December 30, 2025

Certification

Welocalize Translations

AFFIDAVIT OF ACCURACY:

I, Matthew Murphy, hereby declare under penalty of perjury as follows:

1. I am fluent in both the Japanese and English languages, and I have experience translating technical documents between the two languages.
2. I am the translator of the attached English translation of the attached Japanese Patent Application No. JP2002374294A, including its figures, entitled "Policy Server," filed June 14, 2001 and published December 26, 2002.
3. I declare that all statements made herein of my own knowledge are true, accurate, and complete and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code.

Matthew Murphy, Certified Translator

Location: Fukuoka, Japan

Date: 12/30/2025

Matthew Murphy 

Project Number: DUMO_2512_P0009

136 Madison Avenue, 6th Floor
New York, NY 10016
212.581.8870

(19) Japan Patent Office (JP)

(12) **Japanese Unexamined Patent Publication**(A)

(11) Patent Application Publication No.
JP 2002-374294 A
(P2002-374294A)

(43) Publication Date December 26, 2002 (12/26/2022)

(51) Int.Cl.[7]	Ident. Code	FI	Theme Code (Reference)
H04L 12/56	200	H04L 12/56	200E 5K030

Examination Request: Not yet Total No. of Claims: 5 OL (Total 12 pages)

(21) Application No. JP 2001-179502 (P2001-179502)

(22) Application Date June 14, 2001 (06/14/2001)

(71) Applicant 000005108
Hitachi, Ltd.
4-6, Kanda-Surugadai, Chiyoda-ku, Tokyo-to

(72) Inventor Masanori Taira
C/o Hitachi, Ltd. Network Platform Division,
890 Kashimada, Saiwai-ku, Kawasaki-shi,
Kanagawa-ku

(74) Agent 100075096
Yasuo Sakuta, Patent Attorney

Continued on last page

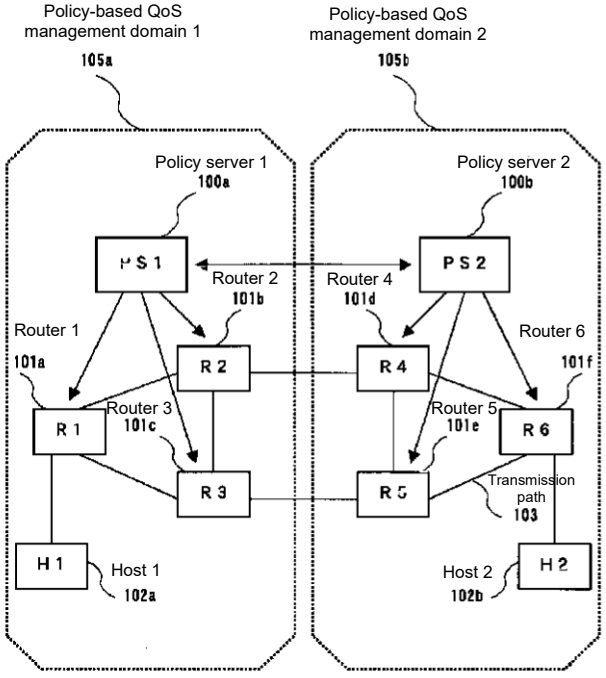
(54) [Title of Invention] POLICY SERVER

(57) [Abstract]

[Problem] Since current policy servers do not have means for exchanging policy control information between themselves, it has been impossible to achieve interoperability of services between ISPs in a policy-based network.

[Resolution Means] A policy server that performs policy control on communication devices configuring a policy-based network determines, based on topology information, whether the identified communication traffic deviates from the identified control traffic, and when such deviates, determines, based on the topology information, whether the communication traffic will pass through the control traffic of another policy server, and when such will pass through, performs control on the other policy server to transfer, via a network interface, policy control information that includes topology information including communication route information for identifying the communication traffic and QoS control information for the communication traffic.

[FIG. 1]



Cisco Systems, Inc. v. OptimNet LLC
Exhibit 1014

[Scope of Patent Claims]

[Claim 1] A policy server, having: a control unit that instructs a communication device configuring a policy-based network to perform policy control; and

a main memory for storing topology information including communication route information for identifying communication traffic and policy control route information for identifying control traffic configured by the communication device instructed to perform the policy control, andQoS control information for each piece of communication traffic, wherein:

the control unit determines, based on the topology information stored in the main memory, whether the identified communication traffic deviates from the identified control traffic,

and when it is determined that such deviates, further determines, based on the topology information stored in the memory, whether the communication traffic will pass through the control traffic of another policy server, and

when it is determined that the communication traffic will pass through, performs control on the other policy server to transfer, via a network interface, policy control information that includes topology information including communication route information for identifying the communication traffic stored in the main memory and the QoS control information for the communication traffic.

[Claim 2] The policy server according to claim1, wherein:

the policy control information stored in the main memory further includes policy control information for each piece of communication traffic received from the other policy server.

[Claim 3] The policy server according to claim 1 or 2, wherein:

the policy control information further includes a transfer history of the policy control information.

[Claim 4] The policy server according to claim 1 or 2, wherein:

the policy control information *further* includes time information indicating a start time of policy control or a release time of policy control for the communication device.

[Claim 5] The policy server according to claim 1 or 2, further having:

a user interface for inputting the communication route information and the QoS control information.

[Detailed Description of Invention]

[0001]

[Technical Field of Invention] The present invention relates to a communication device communication device policy server that instructs communication devices (layer 2 switches, layer 3 switches, routers, bandwidth control devices, and the like) configuring a specific policy network from among a plurality of policy-based networks configured by a communication device that is instructed by policy servers to perform policy control, to perform policy control.

[0002]

[Conventional Art] When controlling quality of service (Quality of Service, hereinafter; QoS) in a network configured by various communication devices (layer 2 switches, layer 3 switches, routers, bandwidth control devices, and the like), QoS control settings must be configured for each communication device. For relatively small networks, QoS control within the network can be guaranteed by the network administrator configuring settings for communication devices individually.

[0003] However, when the network scale becomes as large as an in-house LAN (Local Area Network) and the number of communication device increases, it becomes time-consuming for the network administrator to configure QoS control settings for each piece of equipment, and there is also a possibility that QoS control within the network will not be able to be guaranteed due to input errors, and the like.

