQUEST (S02)
AUTHENTICATION RESPONSE (S03)
AUTHENTICATION RESPONSE (S04)

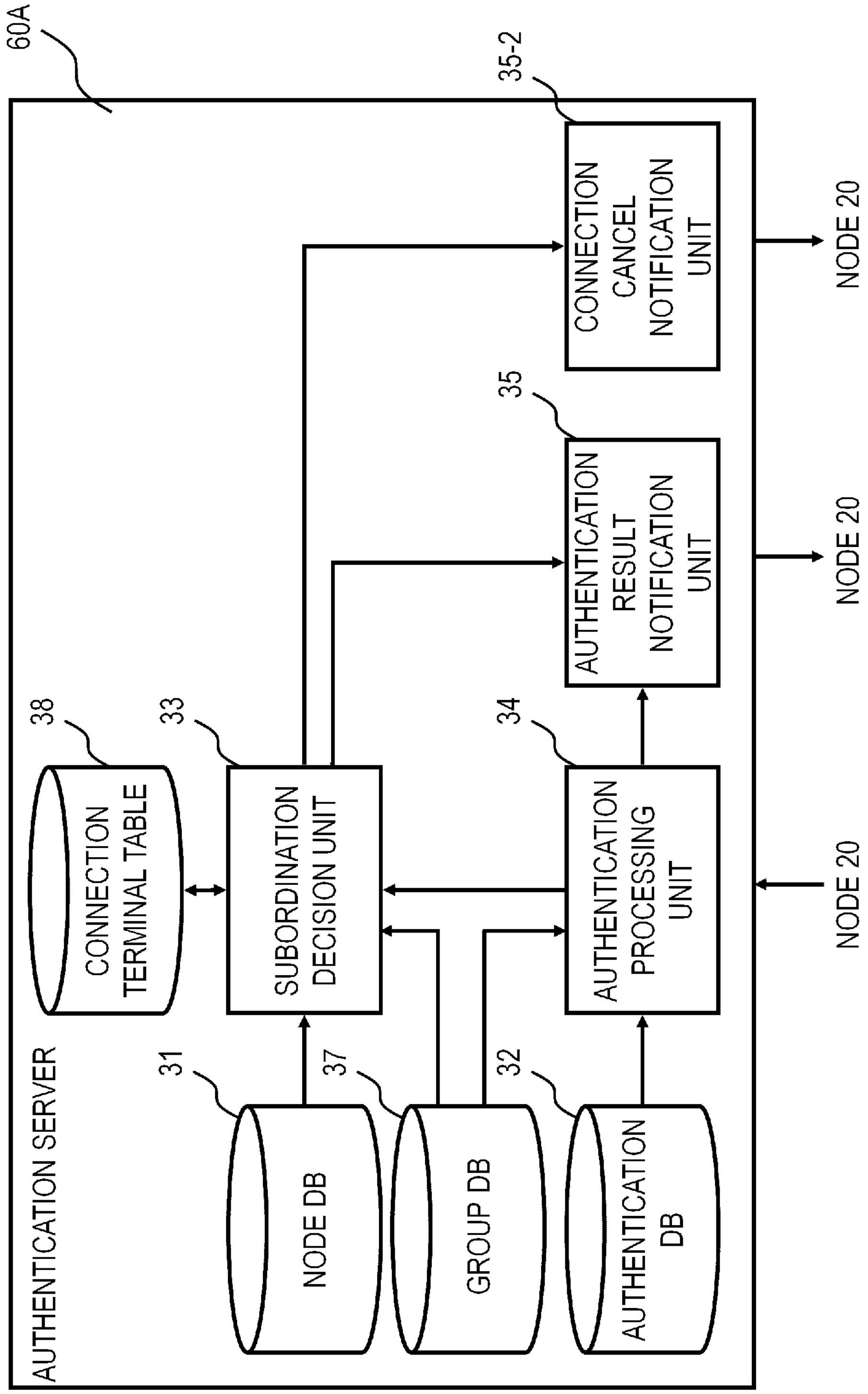
[Fig. 19]


AUTHENTICATION SERVER 60
NODE 20
TERMINAL 10B
TERMINAL 10A
AUTHENTICATION REQUEST (S11)
AUTHENTICATION REQUEST (S12)
AUTHENTICATION CANCEL(S13)
AUTHENTICATION CANCEL(S14)
AUTHENTICATION RESPONSE (S15)
AUTHENTICATION RESPONSE (S16)
AUTHENTICATION REQUEST (S17)
AUTHENTICATION REQUEST (S18)
AUTHENTICATION RESPONSE (S19)
AUTHENTICATION RESPONSE (S20)

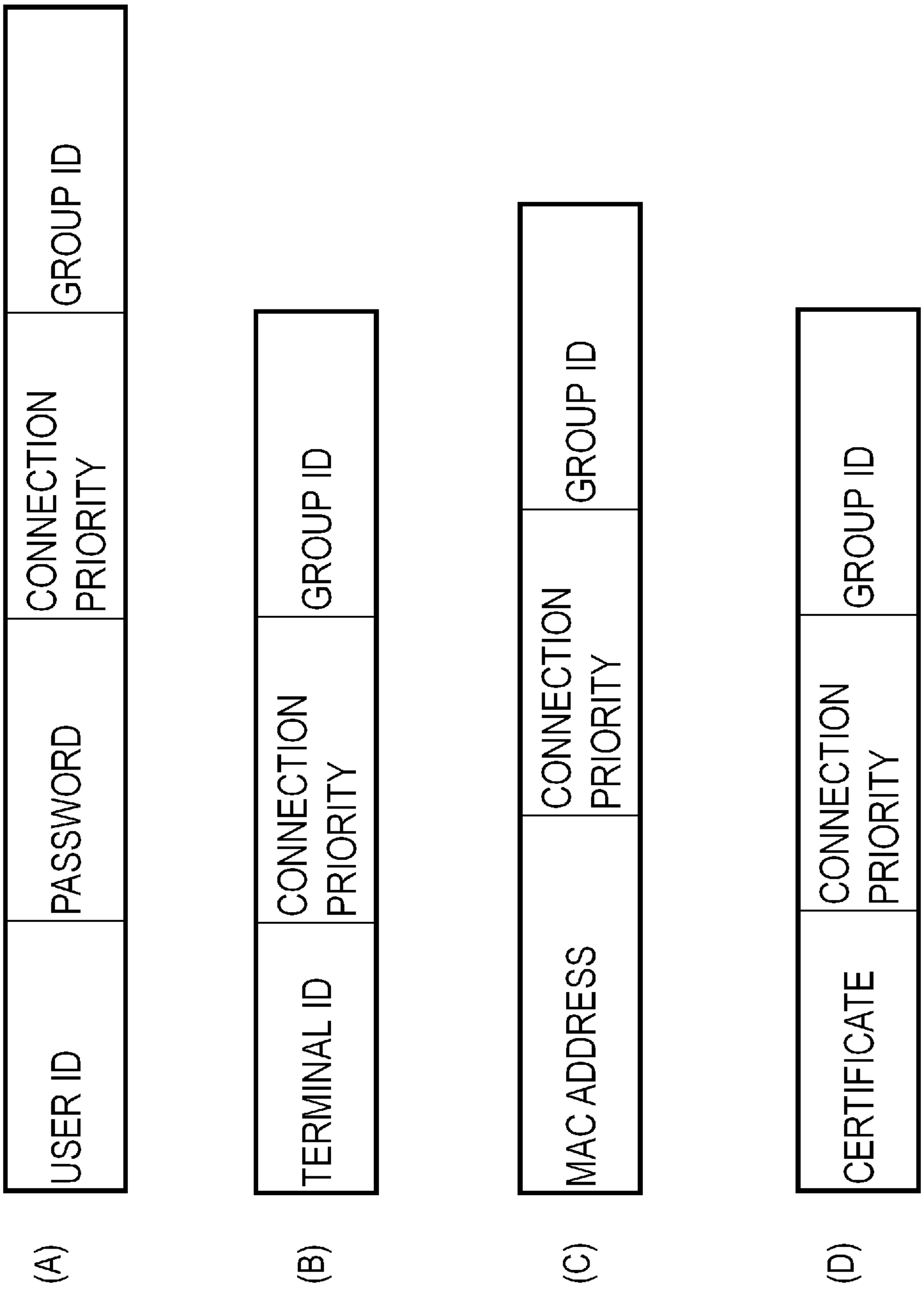
[Fig. 20]


START
S201
AUTHENTICATION PROCESSING
S202
AUTHENTICATION SUCCESS?
No
Yes
S203
TRANSMIT RESPONSE (FAILED)
S204
SEARCH NODE SUBNETS
S205
DECIDE ON SUBNET
S206
SEARCH CONNECTION TERMINALS
S207
LESS THAN UPPER LIMIT?
No
Yes
S208
LOWER PRIORITY?
No
Yes
S209
DECIDE ON CONNECTION CANCEL TERMINAL
S210
NOTIFY CONNECTION CANCEL
S211
UPDATE CONNECTION TERMINAL
S212
TRANSMIT RESPONSE (SUCCESS)
END

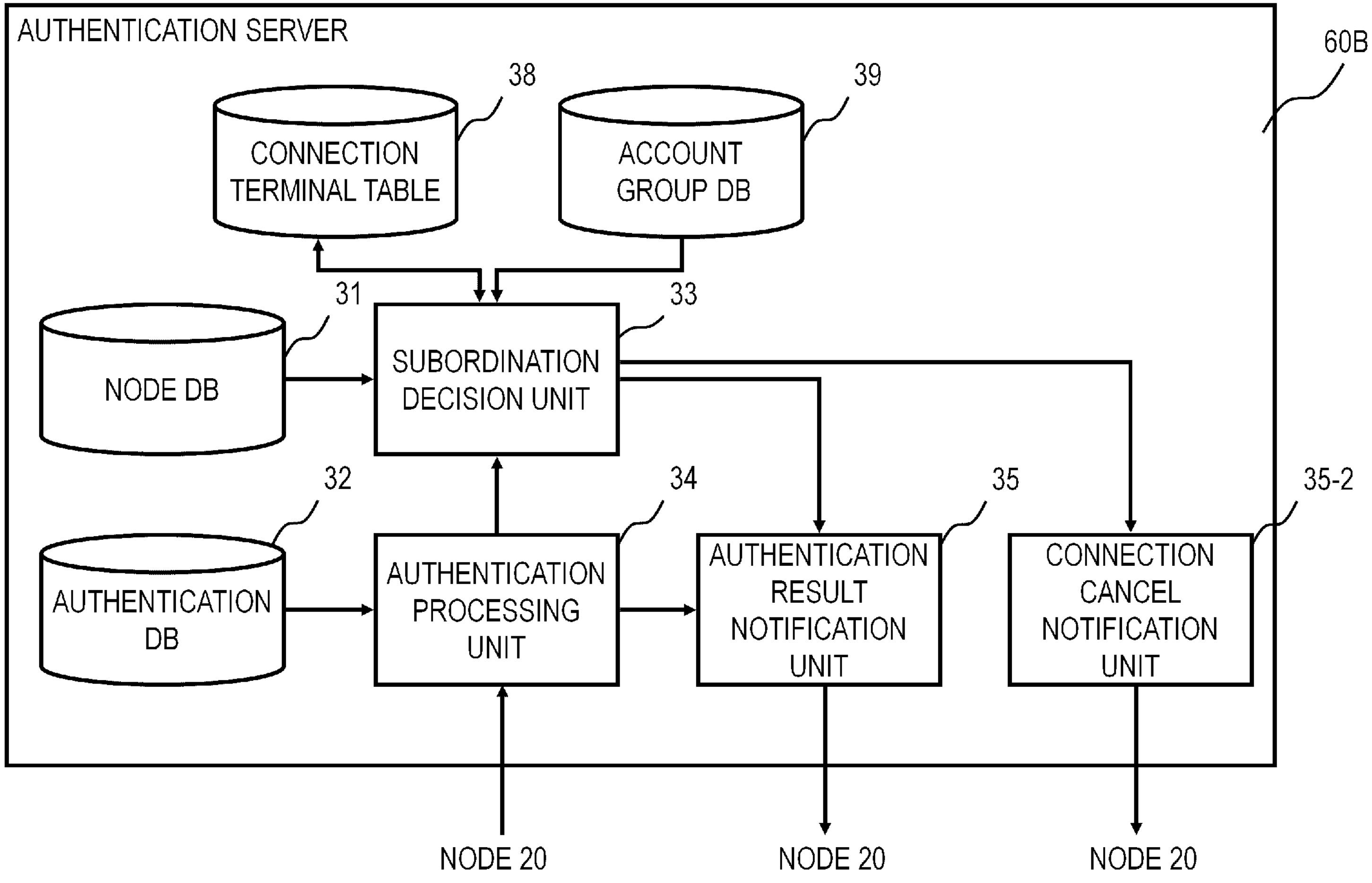
[Fig. 21]


60A
AUTHENTICATION SERVER
NODE DB
31
GROUP DB
37
AUTHENTICATION DB
32
CONNECTION TERMINAL TABLE
38
SUBORDINATION DECISION UNIT
33
AUTHENTICATION PROCESSING UNIT
34
AUTHENTICATION RESULT NOTIFICATION UNIT
35
CONNECTION CANCEL NOTIFICATION UNIT
35-2
NODE 20
NODE 20
NODE 20

[Fig. 22]


USER ID
PASSWORD
CONNECTION PRIORITY
GROUP ID
(A)
TERMINAL ID
CONNECTION PRIORITY
GROUP ID
(B)
MAC ADDRESS
CONNECTION PRIORITY
GROUP ID
(C)
CERTIFICATE
CONNECTION PRIORITY
GROUP ID
(D)

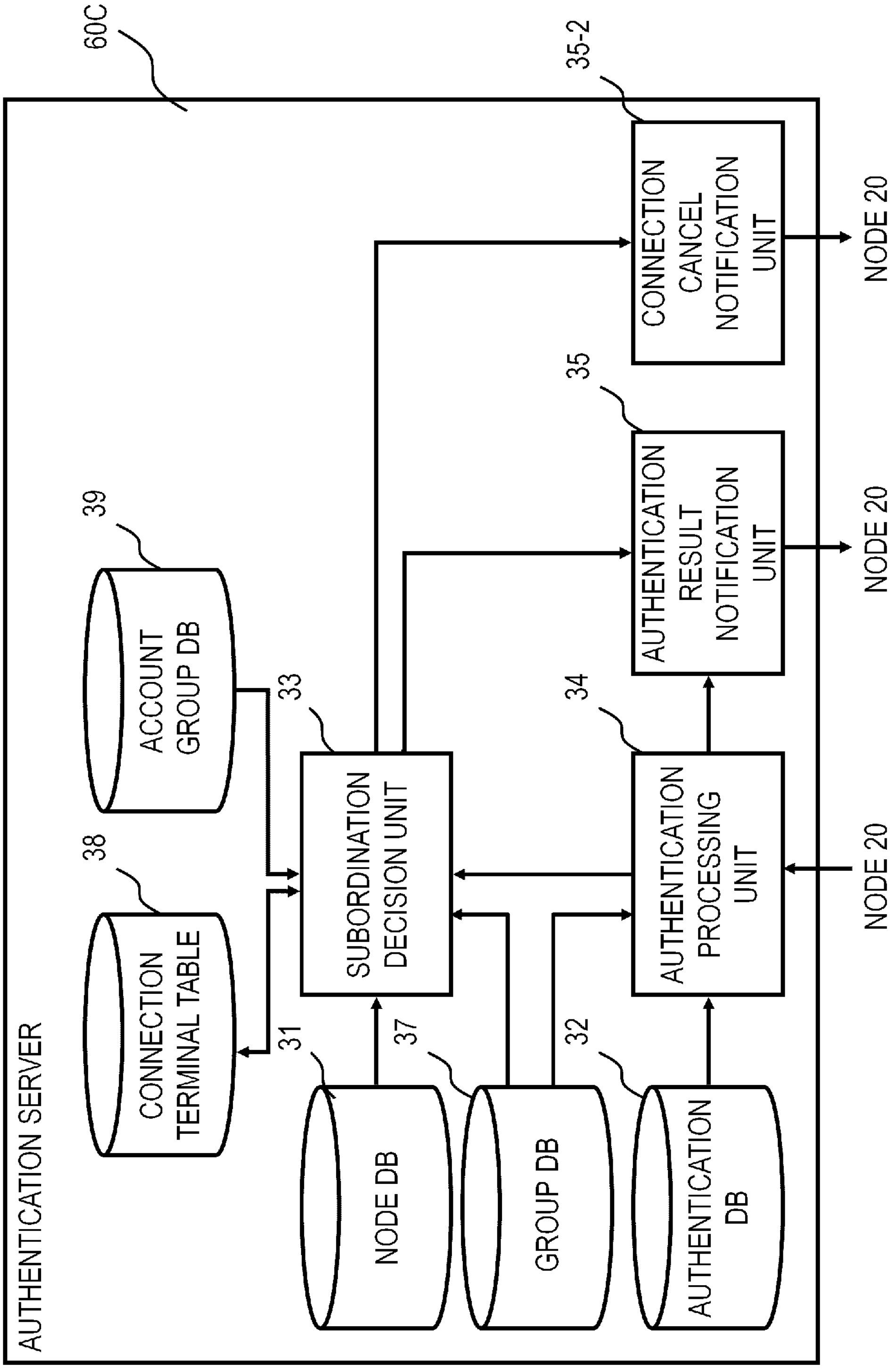
[Fig. 23]


