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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
25 April 2013 (25.04.2013)

WIPO | PCT

(10) International Publication Number
WO 2013/059744 A1

(51) International Patent Classification:
H04L 12/24 (2006.01) *H04L 12/859* (2013.01)
H04L 12/851 (2013.01)

(21) International Application Number:
PCT/US2012/061216

(22) International Filing Date:
19 October 2012 (19.10.2012)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
61/550,344 21 October 2011 (21.10.2011) US
13/655,399 18 October 2012 (18.10.2012) US

(71) Applicant: **QUALCOMM INCORPORATED** [US/US]; ATTN: International IP Administration, 5775 Morehouse Drive, San Diego, California 92121-1714 (US).

(72) Inventors: **DUNLAP, Wayne G.**; c/o QUALCOMM Incorporated, 5775 Morehouse Drive, San Diego, California 92121 (US). **MENCHACA, Benjamin M.**; c/o QUALCOMM Incorporated, 5775 Morehouse Drive, San Diego, California 92121 (US). **NOWAKOWSKI, Ryan A.**; c/o QUALCOMM Incorporated, 5775 Morehouse Drive, San Diego, California 92121 (US).

(74) Agents: **LEWIN, Mario J.** et al.; 15201 Mason Road, Suite 1000-312, Cypress, Texas 77433 (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, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

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

Published:

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

— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments (Rule 48.2(h))*

(54) **Title**: CLOUD COMPUTING ENHANCED GATEWAY FOR COMMUNICATION NETWORKS

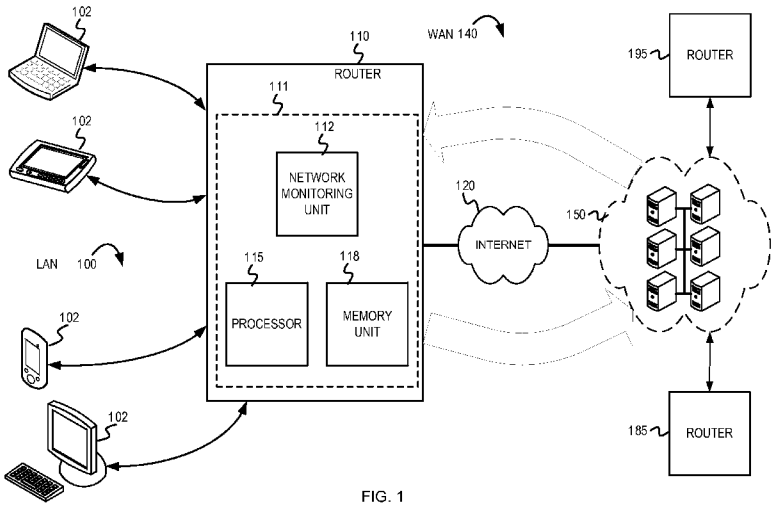

FIG. 1

(57) **Abstract**: A network traffic managing node of a local area network, such as a router or gateway, can monitor network traffic of the local area network. A network event associated with the local area network is detected using the network traffic managing node. The network event is reported from the network traffic managing node to one or more servers of a cloud-based computing network. A network policy update for the network traffic managing node is received from the cloud-based computing network. The network policy update is based, at least in part, on a type of network event reported to the cloud-based computing network. The network policy update is implemented at the network traffic managing node to process and/or resolve the network event.

WO 2013/059744 A1

CLOUD COMPUTING ENHANCED GATEWAY FOR COMMUNICATION NETWORKS

RELATED APPLICATIONS

[0001] This application claims the priority benefit of U.S. Provisional Application Serial No. 61/550,344 filed on Oct 21, 2011, and U.S. Application Serial No. 13/655,399 filed Oct 18, 2012.

BACKGROUND

[0002] Embodiments of the inventive subject matter generally relate to the field of communication networks and, more particularly, to a cloud computing enhanced gateway for communication networks.

[0003] Local area networks (LANs), such as home or office networks, typically include a router (or gateway) that connects the LAN to a wide area network (WAN) and routes packets between the two networks. Various network devices in a LAN can access and download information from the Internet via a router, and the router can manage the various packet streams from the different network devices accessing the Internet. The router of the LAN can also provide various network administrator options for configuring and customizing the operations of the router. However, network administrators typically have to manually configure the router based on the limited information known to the network administrator regarding the network traffic and network conditions.

SUMMARY

[0004] In some embodiments, a method comprises: monitoring network traffic of a local area network (LAN); detecting a network event associated with the LAN; reporting the network event to one or more servers of a cloud-based computing network; receiving a network policy update for the LAN from the one or more servers of the cloud-based computing network, wherein the network policy update is based, at least in part, on a type of network event reported to the one or more servers of the cloud-based computing network; and implementing the network policy update at the LAN.

[0005] In some embodiments, said monitoring, detecting, reporting, receiving, and implementing are performed by a network traffic managing node of the LAN.

[0006] In some embodiments, the network traffic managing node comprises a router of the LAN.

[0007] In some embodiments, the network traffic managing node comprises a computer system includes one or more of a router, an access point, a cable modem, and a network switch of the LAN.

[0008] In some embodiments, said detecting the network event associated with the LAN comprises at least one of detecting an oversubscription event at the LAN, detecting an unknown packet stream at the LAN, and detecting a network failure event at the LAN.

[0009] In some embodiments, said implementing the network policy update comprises implementing the network policy update after configuration of a network traffic managing node of the LAN to process and resolve the network event.

[0010] In some embodiments, said monitoring network traffic of the LAN comprises monitoring network traffic sent from one or more of a plurality of network devices of the LAN to a wide area network and monitoring network traffic sent from a remote network node of the wide area network to one or more of the plurality of network devices of the LAN.

[0011] In some embodiments, wherein the network policy update received from the one or more servers of the cloud-based computing network is based on the type of network event reported to the one or more servers of the cloud-based computing network and based on an analysis of aggregate data associated with the type of network event that is collected at the cloud-based computing network from a plurality of additional local area networks.

[0012] In some embodiments, further comprises detecting network activity associated with the LAN; reporting the network activity associated with the LAN to one or more servers of a cloud-based computing network; and receiving network alerts at the LAN from the cloud-based computing network.

[0013] In some embodiments, a method comprises: classifying a plurality of packet streams detected at a network traffic managing node of a local area network (LAN); detecting an

unknown packet stream at the network traffic managing node; selecting a default classification for the unknown packet stream; reporting information associated with the unknown packet stream from the network traffic managing node to one or more servers of a cloud-based computing network; receiving, at the network traffic managing node, a packet stream detection policy update for the unknown packet stream from the cloud-based computing network; and implementing the packet stream detection policy update at the network traffic managing node for subsequently detecting and classifying the unknown packet stream.

[0014] In some embodiments, said classifying the plurality of packet streams detected at the network traffic managing node comprises detecting packet stream characteristics associated with the plurality of packet streams; determining an application associated with each of the plurality of packet streams based, at least in part, on the corresponding packet stream characteristics; and classifying each of the plurality of packet streams based, at least in part, on the application associated with each of the packet streams.

[0015] In some embodiments, said classifying the plurality of packet streams detected at the network traffic managing node comprises classifying the plurality of packet streams based on at least one of an application associated with each of the plurality of packet streams and an application type associated with each of the plurality of packet streams.

[0016] In some embodiments, said detecting the unknown packet stream at the network traffic managing node and selecting the default classification for the unknown packet stream comprises determining that an application associated with a packet stream received at the network traffic managing node is unknown; and selecting the default classification for the unknown packet stream in response to determining the application is unknown.

[0017] In some embodiments, wherein said detecting the unknown packet stream at the network traffic managing node and selecting the default classification for the unknown packet stream comprises determining that an application associated with a packet stream received at the network traffic managing node is unknown; determining an application type associated with the unknown packet stream; and selecting the default classification for the unknown packet stream based on the application type associated with the unknown packet stream.

[0018] In some embodiments, said reporting information associated with the unknown packet stream from the network traffic managing node to one or more servers of a cloud-based computing network comprises reporting packet stream characteristics associated with the unknown packet stream.

[0019] In some embodiments, the method further comprises, in addition to receiving the packet stream detection policy update, receiving information indicating an application associated with the unknown packet stream and a classification for the unknown packet stream.

[0020] In some embodiments, said implementing the packet stream detection policy update at the network traffic managing node for subsequently detecting and classifying the unknown packet stream comprises detecting, at the network traffic managing node, packet stream characteristic associated with a previously unknown packet stream according to the packet stream detection policy update; determining an application associated with the packet stream characteristics according to the packet stream detection policy update; and selecting a classification for the previously unknown packet stream based on the application associated with the packet stream characteristics.