[0004] As means for solving this problem, a policy-based QoS network system was devised. The system manages the contents of QoS control settings within the network as policies, and a policy server managing such configures QoS control settings for all communication devices within the network to use a policy distribution protocol (Common Open Policy Service; hereinafter COPS), a command line interface (Command Line Interface; hereinafter CLI), or the like, thereby guaranteeing consistent QoS control within the network. In this system, a single policy server is deployed in a single management network, and the network administrator is able to operate the policy server to guarantee QoS control within the network. For example, Hitachi's JP1 series is a policy-based network management product.

[0005]

[Problem to be Solved by Invention] In recent years, Internet infrastructure has become widespread, and data communication costs using IP (Internet Protocol) networks have begun to decrease, leading to a trend of many users and various types of traffic converging into IP networks. For example, new technology is emerging that allows voice communication over the telephone to be carried out using IP networks, and it is conceivable to assemble internal telephone lines within a company using an internal LAN. Consequently, the number of different types of communication devices assembling the LAN will increase even further, and when QoS is guaranteed using a policy-based QoS network, the load on the policy server to configure the settings for various pieces of network equipment will increase, which could result in setting delays. In such a case, despite being configured to prioritize internal telephone traffic over other data traffic at a certain time, a policy server setting delay may prevent priority control from being carried out at the time desired by the network administrator.

[0006] Furthermore, when assembling an internal

telephone network or the like that guarantees QoS for voice calls on an internal LAN, it is necessary to guarantee QoS control between sites for eachL AN. For example, in a company having a plurality of branch offices, it is necessary to guarantee QoS control between the LANs of each branch office. However, the LANs are usually managed the respective sites, and when guaranteeing QoS in a policy-based QoS network, it is common to place a policy server on each LAN for management. This makes it necessary to interwork policy control information between policy servers, which was not necessary in the past.

[0007] Currently, ISPs (Internet Service Providers) generally use best-effort network systems, that is, they do not perform QoS control. However, with the recent increase in the number of Internet users, congestion tends to occur due to a lack of network line capacity. *Therefore, it is conceivable that* ISPs will adopt policy-based QoS networks in the future, and QoS services will emerge that differentiate traffic priorities for each user. It is conceivable that this will also enable interoperability and the like of QoS services between ISPs. For example, when a user of a certain ISP accesses a server of another ISP, the QoS of the traffic is guaranteed in the same way within each ISP's network. However, since current policy servers do not have means for exchanging policy control information between themselves, it has been impossible to achieve interoperability of QoS services between ISPs in a policy-based QoS network.

[0008] The present invention has been conceived in view of such problems, and an object thereof is to provide a policy server enabling distribution of an increased load on the policy server caused by an increase in communication devices deployed within a network by deploying a plurality of policy servers and managing the network using the plurality of policy servers, and furthermore, in regard to the setting of policy control information between a plurality of domain networks of other ISPs (Internet Service Providers) and the like, which was previously impossible, a policy server wherein a plurality of policy servers between domain networks exchange policy control information, thus enabling the setting of policy control information for network equipment via a plurality of domain networks.

[0009]

[Means for Solving the Problem] In order to achieve the foregoing object, the present invention provides the following resolution means.

[0010] Provided is a policy server, having: a control unit that instructs a communication device configuring a policy-based network to perform policy control; and a main memory for storing topology information including communication route information for identifying communication traffic and policy control route information for identifying control traffic configured by the communication device instructed to perform the policy control, and policy control information for each piece of communication traffic, wherein: the control unit determines, based on the topology information stored in the main memory, whether the identified communication traffic deviates from the identified control traffic, and when such deviates, determines, based on the topology information stored in the main memory, whether the communication traffic will pass through the control traffic of another policy server, and when the communication traffic will pass through, performs control on the other policy server to transfer, via a network interface, policy control information that includes topology information including communication route information for identifying the communication traffic and QoS control information for the communication traffic.

[0011] Moreover, provided is a policy server that further includes a transfer history of the policy control information. Communication device Communication device Communication device Communication device Communication device Communication device

[0012]

[Embodiments of Invention] Hereinafter, the present invention will be described using one example of an embodiment.

[0013] FIG. 1 shows one example of a configuration of a policy-based QoS network.

[0014] The network is composed of two policy servers (100a to 100b), a plurality of communication devices (routers) (101a to 101f), communication devices (102a to 102b) such as hosts and servers connected to the communication devices, and a transmission path (103). Communication between the two policy servers (100a to 100b) is carried out via the communication devices (101a to 101f).

[0015] FIG. 2 shows a configuration of a policy server.

[0016] That is, the policy server is composed of: a control unit (202) connected by a bus (201); a main memory (203) that accumulates and holds the policy control information shown in FIG. 3 and the topology information shown in FIG. 6; a user interface unit (204) through which a network administrator inputs the policy control information using a GUI (Graphical User Interface); a network interface unit (205) that the control unit (202) uses when communicating with other policy servers or communication devices or the like; and a clock unit (206) that serves as a time reference when the control unit (202) performs QoS control setting release for each communication device according to the setting time information in the policy control information.

[0017] The processes executed by the control unit (202) consist of a time calibration process for calibration between policy servers, the clock used when setting and releasing QoS information for the communication device, a topology information collection process for collecting topology information used when calculating the route of traffic to be subjected to QoS control from each communication device, and a policy control process for setting QoS control information in the communication device and transferring policy control information to other policy servers, and each process is processed in parallel.

[0018] FIG. 9 shows a typical configuration in which the

hosts (102a, 102b) are user terminals that receive QoS services.

[0019] That is, the policy server is composed of a control unit (902) connected by a bus (901), a main memory (903) that stores data used by applications (WEB, image, audio data, and the like) operated by the control unit (902), a display viewing unit (904) for the user to view images, a key input operation unit (905) for the user to operate the host terminal, and a network interface unit (906) that the control unit (902) uses to communicate with other hosts and servers.

[0020] FIG. 10 shows a typical configuration in which routers (101a to 101f) are devices for relaying communications between hosts (102a, 102b).

[0021] That is, the policy server is composed of a control unit (1002) connected by a bus (1001), a main memory (1003) that stores routing information and the like used by the routing protocol (RIP, OSPF, BGP, or the like) operated by the control unit (1002), a routing processing unit (1004) that performs routing processing and relays communication data between network interfaces, and network interface units (1005 to 1007) that connect to a plurality of various network devices such as other routers and hosts.