60B
AUTHENTICATION SERVER
38
CONNECTION TERMINAL TABLE
39
ACCOUNT GROUP DB
31
NODE DB
33
SUBORDINATION DECISION UNIT
32
AUTHENTICATION DB
34
AUTHENTICATION PROCESSING UNIT
35
AUTHENTICATION RESULT NOTIFICATION UNIT
35-2
CONNECTION CANCEL NOTIFICATION UNIT
NODE 20
NODE 20
NODE 20

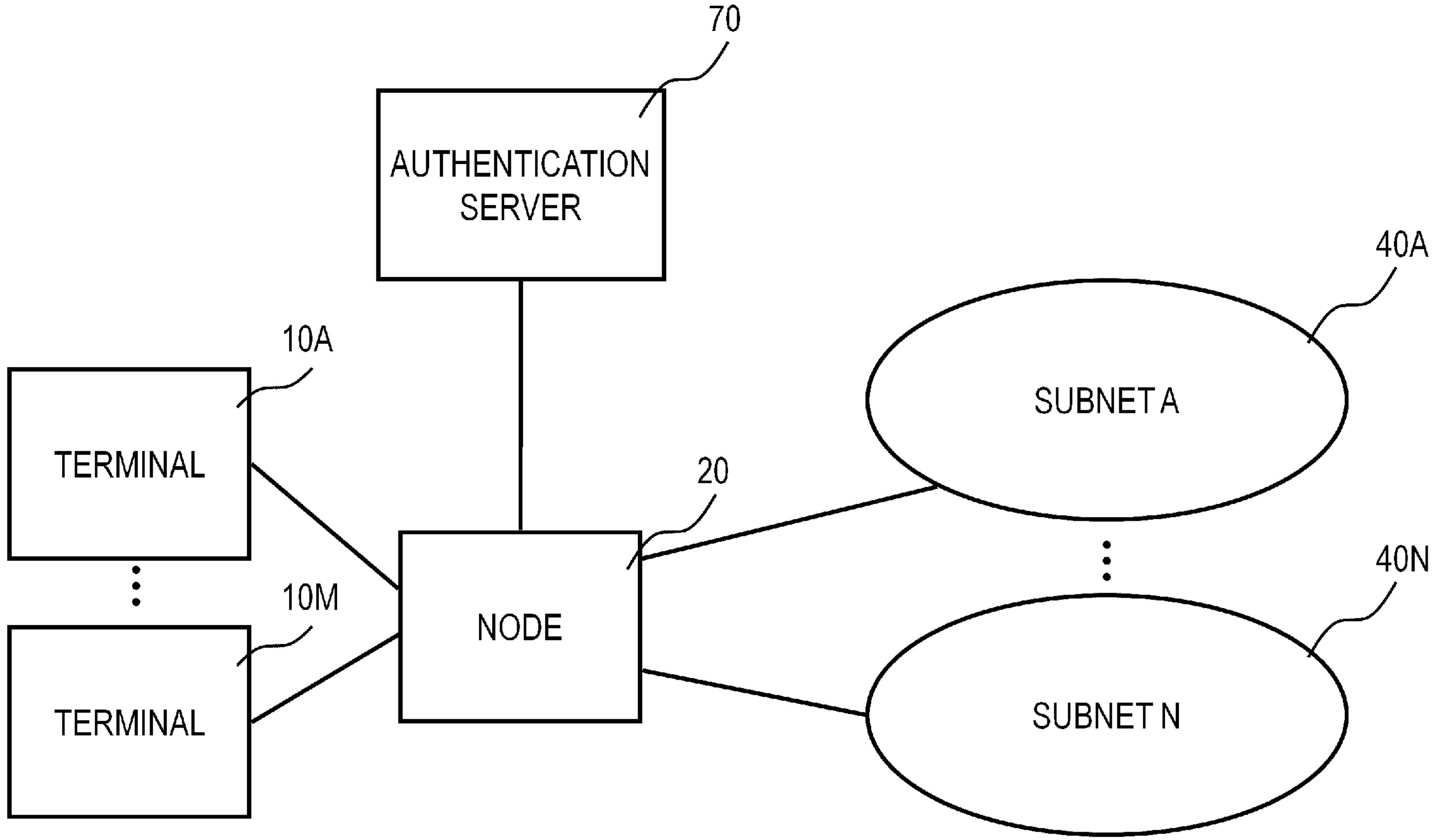
[Fig. 24]

| | | | | |
|---|---|---|---|---|
| ACCOUNT GROUP ID | CONNECTION PRIORITY | ACCOUNT | ... | ACCOUNT |

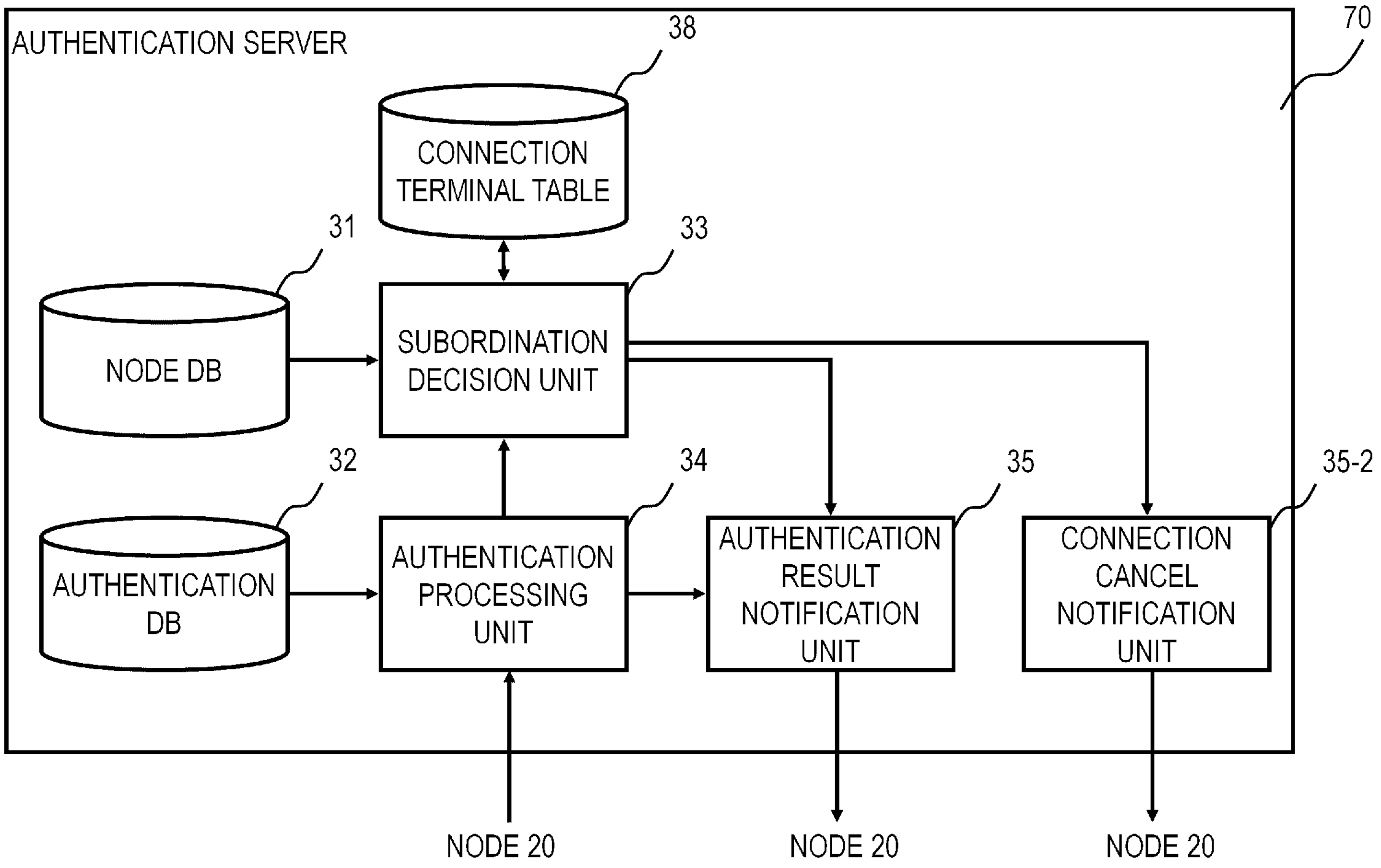
[Fig. 25]


60C
AUTHENTICATION SERVER
CONNECTION TERMINAL TABLE
38
ACCOUNT GROUP DB
39
SUBORDINATION DECISION UNIT
33
NODE DB
31
GROUP DB
37
AUTHENTICATION DB
32
AUTHENTICATION PROCESSING UNIT
34
AUTHENTICATION RESULT NOTIFICATION UNIT
35
CONNECTION CANCEL NOTIFICATION UNIT
35-2
NODE 20
NODE 20
NODE 20

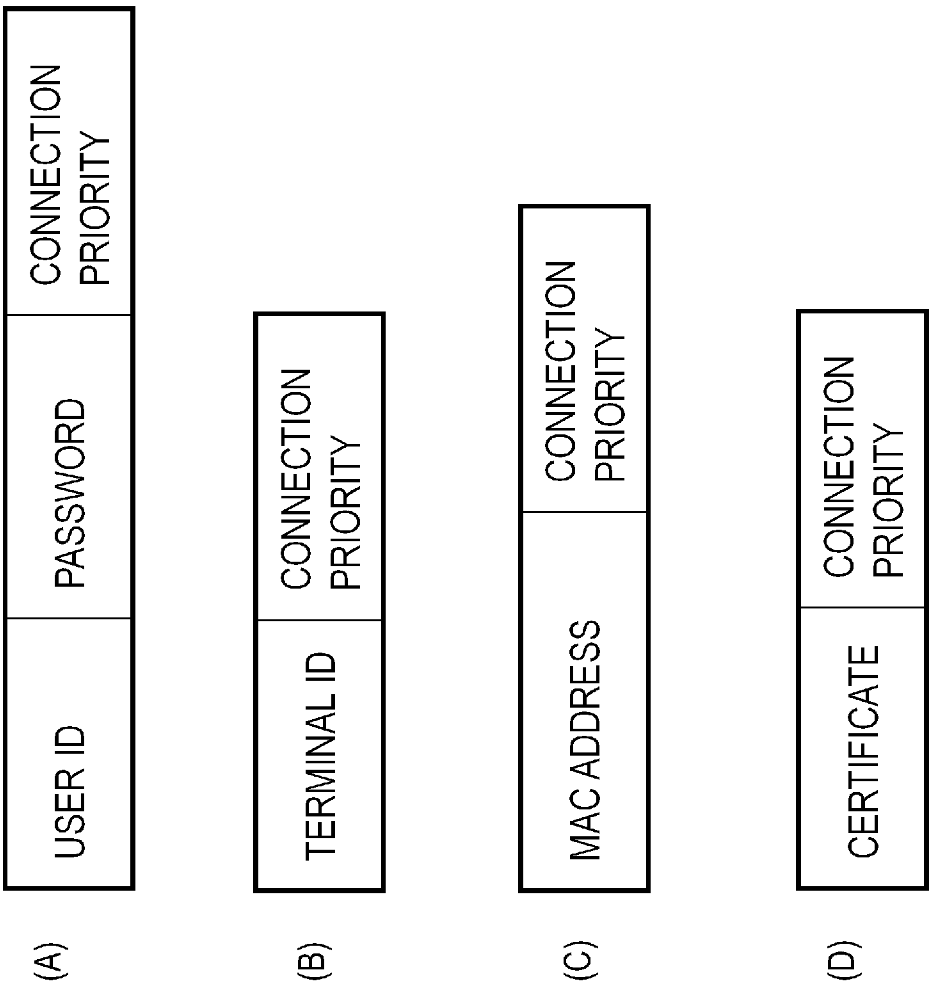
[Fig. 26]


70
AUTHENTICATION SERVER
40A
SUBNET A
10A
TERMINAL
20
NODE
10M
TERMINAL
40N
SUBNET N

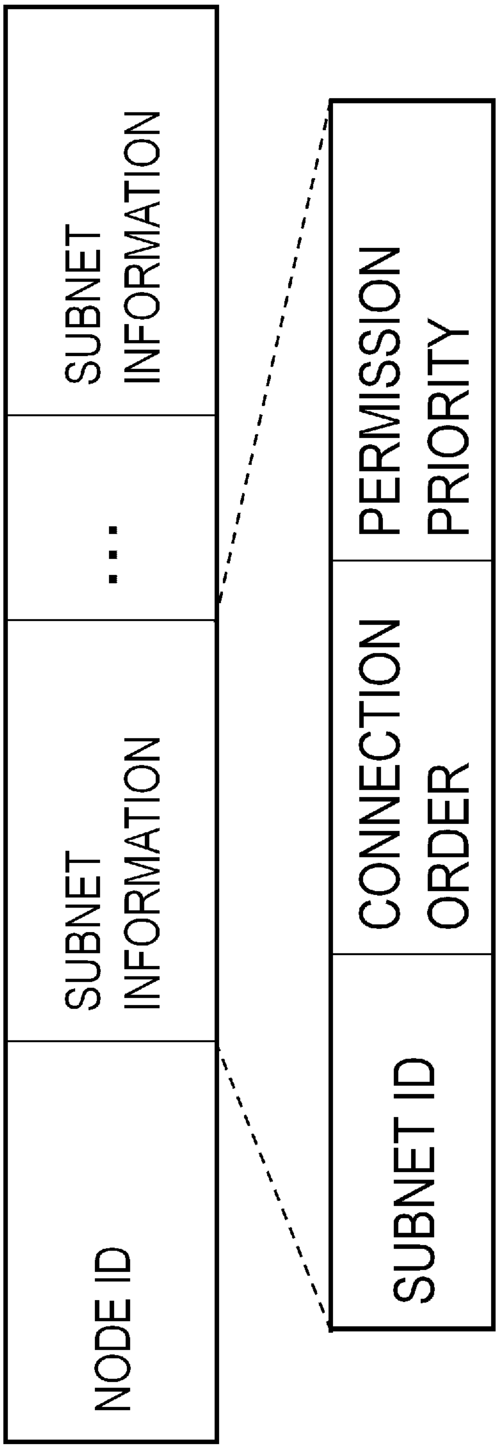
[Fig. 27]


70
AUTHENTICATION SERVER
38
CONNECTION TERMINAL TABLE
31
NODE DB
33
SUBORDINATION DECISION UNIT
32
AUTHENTICATION DB
34
AUTHENTICATION PROCESSING UNIT
35
AUTHENTICATION RESULT NOTIFICATION UNIT
35-2
CONNECTION CANCEL NOTIFICATION UNIT
NODE 20
NODE 20
NODE 20

