



(51) International Patent Classification:

H04L 29/06 (2006.01) H04L 12/803 (2013.01)
H04L 29/08 (2006.01)

(21) International Application Number:

PCT/US2015/058987

(22) International Filing Date:

4 November 2015 (04.11.2015)

(25) Filing Language:

English

(26) Publication Language:

English

(71) Applicant: HEWLETT PACKARD ENTERPRISE DEVELOPMENT LP [US/US]; 11445 Compaq Center Drive West, Houston, Texas 77070 (US).

(72) Inventor: WANG, Xiaoyi; 1160 Enterprise Way, Sunnyvale, California 94089 (US).

(74) Agents: PINKSTON, Caroline et al.; Hewlett Packard Enterprise, 3404 E. Harmony Road, Mail Stop 79, Fort Collins, Colorado 80528 (US).

(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, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, 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, ST, 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).

Declarations under Rule 4.17:

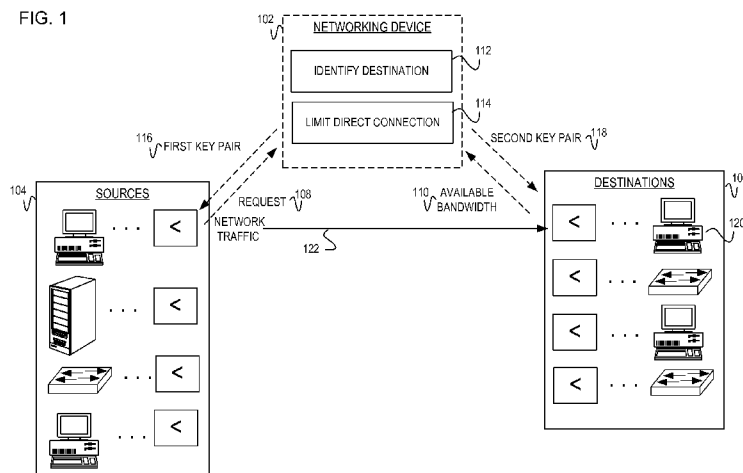
- as to the identity of the inventor (Rule 4.17(i))
- as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii))

Published:

- with international search report (Art. 21(3))

(54) Title: DIRECT CONNECTION LIMITATION BASED ON A PERIOD OF TIME

FIG. 1



(57) Abstract: Examples herein disclose a facilitation of a direct connection between a source and a destination. In response to a request from the source to facilitate the direct connection, the examples identify the destination among multiple destinations based on available bandwidth from the multiple destinations. The examples transmit a security token to the identified destination for authentication of traffic from the source, wherein the source includes an indication of a period of time. Based on the indication of the period of time, the examples limit the direct connection.

DIRECT CONNECTION LIMITATION BASED ON A PERIOD OF TIME

BACKGROUND

[0001] In network load balancing, a networking component may balance traffic across multiple links. Balancing traffic across the multiple links gives the networking component the ability to spread out an amount of the bandwidth for processing network traffic.

BRIEF DESCRIPTION OF THE DRAWINGS

[0002] In the accompanying drawings, like numerals refer to like components or blocks. The following detailed description references the drawings, wherein:

[0003] FIG. 1 is a block diagram of an example system including a networking device to identify a destination in response to a request from a source, the networking device transmits key pairs to the source and identified destination to limit a direct connection;

[0004] FIG. 2 is an illustration of example communications between a source, load balancers, and a destination;

[0005] FIG. 3 is a flowchart of an example method executable by a networking device to limit a direct connection between a source and identified destination based on an indication of period of time in a key pair;

[0006] FIG. 4 is a flowchart of an example method executable by a networking device to limit a direct connection between a source and an identified destination via a transmission of a stop signal to the source based on an expiration of a period of time;

[0007] FIG. 5 is a block diagram of an example computing device with a processing resource to execute instructions in a machine-readable storage medium for limiting a direct connection based on a period of time; and

[0008] FIG. 6 is a block diagram of an example computing device with a processing resource to execute instructions in a machine-readable storage medium for limiting a direct connection between a source and an identified destination by tracking a period of time based on arrival of traffic to the identified destination.

DETAILED DESCRIPTION

[0009] In a networking system, a load balancer serves as a centralized topology where the load balancer performs load balancing across multiple destinations. As used herein, the term “load balancing” refers to the distribution of the network traffic (e.g., packets) among multiple destinations (e.g., computing devices). To implement the load balancing operation, upon arrival of the traffic, a networking device performs a round robin to distribute the traffic out accordingly. In this example, the networking device serves as the centralized topology to receive traffic and then distribute. However, the networking device may become a bottleneck of the networking system if the load balancer handles too much traffic at a given period of time. This may cause packet loss and networking system slow down. Forming a continuous direct connection between a source and destination may be ineffective as traffic patterns vary over time and the continuous direct connection may be more susceptible to security attacks.

[0010] To address these issues, examples disclosed herein provide an efficient mechanism to the aforementioned load balancing. The examples disclose a networking device to perform load balancing without the arrival of traffic to the networking device. The networking device implements the load balancing through an establishment and facilitation of a direct connection between a source and a destination. The networking device receives a connection request from the source and identifies the destination from multiple destinations based on available bandwidth. Identifying the destination based on the available bandwidth allows the networking device to balance traffic across those destinations which have the capability to support the traffic. Balancing the traffic based on the available bandwidth at the destinations, prevents traffic loss.

[0011] Additionally, the networking device establishes and facilitates the direct connection based on a transmission of first and second key pairs. Transmitting the first and the second key pairs to the source and identified destinations provides a security function to authenticate the source to the identified destination. Based on the first and the second key pairs, the source and the destination form an exclusive direct connection to transmit traffic. Authenticating the source to establish the direct connection ensures a secure connection exclusively between the source and the identified destination.

[0012] In another example, the networking device limits the direct connection based on a period of time. Limiting the direct connection in accordance to the period of time is an effective approach which rebalances traffic patterns over time.