[0022] Here, as an example, the processing operation of each policy server when providing a bandwidth guarantee to HTTP traffic sent from a host 1 (102a) to a host 2 (102b) in the policy-based QoS network of FIG. 1 will be described. Moreover, in FIG. 1, a policy server 1 (100a) manages a policy-based QoS management domain 1 (105a) composed of routers R1 (101a), R2 (101b), and R3 (101c), and a policy server 2 (100b) manages a policy-based QoS management domain 2 (105b) consisting of routers R4 (101d), R5 (101e), and R6 (101f).

[0023] FIG. 4 shows a flow diagram of the policy control process executed by the control unit (202) of the policy server.

[0024] The policy control process executed by the control unit (202) of the policy server 1 (100a) is started by the network administrator of the policy-based QoS management domain 1 (105a) inputting policy control information (300) for HTTP traffic to be sent from the host 1 (102a) to the host 2 (102b) via the user interface (204) of the policy server 1 (100a) (F401). This process may also be started by receiving policy control information (300) from a policy server managing another network via the network interface (205) (F402), or by receiving a policy control information setting request from the host 1 (102a) (F408).

[0025] FIG. 3 shows an example of a configuration of policy control information (300) that is set by the network administrator of the policy-based QoS management domain 1 (105a) via the user interface (204) of the policy server 1 (100a).

[0026] That is, the policy control information (300) is composed of host information (301) indicating the IP addresses of the source host and destination host of the traffic to be subjected to QoS control, flow type information (302) indicating the flow characteristics of the traffic to be subjected to QoS control, QoS control information (303) indicating the QoS control content to be set for the communication device, setting time information (304) indicating the time to set and release QoS control for the communication device, and transfer information (305) indicating the transfer history of the policy control information (300). *Here,*the policy control information includes host information (301) indicating the IP addresses of the source host and destination host of the communication traffic, and is stored in the main memory (203) of the policy server for each piece of communication traffic. The host information (301) includes the IP address (301a) of the host sending the traffic and the IP address (301b) of the host receiving the traffic. The flow type information (302) includes a protocol number (302a) indicating a protocol such as TCP, UDP, or ICMP as the flow type of traffic to be subjected to QoS control, a source port number (302b) and a destination port number (302c) used in TCP or UDP, and a DSCP detected value (302d) in Diffserv (differentiated services, one of the QoS control technologies). The data format of the IP addresses (301a, 301b), protocol number (302a), and port numbers (302b, 302c) follows the notation specified in the Internet Standard Specifications (RFC). The DSCP detected value (302d) is expressed as a value between 0 and 63, and is used to associate with transmission priority in Diffserv. The QoS control information (303) includes transmission priority information (303a), guaranteed bandwidth information (303b), limited bandwidth information (303c), and a DSCP rewrite value (303d) in Diffserv, which are QoS control details. The transmission priority information (303a) is indicated by numbers 1 to 8, with 1 meaning the highest transmission priority and 8 meaning the lowest transmission priority. The guaranteed bandwidth information (303b) indicates, in Kbit/s, the value that guarantees the bandwidth of the line to be used. A value of 0 means no bandwidth is guaranteed. The limited bandwidth information (303c) indicates, in Kbit/s, the upper limit value for the bandwidth of the line to be used. A value of 0 means no bandwidth limitations are imposed. The DSCP rewrite value (303d) is expressed as a value between 0 and 63, and is used to associate with transmission priority in Diffserv. Of the policy control information (300), the host information (301), flow type information (302), and QoS control information (303) correspond to setting values for the communication device. Once this information is set, the communication device performs QoS control according to the QoS control information (303) on traffic that matches the conditions of the host information (301) and the flow type information (302). The setting time information (304) includes QoS setting start time information (304a), which is the time when the host information (301), the flow type information (302), and the QoS control information (303) are set in the communication device, and QoS setting release time information (304b), which is the time when the set host information (301), the flow type information (302), and the

QoS control information (303) are released. The QoS setting start release time information (304a, 304b) is expressed in years, months, days, hours, minutes, and seconds. The transfer information (305) includes transfer history information (305a) when the policy control information (300) is transferred to another policy server. The transfer history information (305a) indicates the IP address of the policy server that forwarded the policy control information (300). Of the policy control information (300), the host information (301), the flow type information (302), the QoS control information (303), and the setting time information (304) are set by the network administrator via the user interface of the policy server. Of the policy control information (300), the transfer information (305) is set by the control unit (202) of the policy server when transferring the policy control information.

[0027] The policy server 1 (100a) receives policy control information (300) set by the network administrator of the policy-based QoS management domain 1 (105a) via the user interface (204) and stores such in the main memory (203). Next, the policy server 1 (100a) reads the source host IP address (301a) and receiving host IP address (301b) of the host information (301) from the policy control information (300), and confirms that the traffic to be subjected to QoS control is traffic sent from the host 1 (102a) to the host 2 (102b). Based on this information and the topology information of the policy-based QoS management domain 1 (105a) stored in the main memory (203) of the policy server 1 (100a), the route through which the traffic will pass is identified. As an example, it is assumed here that the traffic will pass through the route of host 1 (102a) - router 1 (101a) - router 2 (101b) and arrive at the network (105b) managed by policy server 2 (100b).

[0028] FIG.6 shows an example of a configuration of topology information stored in the main memory (203) of the policy server 1 (100a).

[0029] In other words, the topology information (600) is composed of information elements for all communication devices present in the network, each information element corresponding to one communication device and including both the IP address (601a) of the communication device in the management network and the routing information held by the communication device, that is, the information for a plurality of sets of information (601b-1 to 601b-M1), each set including the destination network IP address and the IP address of the next-hop communication device for that destination. This topology information (600) is used to calculate which communication device the traffic to be subjected to QoS control should pass through.

[0030] FIG. 8 shows a flow diagram of the topology information collection process.