[0021] In some embodiments, a method comprises: receiving, at one or more servers of a cloud-based computing network, a report message from a router of a local area network (LAN) indicating a network event that was detected at the router; determining a type of network event that was detected by the router at the LAN; aggregating data associated with the type of network event reported by the router with data previously received from other routers that also detected the type of network event; analyzing the aggregate data associated with the type of network event; determining network policy updates associated with the type of network event based on results of the analysis of the aggregate data associated with the type of network event; and sending the network policy updates to the router of the LAN to configure the router with the network policy updates associated with the type of network event.

[0022] In some embodiments, said determining the type of network event that was detected by the router at the LAN comprises determining that the type of network event is one of an oversubscription event at the LAN, a detection of an unknown packet stream at the router, a receipt of a network analysis report from the router, and a detection of a network failure event at the LAN.

[0023] In some embodiments, the method further comprises sending commands to the router of the LAN based on results of the analysis of the aggregate data associated with the type of network event to request a temporary storage of content at the router.

[0024] In some embodiments, said determining network policy updates associated with the type of network event based on results of the analysis of the aggregate data associated with the type of network event comprises determining network policy updates for processing and resolving the type of network event detected at the router.

[0025] In some embodiments, a network router comprises one or more processors; and one or more memory units configured to store one or more instructions which, when executed by the one or more processors, causes the network router to perform operations that comprise: monitoring network traffic of a local area network (LAN); detecting a network event associated with the LAN; reporting the network event to one or more servers of a cloud-based computing network; receiving a network policy update for the network router from the one or more servers of the cloud-based computing network, wherein the network policy update is based, at least in part, on a type of network event reported to the one or more servers of the cloud-based computing network; and implementing the network policy update at the network router.

[0026] In some embodiments, the network event associated with the LAN comprises one of an oversubscription event at the LAN, an unknown packet stream received at the network router, and a network failure event at the LAN.

[0027] In some embodiments, the one or more instructions executed by the one or more processors causes the network router to perform operations that further comprise processing and resolving the network event by implementing the network policy update after configuration of the network router.

[0028] In some embodiments, the one or more instructions executed by the one or more processors causes the network router to perform operations that further comprise detecting network activity associated with the LAN; reporting the network activity associated with the LAN to one or more servers of a cloud-based computing network; and receiving network alerts at the network router from the cloud-based computing network.

[0029] In some embodiments, a network router comprises a processor; and a network monitoring unit coupled with the processor and configured to: classify a plurality of packet streams detected at the network router of a local area network (LAN); detect an unknown packet stream received at the network router; select a default classification for the unknown packet stream; report information associated with the unknown packet stream to one or more servers of a cloud-based computing network; receive, from the cloud-based computing network, a packet stream detection policy update for the unknown packet stream; and implement the packet stream detection policy update at the network router for subsequently detecting and classifying the unknown packet stream.

[0030] In some embodiments, the network monitoring unit configured to classify the plurality of packet streams detected at the network router comprises the network monitoring unit configured to detect packet stream characteristics associated with the plurality of packet streams; determine an application associated with each of the plurality of packet streams based, at least in part, on the corresponding packet stream characteristics; and classify each of the plurality of packet streams based, at least in part, on the application associated with each of the packet streams.

[0031] In some embodiments, the network monitoring unit configured to classify the plurality of packet streams detected at the network router comprises the network monitoring unit configured to classify the plurality of packet streams based on at least one of an application associated with each of the plurality of packet streams and an application type associated with each of the plurality of packet streams.

[0032] In some embodiments, the network monitoring unit configured to detect the unknown packet stream at the network traffic managing node and select the default classification for the unknown packet stream comprises the network monitoring unit configured to determine that an application associated with a packet stream received at the network router is unknown; and select the default classification for the unknown packet stream in response to determining the application is unknown.

[0033] In some embodiments, the network monitoring unit configured to detect the unknown packet stream at the network router and select the default classification for the unknown packet stream comprises the network monitoring unit configured to determine that an application

associated with a packet stream received at the network router is unknown; determine an application type associated with the unknown packet stream; and select the default classification for the unknown packet stream based on the application type associated with the unknown packet stream.

[0034] In some embodiments, the network monitoring unit configured to report information associated with the unknown packet stream to one or more servers of a cloud-based computing network comprises the network monitoring unit configured to report packet stream characteristics associated with the unknown packet stream.

[0035] In some embodiments, the network monitoring unit configured to implement the packet stream detection policy update at the network router for subsequent detection and classification of the unknown packet stream comprises the network monitoring unit configured to detect packet stream characteristic associated with a previously unknown packet stream according to the packet stream detection policy update; determine an application associated with the packet stream characteristics according to the packet stream detection policy update; and select a classification for the previously unknown packet stream based on the application associated with the packet stream characteristics.

[0036] In some embodiments, one or more machine-readable storage media having stored therein instructions, which when executed by one or more processors causes the one or more processors to perform operations that comprise: classifying a plurality of packet streams detected at a local area network (LAN); detecting an unknown packet stream at the LAN; selecting a default classification for the unknown packet stream; reporting information associated with the unknown packet stream to one or more servers of a cloud-based computing network; receiving a packet stream detection policy update for the unknown packet stream from the cloud-based computing network; and implementing the packet stream detection policy update for subsequently detecting and classifying the unknown packet stream.

[0037] In some embodiments, said operation of classifying the plurality of packet streams detected at the LAN comprises classifying the plurality of packet streams based on at least one of an application associated with each of the plurality of packet streams and an application type associated with each of the plurality of packet streams.

[0038] In some embodiments, said operations of detecting the unknown packet stream and selecting the default classification for the unknown packet stream comprises determining that an application associated with a packet stream received at LAN is unknown; and selecting the default classification for the unknown packet stream in response to determining the application is unknown.

[0039] In some embodiments, said operations of detecting the unknown packet stream and selecting the default classification for the unknown packet stream comprises determining that an application associated with a packet stream received at the LAN is unknown; determining an application type associated with the unknown packet stream; and selecting the default classification for the unknown packet stream based on the application type associated with the unknown packet stream.

BRIEF DESCRIPTION OF THE DRAWINGS

[0040] The present embodiments may be better understood, and numerous objects, features, and advantages made apparent to those skilled in the art by referencing the accompanying drawings.

[0041] **Figure 1** is an example block diagram illustrating a cloud computing enhanced router for a communication network, according to some embodiments;

[0042] **Figure 2** is a flow diagram illustrating example operations for implementing the cloud computing enhanced router for a local area network shown in Figure 1, according to some embodiments;

[0043] **Figure 3** is a flow diagram illustrating example operations for implementing the cloud computing enhanced router system shown in Figure 1, according to some embodiments;

[0044] **Figure 4** is a flow diagram illustrating example operations for implementing packet stream detection in the cloud computing enhanced router described in Figures 1-3, according to some embodiments; and

[0045] **Figure 5** is a block diagram of one embodiment of a network device including a mechanism for local area network routing, monitoring and cloud-based support, according to some embodiments.

DESCRIPTION OF EMBODIMENT(S)

[0046] The description that follows includes exemplary systems, methods, techniques, instruction sequences and computer program products that embody techniques of the present inventive subject matter. However, it is understood that the described embodiments may be practiced without these specific details. For instance, although examples refer to utilizing the cloud computing enhanced routers in home local area networks (LANs), in other examples the cloud computing enhanced routers can be used in any suitable type of network, such as an office network, a multi-dwelling network, a university network, etc. In other instances, well-known instruction instances, protocols, structures and techniques have not been shown in detail in order not to obfuscate the description.

[0047] Routers (or gateways) for communication networks are becoming increasingly complex. At the same time, competition is pushing to reduce the cost of routers. As a result, the processing power in home LAN routers today is not sufficient to leverage the sophisticated algorithms that would enhance the power of the routers, both from a performance point of view and a feature point of view. Furthermore, all routers inherently have a limited amount of available resources, such as processing power, storage, software, and other features.