[0013] FIG. 1 is a block diagram of an example system including a networking device 102 to identify a destination 120 among multiple destinations 106 in response to a request 108 from a source 104. The networking device 102 identifies the destination 120 based on available bandwidth from the multiple destinations 106 at module 112. In response to identifying the destination 120, the networking device 102 transmits a first key pair 116 to the source 104 and a second key pair 118 to the identified destination 120. The first and the second key pairs 116 and 118 indicate a period of time. The networking device 102 limits a direct connection 120 between the source 104 and the identified destination 120 in accordance with the indicated period of time at module 114. The direct connection 120 is considered a link formed between the source 104 and the identified destination 120 so that network traffic is transmitted over this link. The system in FIG. 1 represents a load balancing network system. The load balancing network system is a system in which the networking device 102 is capable of facilitating direct connections between the sources and the destinations 106 such that networking traffic is distributed among the direct connections. As such, implementations of the system include a domain name system (DNS) network, wide area network, legacy network, local area network (LAN), Ethernet, optic cable network, software defined network (SDN), or other type of networking system capable of balancing network traffic through the formation of the direct connections. Although FIG. 1 illustrates the system with components 102, 104, and 106 implementations should not be limited as the system may include additional components such as an additional networking device, etc.

[0014] The networking device 102 is a component within the system capable of balancing network traffic through the facilitation of direction connections between the source(s) 104 and the multiple destinations 106. Implementations of the networking device 102 include, by way of example, a router, switch, server, networking switch, virtual networking component, mobile device, computing device, or other type of networking component capable of facilitating direct connections for the transmission of network traffic.

[0015] The source 104 is a computing component which receives network traffic and in turn transmits the request 108 for facilitation of the direct connection 122. Each source 104 may additionally include a connector (as indicated to the right of each source 104) to provide an interface between the component and the networking system. Depictions of the source(s) 104 are meant for illustrative purposes and not meant for limiting the technology. For example, the source

104 may include a different component such as a router, server, a networking system, or other networking component.

[0016] From among the multiple destinations 106, the networking device 102 identifies the destination 120. The identified destination 120 is determined in response to the networking device 102 receiving the request 108 from the source 104. The identified destination is determined based on the available bandwidth 110 from each of the destinations 106. Each of the multiple destinations 106 include a connector in which to interface to the networking system. Depictions of the identified destination 106 are meant for illustrative purposes and not meant for limiting the technology. For example, the identified destination 106 may include a router, computing device, switch, server, networking appliance, networking system, other networking component.

[0017] The request 108 is a data signal from the source 104 to the networking device 102 to facilitate the direct connection 122. In one implementation, the request 108 may define the network traffic as a number of events or processes over a period of time at the source 104. The number of events or processes occurring at the source 104 over the period of time, allows the networking device 102 to determine the amount of necessary bandwidth for processing the network traffic. For example, the request 108 may include events per second (EPS) information for the networking device 102 in turn to identify the destination 120.

[0018] The available bandwidth 110 is a bit-rate of available or free information capacity each of the multiple destinations 106 may be capable of accommodating. As such, each of the multiple destinations 106 may perform an analysis at their respective location to determine the available bandwidth. This available bandwidth is transmitted for the networking device 102 to track the bandwidth capability at each of the destinations 106. In one implementation, in addition to the available bandwidth, each destination 106 may also provide health information indicating the connectivity to the network. This implementation may be discussed in detail in later figures.

[0019] At modules 112-114, the networking device 102 determines the identified destination 120 and limits the direct connection 122 to the period of time. The networking device 102 uses the available bandwidth 110 as transmitted by the multiple destinations 106 to determine the identified destination 120 from the multiple destinations 106. Additionally, the networking device 102 limits the direct connection 122 by tracking the period of time. The modules 112-114 may include, by way of example, instructions (e.g., stored on a machine-readable medium) that, when executed (e.g., by the networking device 102), implement the functionality of modules 112-114.

Alternatively, or in addition, the modules 112-114 may include electronic circuitry (i.e., hardware) that implements the functionality of modules 112-114.

[0020] The first and second key pairs 116 and 118 is a cryptographic security function in which to encrypt and decrypt information from the source 104. In this manner, the identified destination 120 authorizes the direct connection 122 to the source 104. For example, a public key may be used at the source 104 to encrypt data which is transmitted to the identified destination 120. The identified destination 120 receives the encrypted data and uses the private key transmitted in the second key pair 118 to decrypt the data. Thus based on this decrypted data, the identified destination 120 may authorize the direct connection 122 with the source 104. These key pairs 116 and 118 provide the security feature in prevent tampering or receiving traffic from an unauthorized source. As such, each key pair 116 and 118 may include a public key and a private key for encryption and decryption, accordingly. In one implementation, the first key pair 116 and the second key pair 118 are two different types of key pairs. For example, the first key pair 116 may be a symmetric key pair and the second key pair 118 may be an asymmetric key pair. In a further implementation, the networking device 102 may transmit a security token to the identified destination in place of the first and the second key pairs. The security token may include a security function in which the identified destination 120 may authorize or authenticate the transmission of network traffic from the source 104.

[0021] The direct connection 122 is considered a communication link enabled exclusively between the source 104 and the identified destination 120. This communication link 122 connects the source 104 and the identified destination 120 for the transmission of the network traffic from the source 104. The direct connection 122 is authorized based on the first and the second key pairs 116 and 118 transmitted by the networking device 102. The direct connection is limited in the sense that upon arrival of the network traffic, the identified destination 120 transmits an activation signal to the networking device 102 to track a countdown of the period of time. The period of time may be defined by an administrator or dynamically calculated based on the amount of necessary bandwidth to process network traffic. Upon the expiration of this period of time, the networking device 102 transmit a stop signal to the source 104 to cease the transmission of the networking traffic.

[0022] FIG. 2 is an illustration of example communications between a networking device 202 to a source 204 and destination(s) 206 to facilitate a direct connection between the source 204 and

an identified destination. Specifically, the networking device includes a first load balancer 224 to limit a period of time of the direct connection. A second load balancer 226 handles the facilitation of the direct connection should the first load balancer 224 become unavailable. As such, FIG. 2 illustrates the first load balancer 224 handling much of the task load and correspondence while the second load balancer 226 acts as more of a shadow of the first load balancer 224. Acting as more of shadow, ensures the load balancer 226 may pick up where the first load balancer 224 left off to handle the establishment of the direct connection and limitations thereof. The load balancer 224 and 226. Implementations of the load balancers 224 and 226 include by way of example, instructions executable by the networking device 202. Alternatively, or in combination, the load balancer 224 and 226 may include electronic circuitry or components.

[0023] The multiple destinations 206 transmit available bandwidth and health information continuously to the networking device 202. The health information is a heart beat signal indicating the health of each destination. Receiving the health information, the networking device 202 may accurately determine if a particular destination is offline. Thus, the networking device 202 may appropriately and accurately facilitate the establishment of the direct connection to source(s) and destinations(s).