[0031] This process is started once an hour to obtain the topology configuration of the communication device. Note that this startup interval may be changed via the settings. FIG. 12 shows a list of communication devices from which topology information is collected in this process. This list (1200) is configured by the network administrator of policy-based QoS management domain 1 (105a) via the user interface (204) of policy server 1 (100a) when constructing the network, and is stored in the main memory (203) of policy server 1 (100a). More specifically, the constituent elements of the managed communication device list (1200) stored in the main memory (203) of the policy server 1 (100a) that manages the communication devices within the policy-based QoS management domain 1 (105a) are the IP addresses of the router 1 (101a), the router 2 (101b), and a router 3 (101c). The control unit (202) of the policy server 1 (100a) collects the routing route information MIB stored in the main memory (1003) of the communication devices being managed, that is, the communication devices present in the managed communication device list (1200), in accordance with the SNMP (Simple Network Management Protocol), which is an Internet standard management data MIB (Management Information Base) collection protocol (F801). The contents of the MIB are learned by standard routing protocols such as OSPF (Open Shortest Path First), RIP (Routing Information Protocol), and BGP (Border Gateway Protocol) that operate in the control unit (1002) of the communication device, and are composed of the destination network IP address of the routing route information stored in the main memory (1003) of the communication device, and the IP address information (601b-1 to 601b-M1) of the next-hop communication device for that destination. The control unit (202) of the policy server 1 (100a) accumulates the IP address (601a) of the communication device and the routing route information collected by the MIB, namely the destination network IP address and the next-hop communication device IP address information (601b-1 to 601b-M1) for that destination, in the main memory (203) of the policy server 1 (100a) (F802). These operations (F801 toF802) are performed for all communication devices present in the managed communication device list (1200) (F803). The above is the topology information collection process. This process makes it possible to obtain the topology configuration of the communication device, which in turn makes it possible to calculate the route of traffic to be subjected to QoS control.

[0032] Next, the control unit (202) of the policy server 1 (100a) calculates the route of the traffic to be subject to the QoS settings based on the source host IP address (301a) and receiving host IP address (301b) of the host information (301) stored in the main memory (203) and the topology information (600) (F403). The calculation method will be described next. The control unit (202) of the policy server 1 (100a) reads the policy control information (300) stored in the main memory (203) and confirms, based on the source host IP address (301a) in the host information (301), that the source of the traffic subject to the QoS control settings is the host 1 (102a). In order to identify the route that the traffic from this host 1 (102a) will take, the control unit (202) of policy server 1 (100a) then reads the routing information (601b-1 to 601b-M1) of the router 1 (101a), which is the communication device to which the host 1 (102a) is connected, from the topology information (600) stored in the main memory (203). Furthermore, from

the further loaded routing information (601b-1 to 601b-M1), it checks the next-hop communication device IP address when the destination network IP address matches the receiving host IP address (301b) in the host information (301). More specifically, when the receiving host IP address (301b) is the host 2 (102b), the next-hop communication device IP address of the router1(101a) indicates router 2 (101b). Similarly, for the router 2 (101b), the control unit (202) of the policy server 1 (100a) reads the routing information (602b-1 to 602b-M2) of the router 2 (101b) from the topology information (600) that was read earlier, and confirms that the next-hop communication device is a router 4 (101d). Next, in order to identify the next-hop communication device of the router 4 (101d), the control unit (202) of the policy server 1 (100a) searches for information on the router 4 (101d) from the topology information (600) stored in the main memory (203). However, since the router 4 (101d) does not exist in the policy-based QoS management domain 1 (105a), the control unit (202) confirms that there is no information on the router 4 (101d) in the topology information (600) stored in the main memory (203) of policy server 1 (100a). That is, the control unit (202) determines that the route of traffic sent from the host 1 (102a) to the host 2 (102b) deviates from the policy-based QoS management domain 1 (105a) managed by the policy server 1 (100a) (F405). In this manner, when there is a route that deviates from the network, the control unit (202) of the policy server 1 (100a) next determines whether the network adjacent to the network and that is the next route is a policy-based network using the policy-based QoS management domain list (1300) stored in the main memory (203) (F406). That is, the control unit (202) compares the management network IP addresses and address masks (1301b-n, 1302b-n, ...) of the policy-based QoS management domain list (1300) stored in the main memory (203) to the IP address of the router 4 (101d) to find a matching list. When there is a matching list, this indicates that the router is within a policy-based network and that the domain the router is in is managed by the policy server at the top of the list. As for the router 4 (101d), it is confirmed that such is present in the network managed by policy server 2 (100b) based on the policy-based QoS management domain list (1300) stored in the main memory (203) of policy server 1 (100a). The policy-based QoS management domain list (1300) stored in the main memory (203) of the policy server 1 (100a) is preconfigured by the network administrator of the policy-based QoS management domain 1 (105a) via the user interface (204) of the policy server 1 (100a) when constructing the network. Since this determination (F406) confirmed that the network including the router 4 (101d), which is the next route after router 2 (101b) for traffic sent from the host 1 (102a) to the host 2 (102b), is a policy-based network, the control unit (202) of the policy server 1 (100a) transfers the policy control information (300) stored in the main memory (203) of the policy server 1 (100a) to the policy server 2 (100b), which manages the adjacent policy-based QoS network (105b) via the network interface unit (205) (F407). Additionally, when transferring the policy control information (300), the IP address of the originating policy server is added to the transfer history information (305a) of the policy control information (300). This leaves a history of the policy-based QoS management domain network through which the policy control information (300) has been relayed.

[0033] The control unit (202) of the policy server 2 (100b) that has received the information stores the policy control information (300) in the main memory (203), and also initiates the policy control process upon receiving the policy control information (300) from the policy server 1 (100a) (F402). The processing after the process is initiated is the same as that of the policy server 1 (100a). Specifically, based on the policy control information (300) received from the control unit (202) of policy server 1 (100a) and the network topology information (600) of the policy-based QoS management domain 2 (105b) stored in the main memory (203) of the policy server 2 (100b), the control unit (202) of the policy server 2 (100b) identifies a route within the policy-based QoS management domain 2 (105b) for traffic sent from the host 1 (102a) to the host 2 (102b) (F403), and determines whether the route deviates from its own network by checking the management network relay list (1200) stored in the main memory (203) of policy server 2 (100b) (F405). In this case, because the traffic passes through the router 4 (101d) to router 6 (101f) and reaches the host 2 (102b), the route does not deviate from the local network.

[0034] Next, the control unit (202) of the policy server 1 (100a) and the policy server 2 (100b) reads out the QoS setting start time (304a) from among the policy control information (300) saved in the main memory (203), and waits until the clock unit (206) reaches the start time (304a).