[0048] **Figure 1** is an example block diagram illustrating a cloud computing enhanced router for a communication network, according to some embodiments. The LAN 100 comprises a plurality of network devices 102 and a router 110. The plurality of network devices 102 may include various type of wired and wireless networking devices, such as notebook computers, tablet computers, mobile phones, desktop computers, digital cameras, televisions, gaming consoles, smart appliances, and other suitable devices. The router 110 (or gateway) is a node in a communication network that receives and routes packets from and to the communication network. The router 110 is a network traffic managing node between two or more networks that receives, processes, and routes packets associated with the networks. It is noted, however, that in other embodiments the LAN 100 may include other types of network traffic managing nodes and/or network traffic managing nodes that are configured to perform various functions for the network(s), e.g., a server computer system that incorporates one or more of a cable modem, gateway/router, wireless access point, bridge, switch and/or storage, which may also implement the functionality describe herein with reference to Figures 1-5. As shown in Figure 1, the router 110 allows the network devices 102 of the LAN 100 to access the WAN 140 and receive content

from the WAN 140. The LAN 100 is one of many LANs that form the WAN 140, which is may be generally referred to as the Internet 120. As illustrated, the WAN 140 may also include various networks of servers (and other network devices and software). In one example, a network of servers can implement cloud computing on the Internet 120, which will be referenced herein as the cloud computing network 150 (or the cloud 150). The router 110 may allow the LAN 100 to obtain the benefit of various services provided by the cloud 150 via the Internet 120. Various other routers (e.g., routers 185 and 195) servicing other LANs can also connect to the cloud 150. Since all the routers are connected to the Internet, using cloud computing resources available at the cloud 150 to augment the routers can result in more sophisticated routers and also reduce the cost of the routers.

[0049] The cloud 150 may be configured to use the concept of crowdsourcing to collect statistics from various routers connected to the Internet 120 and refine the network management algorithms running in the routers, which can result in smarter "learning" routers that leverage the experience of all the other routers connected to the cloud 150. In some embodiments, the router 110 (and also various routers such as routers 185 and 195) can report various types of network events, statistical information and other network activity to the cloud 150. For example, as will be described further below, the router 110 can report information associated with packet streams that are received at the router that are unknown, and oversubscription events in the LAN 100 that are detected by the router. The cloud 150 can aggregate data associated with the network events reported by various routers and analyze the data to improve and update router policies and procedures (e.g., update the network management algorithms stored at the routers). The router 110 can also send network activity reports to the cloud 150 to allow the cloud to perform network analysis on the LAN 100 and send network alerts to the router. In addition to the router 110 reporting network activity, the router 110 can utilize storage at the cloud 150. The cloud 150 can monitor the network activity and storage utilization to personalize services and offer suggestions for the LAN 100 and the users of the LAN 100 (e.g., perform common file and software downloads during off-peak nighttime hours).

[0050] In some implementations, the router 110 may be configured to intelligently detect the applications generating and processing packet streams to and from the WAN 140 through the router 110. For example, the router 110 may detect a packet stream from a Netflix® video streaming application (e.g., implemented in a first network device 102) and a packet stream from

a file download application (e.g., bit torrent implemented in a second network device 102) actively sending packets through the router 110. In some examples, the servers that provided the video streaming service (or other content) can stream the video content to the LAN 100 via the router 110 and to a client application being executed at one of the network devices 102. However, in some cases, the router 110 may detect an unknown packet stream, or determine that a packet stream is unrecognizable. In other cases, a known application with known stream "fingerprints" or stream characteristics may change the packet streams it produces (i.e., change the stream characteristics), which can make a previously detectable packet stream undetectable. In one implementation, the router 110 can be configured to send information (e.g., stream characteristics) about all unknown packet streams to one or more servers of the cloud computing network 150. The cloud 150 can access the related aggregate data that has been collected from various other routers regarding unknown packet streams. Based on performing packet inspection and/or statistical analysis on the related aggregate data, and also based on continuously monitoring packet streams from various service providers on the Internet 120, the cloud 150 can intelligently identify the unknown packet streams. Then, the cloud 150 can download new detection rules to the router 110 (and also to the other routers such as router 185 and 195).

[0051] In some implementations, the router 110 may be configured with algorithms to detect the most common application packet streams (e.g., the top 100 applications) that are sent via the Internet. Any other unknown packet streams that pass through the router 100 can be sent to the cloud 150 for detection and identification. In one example, after the unknown packet information is sent to the cloud 150 for further analysis, the router 110 may temporarily assign the unknown packet stream a default classification. For example, although the router 110 may not be able to detect the specific application associated with the packet stream, the router 110 can determine the packet stream is streaming video and can temporarily assign a default classification for video traffic. In other words, even though the router 110 may not be able to detect the specific application, the router 110 may detect the application type (e.g., video traffic) and select a default classification for the unknown packet stream based on the application type. After the cloud 150 determines the new detection rules, the results can be sent back to the router 110 and the router 110 can implement the new detection rules to identify and process the packet stream appropriately. This creates a self-feedback loop where the router 110 runs the detection algorithms, collects statistics that are sent to the cloud 150, the statistics from various routers are

aggregated and analyzed at the cloud 150, and new detection algorithms are subsequently determined and sent out to all the routers.

[0052] In some implementations, the router 110 can also report oversubscription events in the LAN 100. The router 110 can report how the router handled different types of oversubscription events in the LAN 100. In one example, some users of the LAN 100 may initiate five different video streaming applications to simultaneously stream five movies from the WAN 140 through the router 110 and to the different network devices 102 of the LAN. In this situation, the network will likely not have the enough bandwidth to support the five different packet streams for the five difference video streaming applications, and therefore the router will detect an oversubscription event. The router 110 can implement one technique to resolve the oversubscription event and report the technique that was used and the results to the cloud 150. For example, the router 110 can determine to decrease the bandwidth of all the video streams by a certain percentage (e.g., 10-20%). The servers in the cloud 150 can use the aggregate data collected from other routers for a similar scenario, perform analysis, and determine there is better technique to handle the oversubscription event that the router 110 encountered. The servers in the cloud 150 can then provide the details regarding the new oversubscription resolution technique to the router 110, i.e., one or more servers of the cloud 150 can program the router 110 with a new algorithm to resolve that type of oversubscription event. For example, the cloud 150 may determine that instead of reducing the bandwidth of all five video streams by 15%, the router 110 should maintain an optimal bandwidth for 4 of the video streams, and reduce the bandwidth of one of the video streams to a minimum acceptable level.

[0053] In some implementations, the router 110 can also report some or all of the network activity to the cloud 150 and store most or all of the data in the cloud 150. In response to detecting reports and collecting data from the router 110, the cloud 150 can perform network analysis on the LAN 100 and also send network alerts. The cloud 150 can perform network analysis over weeks, months, and years, without the limitation that a local network router or other device would inherently have, such as limited resources and storage. In one example, based on the network activity reports, the cloud 150 can determine that a certain device or class of devices uses a disproportionate amount of bandwidth when the device is active (e.g., the device continuously transmits). The cloud 150 can monitor the LAN 100 and send a network alert when it detects the device is active and exhibiting such a behavior. In another example, the

cloud 150 can detect that the upstream traffic is overloaded, and send a network alert to the router 110 suggesting that the router 110 reduce the advertised available bandwidth in half (e.g., from 10mbps to 5mbps) to reduce the upstream traffic and potentially obtain better performance. It is noted that the router 110 can report other types of network events. In some cases, the router 110 can report network failures to the cloud 150, and the cloud 150 can determine resolution procedures based on the aggregate data and report the solution to the router 110 (e.g., configuration updates or new resolution procedure steps). In some implementations, since the cloud 150 is receiving most or all of the network activity and network events associated with the LAN 100 from the router 110, the cloud 150 can also offer other personalized services for the LAN 100. For example, the cloud 150 can detect that a software program (e.g., Adobe® Acrobat®) in one or more of the network devices 102 is configured for automatic updates (or the user regularly checks for updates). When the cloud 150 receives information from another router that a user is downloading an update, it can inform other routers that have updated the application in the past that an update is available and that the router should download it (e.g., temporarily store it in cache) when traffic is light (e.g., at off-peak hours). In another example, the cloud 150 can detect that one of the users downloads e-books from a certain author when the e-books are released. Based on this activity, the cloud 150 can automatically download the e-book to the local storage at the router 110 when the author releases a new e-book, so the user can access and download the e-book locally without using the WAN link.

[0054] As shown in Figure 1, in some embodiments, the router 110 may include a network monitoring unit 112, one or more processors 115, and a memory unit 118. The network monitoring unit 112, the one or more processors 115, and the memory unit 118 of the router 110 may be configured to implement the network event monitoring and reporting operations described herein, which operate in conjunction with the cloud computing network 150. In some embodiments, the one or more processors 115 of the router 110 can execute program instructions (e.g., stored in the memory unit 118) associated with the network monitoring unit 112 to implement the network event monitoring and reporting techniques described herein, such as the reporting of unknown packet streams and oversubscription events to the cloud 150 and the implementation of the new detection and resolution policies based on information obtained from the cloud 150. In some implementations, the router 110 may include a network interface card (or module) 111. The network interface card 111 may implement the network monitoring unit 112, the one or more processors 115, and a memory unit 118 (e.g., in one or more integrated circuits).