[0024] The source 204 initiates the establishment of the direct connection through a transmission of a connection request to the networking device 202. The networking device 202 receives the connection request which is circulated to the first load balancer 224. The first load balancer 224 in response to the connection request, identifies the particular destination in which to form the direct connection. Upon identifying the destination, the first load balancer 224 transmits a response including a first key pair and an internet protocol (IP) address of the identified destination to the source 204. In addition to transmitting the first key pair, the first load balancer 224 transmits the second key pair to the identified destination. Transmitting these key pairs, the identified destination authenticates the traffic from the source 204. Upon validation of the key pairs to the source 204 and the identified destination, the establishment of the direct connection is formed. Upon forming the direct connection, the source 204 transmits traffic to the identified destination using the IP address sent in the response from the load balancer 224. Based on the arrival of the traffic from the source 204, the identified destination transmits an activation signal to the first load balancer 224. The activation signal indicates to the first load balancer 224 to track a period of time associated with the key pairs. The first load balancer 224 performs a count of the

period of time to determine the expiration. Based on reaching the expiration of the period of time, the first load balancer 224 transmits a stop signal to both the source 204 and the identified destination to break or interrupt the direct connection.

[0025] FIG. 3 is a flowchart of an example method to limit a direct connection between a source and an identified destination based on an indication of a period of time. The method is executable by a networking device to limit the direct connection. The networking device identifies a destination among multiple destinations in response to a request from a source. The request includes a communication to the networking device from the source to facilitate the direct connection. In an implementation, the request may include information on an amount of bandwidth corresponding to network traffic at the source. For example, the request may include a number of events per second which corresponds to the amount of the traffic at the source. The networking device utilizes this information to identify which destination may handle the network traffic. In another implementation, the networking device identifies the destination based on an amount of bandwidth available at each of the destinations. The amount of available bandwidth may correspond to the bandwidth information in the request to ensure the traffic is accurately balanced. Upon identifying the destination, the networking device transmits a first key pair to the source and a second key pair to the identified destination. The first and second key provides a security feature in the system through the authentication of the source and/or traffic from the source to the identified destination. Using the key pairs to authenticate the source to the identified destination, the direct connection may be set-up to allow the transmission of the traffic. The first and the second key pairs indicate the period of time in which to limit the direct connection. In discussing FIG. 3, references may be made to the components in FIGS. 1-2 to provide contextual examples. In one implementation, the networking device 102 executes operations 302-306 to facilitate and limit the direct connection. Although FIG. 3 is described as implemented by the networking device 102, it may be executable on other suitable components. For example, FIG. 3 may be implemented in the form of executable instructions on a machine-readable storage medium 504 and 604 as in FIGS. 5-6.

[0026] At operation 302 in response to receipt of the request by the source, the networking device identifies the destination. The destination is identified based on the amount of available bandwidth from multiple destinations. The amount of available bandwidth is the amount of bandwidth capacity usable at each of the destinations for processing network traffic. The

networking device uses the request from the source that may include the necessary bandwidth for processing the network traffic. Based on the necessary bandwidth, the networking device determines which of the destinations has the available bandwidth to handle the network traffic.

[0027] At operation 304, upon identification of the destination, the networking device transmits the first key pair to the source and the second key pair to the identified destination. In one implementation, the second key pair indicates the period of time to limit the direct connection.

[0028] At operation 306, the networking device limits the direct connection in accordance with the indicated period of time. The direct connection may be limited according to the period of time which may be tracked by the identified destination or the networking device. In this implementation, the identified destination transmits an activation signal to the networking device upon the arrival of network traffic. Based on receiving the activation signal, the networking device tracks the period of time. Tracking the period of time, the networking device determines when the ending for the period of time occurs. This expiration of time signals to the networking device to transmit a stop signal to the source and the identified destination to cease the transmission of network traffic. The stop signal signifies to the source to cease transmission of the network traffic and to the identified destination to cease the acceptance of the traffic. If the transmission of the network traffic is incomplete, the source may transmit an additional request to the networking device for another direct connection.

[0029] FIG. 4 is a flowchart of an example method to limit a direct connection via a transmission of a stop signal based on an expiration of a period of time. The method illustrated in FIG. 4 is executable by a networking device to limit the direct connection based on the expiration of the time period. The networking device receives from multiple destinations, health information and bandwidth available at each destination. In turn upon receive a request from a source to facilitate the direct connection, the networking device identifies the destination with which to initiate the direct connection from the source. The networking device identifies the destination among the multiple destinations based on the health information and available bandwidth. Upon identifying the destination, the networking device transmits a first key pair to the source and a second key pair to the identified destination. The key pairs are associated with a period of time, so when networking traffic arrives at the identified destination from the source, the networking device receives an activation signal. The activation signal indicates to the networking device to initiate a tracking of the period of time. Tracking the period of time, the networking device limits

the direct connection by transmitting a stop signal to the source based on an expiration of the period of time. In discussing FIG. 4, references may be made to the components in FIGS. 1-2 to provide contextual examples. In one implementation, the networking device 102 executes operations 402-418 to facilitate and limit the direct connection. Although FIG. 4 is described as implemented by the networking device 102, it may be executable on other suitable components. For example, FIG. 4 may be implemented in the form of executable instructions on a machine-readable storage medium 504 and 604 as in FIGS. 5-6.

[0030] At operation 402, the networking device receives health information and available bandwidth from each of the destinations. The destinations may continuously transmit health information, such as heart beat signals to the networking device indicating the health of each destination. Along with the heart beat signals, the networking device receives the available bandwidth of each of the destinations, to appropriately facilitate direct connections and thus distribute the network traffic through the direct connections.

[0031] At operation 404, the networking device receives the connection request from the source. The connection request includes information identifying the source and the amount of necessary bandwidth to process network traffic. In implementations, the connection request defines a number of events/processes over a period of time corresponding to the network traffic at the source 104. For example, the request may include the events per second (EPS) information for the networking device in turn to identify the destination.

[0032] At operation 406, in response to receive the connection request from the source, the networking device identifies the destination to form the direct connection based on the health information and available bandwidth. Operation 406 may be similar in functionality to operation 302 as in FIG. 2.