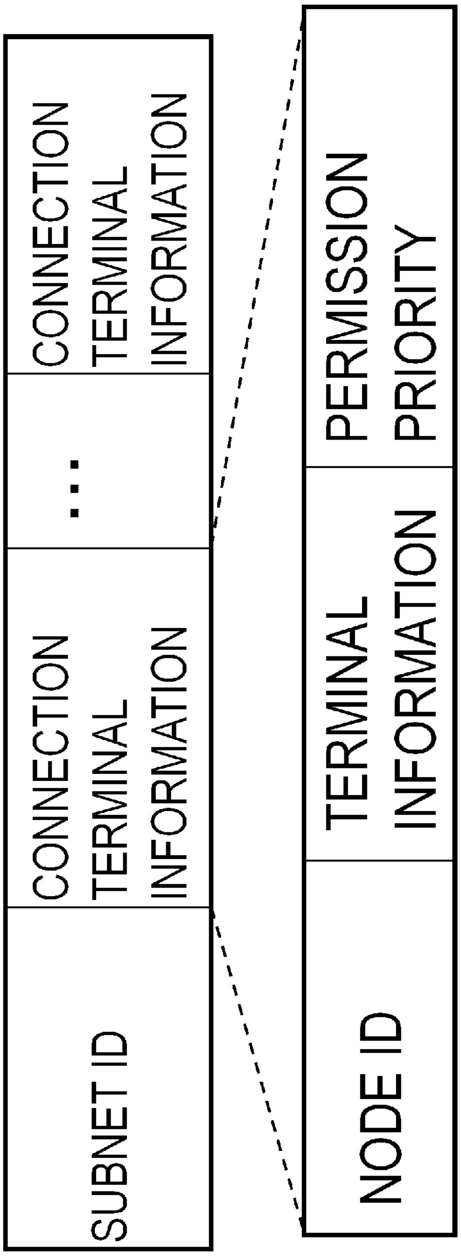
[Fig. 28]


(A)
USER ID
PASSWORD
CONNECTION PRIORITY
(B)
TERMINAL ID
CONNECTION PRIORITY
(C)
MAC ADDRESS
CONNECTION PRIORITY
(D)
CERTIFICATE
CONNECTION PRIORITY

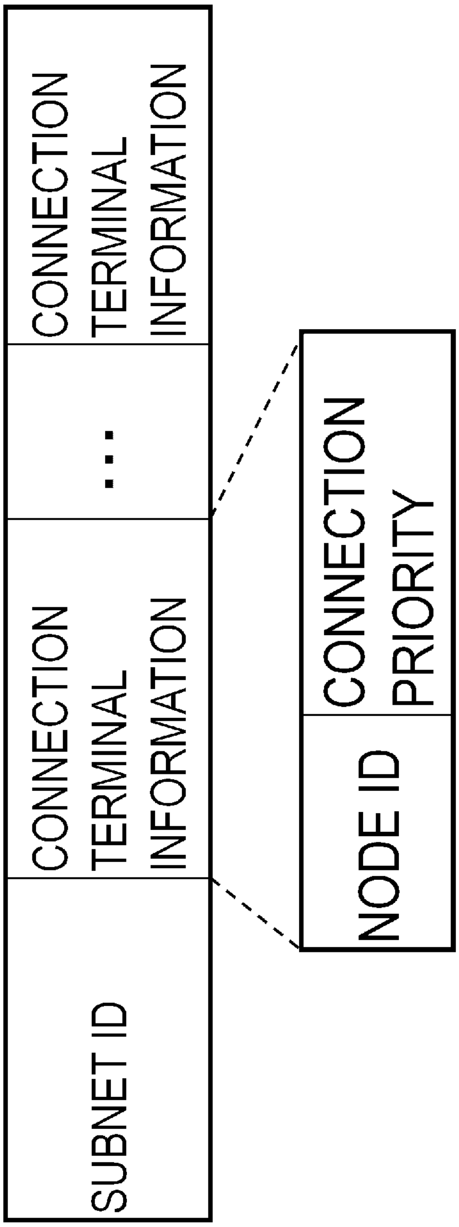
[Fig. 29]


NODE ID
SUBNET INFORMATION
...
SUBNET INFORMATION
SUBNET ID
CONNECTION ORDER
PERMISSION PRIORITY

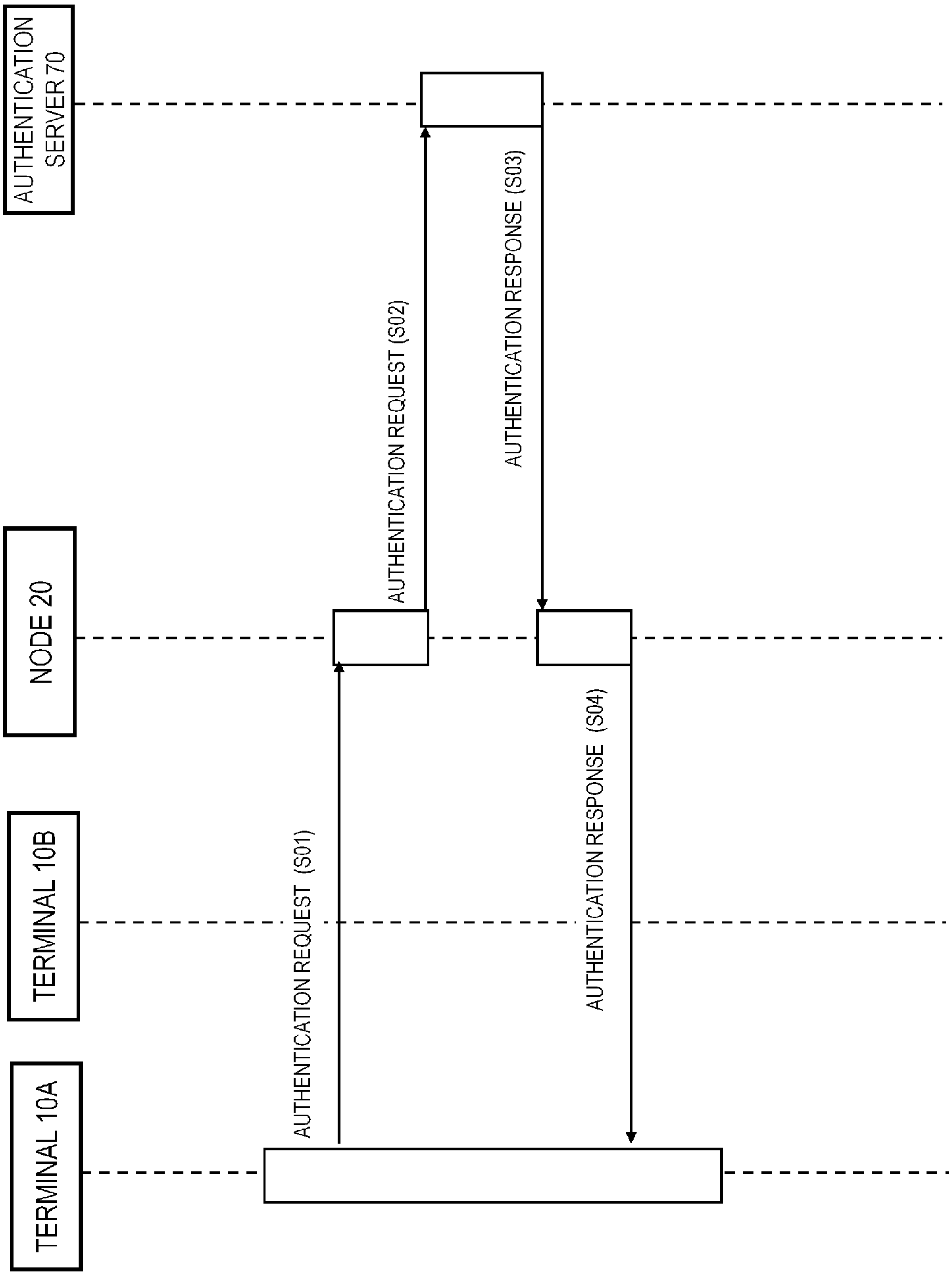
[Fig. 30]


SUBNET ID
CONNECTION TERMINAL INFORMATION
...
CONNECTION TERMINAL INFORMATION
NODE ID
TERMINAL INFORMATION
PERMISSION PRIORITY

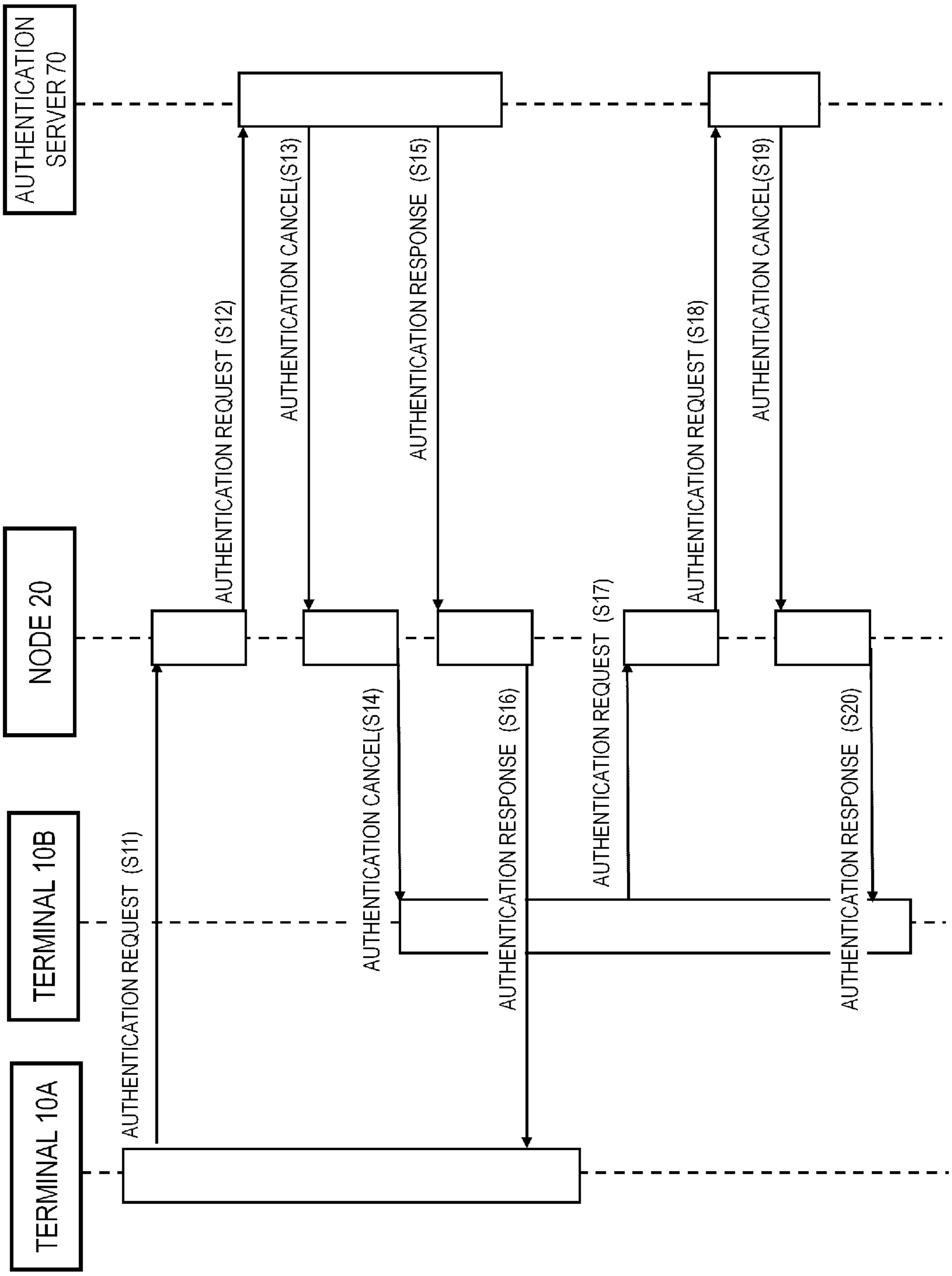
[Fig. 31]


SUBNET ID
CONNECTION TERMINAL INFORMATION
...
CONNECTION TERMINAL INFORMATION
NODE ID
CONNECTION PRIORITY

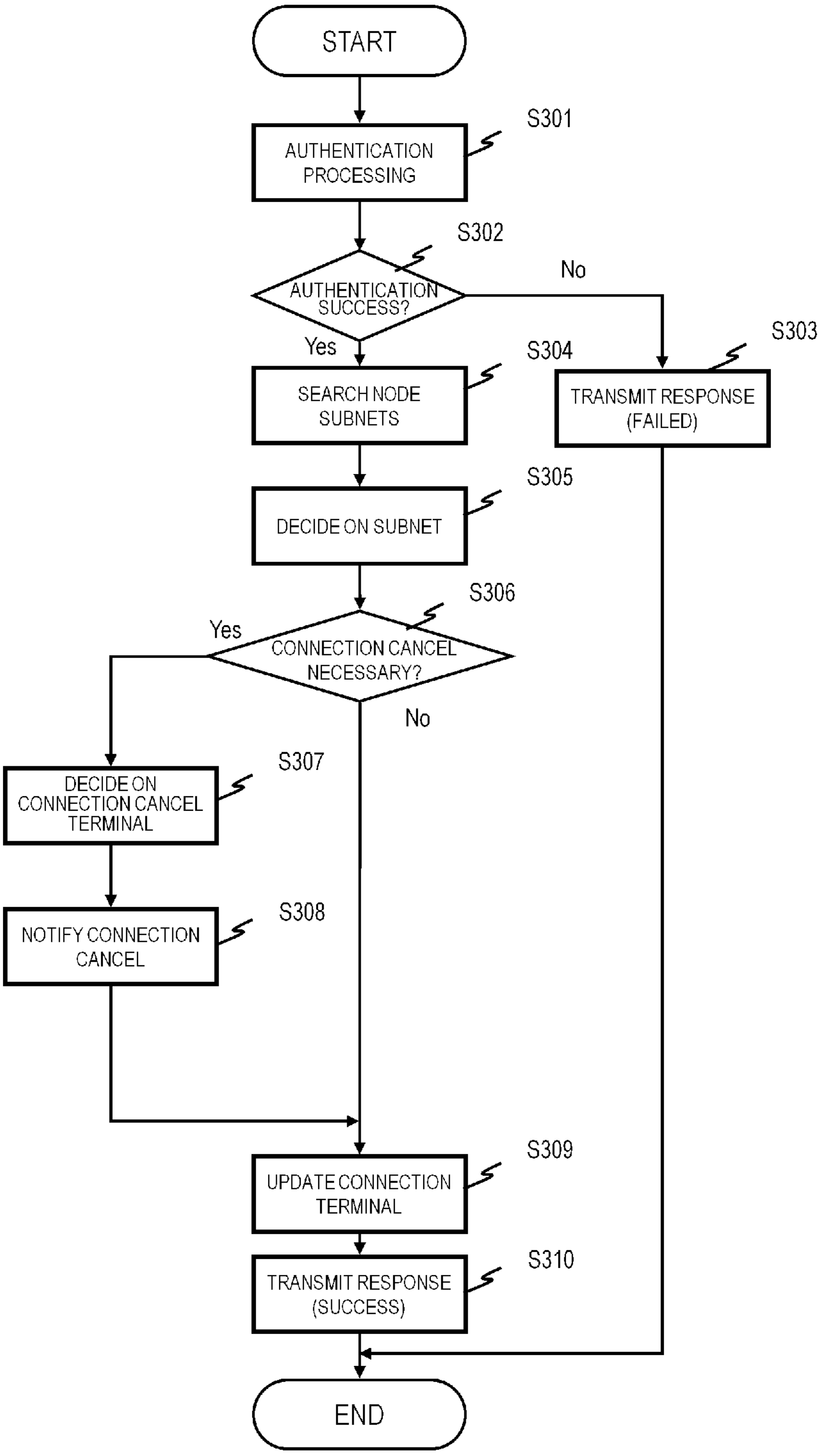
[Fig. 32]


AUTHENTICATION SERVER 70
NODE 20
TERMINAL 10B
TERMINAL 10A
AUTHENTICATION REQUEST (S01)
AUTHENTICATION REQUEST (S02)
AUTHENTICATION RESPONSE (S03)
AUTHENTICATION RESPONSE (S04)