[0035] The time of each policy server is calibrated by the time calibration process shown in FIG. 7. This process initiates once a day to calibrate the time between the policy servers. Note that this startup interval may be changed via the settings. The control unit (202) operates in accordance with the Internet standard time calibration protocol NTP (Network Time Protocol). That is, the control unit (202) confirms the time from the NTP server via the network interface unit (205) (F701). It is assumed that there is one NTP server in the network. Next, the control unit (202) sets the time confirmed in F701 in the clock unit (206) (F702). The above is the time calibration process. This process allows the clocks of all of the policy servers to be synchronized with the clock of a single NTP server, making it possible to simultaneously execute QoS control and release for communication devices managed by a plurality of policy servers according to the same policy control information.

[0036] When the time comes, the control units (202) of the policy server 1 (100a) and the policy server 2 (100b) read

out the host information (301), the flow type information (302), and the QoS control information (303) from the policy control information (300) saved in the main memory (203), and configure the settings via the network interface (205) for the route of the network, that is, for the router 1 (101a) and the router 2 (101b) managed by the policy server 1 (100a), and for the router 4 (101d) and the router 6 (101f) managed by the policy server 2 (100b). The control unit (1002) of the communication devices (101a, 101b, 101d, 101f) that received the settings stores the host information (301), the flow type information (302), and the QoS control information (303) in the main memory (1003). The control unit (1002) also sets the same information in the routing processing unit (1004). The routing processing unit (1004) of the communication devices (101a, 101b, 101d, 101f) configured with this information initiates QoS control according to the QoS control information (303) for traffic matching the conditions of the host information (301) and the flow type information (302). Next, the control units (202) of the policy server 1 (100a) and the policy server 2 (100b) each read out the QoS setting release time (304b) from the policy control information (300) saved in the main memory (203), and wait until the clock unit (206) reaches the release time (304b). When the time arrives, the control unit (202) then releases the QoS settings for the communication devices (101a, 101b, 101d, 101f) present on the route of the network via the network interface (205) (F404).

[0037] As a result of the above-described processing of the policy server, it becomes possible to divide the policy-based QoS network and perform policy-based QoS control using a plurality of policy servers.

[0038] Next, as a second embodiment of the invention, an operation of boundary communication devices when a non-policy-based QoS network intervenes between a plurality of policy-based QoS networks will be described with reference to FIG. 5.

[0039] As an example, a processing operation for applying QoS control to traffic sent from a host 1 (502a) to a host 2 (502b) is described.

[0040] In response to a policy control information setting request from the host 1 (502a), a control unit (202) of a policy server 1 (500a) receives policy control information (300) for the traffic sent from the host 1 (502a) to the host 2 (502b). The policy server 1 (500a) reads host information (301) from the received policy control information (300) and confirms that traffic subject to QoS control is the traffic sent from the host 1 (502a) to the host 2 (502b). Based on this information and topology information (600) of a network (505a) managed by policy server 1 (500a) stored in a main memory (203), a route through which traffic passes is identified. Route identification means are the same as in the first embodiment. Here, traffic passes through the route of host 1 (502a) - router 1 (501a) - router 2 (501b) and arrives at an adjacent network (505c). The policy server 1 (500a) configures the router 1 (501a) and the router 2 (501b) on the route to apply QoS control to traffic in accordance with conditions of flow type information and QoS control information in the policy control information.

[0041] Next, the policy server (500a) confirms from the topology information of the network (505a) that it manages that traffic will be transferred from the router 2 (501b) to a router 3 (501c) located in the non-policy-based network (505c). Since the network (505c) is non-policy based, it is not possible to read the network topology information. As means for the policy server (500a) to confirm the topology information of this non-policy-based network, a route is identified using a route investigation command such as a traceroute command. FIG. 11 shows a flowchart of route search means such as a traceroute command. The traceroute command is executed from the upstream router (501b) on the traffic route that is connected to the non-policy-based QoS network to the traffic receiving host (502b).

[0042] This reveals that the route from the router 2 (501b) to the host 2 (502b) is router 2 (501b) - router 3 (501c) - router 4 (501d) - router 5 (501e) - router 6 (501f) - host 2 (502b). Based on this route information, a determination is made as to which network each passed router belongs and whether the network is a policy-based QoS network. That is, it is confirmed that the router 3 (501c) and the router 4 (501d) belong to the non-policy-based network (505c), and the router 5 (501e) and the router 6 (501f) belong to the policy-based QoS network 2 (505b).

[0043] The policy server 1 (500a) confirms that the router 5 (501e) and router 6 (501f) belonging to the policy-based QoS network 2 (505b) are present on the route of the traffic, and sends policy control information for the traffic and information indicating that the route of the traffic passes through the router 5 (501e) to the policy server 2 (500b) which manages the network (505b).

[0044] Upon receiving the information, the policy server 2 (500b) performs the same process as the policy server 1 (500a). That is, the route through which the traffic passes is identified based on the policy control information, the information indicating that the traffic passes through the router 5 (501e), and the topology information of the network managed by the policy server (500b). The policy server (500b) configures the router 5 (501e) and the router 6 (501f) on the route to apply QoS control to the traffic in accordance with the conditions for the flow type information and QoS control information in the policy control information.

[0045] The above-described policy server processing makes it possible to configure QoS control information for traffic within each policy-based QoS network when a non-policy-based QoS network is interposed between a plurality of policy-based QoS networks. In this configuration, traffic is not guaranteed end-to-end QoS, but

it is effective at such times as when the bandwidth of the non-policy-based QoS network is larger and the delay is smaller than that of the policy-based QoS network.

[0046]

[Effect of the Invention] According to the present invention, it is possible to distribute an increased load on a policy server caused by an increase in communication devices deployed within a network by deploying a plurality of policy servers and managing the network using the plurality of policy servers.

[0047] Furthermore, in regard to the configuration of policy control information between a plurality of domain networks of other ISPs (Internet Service Providers) and the like, which was previously impossible, a plurality of policy servers between domain networks exchange policy control information to enable the configuration of policy control information for network equipment via a plurality of domain networks.

[Brief Description of Drawings]

[FIG.1] A diagram showing an overview of a configuration of a policy-based QoS network applying the present invention.

[FIG. 2] A diagram showing an overview of a configuration of a policy server applying the present invention.

[FIG. 3] A diagram showing a configuration of policy control information held by a policy server applying the present invention.

[FIG. 4] A diagram showing a policy control process flow for a policy server applying the present invention.

[FIG. 5] A diagram showing an overview of a configuration of the second embodiment of a policy-based QoS network applying the present invention.

[FIG. 6] A diagram showing a configuration of topology information held by a policy server applying the present invention.