In other implementations, the router 110 may include a plurality of network interface cards and circuit boards (including network interface card 111), and the plurality of network interface cards may implement the network monitoring unit 112, the one or more processors 115, and a memory unit 118. Although not shown in Figure 1, in some implementations, the router 110 may include one or more additional processors and memory units (and other components) besides processor(s) 115 and memory unit 118. For example, the router 110 may include one or more processors and one or more memory units in one or more additional circuit boards.

[0055] **Figure 2** is a flow diagram ("flow") 200 illustrating example operations for implementing the cloud computing enhanced router for a local area network shown in Figure 1, according to some embodiments. The flow begins at block 202 of Figure 2.

[0056] At block 202, network traffic of a local area network is monitored using a router. For example, the network monitoring unit 112 of the router 110 (shown in Figure 1) monitors network traffic that is sent from one or more network devices 102 to the WAN 140 (e.g. file uploads), and network traffic that is received at the LAN 100 from the WAN (e.g., video streaming). In addition, the network monitoring unit 112 can monitor network traffic that is sent between the network devices 102 in the LAN 100. After block 202, the flow continues at block 204.

[0057] At block 204, one or more network events associated with the local area network are detected using the router. In some implementations, the network monitoring unit 112 detects one or more network events based on the network traffic of the LAN 100. As described above, in some examples, the network monitoring unit 112 may detect an unknown packet stream that is routed via the router 110 and/or detect an oversubscription event in the LAN 100. The network monitoring unit 112 may also detect other network events, such as network failures or disproportionate use of network bandwidth. After block 204, the flow continues at block 206.

[0058] At block 206, the one or more network events are reported from the router to a cloud computing network. In some implementations, the network monitoring unit 112 may report the one or more network events from router 110 to one or more servers of the cloud computing network 150. In some implementations, instead of reporting all network events or network activities to the cloud computing network 150, the router 110 can be configured to report certain network events ("predefined network events"). For example, the router 110 may be configured

to report only oversubscription events and unknown packet streams to the cloud 150. After block 206, the flow continues at block 208.

[0059] At block 208, a network policy update for the router is received from the one or more servers of the cloud-based computing network. The network policy update is based, at least in part, on a type of network event reported to the one or more servers of the cloud-based computing network. In some implementations, the router 110 receives the network policy update from the cloud 150. The network policy update that is received is based, at least in part, on the type of network event that was reported to the cloud 150. For example, the cloud 150 may determine the network policy update based on the type of network event that was reported and based on results of an analysis that is performed on aggregate data associated with the same type of network event collected from a plurality of local area networks of the WAN 140, as will be further described below with reference to Figure 3. For example, if the network event reported by the router 110 is an unknown packet stream detected at the router 110, the cloud 150 performs an analysis on aggregate data that has been collected from the LAN 100 and from other local area networks in the WAN 140 that also have detected some of the same packet stream characteristics in an unknown packet stream. From the aggregate data, the cloud 150 can determine new packet stream detection policies based on the characteristics of the unknown packet stream for future detection and identification of the unknown packet stream. The cloud 150 can then send the new packet stream detection policies to the router 110 to update the stream detection policies being implemented at the router 110. After block 208, the flow continues at block 210.

[0060] At block 210, the network policy update is implemented at the network traffic managing node after configuration. In some implementations, the network monitoring unit 112 is configured with the network policy update and then implements the network policy update at the router 110 when detecting and processing network events of the LAN 100. For example, in the unknown packet stream example, the network monitoring unit 112 can be updated to implement the new packet stream detection policies received from the cloud 150 for packet stream detection and identification. After block 210, the flow ends.

[0061] **Figure 3** is a flow diagram ("flow") 300 illustrating example operations for implementing the cloud computing enhanced router system shown in Figure 1, according to some embodiments. The flow begins at block 302 of Figure 3.

[0062] At block 302, one or more servers of the cloud computing network 150 receive report messages from the router 110 indicating network events that were detected in the LAN 100. For example, as was previously described above, the router 110 can determine one of the packet streams being routed is unknown, and can send information associated with the unknown packet stream to the cloud 150. As another example, the router 110 can detect an oversubscription event at the LAN 100 and send a report to the cloud 150 indicating the technique that was implemented to attempt to resolve the oversubscription event. In the report, the router 110 can also indicate whether that particular technique was successful in resolving the oversubscription event and the specific results of technique. After block 302, the flow continues at block 304.

[0063] At block 304, the cloud computing network 150 determines the type of network event associated with the report messages received from the router 110. For example, the cloud 150 determines that the report message is associated with an unknown packet stream that was received at the router 110, or that the report message is associated with an oversubscription event detected at the LAN 100. It is noted, however, that the report message may indicate various other network events, as was described above with reference to Figure 1 (e.g., a network failure report). After block 304, the flow continues at block 306.

[0064] At block 306, the cloud computing network 150 aggregates the data associated with the reported network events with data previously received from other routers in other local area networks for detected network events of the same or similar type. For example, the cloud 150 aggregates all the information (e.g., packet stream characteristics) associated with unknown packet streams that have been reported by various routers. As another example, the cloud 150 aggregates all the data (e.g., resolution techniques used and results) associated with oversubscription events of the same or similar type that are reported by various routers. After block 306, the flow continues at block 308.

[0065] At block 308, the cloud computing network 150 analyzes the aggregated data associated with the reported network events of the same or similar type. For example, the cloud 150 analyzes the aggregated data associated with the unknown packet streams that have been

reported by various routers in other local area networks. In one example, the cloud 150 can perform deep packet inspection and statistical analysis on the aggregated data associated with the unknown packet streams, and can analyze the different stream characteristics associated with the unknown packet streams. At the same time, the cloud 150 can continuously monitor packet streams from various service providers on the Internet 120, and identify any changes in the corresponding packet streams, in order to help identify the unknown packet streams. In another example, the cloud 150 can analyze the aggregated data associated with various oversubscription events that have been reported by various routers. The cloud 150 can examine the various techniques used to resolve the oversubscription event and compare the results of implementing the different techniques. After block 308, the flow continues at block 310.

[0066] At block 310, the cloud computing network 150 determines improved network policies or procedures for handling the detected network events and sends the updated network policies or procedures to the router 110 of the LAN 100 to update router configurations. For example, based on the analysis performed in block 308 above, the cloud 150 can determine improved packet stream detection policies (e.g., updated stream characteristic criteria) for detecting the packet streams or can determine improved resolution policies for handling the oversubscription event. After block 310, the flow ends.

[0067] In some implementation, the cloud computing network 150 determines and sends the network policy updates to the router 110 in real time. For example, if the cloud computing network 150 has aggregated sufficient data from the various routers in the WAN 140, and has performed the analysis of the aggregate data, the cloud computing network 150 can send the network policy updates to the router 110 in real time when the router 110 reports the network event. As a result, the router 110 can implement the network policy updates in real time to process and/or resolve the reported network event in real time. In some implementations, after receiving the report message(s) associated with a network event from the router 110, the cloud computing network 150 can continue aggregating additional data associated with the network event from other routers in the WAN 140, and/or may perform additional analysis on the aggregated data. For example, the cloud computing network 150 may determine that it needs to crowd source additional data and/or perform additional analysis in order to determine an improved network policy for the network event. In this example, the cloud computing network 150 would not send the network policy update to the router 110 in real time. Instead, the cloud

computing network 150 would send the network policy update at a later time, and the router 110 would implement the network policy update to process and/or resolve the next occurrence of the network event.

[0068] **Figure 4** is a flow diagram ("flow") 400 illustrating example operations for implementing packet stream detection in the cloud computing enhanced router described in Figures 1-3, according to some embodiments. The flow begins at block 402 of Figure 4.

[0069] At block 402, a plurality of packet streams detected at a router of a local area network are classified. In some implementations, the network monitoring unit 112 of the router 110 (shown in Figure 1) monitors network traffic, detects the plurality of packet streams, and classifies the packet streams. For example, after detecting characteristic and statistics of a packet stream (e.g., using deep packet inspection), the network monitoring unit 112 can determine the application associated with the packet stream and classify the packet stream based on the associated application. In one example, if the packet stream characteristics and statistics indicate the packet stream is distributed from the Netflix® video streaming service, the network monitoring unit 112 classifies the packet stream as a Netflix® application packet stream. After block 402, the flow continues at block 404.

[0070] At block 404, an unknown packet stream is detected at the router. In some implementations, the network monitoring unit 112 detects the packet stream characteristics and statistics, compares the packet stream characteristics and statistics to known packet streams, and determines the packet stream is an unknown packet stream with unknown packet stream characteristics and statistics. After block 404, the flow continues at block 406.