[0033] At operation 408 based on identifying the destination, the networking device transmits the first key pair to the source and the second key pair to the identified destination. In one implementation, the networking device transmits a response along with the first key pair to the source and the second key pair to the identified destination as at operations 410-412. Operation 408 may be similar in functionality to operation 304 as in FIG. 3.

[0034] At operation 410, the networking device transmits the first key pair and along with the response to the source. The first key pair may include an indication of the period of time in which to limit the direct connection. This allows the source to also track when the direct connection may

expired based on the expiration of the period of time. Based on the identification of the destination, the networking device transmits the internet protocol (IP) address of the identified destination. This allows the source to direct the network traffic by encapsulating the traffic with the IP address to ensure the traffic is directed to the identified destination.

[0035] At operation 412, the networking device transmits the second key pair to the identified destination. The second key pair includes the indication of the period of time which instructs the identified destination to transmit the activation signal for counting the period of time. In addition to the second key pair, the networking device may also transmit a message to the identified destination to prepare for the oncoming traffic. In another implementation, in place of transmitted first and the second key pairs, the networking device transmits a security token to the identified destination for authentication of the source.

[0036] At operation 414, the networking device receives the activation signal upon the arrival of the traffic at the identified destination. The activation signal indicates to the networking device to initiate the count of the period of time to limit the direct connections. In this implementation, upon transmitting the activation signal, the direct connection is established.

[0037] At operation 416, the networking device limits the direct connection based on the expiration of the period of time. As such, operation 416 may be similar in functionality to operation 306 as in FIG. 3.

[0038] At operation 418, the networking device limits the direct connection by tracking when reaching the expiration of time. The expiration of time is a period of time which the networking device performs a count to determine when the end of time has been reached. Upon reaching the ending of this time period, the networking device proceeds to transmit the stop signal to the source and identified destination to cease the transmission of traffic over the direct connection.

[0039] FIG. 5 is a block diagram of computing device 500 with a processing resource 502 to execute instructions 506-512 within a machine-readable storage medium 504. Specifically, the computing device 500 with the processing resource 502 is to limit a direct connection between a source and an identified destination according to a period of time. Although the computing device 500 includes processing resource 502 and machine-readable storage medium 504, it may also include other components that would be suitable to one skilled in the art. For example, the computing device 500 may include a controller, memory storage, or other suitable type of component. The computing device 500 is an electronic device with the processing resource 502 capable of executing instructions

506-512 and as such embodiments of the computing device 500 include a networking device, server, switch, router, mobile device, desktop computer, laptop, or other type of electronic device capable of executing instructions 506-512. The instructions 506-512 may be implemented as methods, functions, operations, and other processes implemented as machine-readable instructions stored on the storage medium 504, which may be non-transitory, such as hardware storage devices (e.g., random access memory (RAM), read only memory (ROM), erasable programmable ROM, electrically erasable ROM, hard drives, and flash memory).

[0040] The processing resource 502 may fetch, decode, and execute instructions 506-512 to limit the direct connection between the source and identified destination based on a period of time. Specifically, the processing resource 502 executes instructions 506-512 to: receive a request from the source to facilitate the direct connection; in response to the request, identify the destination among multiple destinations based on the available bandwidth at each destination; upon identifying the destination, transmit the security token to the identified destination; and limit the direct connection based on a period of time.

[0041] The machine-readable storage medium 504 includes instructions 506-512 for the processing resource 502 to fetch, decode, and execute. In another embodiment, the machine-readable storage medium 504 may be an electronic, magnetic, optical, memory, storage, flash-drive, or other physical device that contains or stores executable instructions. Thus, the machine-readable storage medium 504 may include, for example, Random Access Memory (RAM), an Electrically Erasable Programmable Read-Only Memory (EEPROM), a storage drive, a memory cache, network storage, a Compact Disc Read Only Memory (CDROM) and the like. As such, the machine-readable storage medium 504 may include an application and/or firmware which can be utilized independently and/or in conjunction with the processing resource 502 to fetch, decode, and/or execute instructions of the machine-readable storage medium 504. The application and/or firmware may be stored on the machine-readable storage medium 504 and/or stored on another location of the computing device 500.

[0042] FIG. 6 is a block diagram of computing device 600 with a processing resource 602 to execute instructions 606-620 within a machine-readable storage medium 604. Specifically, the computing device 600 with the processing resource 602 is to limit a direct connection between a source and an identified destination by tracking a period of time based on arrival of traffic to the identified destination. Although the computing device 600 includes processing resource 602 and

machine-readable storage medium 604, it may also include other components that would be suitable to one skilled in the art. For example, the computing device 600 may include a controller, memory storage, or other suitable type of component. The computing device 600 is an electronic device with the processing resource 602 capable of executing instructions 606-620 and as such embodiments of the computing device 600 include a networking device, server, switch, router, mobile device, desktop computer, laptop, or other type of electronic device capable of executing instructions 606-620. The instructions 606-620 may be implemented as methods, functions, operations, and other processes implemented as machine-readable instructions stored on the storage medium 604, which may be non-transitory, such as hardware storage devices (e.g., random access memory (RAM), read only memory (ROM), erasable programmable ROM, electrically erasable ROM, hard drives, and flash memory).

[0043] The processing resource 602 may fetch, decode, and execute instructions 606-620 to limit the direct connection between the source and identified destination by tracking a period of time. Specifically, the processing resource 602 executes instructions 606-620 to: receive health information and available bandwidth from multiple destinations; receive a request from the source to facilitate the direct connection; in response to the request from the source, identify the destination among the multiple destinations according to an amount of bandwidth available at each of the destinations; upon identifying the destination, transmit a security token to the identified destination; limit the direct connection between the source and the identified destination through receiving an activation signal from the identified destination to start tracking the period of time; and upon expiration of the period of time, transmit the stop signal to the source and/or identified destination to stop the transmission of traffic to the identified destination.

[0044] The machine-readable storage medium 604 includes instructions 606-620 for the processing resource 602 to fetch, decode, and execute. In another embodiment, the machine-readable storage medium 604 may be an electronic, magnetic, optical, memory, storage, flash-drive, or other physical device that contains or stores executable instructions. Thus, the machine-readable storage medium 604 may include, for example, Random Access Memory (RAM), an Electrically Erasable Programmable Read-Only Memory (EEPROM), a storage drive, a memory cache, network storage, a Compact Disc Read Only Memory (CDROM) and the like. As such, the machine-readable storage medium 604 may include an application and/or firmware which can be utilized independently and/or in conjunction with the processing resource 602 to fetch, decode, and/or execute instructions of the machine-readable storage medium 604. The application and/or firmware may be stored on the

machine-readable storage medium 604 and/or stored on another location of the computing device 600.

