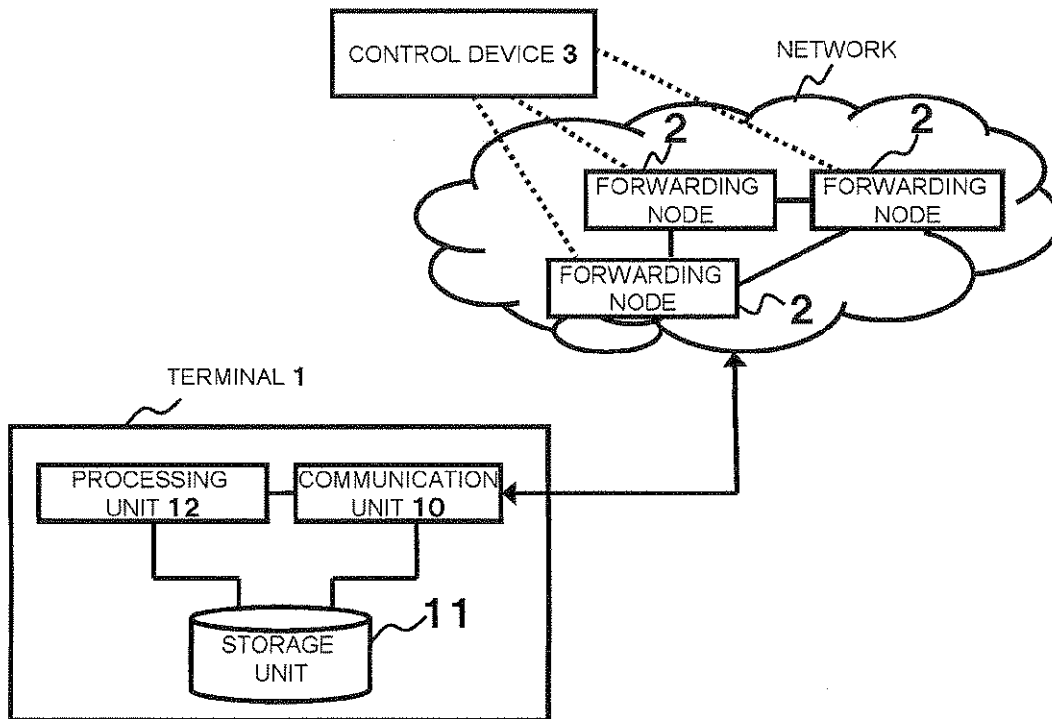
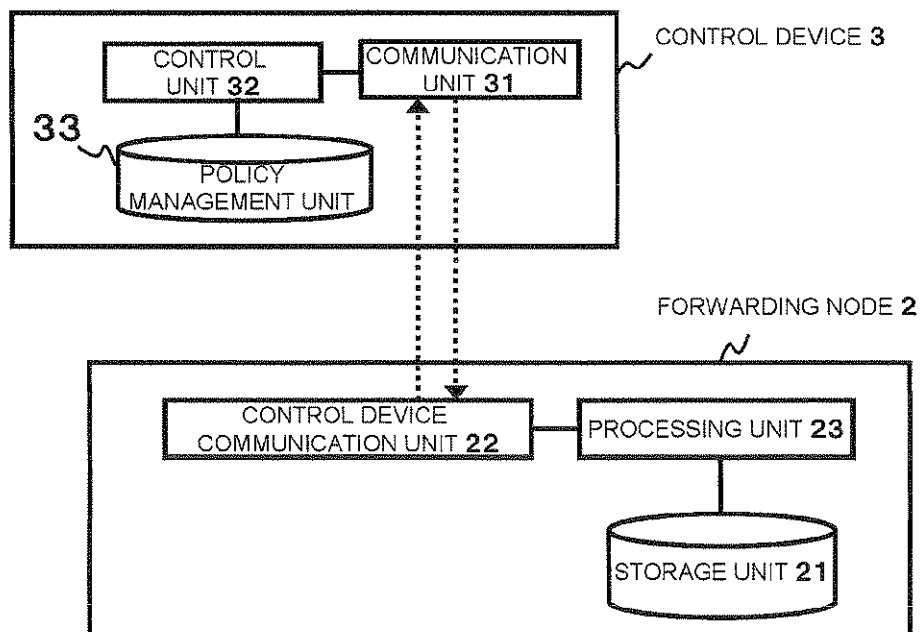


[Fig. 1]