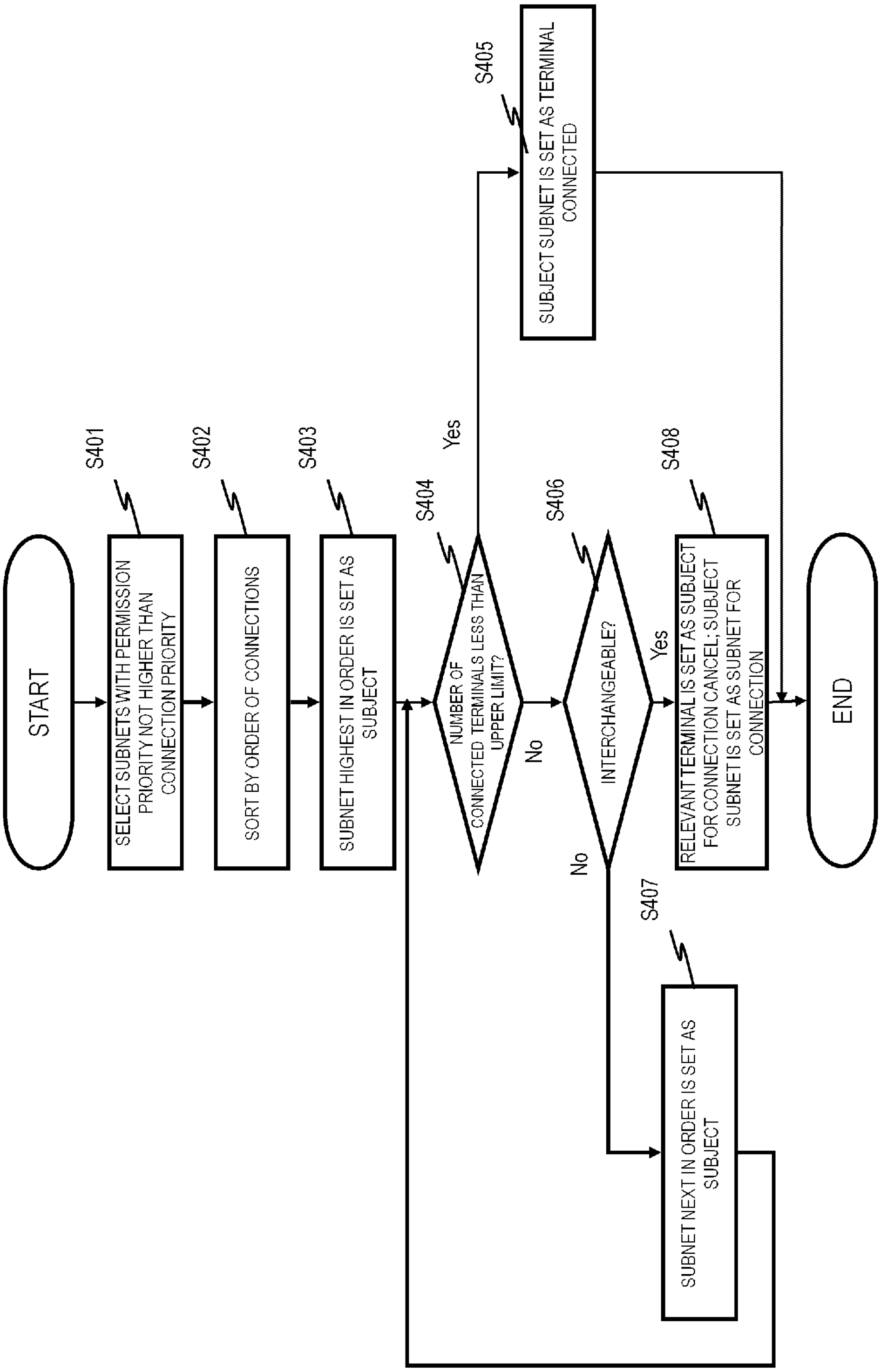
[Fig. 33]


AUTHENTICATION SERVER 70
NODE 20
TERMINAL 10B
TERMINAL 10A
AUTHENTICATION REQUEST (S11)
AUTHENTICATION REQUEST (S12)
AUTHENTICATION CANCEL(S13)
AUTHENTICATION CANCEL(S14)
AUTHENTICATION RESPONSE (S15)
AUTHENTICATION RESPONSE (S16)
AUTHENTICATION REQUEST (S17)
AUTHENTICATION REQUEST (S18)
AUTHENTICATION CANCEL(S19)
AUTHENTICATION RESPONSE (S20)

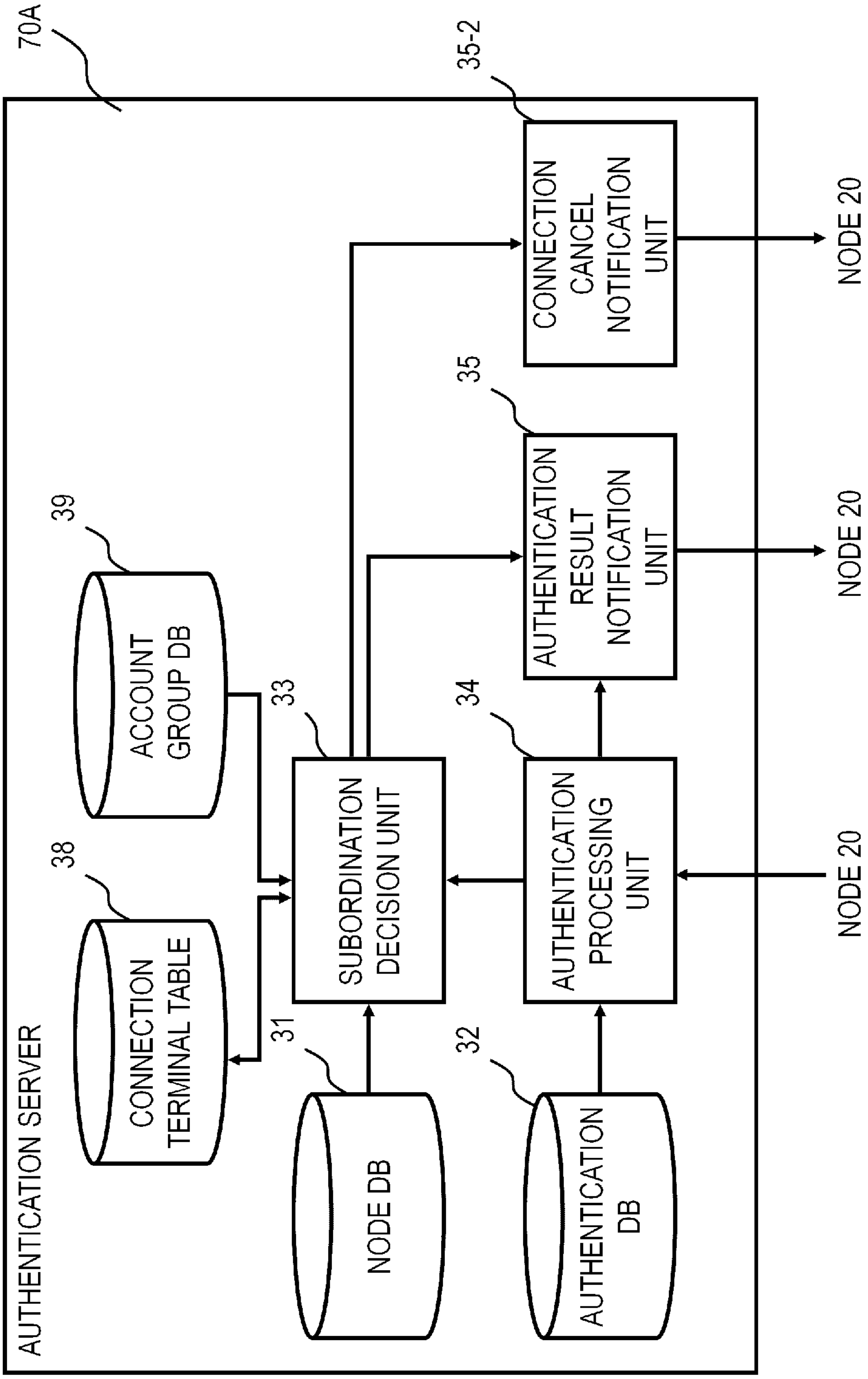
[Fig. 34]


START
AUTHENTICATION PROCESSING
S301
S302
AUTHENTICATION SUCCESS?
No
Yes
S303
TRANSMIT RESPONSE (FAILED)
S304
SEARCH NODE SUBNETS
S305
DECIDE ON SUBNET
S306
CONNECTION CANCEL NECESSARY?
Yes
No
S307
DECIDE ON CONNECTION CANCEL TERMINAL
S308
NOTIFY CONNECTION CANCEL
S309
UPDATE CONNECTION TERMINAL
S310
TRANSMIT RESPONSE (SUCCESS)
END

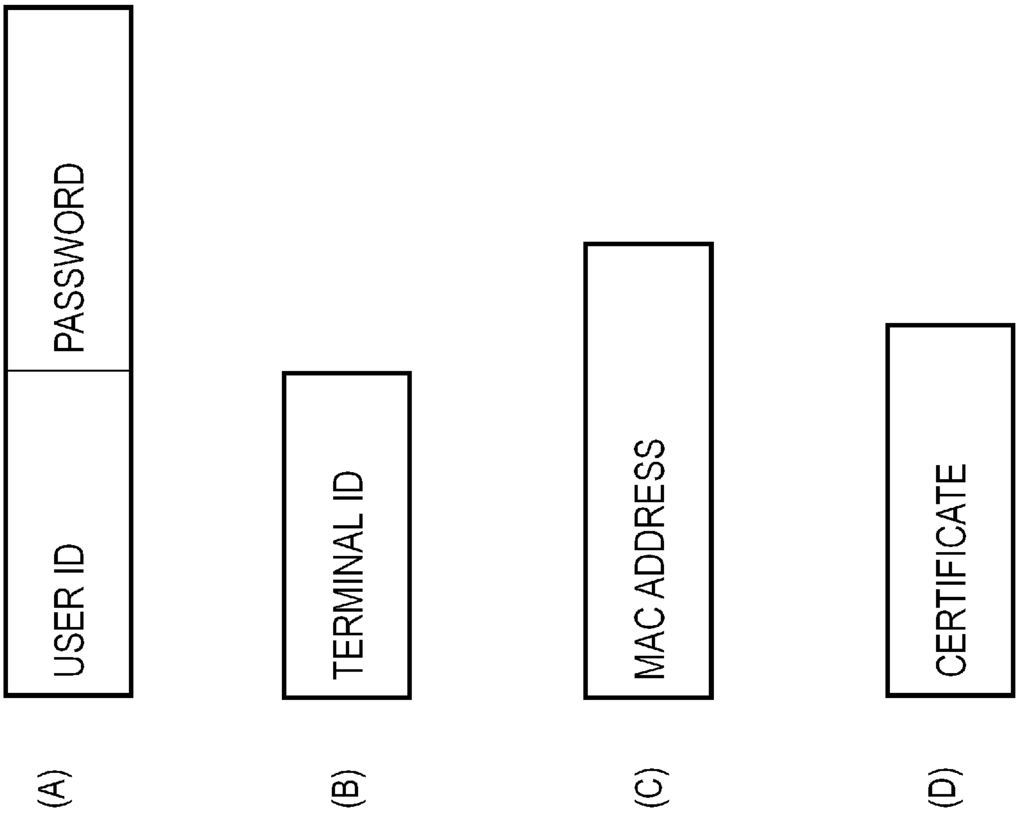
[Fig. 35]


START
S401
SELECT SUBNETS WITH PERMISSION PRIORITY NOT HIGHER THAN CONNECTION PRIORITY
S402
SORT BY ORDER OF CONNECTIONS
S403
SUBNET HIGHEST IN ORDER IS SET AS SUBJECT
S404
NUMBER OF CONNECTED TERMINALS LESS THAN UPPER LIMIT?
Yes
No
S405
SUBJECT SUBNET IS SET AS TERMINAL CONNECTED
S406
INTERCHANGEABLE?
Yes
No
S407
SUBNET NEXT IN ORDER IS SET AS SUBJECT
S408
RELEVANT TERMINAL IS SET AS SUBJECT FOR CONNECTION CANCEL; SUBJECT SUBNET IS SET AS SUBNET FOR CONNECTION
END

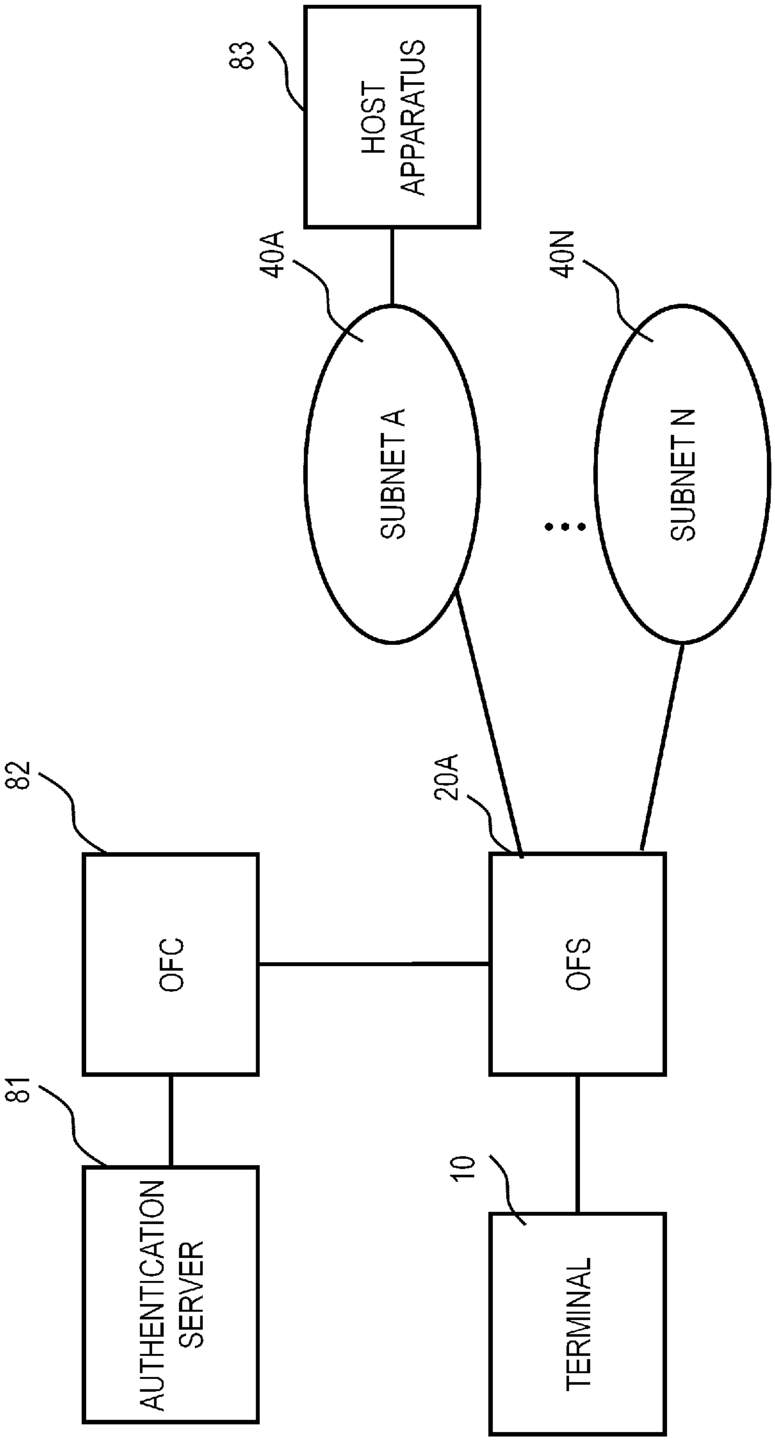
[Fig. 36]