[0071] At block 406, a default classification for the unknown packet stream is selected. In some implementations, even though the network monitoring unit 112 cannot determine the specific application associated with the unknown packet stream, the network monitoring unit 112 may select a default classification based on the application type (e.g., streaming video or audio) associated with the unknown packet stream. For example, the application type of the unknown packet stream may be determined as streaming video or streaming audio, and a default classification maybe assigned to the unknown packet stream based on the application type. In some implementations, the network monitoring unit 112 may not be able to determine both the specific application and the application type associated with an unknown packet stream, and

therefore may temporarily select a default classification for a packet streams with an unknown application and application type. The default classification may be temporarily assigned to allow the unknown packet stream to be processed by the router 110 until the specific application can be determined. For example, the default classification may assign the unknown packet stream minimum and maximum bandwidth requirements and, in some cases, a priority value. In one example, if a default classification is selected for the unknown packet stream based on video streaming as the application type, the default classification assigns minimum and maximum bandwidth requirements that are typical for video streaming applications (e.g., average bandwidth numbers for video streaming applications). After block 406, the flow continues at block 408.

[0072] At block 408, information associated with the unknown packet stream is reported to one or more servers of a cloud computing network. In some implementations, the network monitoring unit 112 can send a report message indicating the packet stream characteristics and statistics associated with the unknown packet stream from the router 110 to the cloud 150 via the Internet. After block 408, the flow continues at block 410.

[0073] At block 410, an updated packet stream detection policy is received from the cloud computing network. In some implementations, the network monitoring unit 112 can receive an updated packet stream detection policy from the cloud 150 that can be used for detecting and classifying the previously unknown packet stream. In one example, the cloud 150 performs an analysis on aggregate data that has been collected from the router 110 and from other local area networks in the WAN 140 that also have detected some of the same packet stream characteristics and statistics in an unknown packet stream. The cloud also continues to collect packet stream characteristics and statistics from service providers and applications in the Internet. From the aggregate data, the cloud 150 can determine new packet stream detection policies based on the characteristics and statistics of the unknown packet stream for future identification and classification of the unknown packet stream. For example, the cloud 150 may determine that the unknown packet stream is from a new audio streaming service that was recently brought online after comparing the packet stream characteristics and statistics from the new audio streaming service with the packet stream characteristics and statistics aggregated by the cloud 150. In another example, the cloud 150 can determine that an existing video streaming service changed

the packet stream characteristics and statistics associated with its service and applications. After block 410, the flow continues at block 412.

[0074] At block 412, the updated packet stream detection policy is implemented at the router. In some implementations, the network monitoring unit 112 implements the updated packet stream detection policy after the router 110 is configured with the new policy. The updated packet stream detection policy can be used for subsequent detection and classification of the previously unknown packet stream. After flow 412, the flow ends.

[0075] It should be understood that Figures 1 – 5 and the operations described herein are examples meant to aid in understanding embodiments and should not be used to limit embodiments or limit scope of the claims. Embodiments may perform additional operations, fewer operations, operations in a different order, operations in parallel, and some operations differently.

[0076] As will be appreciated by one skilled in the art, aspects of the present inventive subject matter may be embodied as a system, method, or computer program product. Accordingly, aspects of the present inventive subject matter may take the form of an entirely hardware embodiment, a software embodiment (including firmware, resident software, micro-code, etc.) or an embodiment combining software and hardware aspects that may all generally be referred to herein as a "circuit," "module" or "system." Furthermore, aspects of the present inventive subject matter may take the form of a computer program product embodied in one or more computer readable medium(s) having computer readable program code embodied thereon.

[0077] Any combination of one or more computer readable medium(s) may be utilized. The computer readable medium may be a computer readable signal medium or a computer readable storage medium. A computer readable storage medium may be, for example, but not limited to, an electronic, magnetic, optical, electromagnetic, infrared, or semiconductor system, apparatus, or device, or any suitable combination of the foregoing. More specific examples (a non-exhaustive list) of the computer readable storage medium would include the following: an electrical connection having one or more wires, a portable computer diskette, a hard disk, a random access memory (RAM), a read-only memory (ROM), an erasable programmable read-only memory (EPROM or Flash memory), an optical fiber, a portable compact disc read-only memory (CD-ROM), an optical storage device, a magnetic storage device, or any suitable

combination of the foregoing. In the context of this document, a computer readable storage medium may be any tangible medium that can contain, or store a program for use by or in connection with an instruction execution system, apparatus, or device. A computer readable signal medium may include a propagated data signal with computer readable program code embodied therein, for example, in baseband or as part of a carrier wave. Such a propagated signal may take any of a variety of forms, including, but not limited to, electro-magnetic, optical, or any suitable combination thereof. A computer readable signal medium may be any computer readable medium that is not a computer readable storage medium and that can communicate, propagate, or transport a program for use by or in connection with an instruction execution system, apparatus, or device. Program code embodied on a computer readable medium may be transmitted using any appropriate medium, including but not limited to wireless, wireline, optical fiber cable, RF, etc., or any suitable combination of the foregoing.

[0078] Computer program code for carrying out operations for aspects of the present inventive subject matter may be written in any combination of one or more programming languages, including an object oriented programming language such as Java, Smalltalk, C++ or the like and conventional procedural programming languages, such as the "C" programming language or similar programming languages. The program code may execute entirely on the user's computer, partly on the user's computer, as a stand-alone software package, partly on the user's computer and partly on a remote computer or entirely on the remote computer or server. In the latter scenario, the remote computer may be connected to the user's computer through any type of network, including a local area network (LAN) or a wide area network (WAN), or the connection may be made to an external computer (for example, through the Internet using an Internet Service Provider).

[0079] Aspects of the present inventive subject matter are described with reference to flowchart illustrations and/or block diagrams of methods, apparatus (systems) and computer program products according to embodiments of the inventive subject matter. It will be understood that each block of the flowchart illustrations and/or block diagrams, and combinations of blocks in the flowchart illustrations and/or block diagrams, can be implemented by computer program instructions. These computer program instructions may be provided to a processor of a general purpose computer, special purpose computer, or other programmable data processing apparatus to produce a machine, such that the instructions, which execute via the

processor of the computer or other programmable data processing apparatus, create means for implementing the functions/acts specified in the flowchart and/or block diagram block or blocks.

[0080] These computer program instructions may also be stored in a computer readable medium that can direct a computer, other programmable data processing apparatus, or other devices to function in a particular manner, such that the instructions stored in the computer readable medium produce an article of manufacture including instructions which implement the function/act specified in the flowchart and/or block diagram block or blocks.

[0081] The computer program instructions may also be loaded onto a computer, other programmable data processing apparatus, or other devices to cause a series of operational steps to be performed on the computer, other programmable apparatus or other devices to produce a computer implemented process such that the instructions which execute on the computer or other programmable apparatus provide processes for implementing the functions/acts specified in the flowchart and/or block diagram block or blocks.

[0082] **Figure 5** is a block diagram of one embodiment of a network device 500 including a mechanism for local area network monitoring and cloud-based support in a wide area network, according to some embodiments. In some implementations, the network device 500 is a network traffic managing node between two or more networks (e.g., a LAN and a WAN) that receives, processes, and routes packets associated with the networks; for example, the network traffic managing node may be a router/gateway of a LAN (e.g., LAN 100 shown in Figure 1). It is noted, however, that in other implementations the network device 500 may be other suitable types of network devices that can be configured to implement the functionality described above with reference to Figures 1-4, such as a cable modem, a wireless access point, a network bridge, a network switch, a desktop computer, a gaming console, a mobile computing device, etc. The network device 500 includes a processor unit 502 (possibly including multiple processors, multiple cores, multiple nodes, and/or implementing multi-threading, etc.). The network device 500 includes a memory unit 506. The memory unit 506 may be system memory (e.g., one or more of cache, SRAM, DRAM, zero capacitor RAM, Twin Transistor RAM, eDRAM, EDO RAM, DDR RAM, EEPROM, NRAM, RRAM, SONOS, PRAM, etc.) or any one or more of the above already described possible realizations of machine-readable storage media. The network device 500 also includes a bus 510 (e.g., PCI, ISA, PCI-Express, HyperTransport®,

InfiniBand®, NuBus, AHB, AXI, etc.), and network interface(s) 508 that include at least one of a wireless network interface (e.g., a Bluetooth interface, a WLAN 802.11 interface, a WiMAX interface, a ZigBee® interface, a Wireless USB interface, etc.) and a wired network interface (e.g., an Ethernet interface, a powerline communication interface, etc.). As illustrated, the network interface(s) 508 also includes a network monitoring unit 512. For example, the network monitoring unit 512 may be implemented within a network interface card or network interface module of the network interface(s) 508. The network monitoring unit 512 may be operable to implement the mechanism for network traffic monitoring, network event detection, and cloud-based access and support (among other features) for the network device 500, as describe above with reference to Figures 1-4.