[FIG. 7] A diagram showing a time calibration process flow for a policy server applying the present invention.

[FIG. 8] A diagram showing a topology information process flow for a policy server applying the present invention.

[FIG. 9] A diagram showing a configuration of a host deployed in a policy-based QoS network applying the present invention.

[FIG.10] A diagram showing a configuration of communication devices deployed in a policy-based QoS network applying the present invention.

[FIG. 11] A diagram showing a flow for searching for routes within a non-policy-based QoS network existing between policy-based QoS networks applying the present invention.

[FIG. 12] A diagram showing a list of managed communication devices held by a policy server applying the present invention.

[FIG. 13] A diagram showing a policy-based QoS management domain list held by a policy server applying the present invention.

[Description of Reference Numerals]

100, 100a, 100b... Policy server

101a, 101b, 101c, 101d, 101e, 101f... Router
102a, 102b... Host
103... Transmission path

105a, 105b... Policy-based QoS management domain
201... Bus
202... Control unit
203... Main memory

204... User interface unit
205... Network interface unit
206... Clock unit
300... Policy control information
301...Host information

302... Flow type information
303... QoS control information
304... Setting time information
305... Policy transfer information

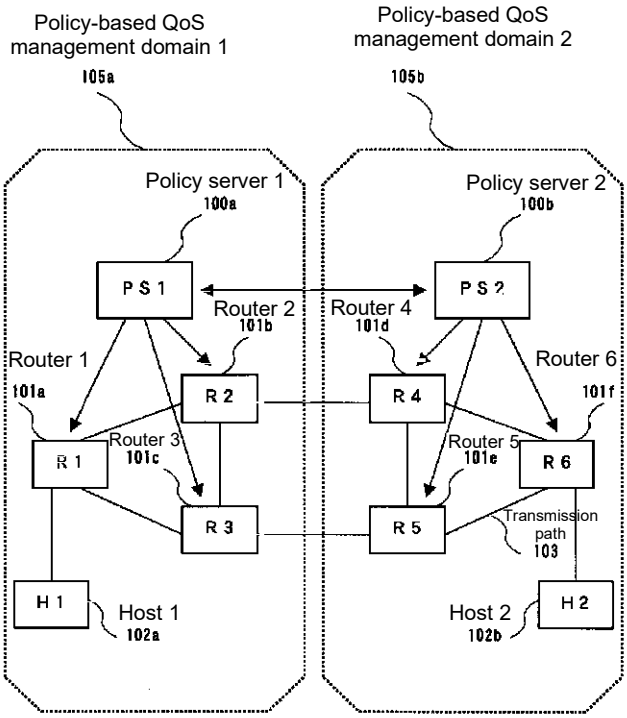
500a, 500b... Policy server
501a, 501b, 501c, 501d, 501e, 501f... Router
502a, 502b... Host
505a, 505b... Policy-based QoS management domain

505c... Non-policy-based QoS management domain
600... Topology information
601a... communication device 1 IP address

601b-1... Adjacent communication device 1 IP address
601b-M1... Adjacent communication device M1 IP address
901... Bus
902... Control unit
903... Main memory
904... Display viewing unit
905... Key input operation unit
906... Network interface unit
1001... Bus
1002... Control unit
1003... Main memory
1004... Routing processing unit
1005... Network interface unit
1006... Network interface unit
1007... Network interface unit
1200... Managed communication device list
1201... communication device 1 IP address
1300... Policy-based QoS management domain list

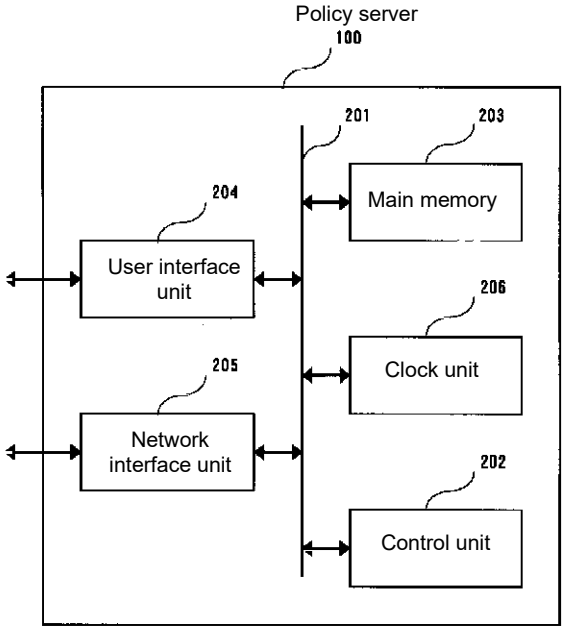
[FIG. 1]

[FIG. 1]



[FIG. 2]

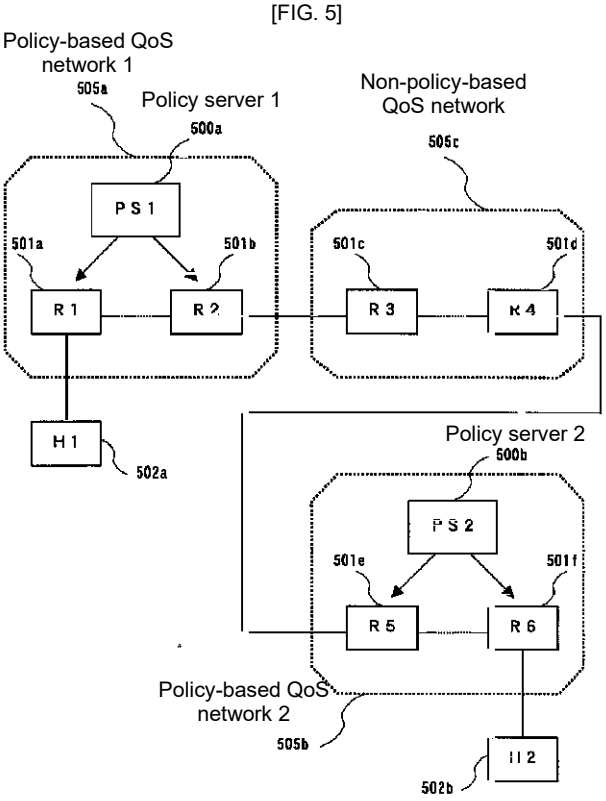
[FIG. 2]