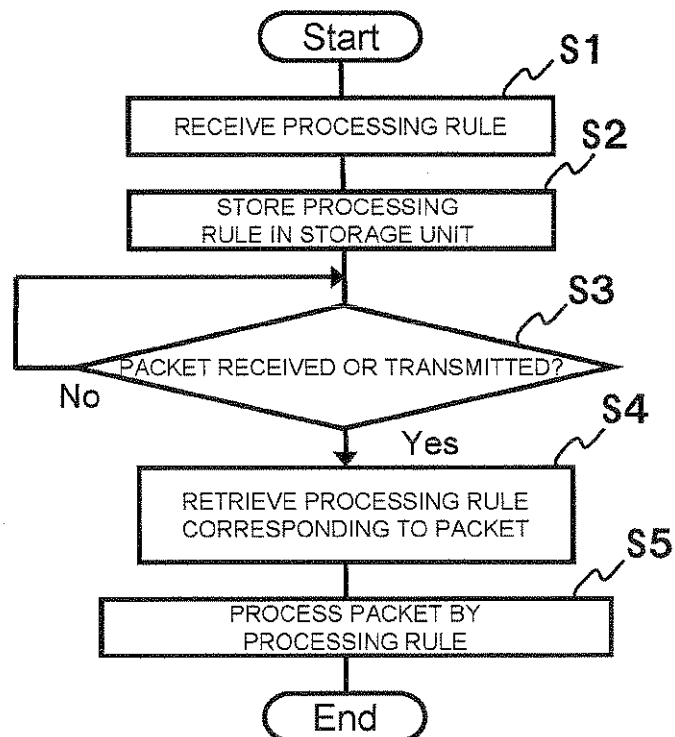
[Fig. 2]



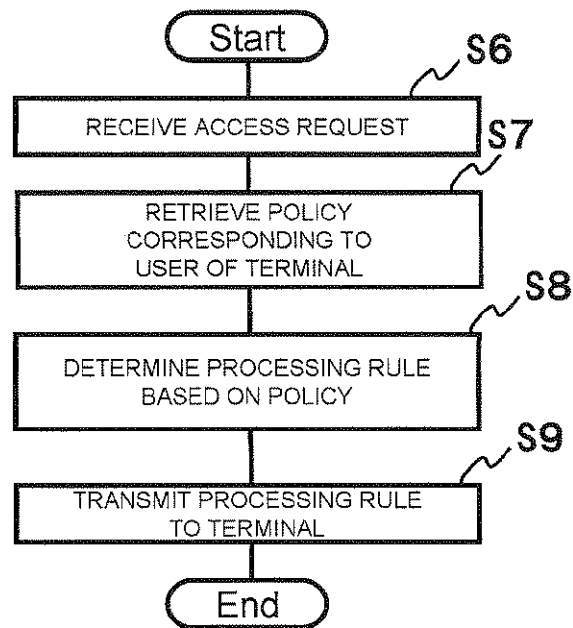
[Fig. 3]

PROCESSING RULE	MATCHING RULE	PROCESSING CONTENT
	FLOW #A	FORWARDING FROM PORT a OF FORWARDING NODE
	FLOW #B	FORWARDING FROM PORT b OF FORWARDING NODE
	• • •	
	ACCESS REQUEST PACKET	FORWARDING TO CONTROL DEVICE
	• • •	

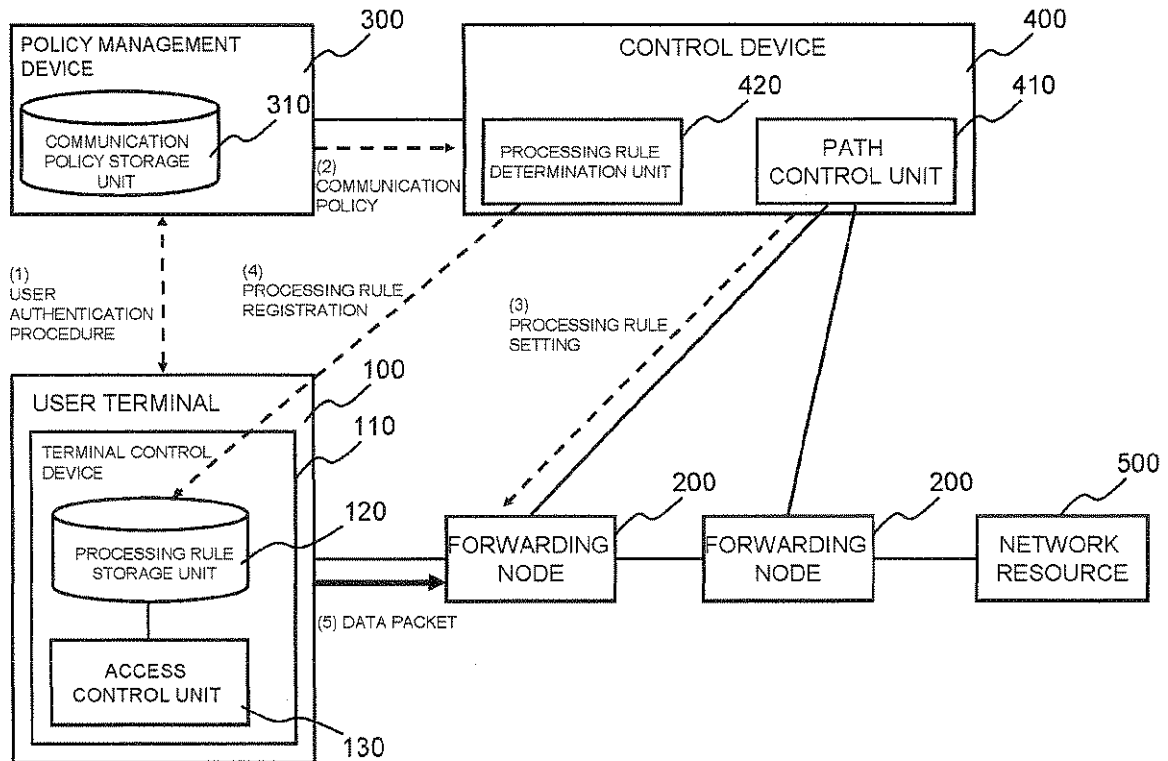
[Fig. 4]