[0083] Any one of these functionalities may be partially (or entirely) implemented in hardware and/or on the processor unit 502. For example, the functionality may be implemented with one or more application specific integrated circuits, one or more system-on-a-chip (SoC), or other type of integrated circuit(s), in logic implemented in the processor unit 502, in a co-processor on a peripheral device or card, in a separate processor and/or memory implemented within the network interface 508, etc. Further, realizations may include fewer or additional components not illustrated in Figure 5 (e.g., video cards, audio cards, additional network interfaces, peripheral devices, etc.). The processor unit 502, the memory unit 506, and the network interfaces 508 are coupled to the bus 510. Although illustrated as being coupled to the bus 510, the memory unit 506 may be coupled to the processor unit 502.

[0084] While the embodiments are described with reference to various implementations and exploitations, it will be understood that these embodiments are illustrative and that the scope of the inventive subject matter is not limited to them. In general, techniques for implementing cloud computing enhanced routers for communication networks as described herein may be implemented with facilities consistent with any hardware system or hardware systems. Many variations, modifications, additions, and improvements are possible.

[0085] Plural instances may be provided for components, operations or structures described herein as a single instance. Finally, boundaries between various components, operations and data stores are somewhat arbitrary, and particular operations are illustrated in the context of specific illustrative configurations. Other allocations of functionality are envisioned and may

fall within the scope of the inventive subject matter. In general, structures and functionality presented as separate components in the exemplary configurations may be implemented as a combined structure or component. Similarly, structures and functionality presented as a single component may be implemented as separate components. These and other variations, modifications, additions, and improvements may fall within the scope of the inventive subject matter.

CLAIMS

1. A method comprising:
monitoring network traffic of a local area network (LAN);
detecting a network event associated with the LAN;
reporting the network event to one or more servers of a cloud-based computing network;
receiving a network policy update for the LAN from the one or more servers of the cloud-based computing network, wherein the network policy update is based, at least in part, on a type of network event reported to the one or more servers of the cloud-based computing network; and
implementing the network policy update at the LAN.

2. The method of claim 1, wherein said monitoring, detecting, reporting, receiving, and implementing are performed by a network traffic managing node of the LAN.

3. The method of claim 2, wherein the network traffic managing node comprises a router of the LAN.

4. The method of claim 2, wherein the network traffic managing node comprises a computer system including one or more of a router, an access point, a cable modem, and a network switch of the LAN.

5. The method of claim 1, wherein said detecting the network event associated with the LAN comprises at least one of detecting an oversubscription event at the LAN, detecting an unknown packet stream at the LAN, and detecting a network failure event at the LAN.

6. The method of claim 1, wherein said implementing the network policy update comprises implementing the network policy update after configuration of a network traffic managing node of the LAN to process and resolve the network event.

7. The method of claim 1, wherein said monitoring network traffic of the LAN comprises monitoring network traffic sent from one or more of a plurality of network devices of the LAN to a wide area network and monitoring network traffic sent from a remote network

node of the wide area network to one or more of the plurality of network devices of the LAN.

8. The method of claim 1, wherein the network policy update received from the one or more servers of the cloud-based computing network is based on the type of network event reported to the one or more servers of the cloud-based computing network and based on an analysis of aggregate data associated with the type of network event that is collected at the cloud-based computing network from a plurality of additional local area networks.

9. The method of claim 1, further comprising:
detecting network activity associated with the LAN;
reporting the network activity associated with the LAN to one or more servers of a cloud-based computing network; and
receiving network alerts at the LAN from the cloud-based computing network.

10. A method comprising:
classifying a plurality of packet streams detected at a network traffic managing node of a local area network (LAN);
detecting an unknown packet stream at the network traffic managing node;
selecting a default classification for the unknown packet stream;
reporting information associated with the unknown packet stream from the network traffic managing node to one or more servers of a cloud-based computing network;
receiving, at the network traffic managing node, a packet stream detection policy update for the unknown packet stream from the cloud-based computing network; and
implementing the packet stream detection policy update at the network traffic managing node for subsequently detecting and classifying the unknown packet stream.

11. The method of claim 10, wherein said classifying the plurality of packet streams detected at the network traffic managing node comprises:
detecting packet stream characteristics associated with the plurality of packet streams;
determining an application associated with each of the plurality of packet streams based, at least in part, on the corresponding packet stream characteristics; and

classifying each of the plurality of packet streams based, at least in part, on the application associated with each of the packet streams.

12. The method of claim 10, wherein said classifying the plurality of packet streams detected at the network traffic managing node comprises classifying the plurality of packet streams based on at least one of an application associated with each of the plurality of packet streams and an application type associated with each of the plurality of packet streams.

13. The method of claim 10, wherein said detecting the unknown packet stream at the network traffic managing node and selecting the default classification for the unknown packet stream comprises:

determining that an application associated with a packet stream received at the network traffic managing node is unknown; and

selecting the default classification for the unknown packet stream in response to determining the application is unknown.

14. The method of claim 10, wherein said detecting the unknown packet stream at the network traffic managing node and selecting the default classification for the unknown packet stream comprises:

determining that an application associated with a packet stream received at the network traffic managing node is unknown;

determining an application type associated with the unknown packet stream; and

selecting the default classification for the unknown packet stream based on the application type associated with the unknown packet stream.

15. The method of claim 10, wherein said reporting information associated with the unknown packet stream from the network traffic managing node to one or more servers of a cloud-based computing network comprises reporting packet stream characteristics associated with the unknown packet stream.

16. The method of claim 10, further comprising, in addition to receiving the packet stream detection policy update, receiving information indicating an application associated with the unknown packet stream and a classification for the unknown packet stream.

17. The method of claim 10, wherein said implementing the packet stream detection policy update at the network traffic managing node for subsequently detecting and classifying the unknown packet stream comprises:

detecting, at the network traffic managing node, packet stream characteristic associated with a previously unknown packet stream according to the packet stream detection policy update;

determining an application associated with the packet stream characteristics according to the packet stream detection policy update; and

selecting a classification for the previously unknown packet stream based on the application associated with the packet stream characteristics.

18. A method comprising:

receiving, at one or more servers of a cloud-based computing network, a report message from a router of a local area network (LAN) indicating a network event that was detected at the router;

determining a type of network event that was detected by the router at the LAN;

aggregating data associated with the type of network event reported by the router with data previously received from other routers that also detected the type of network event;

analyzing the aggregate data associated with the type of network event;

determining network policy updates associated with the type of network event based on results of the analysis of the aggregate data associated with the type of network event; and

sending the network policy updates to the router of the LAN to configure the router with the network policy updates associated with the type of network event.

19. The method of claim 18, wherein said determining the type of network event that was detected by the router at the LAN comprises determining that the type of network event is one of an oversubscription event at the LAN, a detection of an unknown packet stream at

the router, a receipt of a network analysis report from the router, and a detection of a network failure event at the LAN.

20. The method of claim 18, further comprising sending commands to the router of the LAN based on results of the analysis of the aggregate data associated with the type of network event to request a temporary storage of content at the router.

21. The method of claim 18, wherein said determining network policy updates associated with the type of network event based on results of the analysis of the aggregate data associated with the type of network event comprises determining network policy updates for processing and resolving the type of network event detected at the router.

22. A network router comprising:
one or more processors; and
one or more memory units configured to store one or more instructions which, when executed by the one or more processors, causes the network router to perform operations that comprise:
monitoring network traffic of a local area network (LAN);
detecting a network event associated with the LAN;
reporting the network event to one or more servers of a cloud-based computing network;
receiving a network policy update for the network router from the one or more servers of the cloud-based computing network, wherein the network policy update is based, at least in part, on a type of network event reported to the one or more servers of the cloud-based computing network; and
implementing the network policy update at the network router.

23. The network router of claim 22, wherein the network event associated with the LAN comprises one of an oversubscription event at the LAN, an unknown packet stream received at the network router, and a network failure event at the LAN.

24. The network router of claim 22, wherein the one or more instructions executed by the one or more processors causes the network router to perform operations that further comprise

processing and resolving the network event by implementing the network policy update after configuration of the network router.

25. The network router of claim 22, wherein the one or more instructions executed by the one or more processors causes the network router to perform operations that further comprise:
detecting network activity associated with the LAN;
reporting the network activity associated with the LAN to one or more servers of a cloud-based computing network; and
receiving network alerts at the network router from the cloud-based computing network.

26. A network router comprising:
a processor; and
a network monitoring unit coupled with the processor and configured to:
classify a plurality of packet streams detected at the network router of a local area network (LAN);
detect an unknown packet stream received at the network router;
select a default classification for the unknown packet stream;
report information associated with the unknown packet stream to one or more servers of a cloud-based computing network;
receive, from the cloud-based computing network, a packet stream detection policy update for the unknown packet stream; and
implement the packet stream detection policy update at the network router for subsequently detecting and classifying the unknown packet stream.