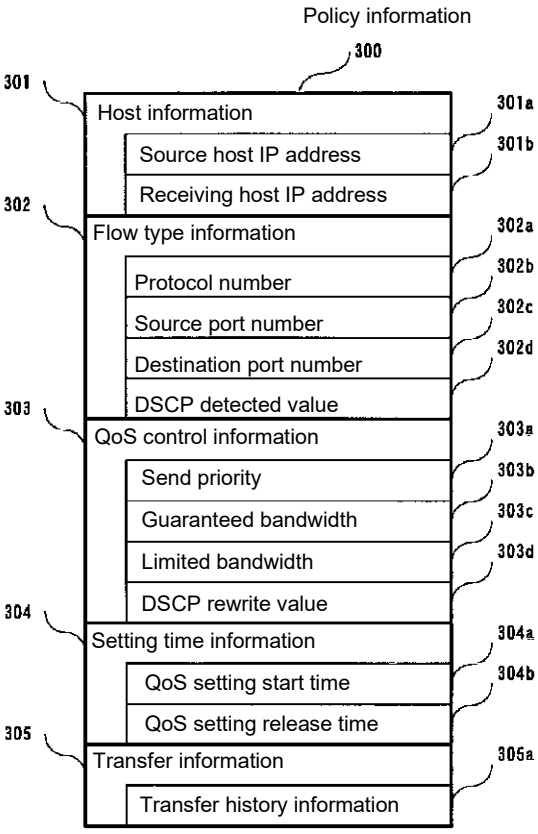
[FIG. 3]

[FIG. 5]

[FIG. 5]



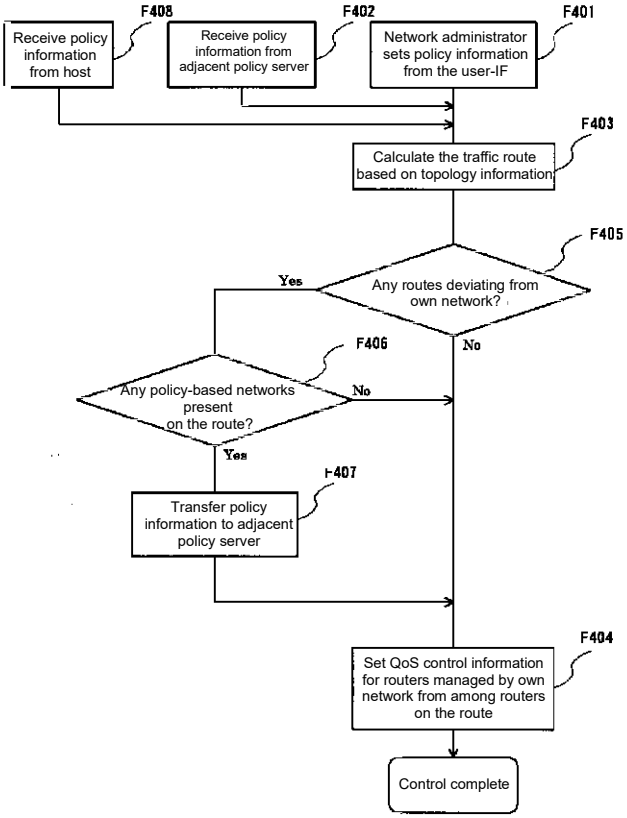
[FIG. 3]



Cisco Systems, Inc. v. OptimNet LLC
Exhibit 1014

[FIG. 4]

[FIG. 4]



[FIG. 6]

[FIG. 6]

Topology information

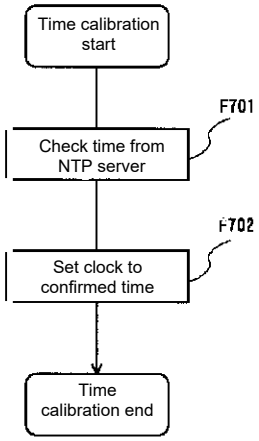
600

601a	Network relay device 1 IP address	
601b-1	Destination network IP address 1	next-hop relay device IP address
	⋮	⋮
601b-M1	Destination network IP address M1	next-hop relay device IP address
602a	Network relay device 2 IP address	
602b-1	Destination network IP address 1	next-hop relay device IP address
	⋮	⋮
602b-M2	Destination network IP address M2	next-hop relay device IP address
	⋮	⋮
60Na	Network relay device N IP address	
60Nb-1	Destination network IP address 1	next-hop relay device IP address
	⋮	⋮
60Nb-MN	Destination network IP address MN	next-hop relay device IP address

[FIG. 8]

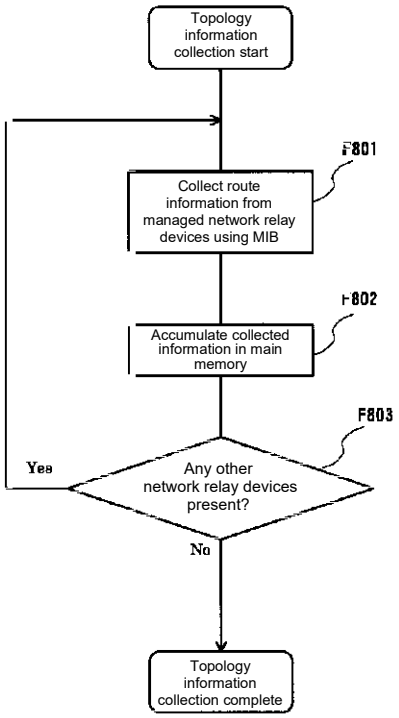
[FIG. 7]

[FIG. 7]



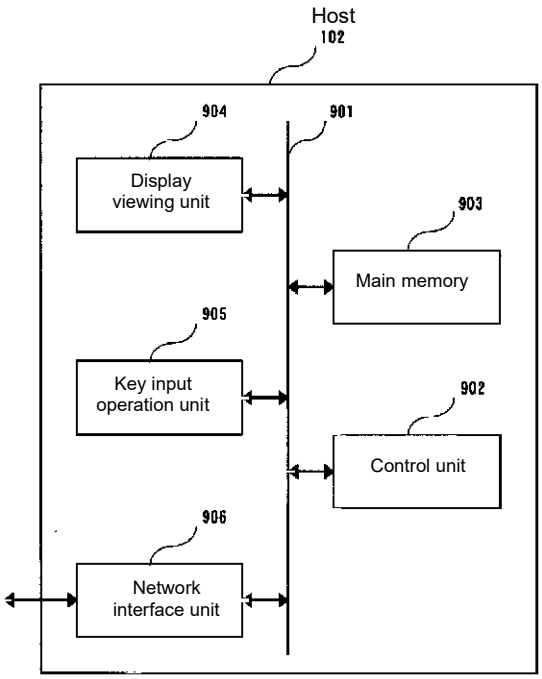
[FIG. 8]