70A
AUTHENTICATION SERVER
38
CONNECTION TERMINAL TABLE
39
ACCOUNT GROUP DB
31
NODE DB
33
SUBORDINATION DECISION UNIT
32
AUTHENTICATION DB
34
AUTHENTICATION PROCESSING UNIT
35
AUTHENTICATION RESULT NOTIFICATION UNIT
35-2
CONNECTION CANCEL NOTIFICATION UNIT
NODE 20
NODE 20
NODE 20

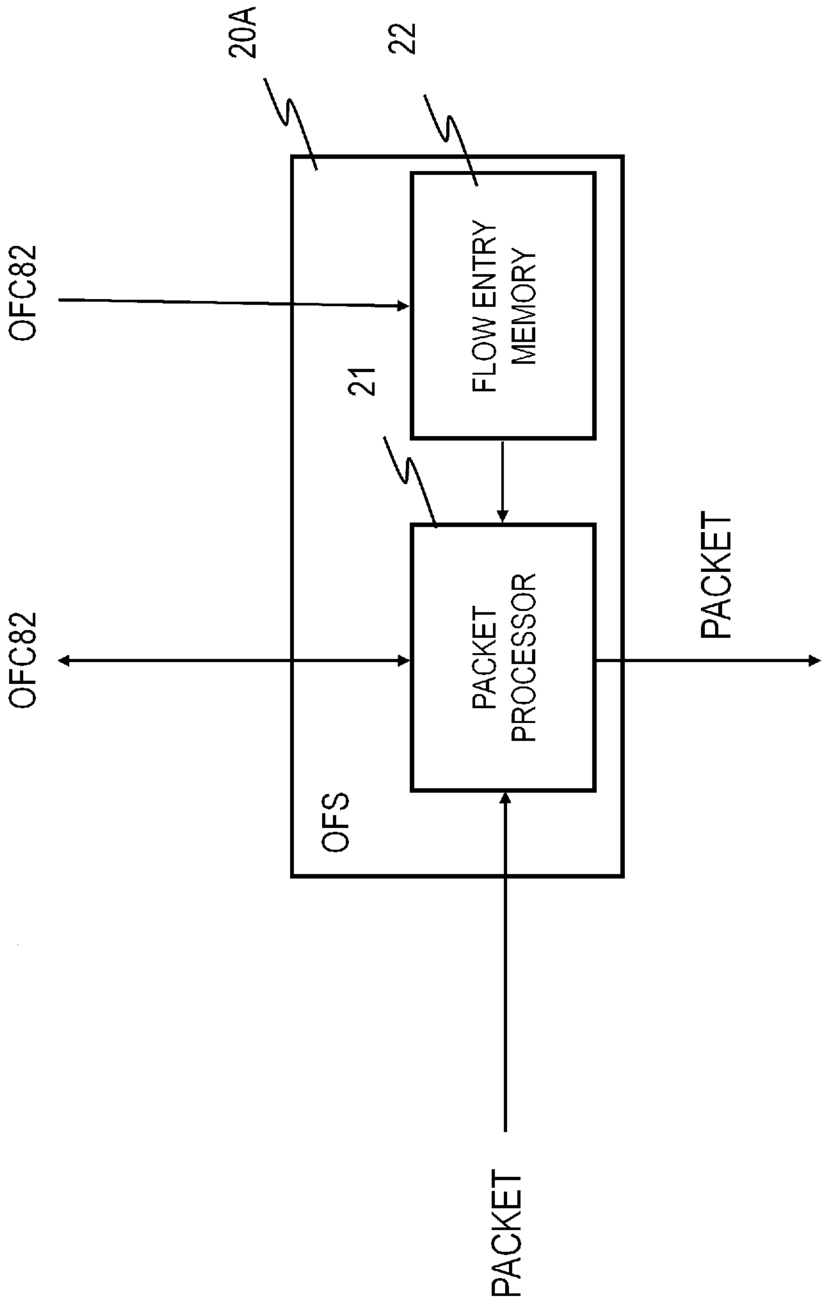
[Fig. 37]



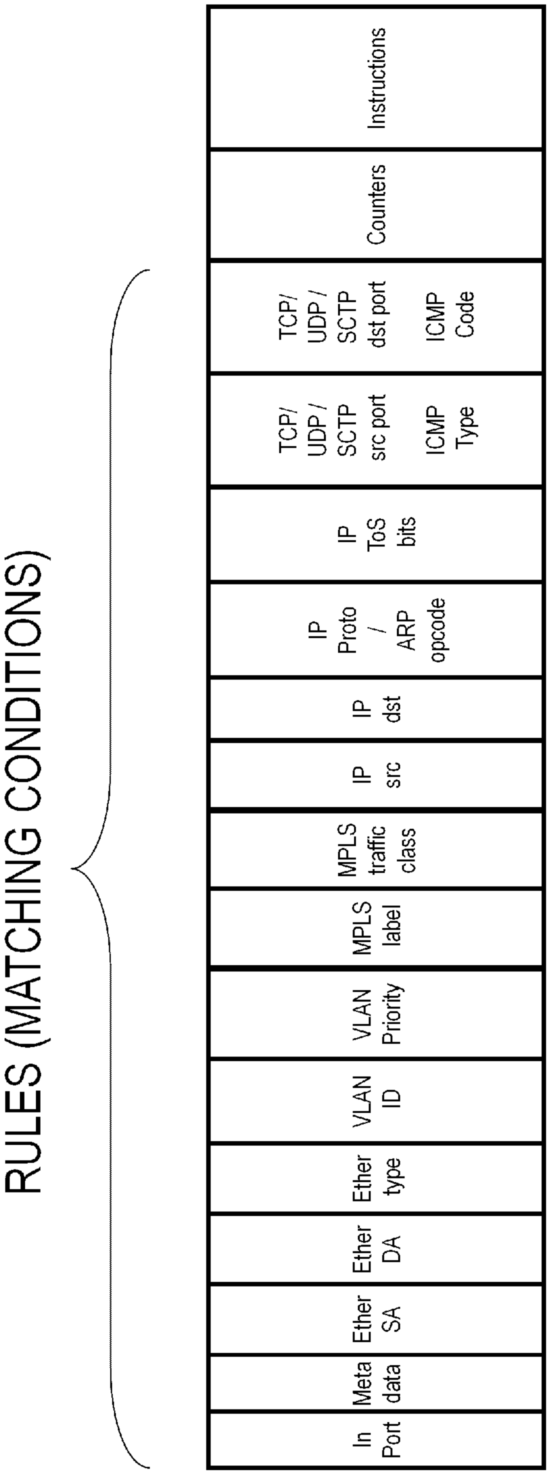
[Fig. 38]


83
HOST APPARATUS
40A
SUBNET A
40N
SUBNET N
...
82
OFC
20A
OFS
81
AUTHENTICATION SERVER
10
TERMINAL

[Fig. 39]


20A
22
OFC82
FLOW ENTRY MEMORY
21
OFC82
PACKET PROCESSOR
PACKET
OFS
PACKET

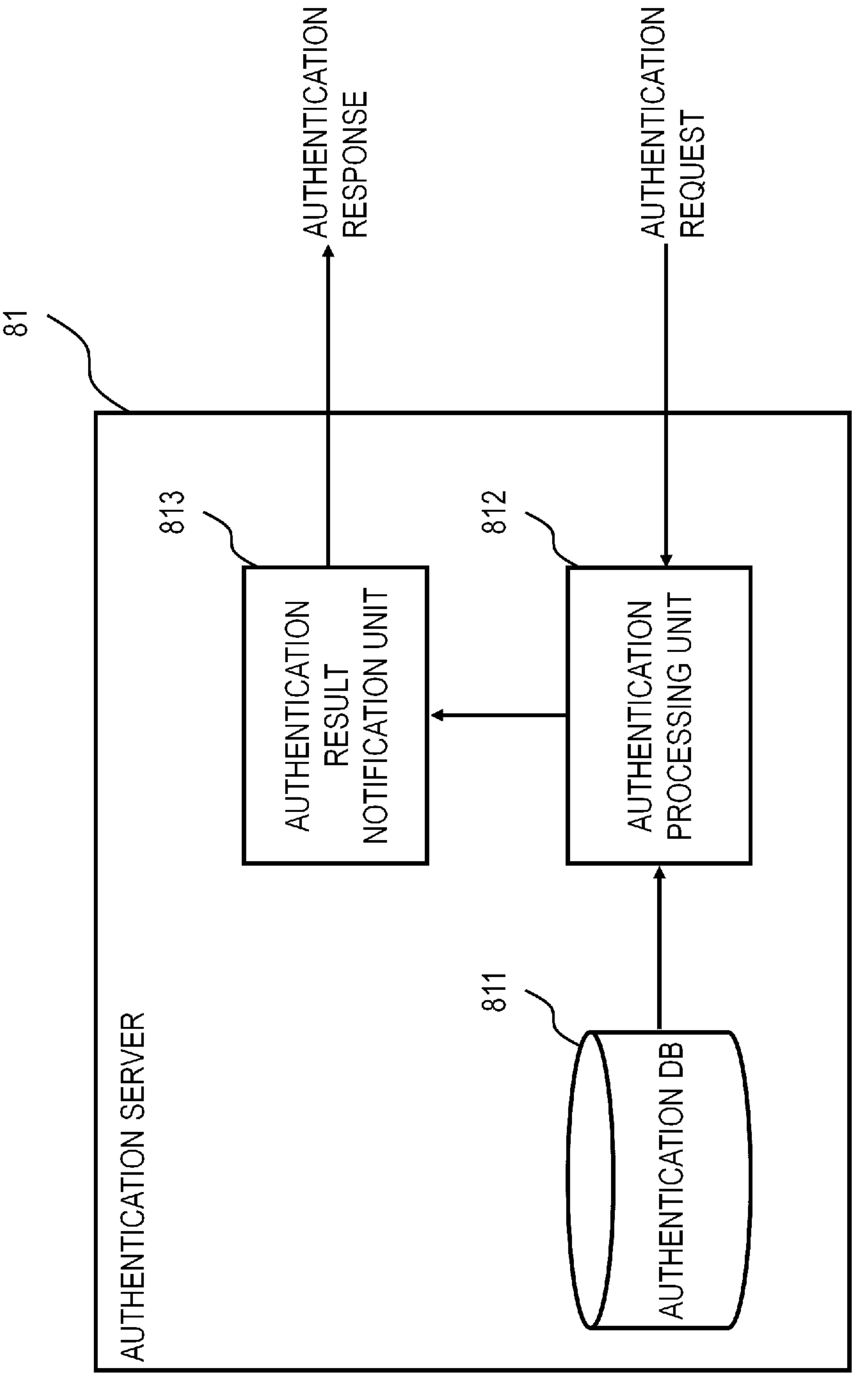
[Fig. 40]


RULES (MATCHING CONDITIONS)
In Port
Meta data
Ether SA
Ether DA
Ether type
VLAN ID
VLAN Priority
MPLS label
MPLS traffic class
IP src
IP dst
IP Proto / ARP opcode
IP ToS bits
TCP/ UDP / SCTP src port
ICMP Type
TCP/ UDP / SCTP dst port
ICMP Code
Counters
Instructions

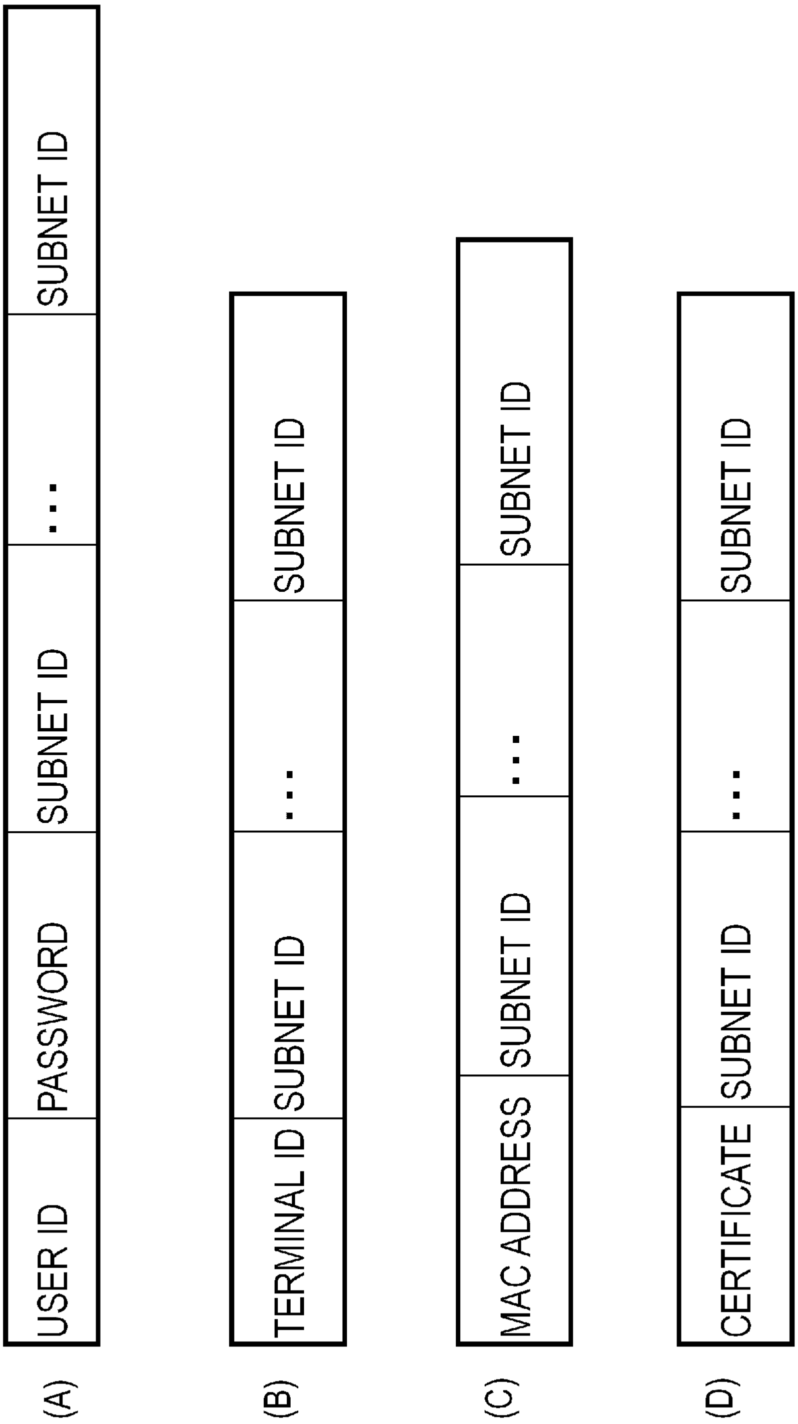
[Fig. 41]

| ACTION NAMES | ACTION CONTENTS |
|---|---|
| OUTPUT | OUTPUT TO SPECIFIED PORT |
| SET_VLAN_VID | ADD & UPDATE VLAN TAG WITH SPECIFIED VLAN ID |
| SET_VLAN_PCP | ADD & UPDATE VLAN TAG WITH SPECIFIED VLAN PRIORITY |
| STRIP_VLAN | REMOVE IEEE802.1Q VLAN TAG |
| SET_DL_SRC | UPDATE MAC SA |
| SET_DL_DST | UPDATE MAC DA |
| SET_NW_SRC | UPDATE IP SA |
| SET_NW_DST | UPDATE IP DA |
| SET_TP_SRC | UPDATE TCP/UDP SOURCE PORT |
| SET_TP_DST | UPDATE TCP/UDP DESTINATION PORT |