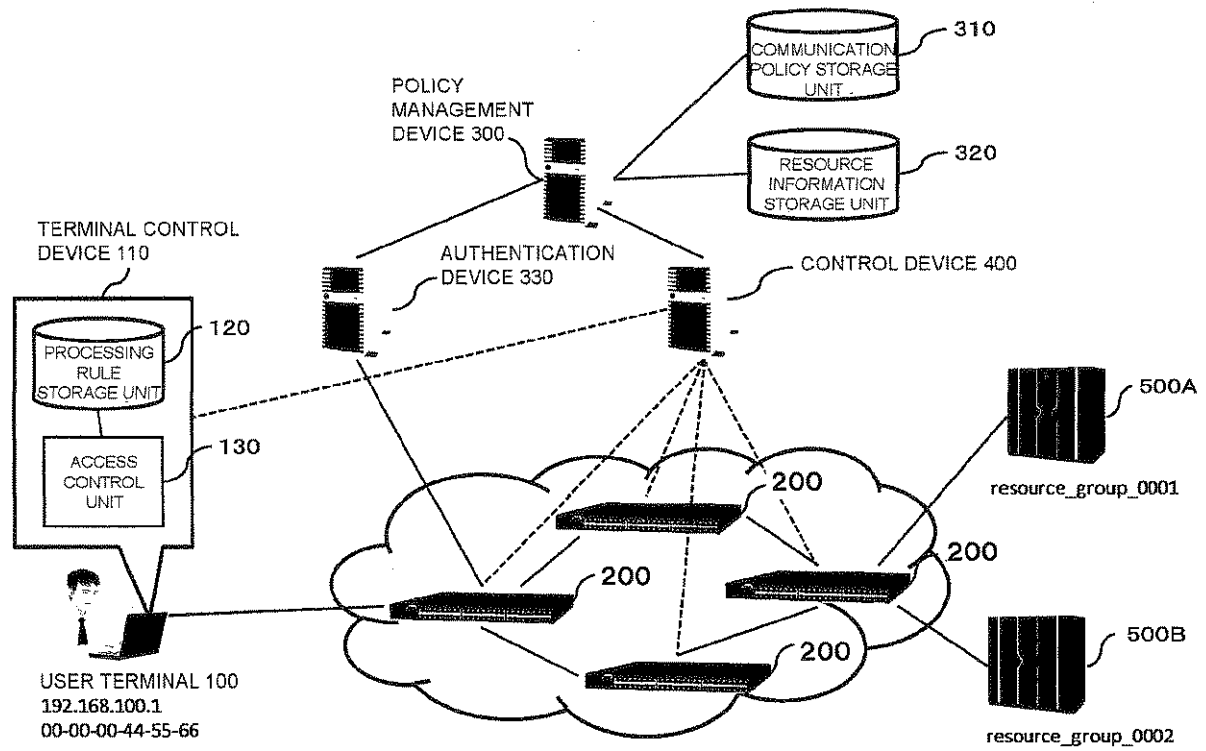
[Fig. 5]



[Fig. 6]



[Fig. 7]



[Fig. 8]

USER ID	ROLE ID	ATTRIBUTE
user1	role_0001	IP:192.168.100.1
	role_0002	MAC:00-00-00-44-55-66
user2	role_0002	IP:192.168.100.2 MAC:00-00-00-77-88-99
:	:	:

[Fig. 9]

ROLE ID	RESOURCE GROUP ID	ACCESS RIGHTS
role_0001	resource_group_0001	allow
role_0001	resource_group_0002	allow
role_0002	resource_group_0001	deny
role_0002	resource_group_0002	allow
:	:	:

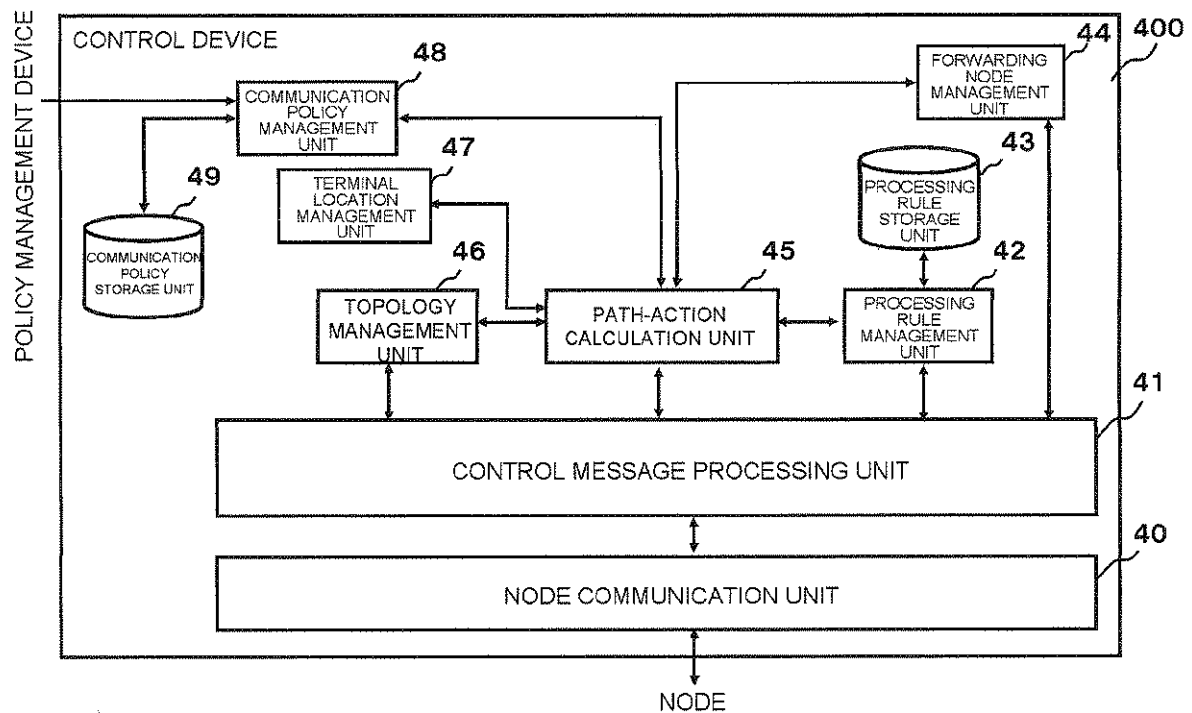
[Fig. 10]

RESOURCE GROUP ID	RESOURCE ID	RESOURCE ATTRIBUTE
resource_group_0001	resource_0001	IP:192.168.0.1 MAC:00-00-00-11-22-33 SERVICE:80/tcp
	resource_0002	IP:192.168.0.2
	resource_0003	IP:10.10.10.0/24
resource_group_0002	resource_000X	IP:YYY.YYY.Y.Y
	:	:
:	:	:

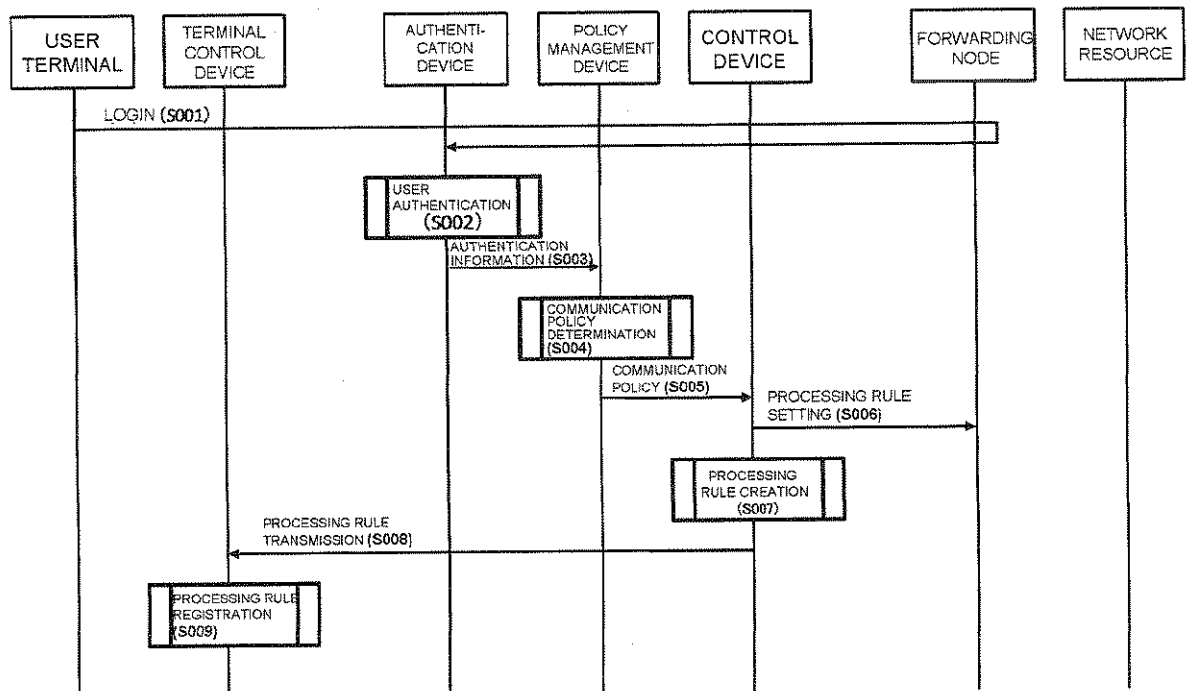
[Fig. 11]