[0045] Although certain embodiments have been illustrated and described herein, it will be greatly appreciated by those of ordinary skill in the art that a wide variety of alternate and/or equivalent embodiments or implementations calculated to achieve the same purposes may be substituted for the embodiments shown and described without departing from the scope of this disclosure. Those with skill in the art will readily appreciate that embodiments may be implemented in a variety of ways. This application is intended to cover adaptations or variations of the embodiments discussed herein. Therefore, it is manifestly intended that embodiments be limited only by the claims and equivalents thereof.

CLAIMSI claim:

1. A method, executable by a networking device, the method comprising:
in response to a request from a source to facilitate a direct connection, identifying a destination among multiple destinations based on available bandwidth from the multiple destinations;
transmitting a first key pair to the source and a second key pair to the identified destination, wherein the transmitted second key pair includes an indication of a period of time; and
limiting the direct connection based on the indication of the period of time.
2. The method of claim 1 comprising:
receiving an activation signal from the destination to track the period of time in response to an arrival of traffic at the destination.
3. The method of claim 1 wherein limiting the direct connection based on the indication of the period of time comprises:
transmitting a stop signal to the source in response to an expiration of the period of time.
4. The method of claim 1 comprising:
receiving health information and the available bandwidth from each of the multiple destinations.
5. The method of claim 1 comprising:
transmitting a response to the source wherein the response includes the first key pair and an Internet Protocol (IP) address to the identified destination.
6. The method of claim 1 comprising:
approving the request from the source prior to transmission of the first and the second key pairs.

7. The method of claim 1 wherein the first key pair and the second key pair are different types of key pairs.
8. The method of claim 1 wherein the request from the source includes an events per second (EPS) information corresponding to traffic at the source.
9. A non-transitory machine-readable storage medium comprising instructions that when executed by a processing resource cause a networking device to:
 - in response to a request from a source to facilitate a direct connection, identifying a destination among multiple destinations based on available bandwidth from the multiple destinations;
 - transmit a security token to the identified destination for authenticating traffic from the source, wherein the security token includes an indication of a period of time; and
 - limit the direct connection based on the indication of the period of time.
10. The non-transitory machine-readable storage medium of claim 9 wherein to limit the direct connection based on the indication of the period of time comprises instructions that when executed by the processing resource cause the networking device to:
 - transmit a signal to stop a transmission of traffic from the source to the destination based upon an expiration of the period of time.
11. The non-transitory machine-readable storage medium of claim 9 comprising instructions that when executed by the processing resource cause the networking device to:
 - track the period of time based upon traffic arrival at the identified destination.
12. The non-transitory machine-readable storage medium of claim 9 comprising instructions that when executed by the processing resource cause the networking device to:
 - transmit a response to the source including an Internet Protocol (IP) address to the identified destination.

13. A system comprising:

a first load balancer adaptable to:

in response to a request from a source to facilitate a direct connection, identify a destination among multiple destinations based on available bandwidth from the multiple destinations;

transmit a first key pair to the source and a second key pair to the identified destination, wherein the transmitted second key pair includes an indication of a period of time; and

limit the direct connection to the source and the identified destination based on the indication of the period of time.

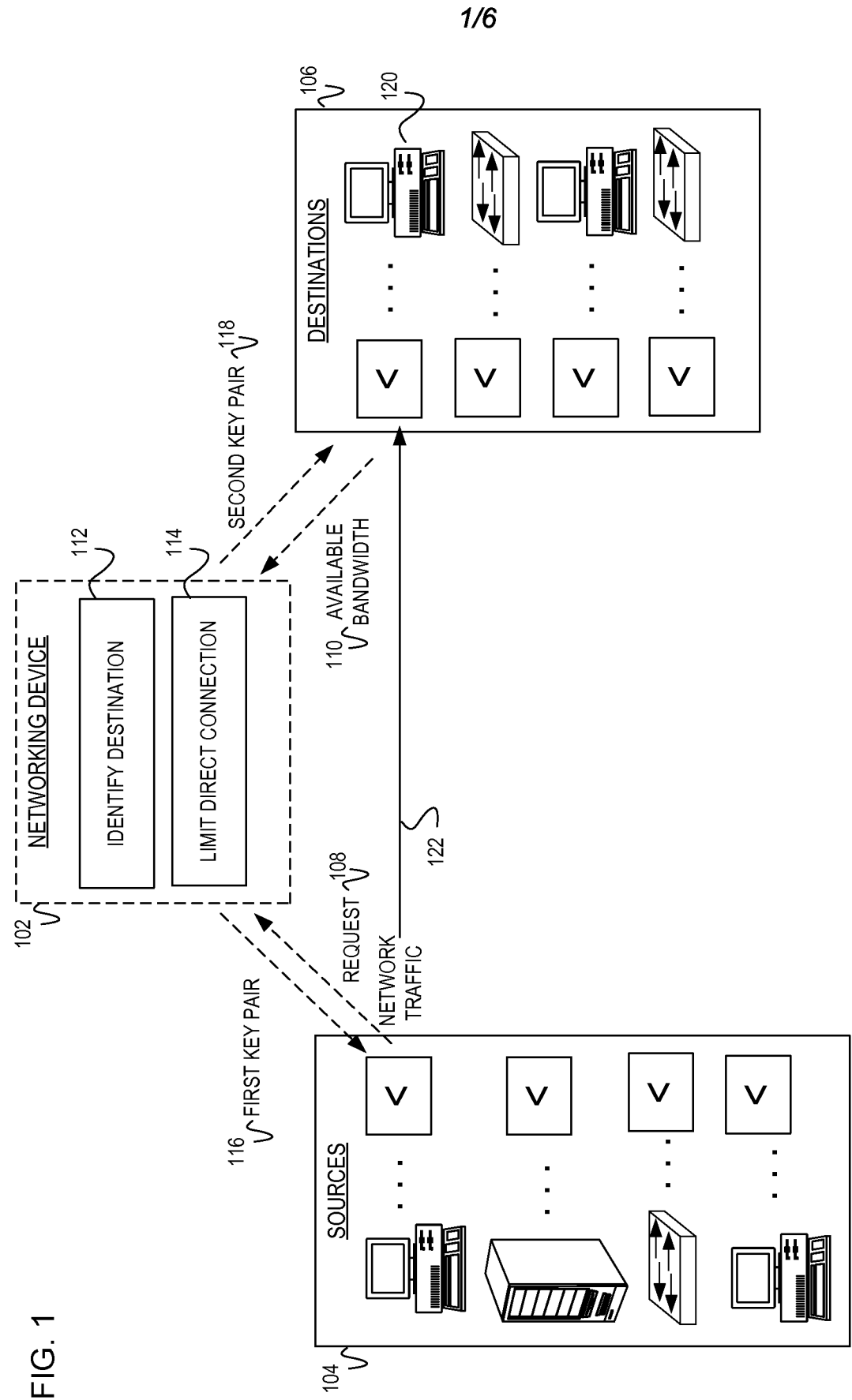
14. The system of claim 13 comprising:

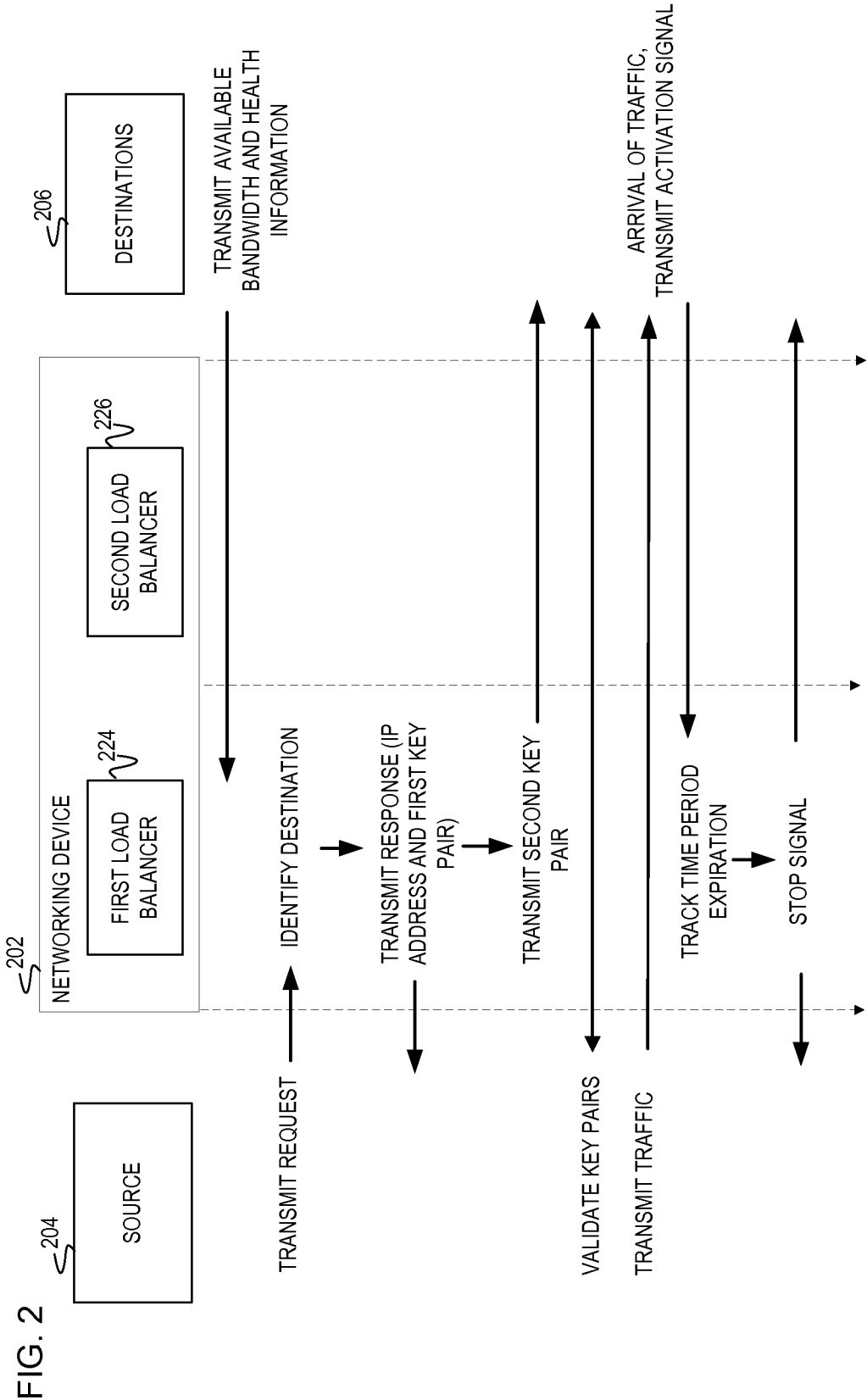
a second load balancer adaptable to handle the facilitation of the direct connection when the first load balancer is unavailable.

15. The system of claim 13 comprising:

the identified destination adaptable to transmit an activation based on an arrival of traffic from the source, wherein the activation signal indicates a tracking of an expiration of the period of time.