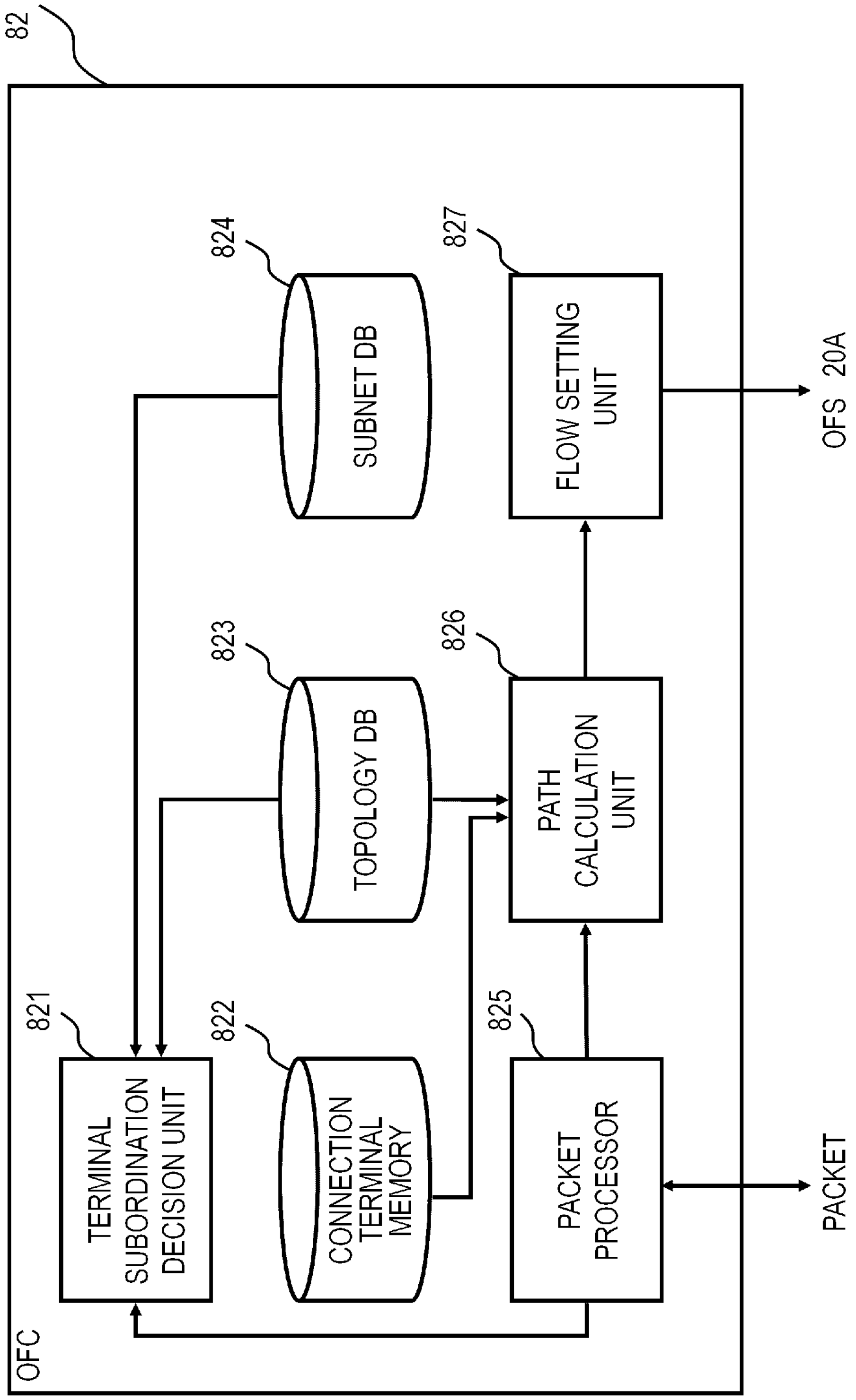
[Fig. 42]


AUTHENTICATION RESPONSE
AUTHENTICATION REQUEST
81
AUTHENTICATION SERVER
813
AUTHENTICATION RESULT NOTIFICATION UNIT
812
AUTHENTICATION PROCESSING UNIT
811
AUTHENTICATION DB

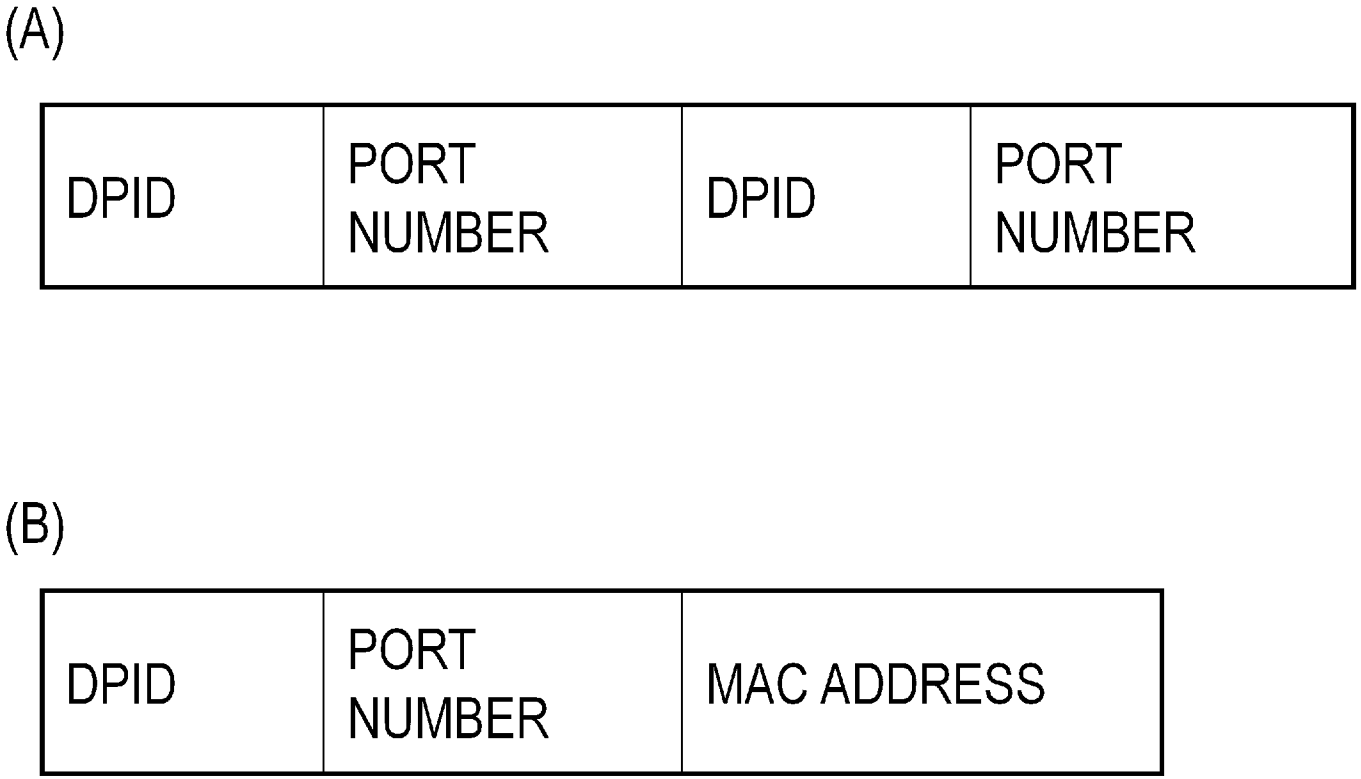
[Fig. 43]


(A)
USER ID
PASSWORD
SUBNET ID
...
SUBNET ID
(B)
TERMINAL ID
SUBNET ID
...
SUBNET ID
(C)
MAC ADDRESS
SUBNET ID
...
SUBNET ID
(D)
CERTIFICATE
SUBNET ID
...
SUBNET ID

[Fig. 44]


82
OFC
821
TERMINAL SUBORDINATION DECISION UNIT
822
CONNECTION TERMINAL MEMORY
823
TOPOLOGY DB
824
SUBNET DB
825
PACKET PROCESSOR
826
PATH CALCULATION UNIT
827
FLOW SETTING UNIT
OFS 20A
PACKET

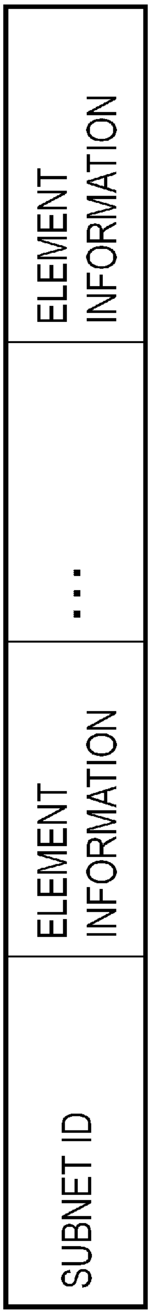
[Fig. 45]


(A)
DPID
PORT NUMBER
DPID
PORT NUMBER
(B)
DPID
PORT NUMBER
MAC ADDRESS

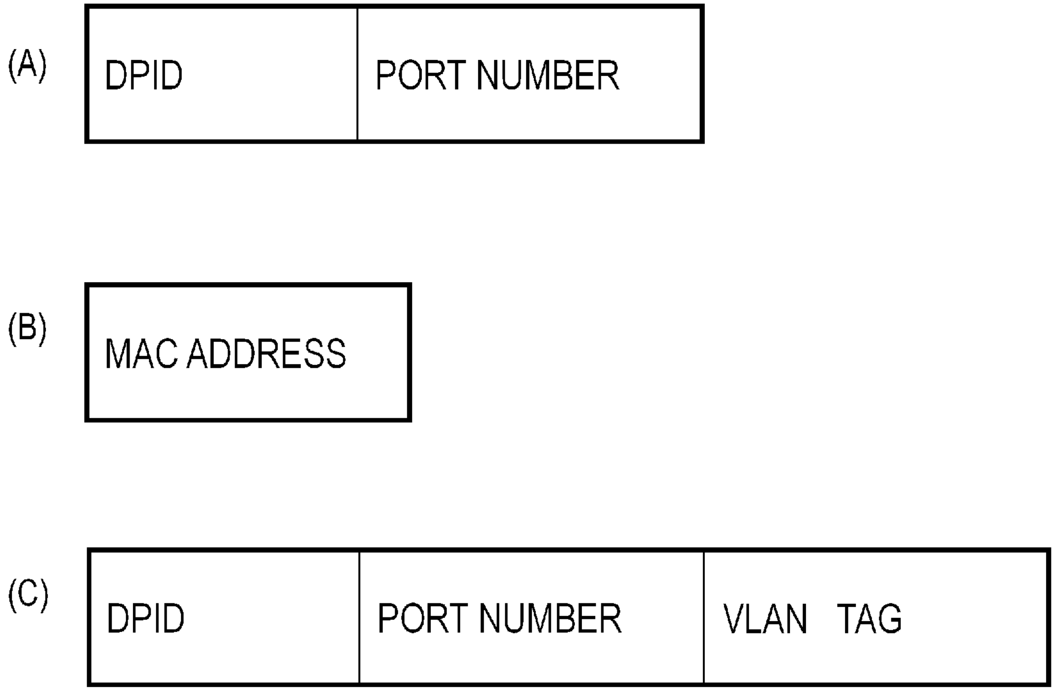
[Fig. 46]

| | | | | | | |
|---|---|---|---|---|---|---|
| DPID | PORT NUMBER | TERMINAL INFORMATION | MAIN SUBNET ID | SUBNET ID | ・・・ | SUBNET ID |

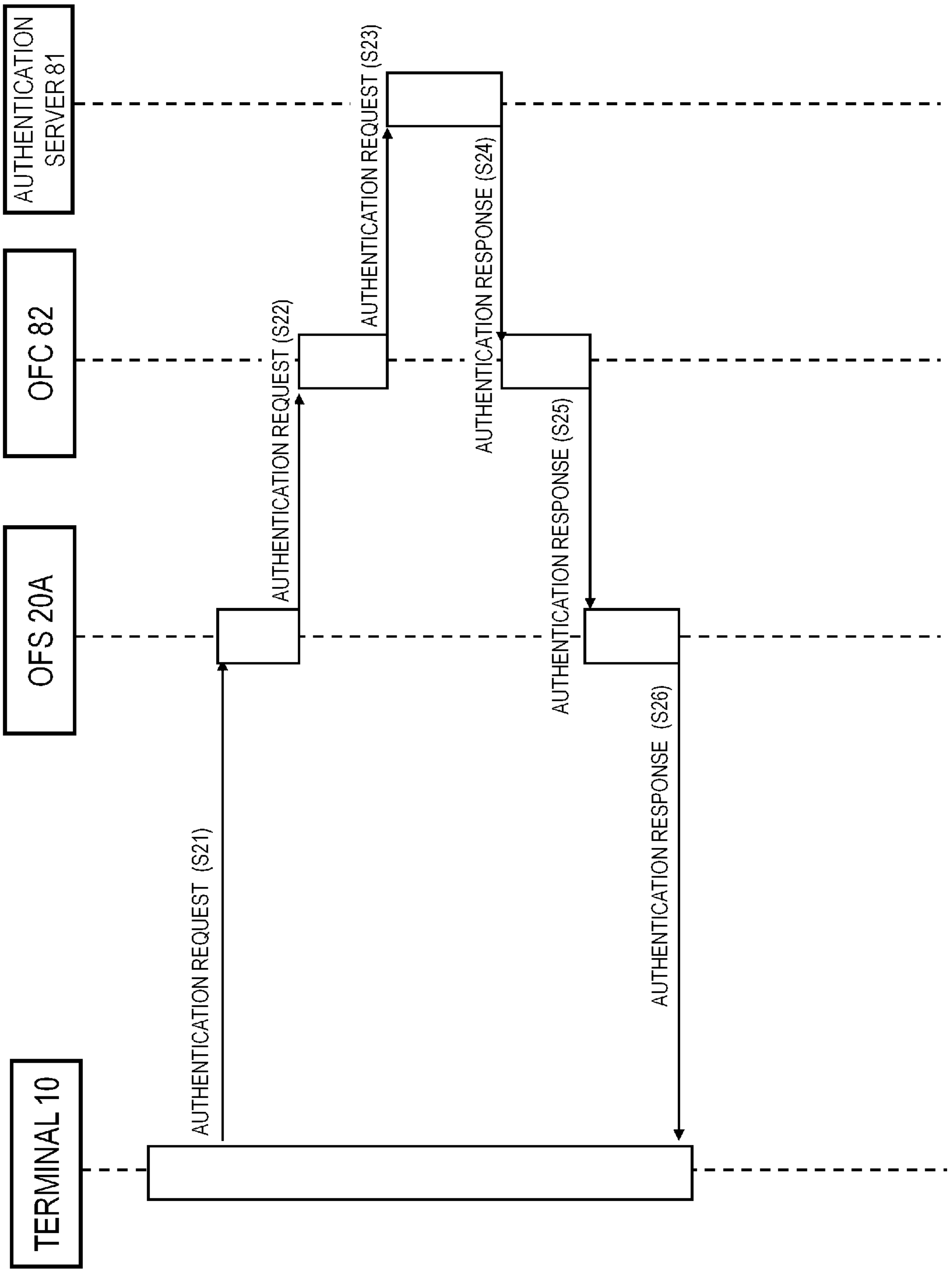
[Fig. 47]