SOURCE	DESTINATION	ACCESS RIGHTS	CONDITION (OPTION)
192.168.100.1	192.168.0.1	allow	80/tcp
00-00-00-44-55-66	192.168.0.2	allow	
192.168.100.1	IP:10.10.10.0/24	allow	
192.168.100.1	192.168.0.3	deny	
:	:	:	:

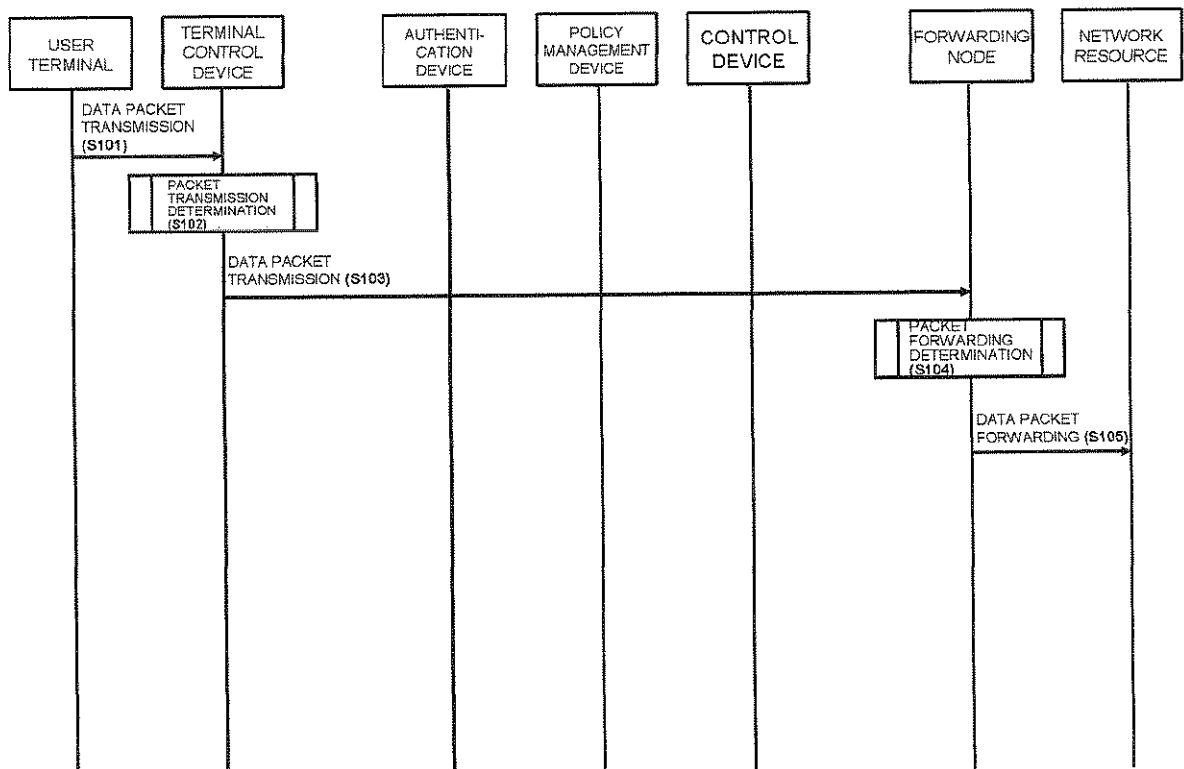
[Fig. 12]



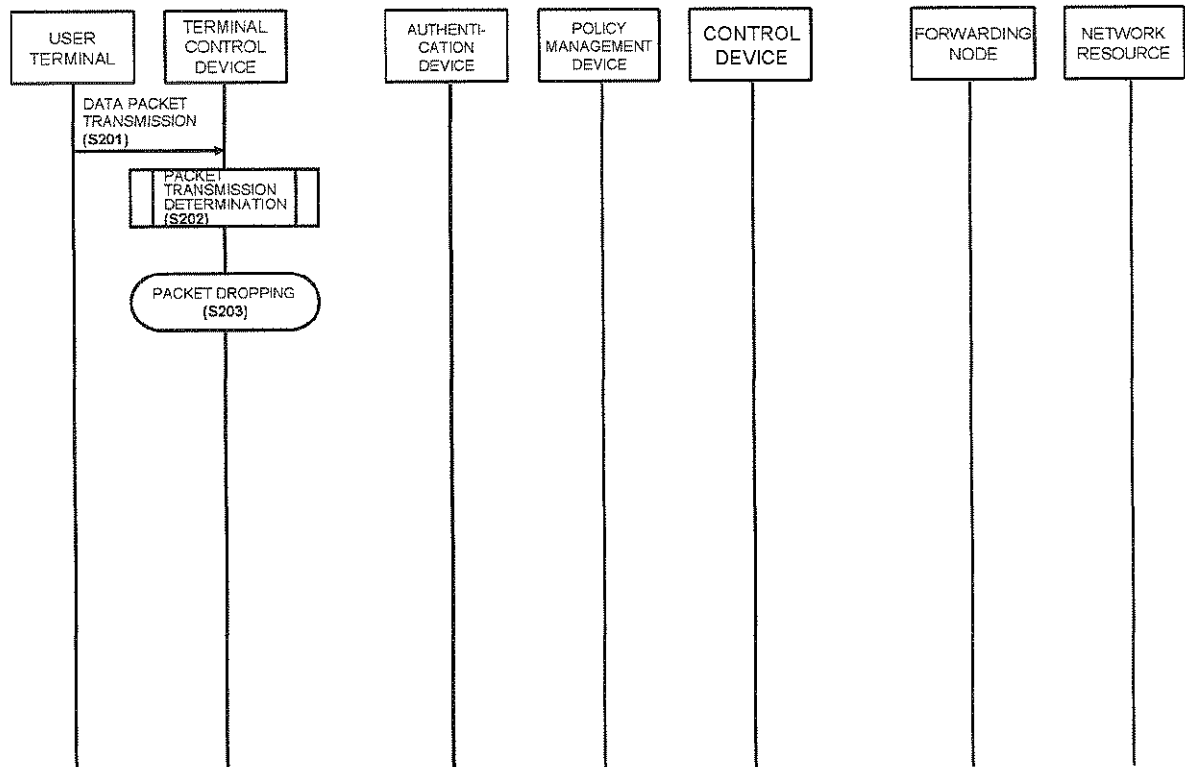
[Fig. 13]