[FIG. 8]



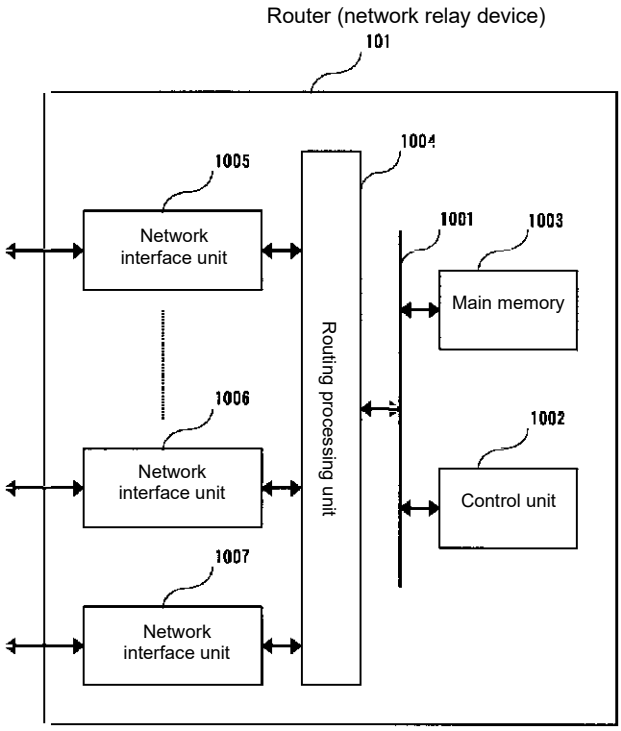
[FIG. 9]

[FIG. 9]



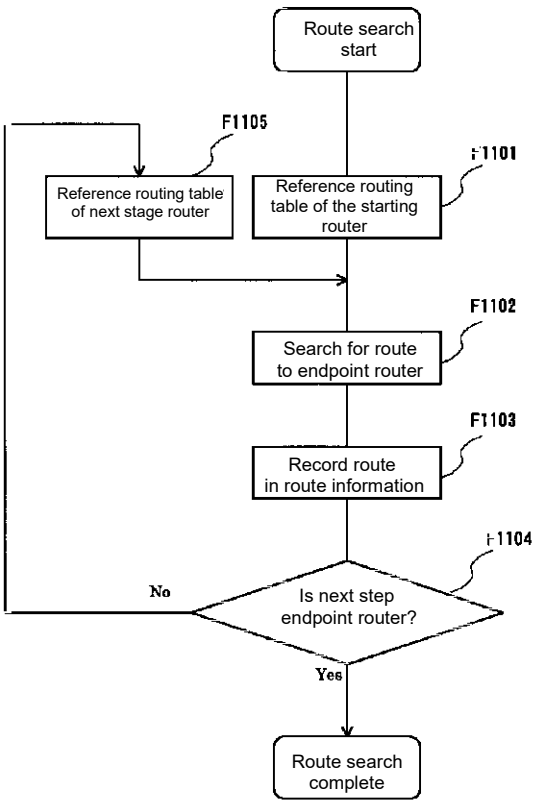
[FIG. 10]

[FIG. 10]



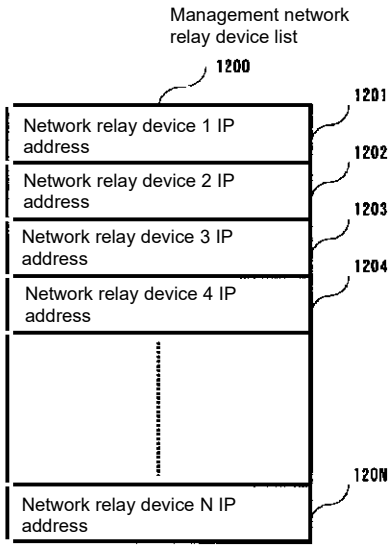
[FIG. 11]

[FIG. 11]



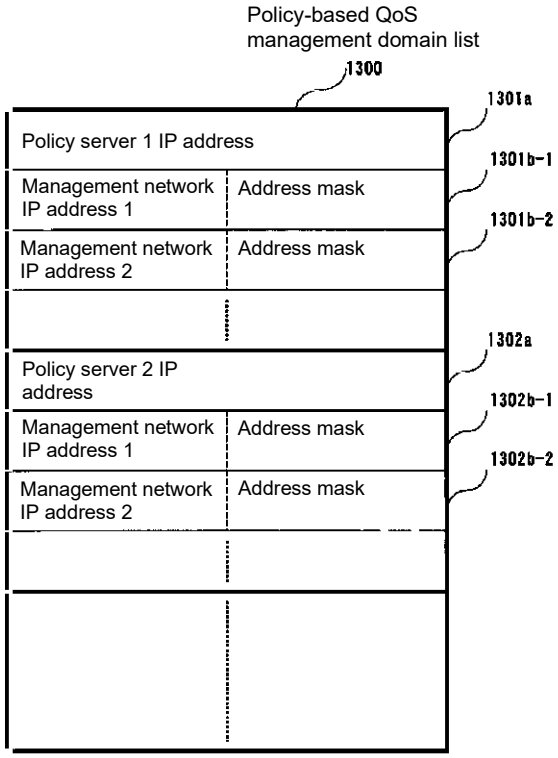
[FIG. 12]

[FIG. 12]



[FIG. 13]

[FIG. 13]



Continued from front page

(72) Inventor Tei Shiina
C/o Hitachi, Ltd. Network Platform Division,
890 Kashimada, Saiwai-ku, Kawasaki-shi,
Kanagawa-ku

(72) Inventor Masaro Suzuki
C/o Hitachi, Ltd. Network Platform Division,
890 Kashimada, Saiwai-ku, Kawasaki-shi,
Kanagawa-ku

F Term (Reference) 5K030 HA08 KA01 KA05 LB05 LC08
LD11 LD18

Cisco Systems, Inc. v. OptimNet LLC
Exhibit 1014