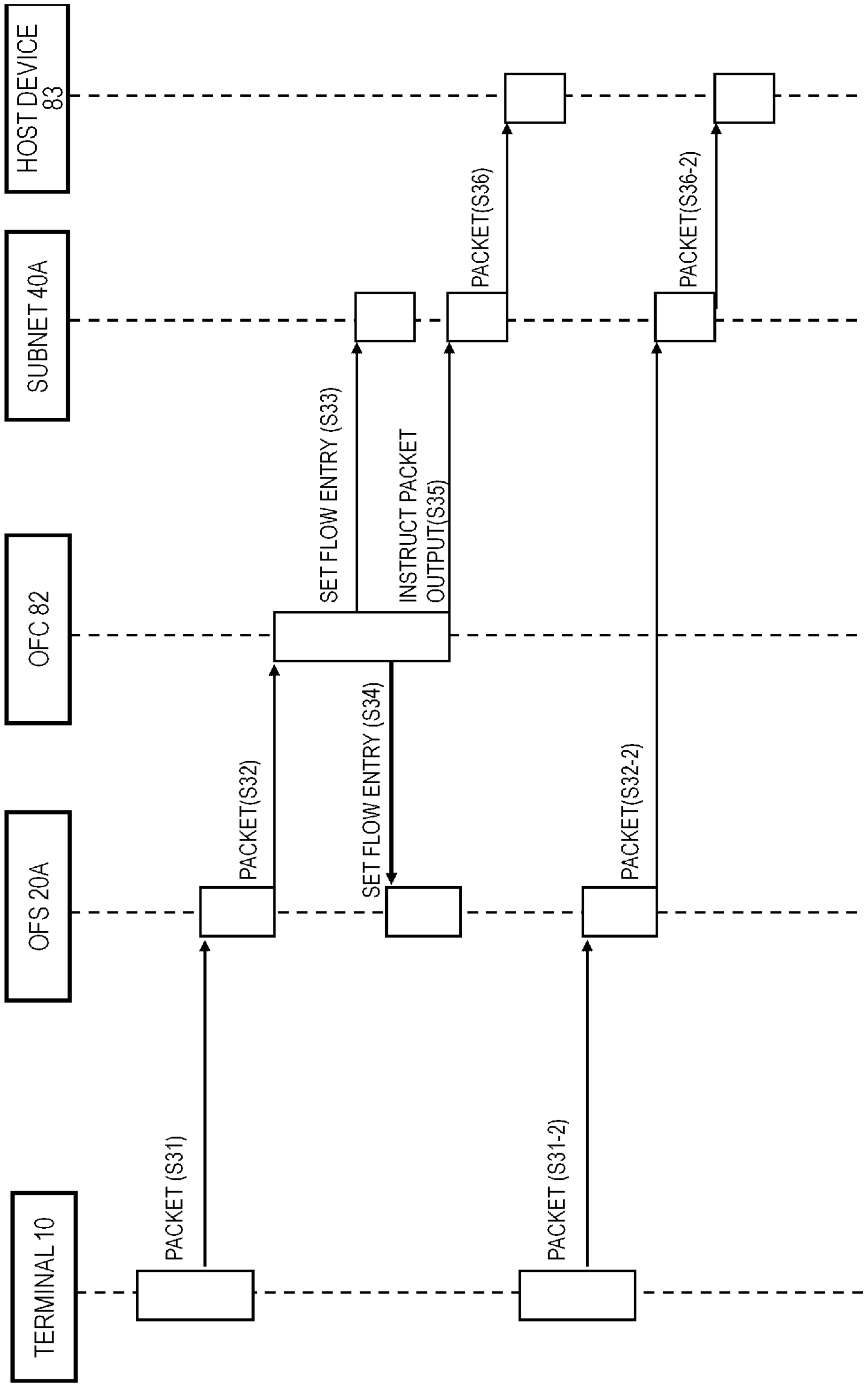
[Fig. 48]



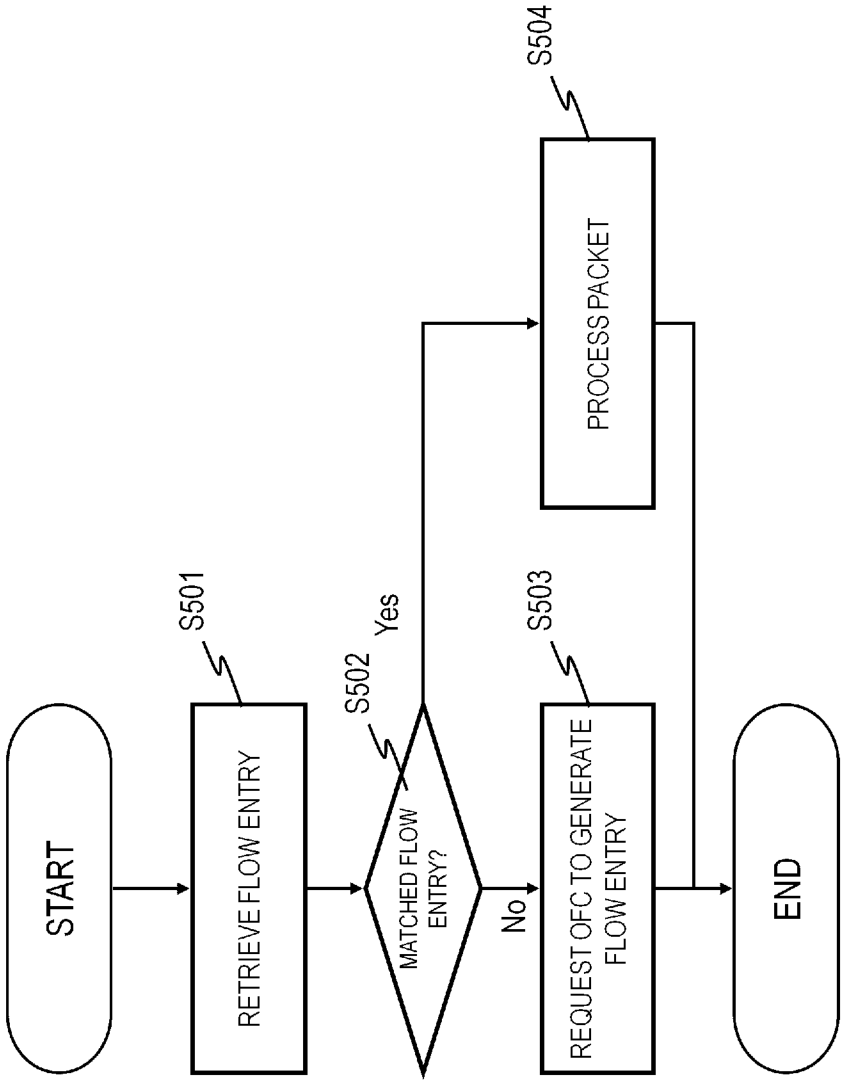
[Fig. 49]


AUTHENTICATION SERVER 81
OFC 82
OFS 20A
TERMINAL 10
AUTHENTICATION REQUEST (S21)
AUTHENTICATION REQUEST (S22)
AUTHENTICATION REQUEST (S23)
AUTHENTICATION RESPONSE (S24)
AUTHENTICATION RESPONSE (S25)
AUTHENTICATION RESPONSE (S26)

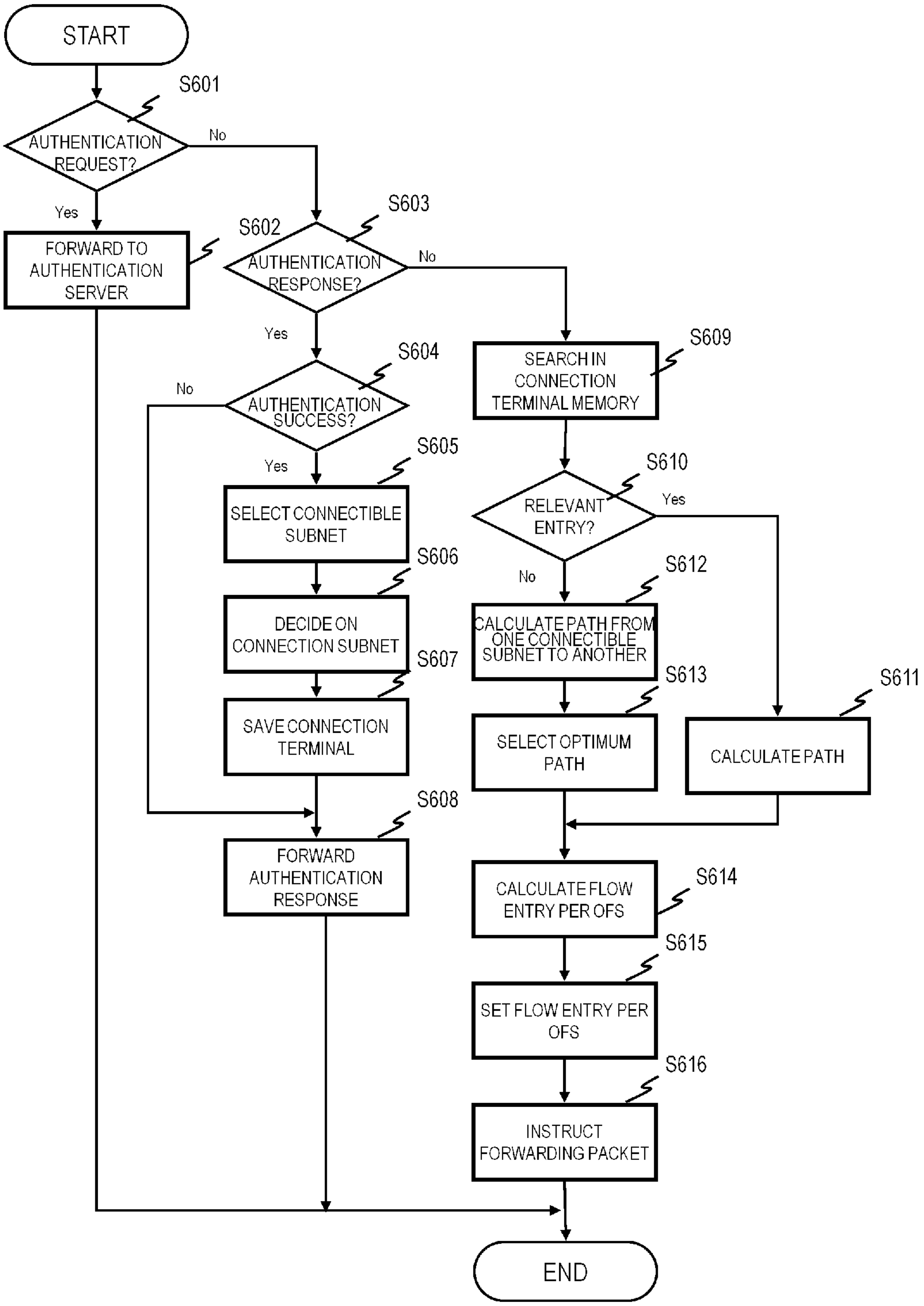
[Fig. 50]


TERMINAL 10
OFS 20A
OFC 82
SUBNET 40A
HOST DEVICE 83
PACKET (S31)
PACKET(S32)
SET FLOW ENTRY (S33)
SET FLOW ENTRY (S34)
INSTRUCT PACKET OUTPUT(S35)
PACKET(S36)
PACKET (S31-2)
PACKET(S32-2)
PACKET(S36-2)

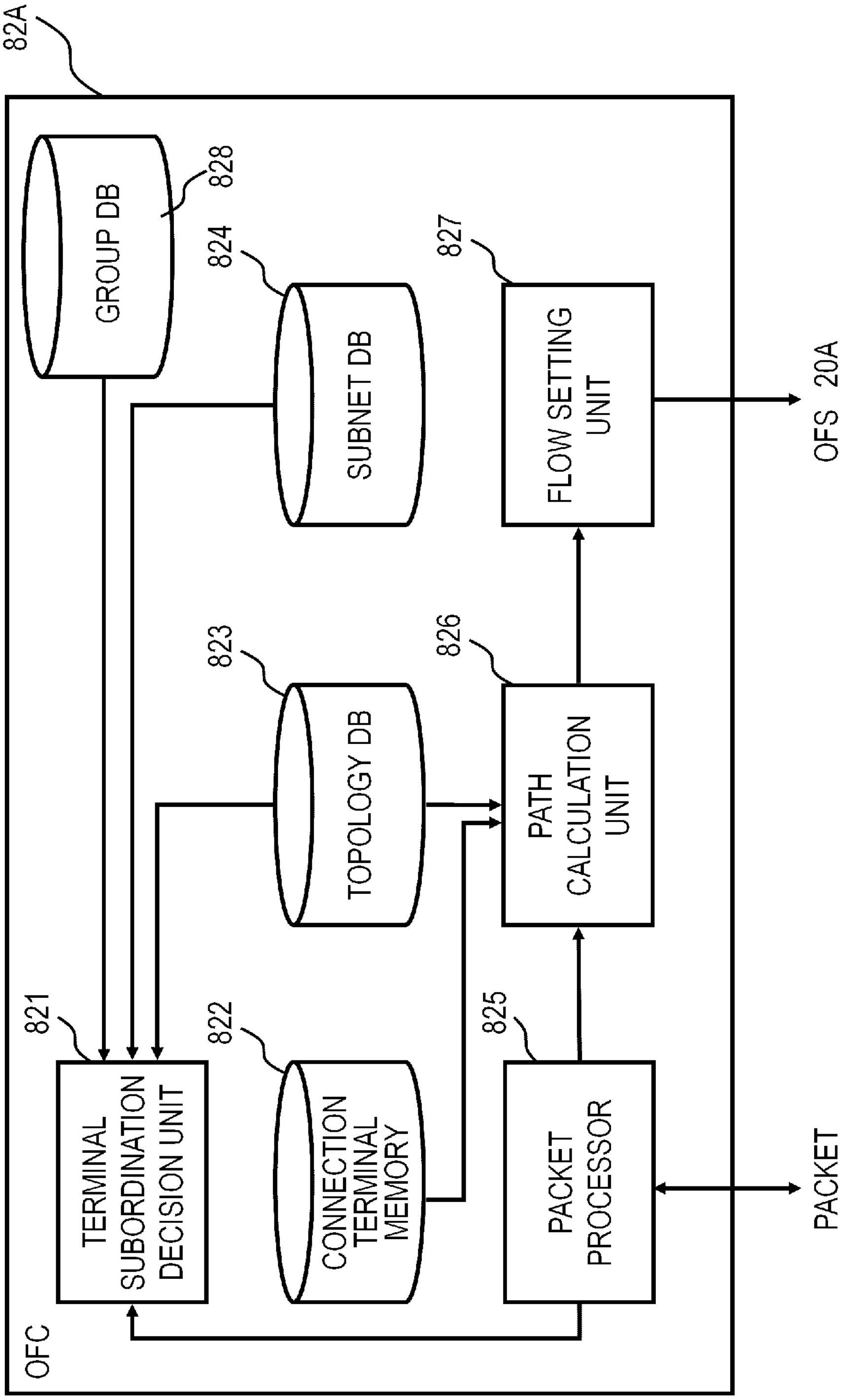
[Fig. 51]


START
RETRIEVE FLOW ENTRY
S501
MATCHED FLOW ENTRY?
S502
Yes
No
REQUEST OFC TO GENERATE FLOW ENTRY
S503
PROCESS PACKET
S504
END

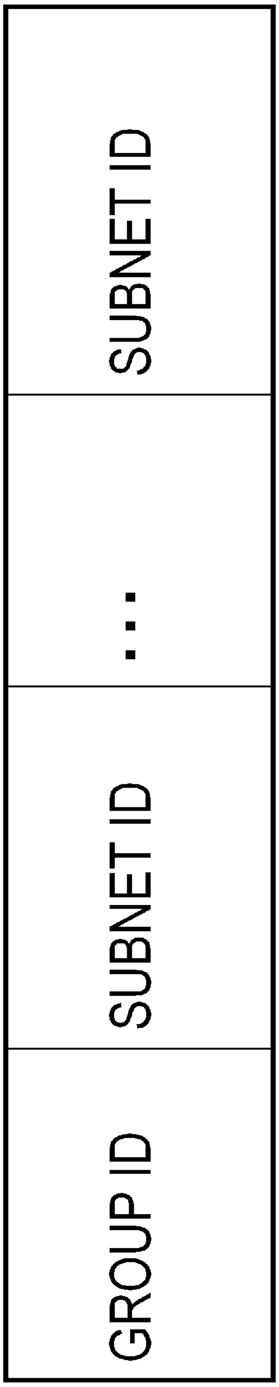
[Fig. 52]


START
S601
AUTHENTICATION REQUEST?
No
Yes
FORWARD TO AUTHENTICATION SERVER
S602
S603
AUTHENTICATION RESPONSE?
No
Yes
S604
AUTHENTICATION SUCCESS?
No
Yes
S605
SELECT CONNECTIBLE SUBNET
S606
DECIDE ON CONNECTION SUBNET
S607
SAVE CONNECTION TERMINAL
S608
FORWARD AUTHENTICATION RESPONSE
S609
SEARCH IN CONNECTION TERMINAL MEMORY
S610
RELEVANT ENTRY?
Yes
No
S612
CALCULATE PATH FROM ONE CONNECTIBLE SUBNET TO ANOTHER
S613
SELECT OPTIMUM PATH
S611
CALCULATE PATH
S614
CALCULATE FLOW ENTRY PER OFS
S615
SET FLOW ENTRY PER OFS
S616
INSTRUCT FORWARDING PACKET
END

[Fig. 53]