FIG. 1





3/6

FIG. 3

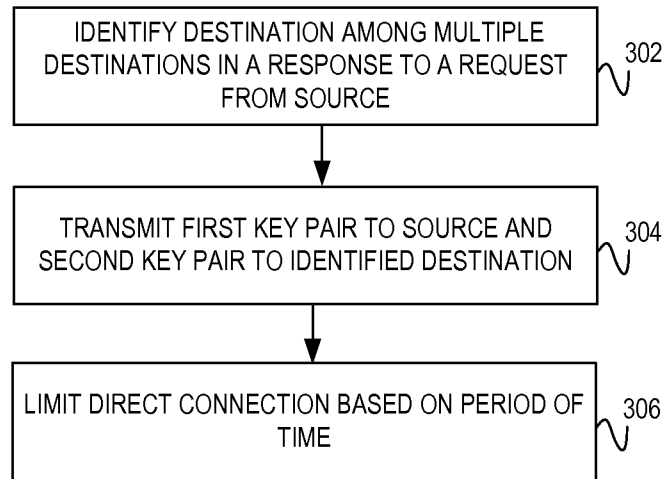
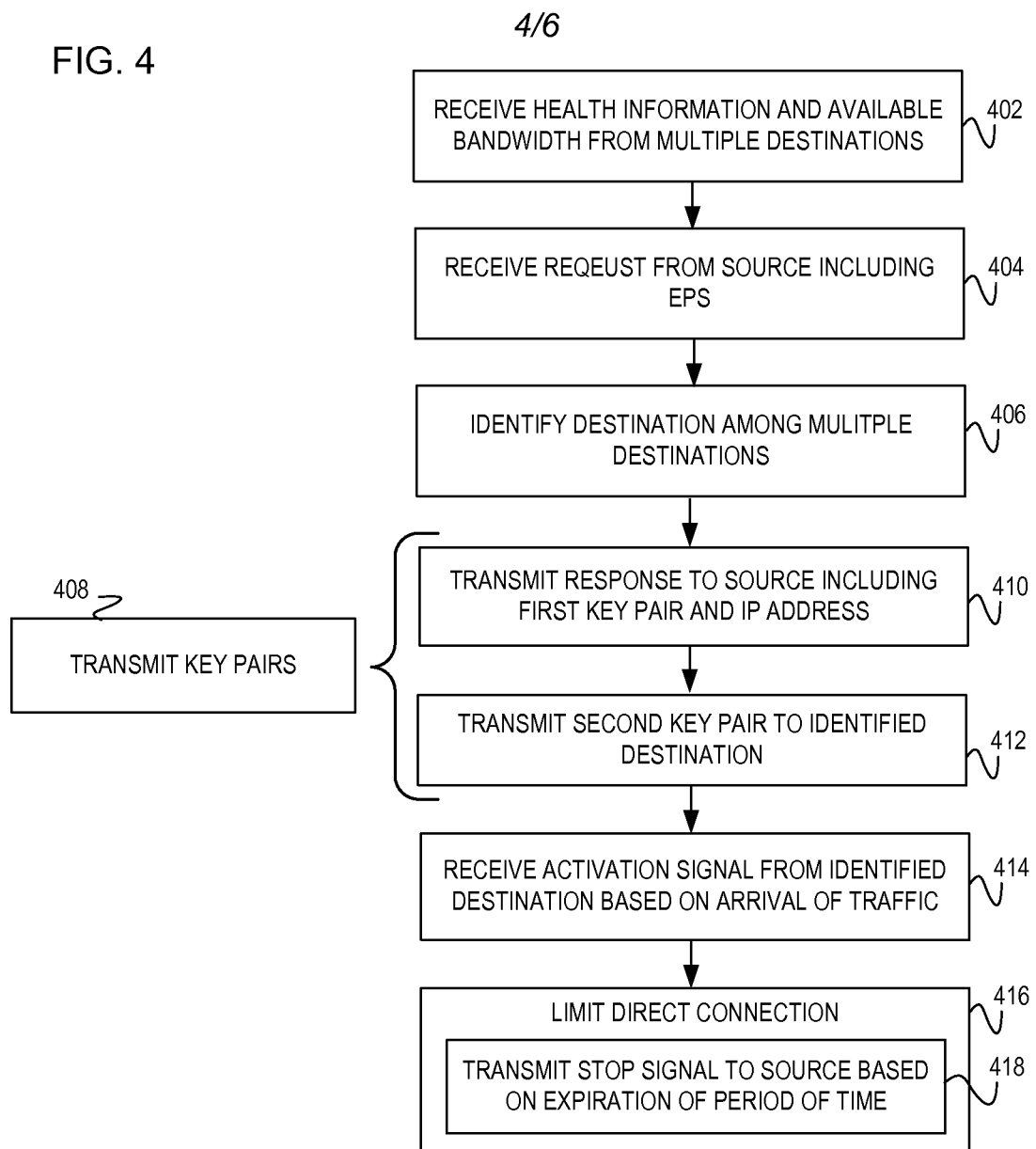
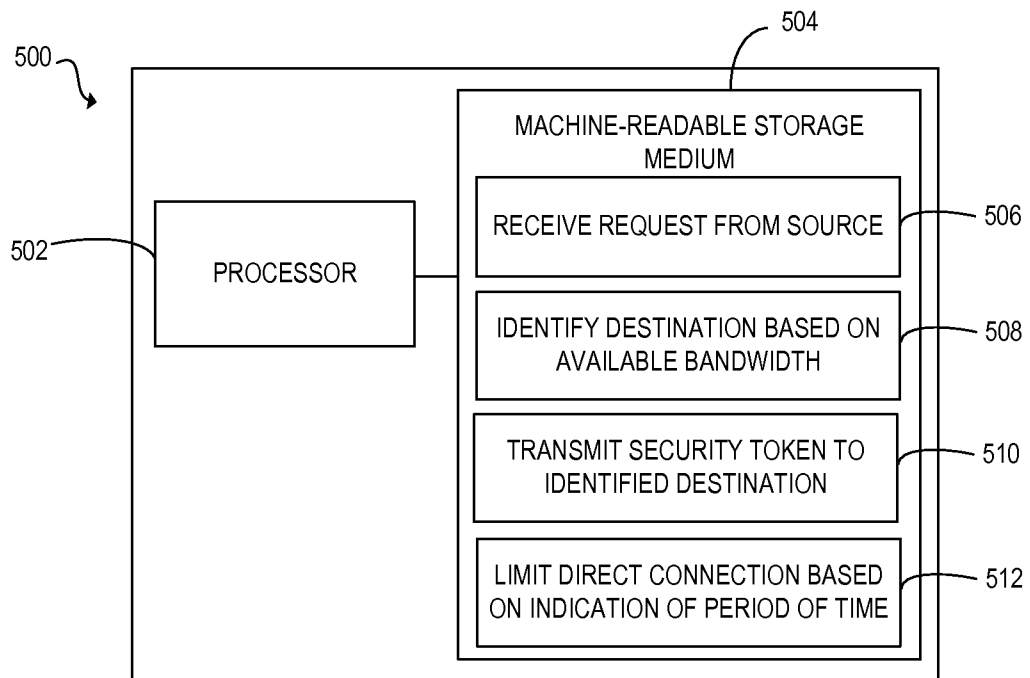