27. The network router of claim 26, wherein the network monitoring unit configured to classify the plurality of packet streams detected at the network router comprises the network monitoring unit configured to:
detect packet stream characteristics associated with the plurality of packet streams;
determine an application associated with each of the plurality of packet streams based, at least in part, on the corresponding packet stream characteristics; and
classify each of the plurality of packet streams based, at least in part, on the application associated with each of the packet streams.

28. The network router of claim 26, wherein the network monitoring unit configured to classify the plurality of packet streams detected at the network router comprises the network monitoring unit configured to classify the plurality of packet streams based on at least one of an application associated with each of the plurality of packet streams and an application type associated with each of the plurality of packet streams.

29. The network router of claim 26, wherein the network monitoring unit configured to detect the unknown packet stream at the network traffic managing node and select the default classification for the unknown packet stream comprises the network monitoring unit configured to:

determine that an application associated with a packet stream received at the network router is unknown; and

select the default classification for the unknown packet stream in response to determining the application is unknown.

30. The network router of claim 26, wherein the network monitoring unit configured to detect the unknown packet stream at the network router and select the default classification for the unknown packet stream comprises the network monitoring unit configured to:

determine that an application associated with a packet stream received at the network router is unknown;

determine an application type associated with the unknown packet stream; and

select the default classification for the unknown packet stream based on the application type associated with the unknown packet stream.

31. The network router of claim 26, wherein the network monitoring unit configured to report information associated with the unknown packet stream to one or more servers of a cloud-based computing network comprises the network monitoring unit configured to report packet stream characteristics associated with the unknown packet stream.

32. The network router of claim 26, wherein the network monitoring unit configured to implement the packet stream detection policy update at the network router for subsequent

detection and classification of the unknown packet stream comprises the network monitoring unit configured to:

detect packet stream characteristic associated with a previously unknown packet stream according to the packet stream detection policy update;

determine an application associated with the packet stream characteristics according to the packet stream detection policy update; and

select a classification for the previously unknown packet stream based on the application associated with the packet stream characteristics.

33. One or more machine-readable storage media having stored therein instructions, which when executed by one or more processors causes the one or more processors to perform operations that comprise:

classifying a plurality of packet streams detected at a local area network (LAN);

detecting an unknown packet stream at the LAN;

selecting a default classification for the unknown packet stream;

reporting information associated with the unknown packet stream to one or more servers of a cloud-based computing network;

receiving a packet stream detection policy update for the unknown packet stream from the cloud-based computing network; and

implementing the packet stream detection policy update for subsequently detecting and classifying the unknown packet stream.

34. The machine-readable storage media of claim 33, wherein said operation of classifying the plurality of packet streams detected at the LAN comprises classifying the plurality of packet streams based on at least one of an application associated with each of the plurality of packet streams and an application type associated with each of the plurality of packet streams.

35. The machine-readable storage media of claim 33, wherein said operations of detecting the unknown packet stream and selecting the default classification for the unknown packet stream comprises:

determining that an application associated with a packet stream received at LAN is unknown; and

selecting the default classification for the unknown packet stream in response to determining the application is unknown.

36. The machine-readable storage media of claim 33, wherein said operations of detecting the unknown packet stream and selecting the default classification for the unknown packet stream comprises:

determining that an application associated with a packet stream received at the LAN is unknown;

determining an application type associated with the unknown packet stream; and

selecting the default classification for the unknown packet stream based on the application type associated with the unknown packet stream.

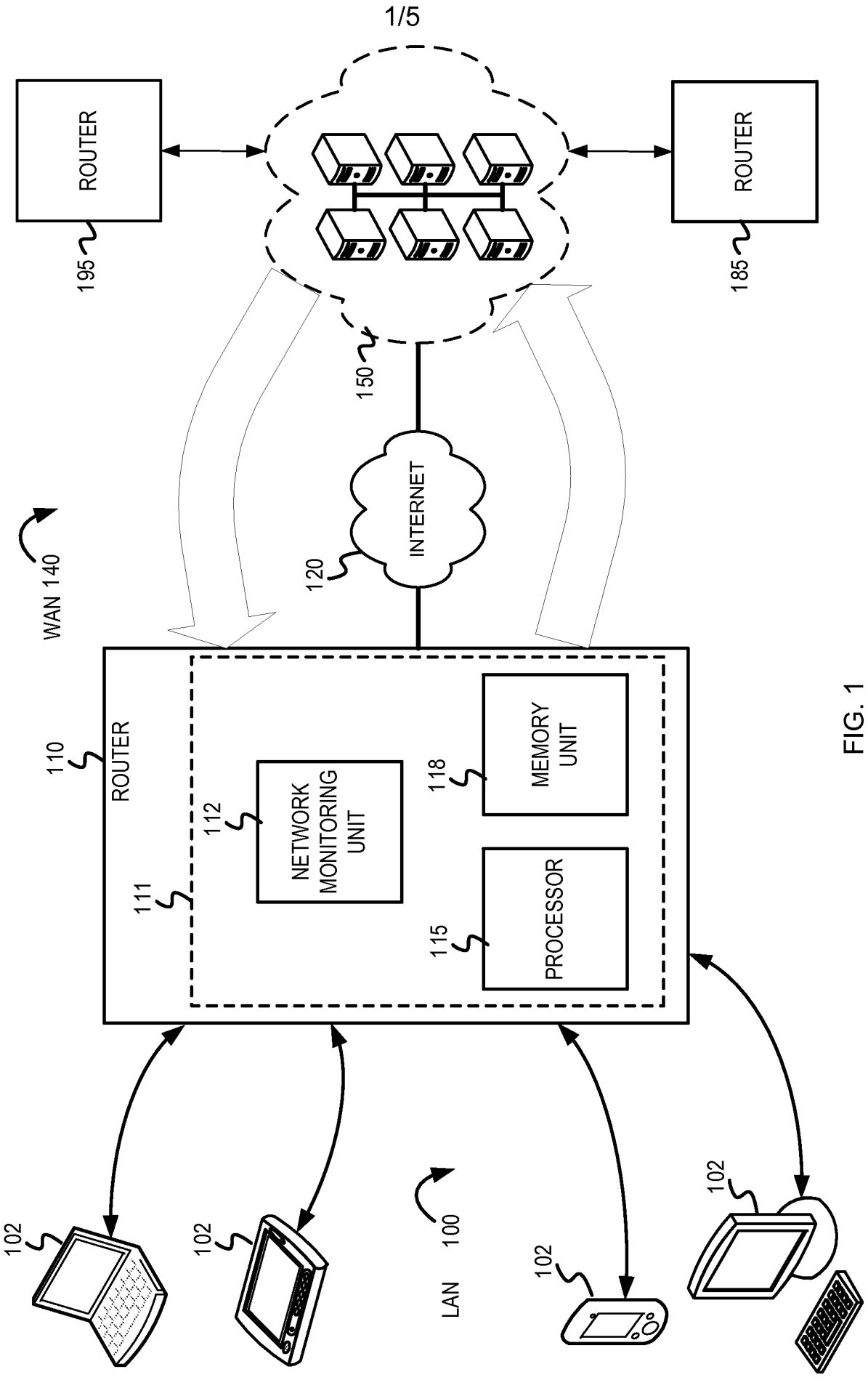
ROUTER
195
ROUTER
185
150
INTERNET
120
WAN 140
110
ROUTER
111
NETWORK MONITORING UNIT
112
MEMORY UNIT
118
PROCESSOR
115
LAN 100
102
102
102
102