82A
OFC
GROUP DB
828
SUBNET DB
824
TOPOLOGY DB
823
CONNECTION TERMINAL MEMORY
822
TERMINAL SUBORDINATION DECISION UNIT
821
FLOW SETTING UNIT
827
PATH CALCULATION UNIT
826
PACKET PROCESSOR
825
OFS 20A
PACKET

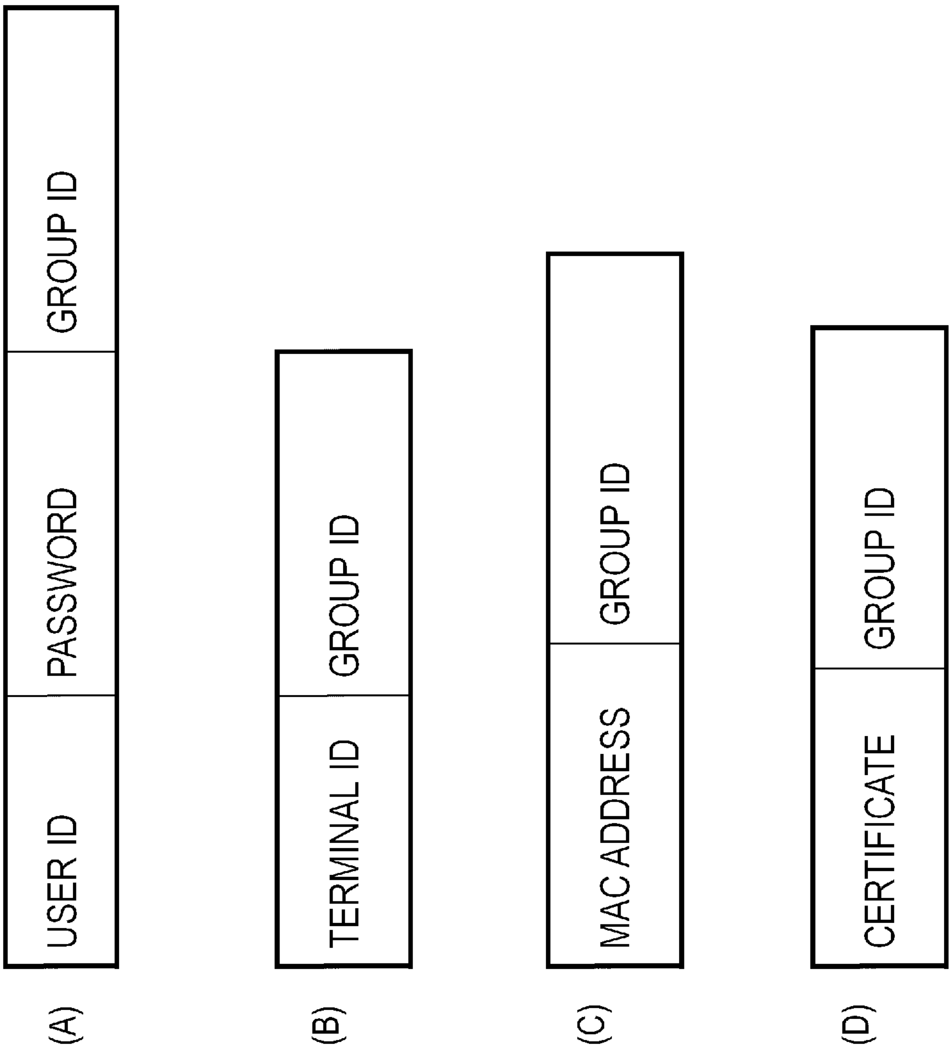
[Fig. 54]



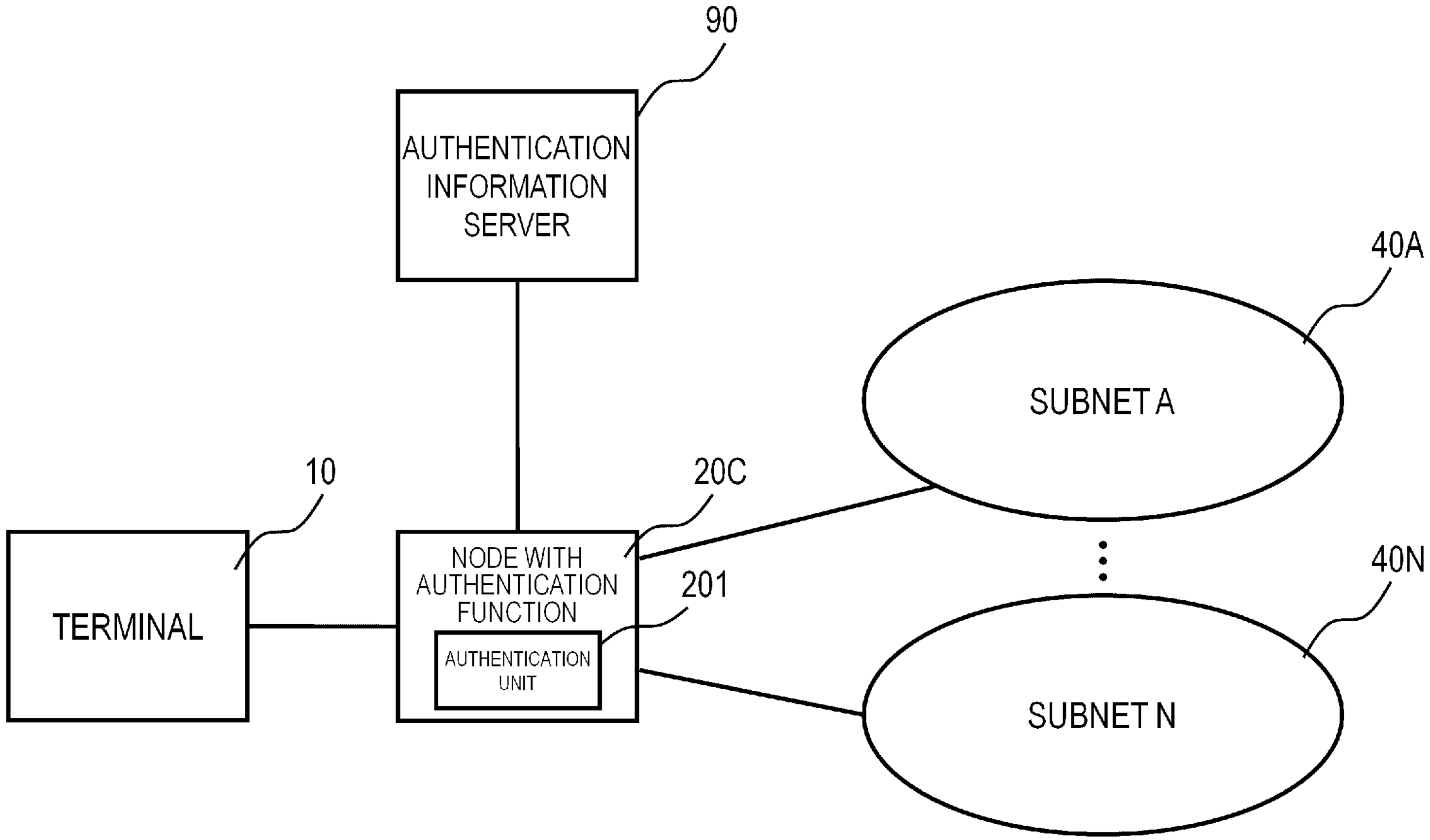
[Fig. 55]

| DPID | PORT NUMBER | TERMINAL INFORMATION | MAIN SUBNET ID | GROUP ID |
|---|---|---|---|---|

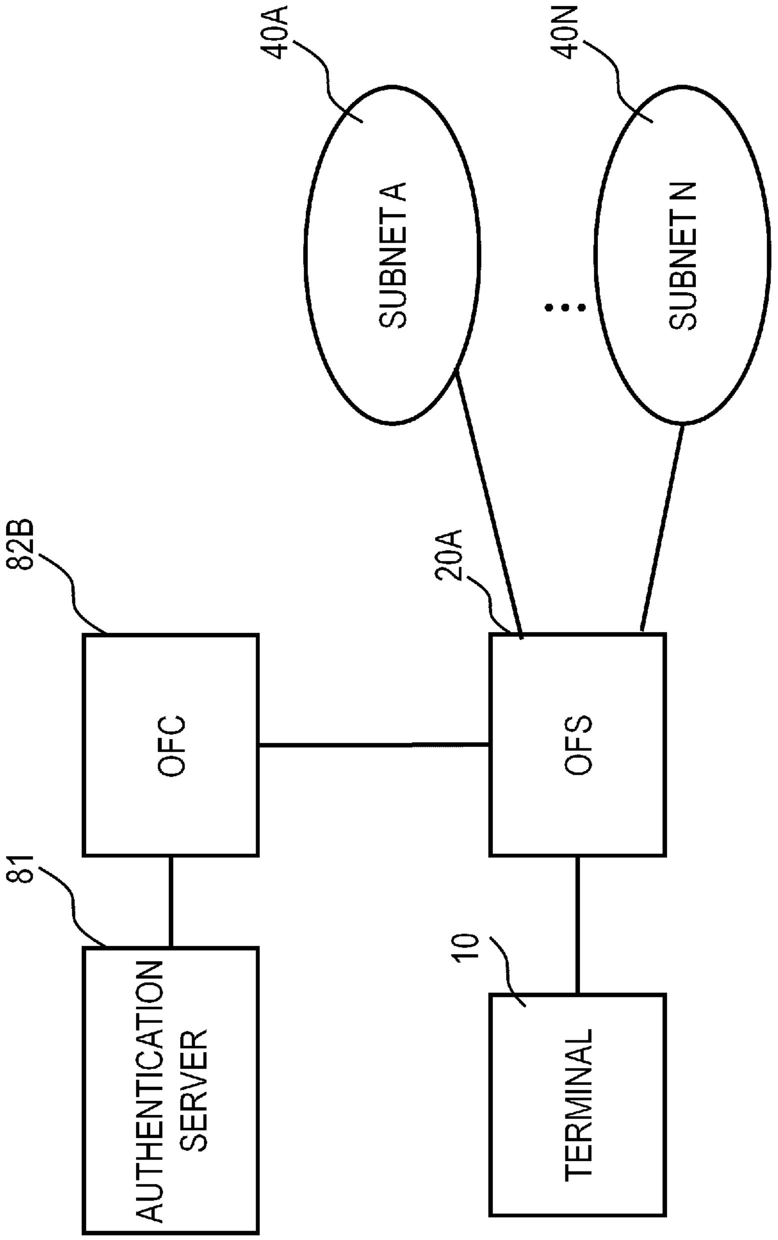
[Fig. 56]


(A)
USER ID
PASSWORD
GROUP ID
(B)
TERMINAL ID
GROUP ID
(C)
MAC ADDRESS
GROUP ID
(D)
CERTIFICATE
GROUP ID

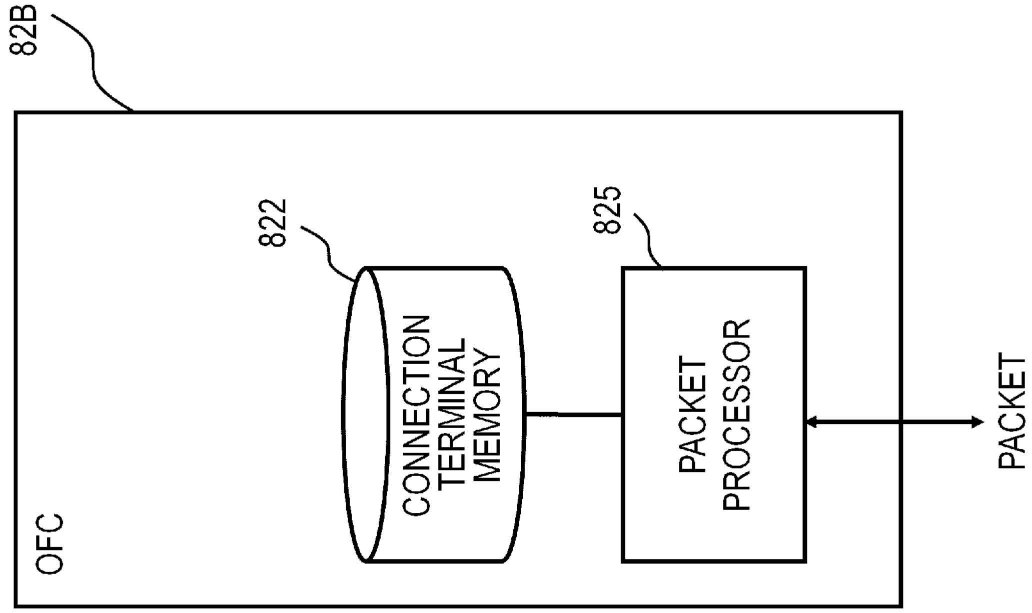
[Fig. 57]


90
AUTHENTICATION INFORMATION SERVER
40A
SUBNET A
10
TERMINAL
20C
NODE WITH AUTHENTICATION FUNCTION
201
AUTHENTICATION UNIT
40N
SUBNET N

[Fig. 58]


40A
SUBNET A
40N
SUBNET N
82B
OFC
20A
OFS
81
AUTHENTICATION SERVER
10
TERMINAL

[Fig. 59]


82B
OFC
822
CONNECTION TERMINAL MEMORY
825
PACKET PROCESSOR
PACKET

# INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2013/004756

A. CLASSIFICATION OF SUBJECT MATTER

Int.Cl. H04L12/46(2006.01)i, G06F21/30(2013.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

Int.Cl. H04L12/46, G06F21/30

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

Published examined utility model applications of Japan 1922-1996
Published unexamined utility model applications of Japan 1971-2013
Registered utility model specifications of Japan 1996-2013
Published registered utility model applications of Japan 1994-2013

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

C. DOCUMENTS CONSIDERED TO BE RELEVANT

| Category* | Citation of document, with indication, where appropriate, of the relevant passages | Relevant to claim No. |
|---|---|---|
| Y | JP 2006-260027 A(Nippon Telegraph and Telephone East Corporation) 2006.09.28<br>Claims:1,2,<br>Paragraphs:[0025]-[0026],[0036]-[0045],[0053]-[0060],<br>Figure:1-7<br>(No Family) | 1-14 |
| Y | JP 2004-312408 A(Hitachi, Ltd.) 2004.11.04<br>Paragraphs:[0009]-[0028], Figures:1-5<br>(No Family) | 1-14 |
| Y | JP 2010-55199 A(Nippon Telegraph and Telephone Corporation) 2010.03.11<br>Claim:1, Paragraphs:[0014]-[0015] (No Family) | 1-14 |

☑ Further documents are listed in the continuation of Box C. □ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

| | |
|---|---|
| Date of the actual completion of the international search<br>02.09.2013 | Date of mailing of the international search report<br>10.09.2013 |
| Name and mailing address of the ISA/JP<br>**Japan Patent Office**<br>3-4-3, Kasumigaseki, Chiyoda-ku, Tokyo 100-8915, Japan | Authorized officer 5X 3047<br>TAMAKI Koji<br>Telephone No. +81-3-3581-1101 Ext. 3596 |

## INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2013/004756

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

| Category* | Citation of document, with indication, where appropriate, of the relevant passages | Relevant to claim No. |
|---|---|---|
| Y | JP 2004-328029 A(NEC Corporation) 2004.11.18 Claim:1 &AU 2004201677 A &CN 1540944 A &EP 1489809 A1 &US 2004/0255166 A1 | 1-14 |
| Y | JP 9-135294 A(FUJITSU) 1997.05.20 Abstract (No Family) | 6 |
| Y | JP 2000-316188 A(KYOCERA Corporation) 2000.11.14 Abstract (No Family) | 6 |
| Y | JP 2002-351761 A(Canon Inc.) 2002.12.06 Abstract (No Family) | 7 |
| Y | JP 2003-87433 A(Nippon Telegraph and Telephone West Corporation) 2003.03.20 Paragraphs:[0019]-[0044] (No Family) | 8 |
| Y | JP 2008-113260 A(Hitachi Communication Technologies, Ltd.) 2008.05.15 Claims:1 &CN 101175034 A &US 2008/0101396 1 &US 2011/0170555 A1 | 8 |