FIG. 4



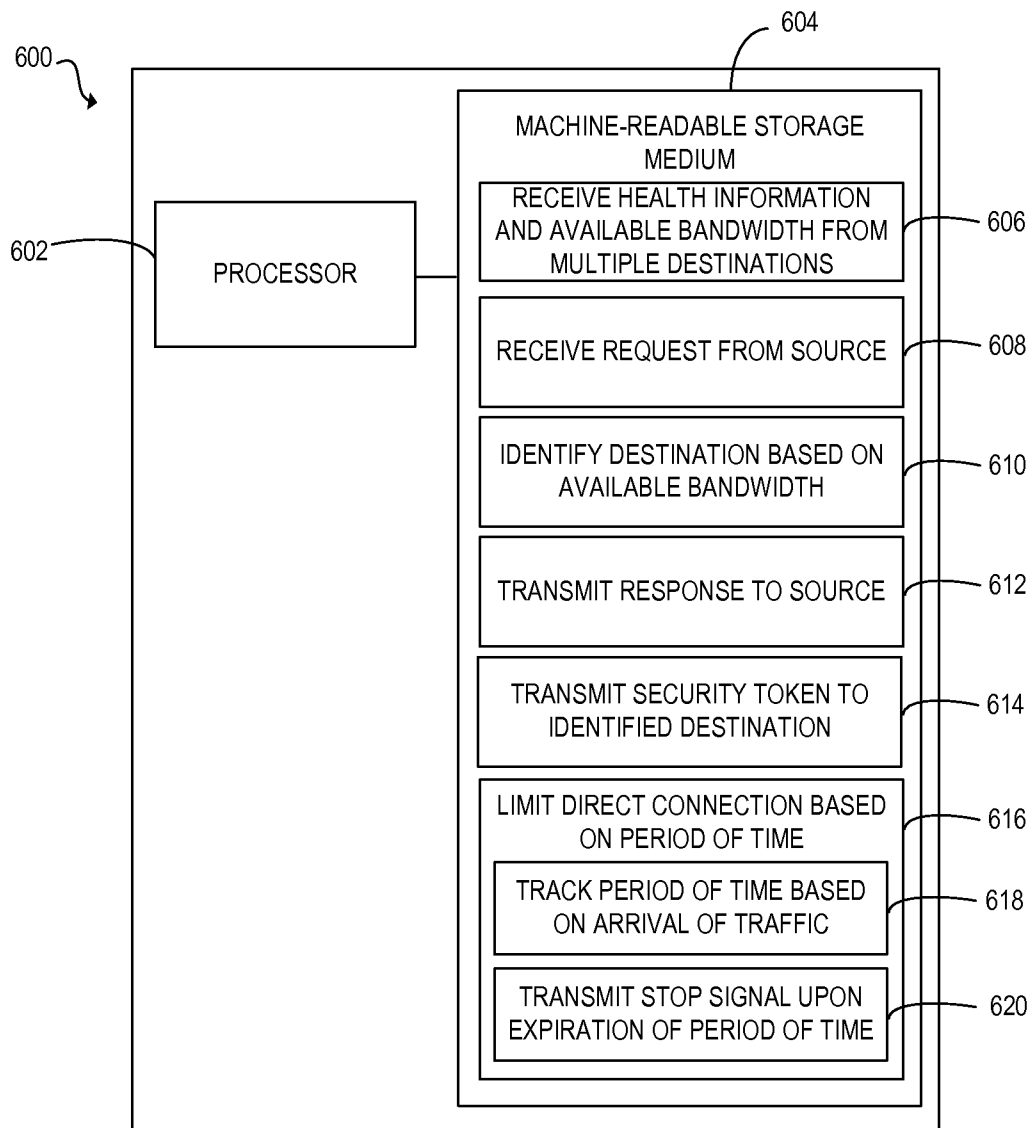
5/6

FIG. 5



6/6

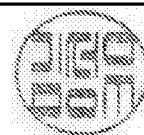
FIG. 6



INTERNATIONAL SEARCH REPORT

International application No.
PCT/US2015/058987

A. CLASSIFICATION OF SUBJECT MATTER H04L 29/06(2006.01)i, H04L 29/08(2006.01)i, H04L 12/803(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) H04L 29/06; G06F 9/54; G06F 15/173; H04L 12/911; H04L 29/00; G06F 9/50; H04L 29/08; H04L 12/803		
Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched Korean utility models and applications for utility models Japanese utility models and applications for utility models		
Electronic data base consulted during the international search (name of data base and, where practicable, search terms used) eKOMPASS(KIPO internal) & Keywords: direct connection, source, destination, key, period of time		
C. DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2014-0258534 A1 (MICROSOFT CORPORATION) 11 September 2014 See paragraphs [0003], [0012]-[0013], [0036], [0049]-[0055], [0065], [0073]; claims 1, 3, 9; and figures 1, 3.	9-11
Y A		1-8, 12-13, 15 14
Y	US 8625803 B1 (SIVASANKAR RADHAKRISHNAN et al.) 07 January 2014 See column 3, line 67 - column 4, line 2; column 6, lines 45-49; column 7, lines 61-63; claim 10; and figure 3.	1-8, 12-13, 15
A	EP 2916225 A1 (CRYTEK GMBH) 09 September 2015 See paragraphs [0052]-[0054], [0083]; and figures 1-2.	1-15
A	US 2014-0359698 A1 (AMAZON TECHNOLOGIES, INC.) 04 December 2014 See paragraphs [0052], [0056]-[0057]; and figures 9-10.	1-15
A	US 2003-0093560 A1 (HIDEAKI ONO et al.) 15 May 2003 See paragraphs [0085]-[0099]; and figures 11-12.	1-15
☐ 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 28 July 2016 (28.07.2016)	Date of mailing of the international search report 01 August 2016 (01.08.2016)	
Name and mailing address of the ISA/KR International Application Division Korean Intellectual Property Office 189 Cheongsa-ro, Seo-gu, Daejeon, 35208, Republic of Korea Facsimile No. +82-42-481-8578	Authorized officer KIM, Seong Woo Telephone No. +82-42-481-3348	



INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.

PCT/US2015/058987

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2014-0258534 A1	11/09/2014	WO 2014-137762 A1	12/09/2014
US 8625803 B1	07/01/2014	US 8995669 B1	31/03/2015
EP 2916225 A1	09/09/2015	None	
US 2014-0359698 A1	04/12/2014	US 8812727 B1	19/08/2014
US 2003-0093560 A1	15/05/2003	CN 100470516 C	18/03/2009
		CN 1416064 A	07/05/2003
		JP 2003-204350 A	18/07/2003
		JP 2008-160814 A	10/07/2008
		JP 4326764 B2	09/09/2009
		JP 4595997 B2	08/12/2010
		US 7711819 B2	04/05/2010