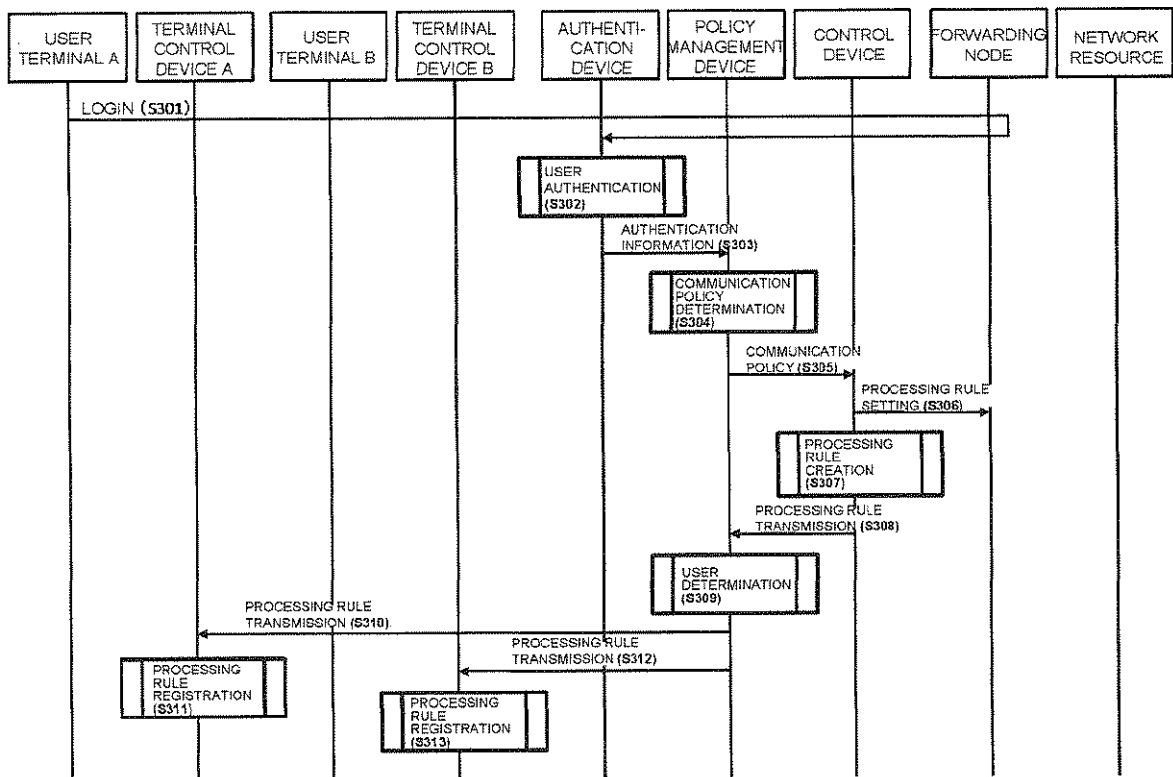
[Fig. 14]



[Fig. 15]



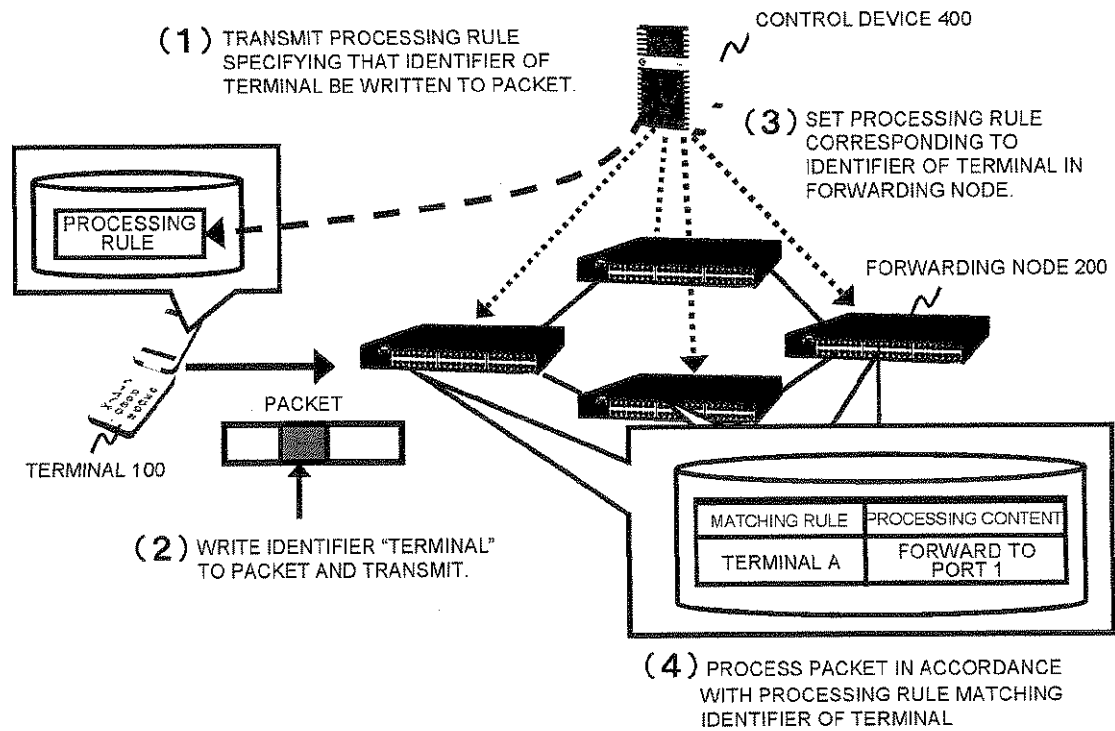
[Fig. 16]



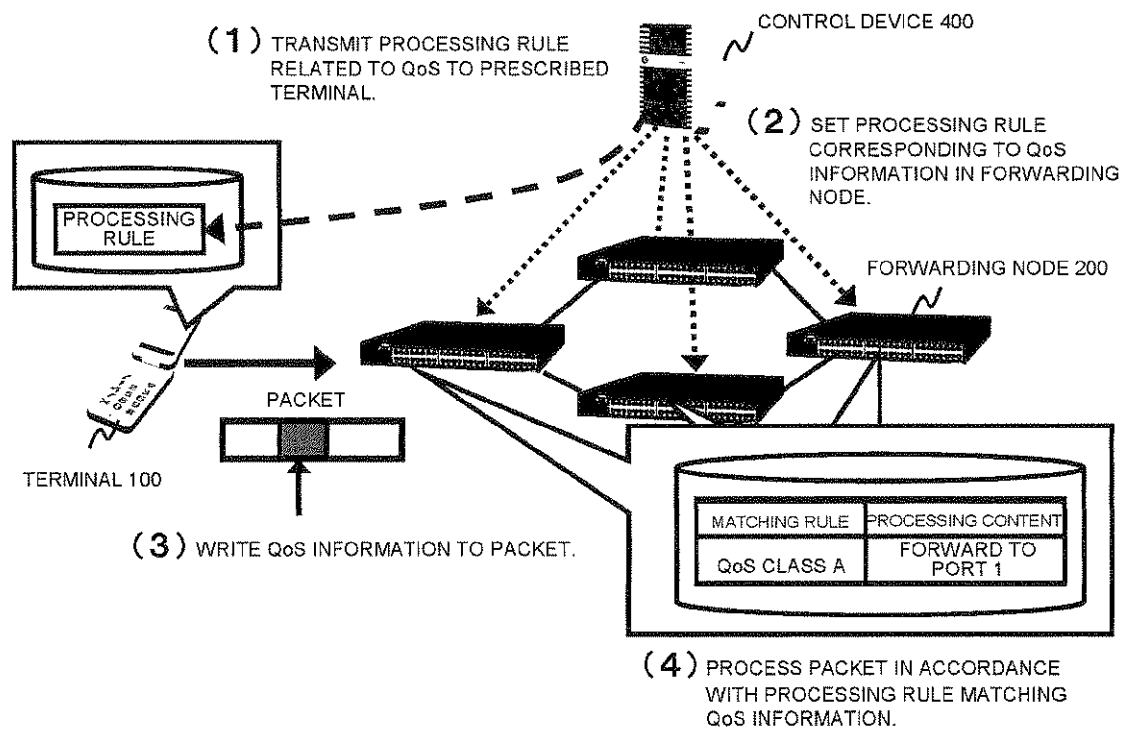
[Fig. 17]

SOURCE	DESTINATION	ACCESS RIGHTS	CONDITION (OPTION)
IP:192.168.100.0/24	192.168.0.3	deny	
:	:	:	:

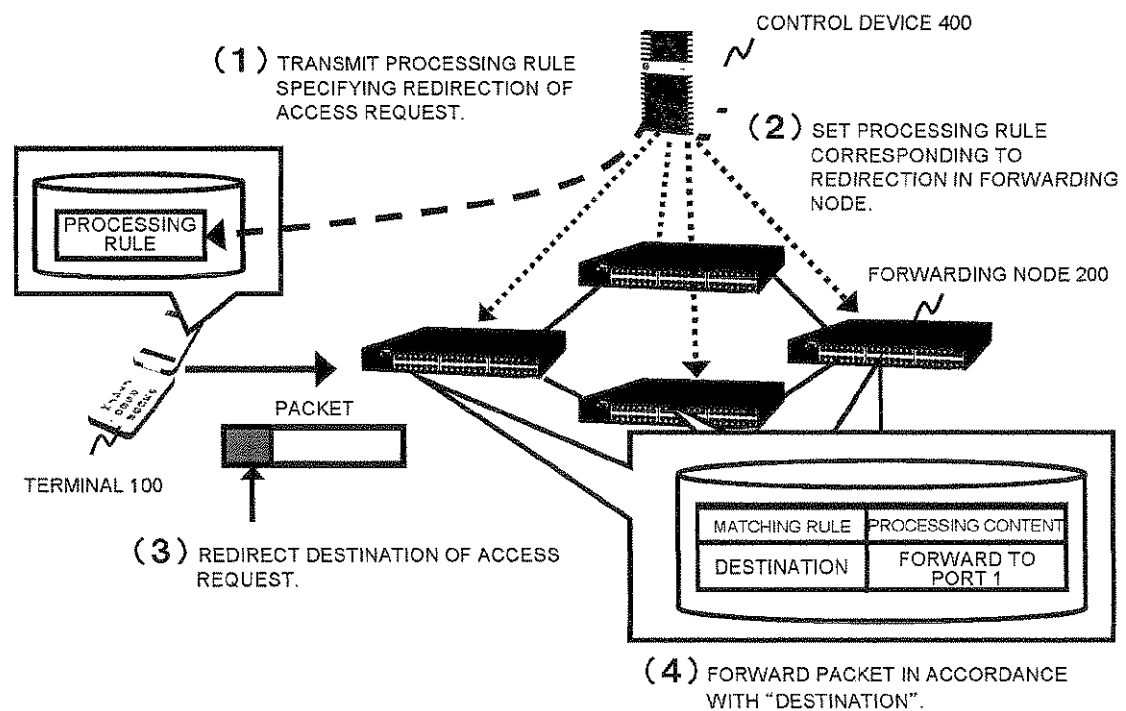
[Fig. 18]



[Fig. 19]



[Fig. 20]




```

sequenceDiagram
    participant UT as USER TERMINAL
    participant TCD as TERMINAL CONTROL DEVICE
    participant AD as AUTHENTICATION DEVICE
    participant PMD as POLICY MANAGEMENT DEVICE
    participant CD as CONTROL DEVICE
    participant FN as FORWARDING NODE
    participant NR as NETWORK RESOURCE

    UT->>TCD: LOGIN (S401)
    TCD->>AD: 
    AD->>PMD: AUTHENTICATION INFORMATION (S403)
    PMD->>CD: COMMUNICATION POLICY (S405)
    CD->>FN: PROCESSING RULE SETTING (S406)
    CD->>TCD: PROCESSING RULE TRANSMISSION (S408)
    TCD->>TCD: PROCESSING RULE REGISTRATION (S409)
    TCD->>TCD: HASH VALUE GENERATION (S411)
    TCD->>CD: HASH VALUE TRANSMISSION (S412)
    CD->>CD: HASH VALUE COLLATION (S413)
    CD->>FN: SETTING OF PROCESSING RULE FOR ACCESS DENIAL (S414)
  
```

The diagram illustrates the following steps in the access control process:

- LOGIN (S401):** Initiated by the User Terminal to the Terminal Control Device.
- AUTHENTICATION INFORMATION (S403):** Sent from the Authentication Device to the Policy Management Device.
- COMMUNICATION POLICY (S405):** Sent from the Policy Management Device to the Control Device.
- PROCESSING RULE SETTING (S406):** Sent from the Control Device to the Forwarding Node.
- PROCESSING RULE TRANSMISSION (S408):** Sent from the Control Device to the Terminal Control Device.
- PROCESSING RULE REGISTRATION (S409):** Local processing within the Terminal Control Device.
- HASH VALUE GENERATION (S411):** Local processing within the Terminal Control Device.
- HASH VALUE TRANSMISSION (S412):** Sent from the Terminal Control Device to the Control Device.
- HASH VALUE COLLATION (S413):** Local processing within the Control Device.
- SETTING OF PROCESSING RULE FOR ACCESS DENIAL (S414):** Sent from the Control Device to the Forwarding Node.

HEADER FIELDS; MATCHING RULE

Wildcards	In Port	Ether SA	Ether DA	Ether type	VLAN ID	VLAN PCP	IP SA	IP DA	IP proto	IP ToS bits	TCP/UDP src port	TCP/UDP dst port	Counters	Actions
-----------	---------	----------	----------	------------	---------	----------	-------	-------	----------	-------------	------------------	------------------	----------	---------