FIG. 1

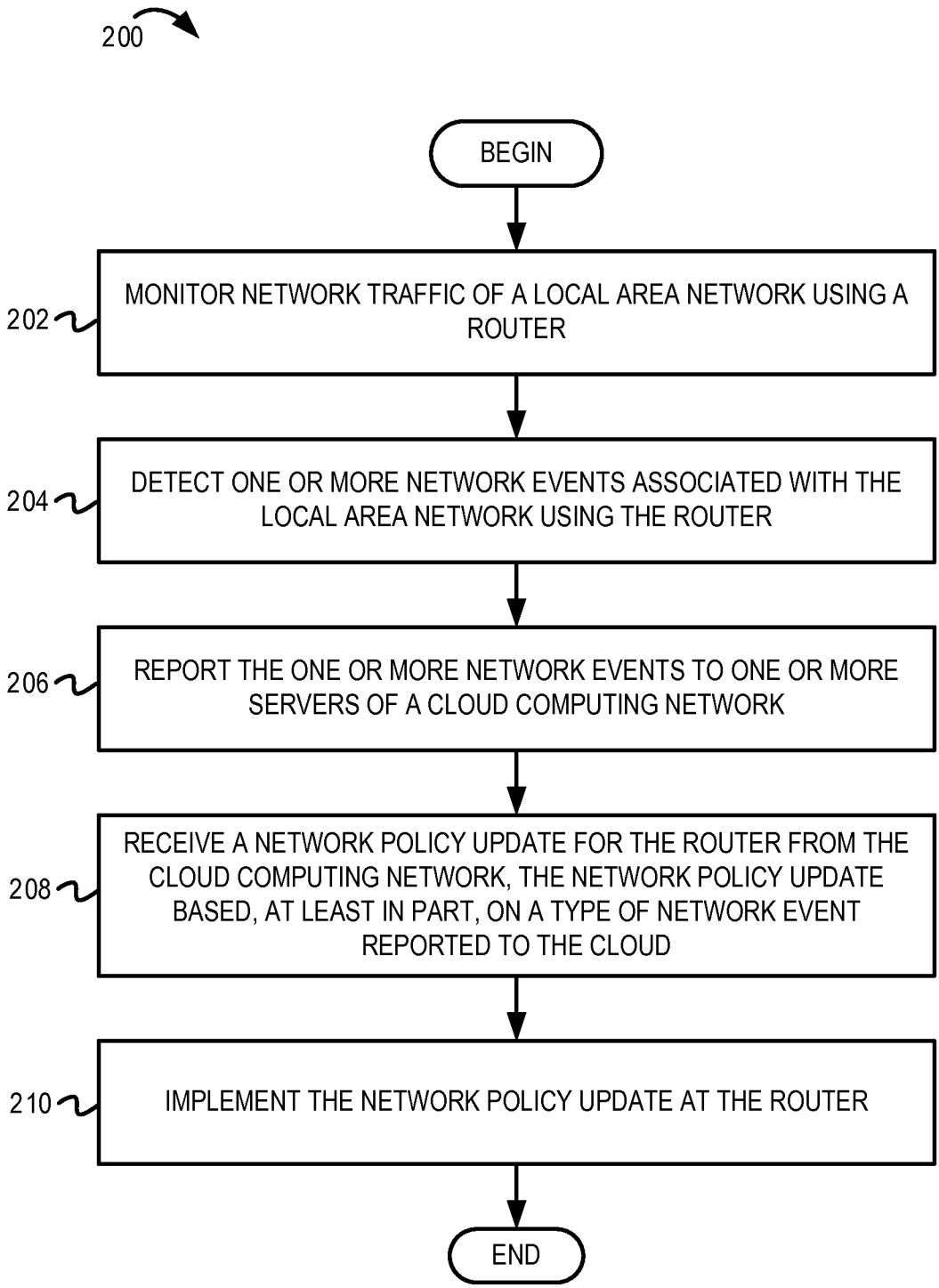
200
BEGIN
202
MONITOR NETWORK TRAFFIC OF A LOCAL AREA NETWORK USING A ROUTER
204
DETECT ONE OR MORE NETWORK EVENTS ASSOCIATED WITH THE LOCAL AREA NETWORK USING THE ROUTER
206
REPORT THE ONE OR MORE NETWORK EVENTS TO ONE OR MORE SERVERS OF A CLOUD COMPUTING NETWORK
208
RECEIVE A NETWORK POLICY UPDATE FOR THE ROUTER FROM THE CLOUD COMPUTING NETWORK, THE NETWORK POLICY UPDATE BASED, AT LEAST IN PART, ON A TYPE OF NETWORK EVENT REPORTED TO THE CLOUD
210
IMPLEMENT THE NETWORK POLICY UPDATE AT THE ROUTER
END

FIG. 2

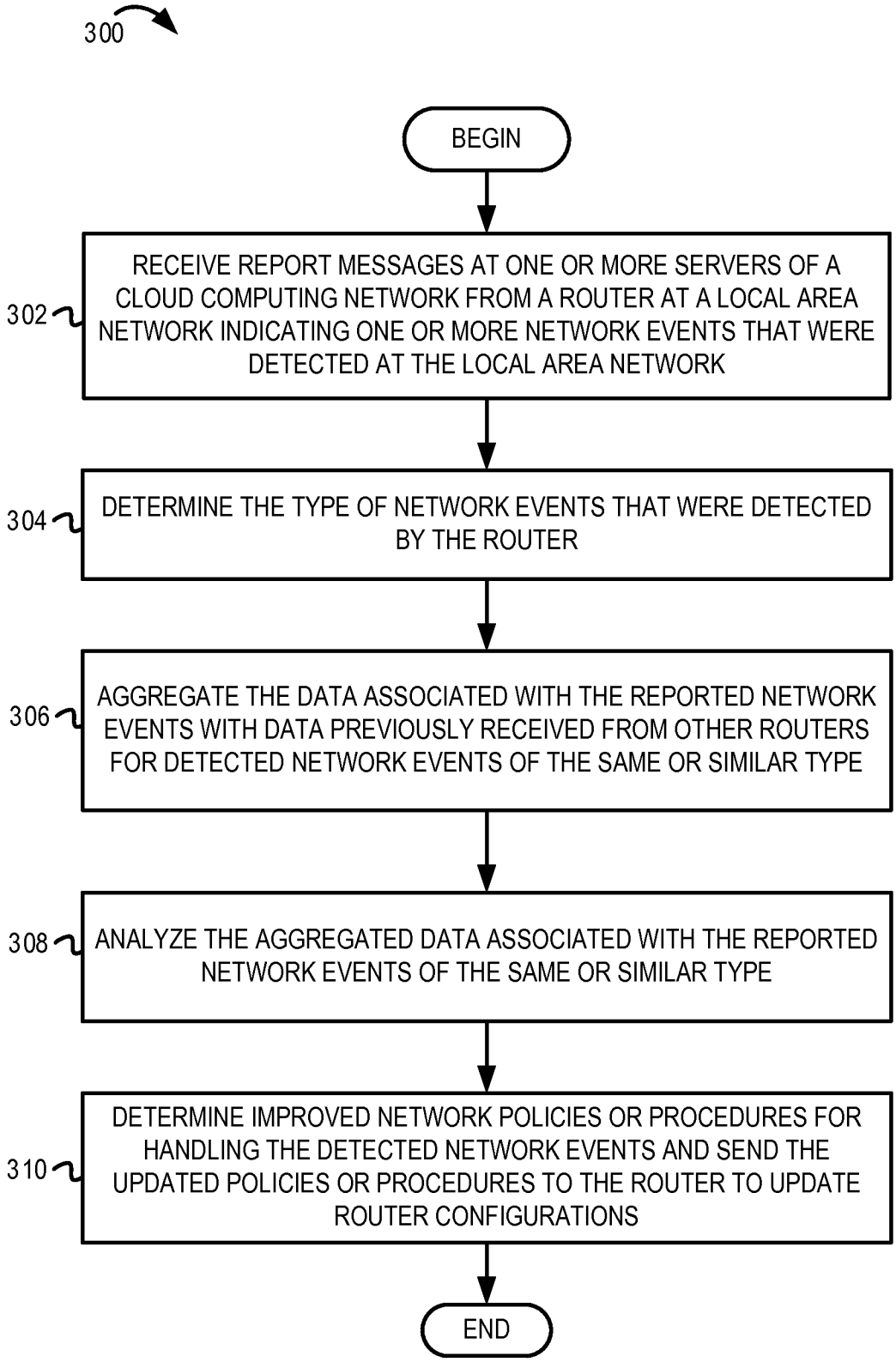
300
BEGIN
RECEIVE REPORT MESSAGES AT ONE OR MORE SERVERS OF A CLOUD COMPUTING NETWORK FROM A ROUTER AT A LOCAL AREA NETWORK INDICATING ONE OR MORE NETWORK EVENTS THAT WERE DETECTED AT THE LOCAL AREA NETWORK
302
DETERMINE THE TYPE OF NETWORK EVENTS THAT WERE DETECTED BY THE ROUTER
304
AGGREGATE THE DATA ASSOCIATED WITH THE REPORTED NETWORK EVENTS WITH DATA PREVIOUSLY RECEIVED FROM OTHER ROUTERS FOR DETECTED NETWORK EVENTS OF THE SAME OR SIMILAR TYPE
306
ANALYZE THE AGGREGATED DATA ASSOCIATED WITH THE REPORTED NETWORK EVENTS OF THE SAME OR SIMILAR TYPE
308
DETERMINE IMPROVED NETWORK POLICIES OR PROCEDURES FOR HANDLING THE DETECTED NETWORK EVENTS AND SEND THE UPDATED POLICIES OR PROCEDURES TO THE ROUTER TO UPDATE ROUTER CONFIGURATIONS
310
END

FIG. 3

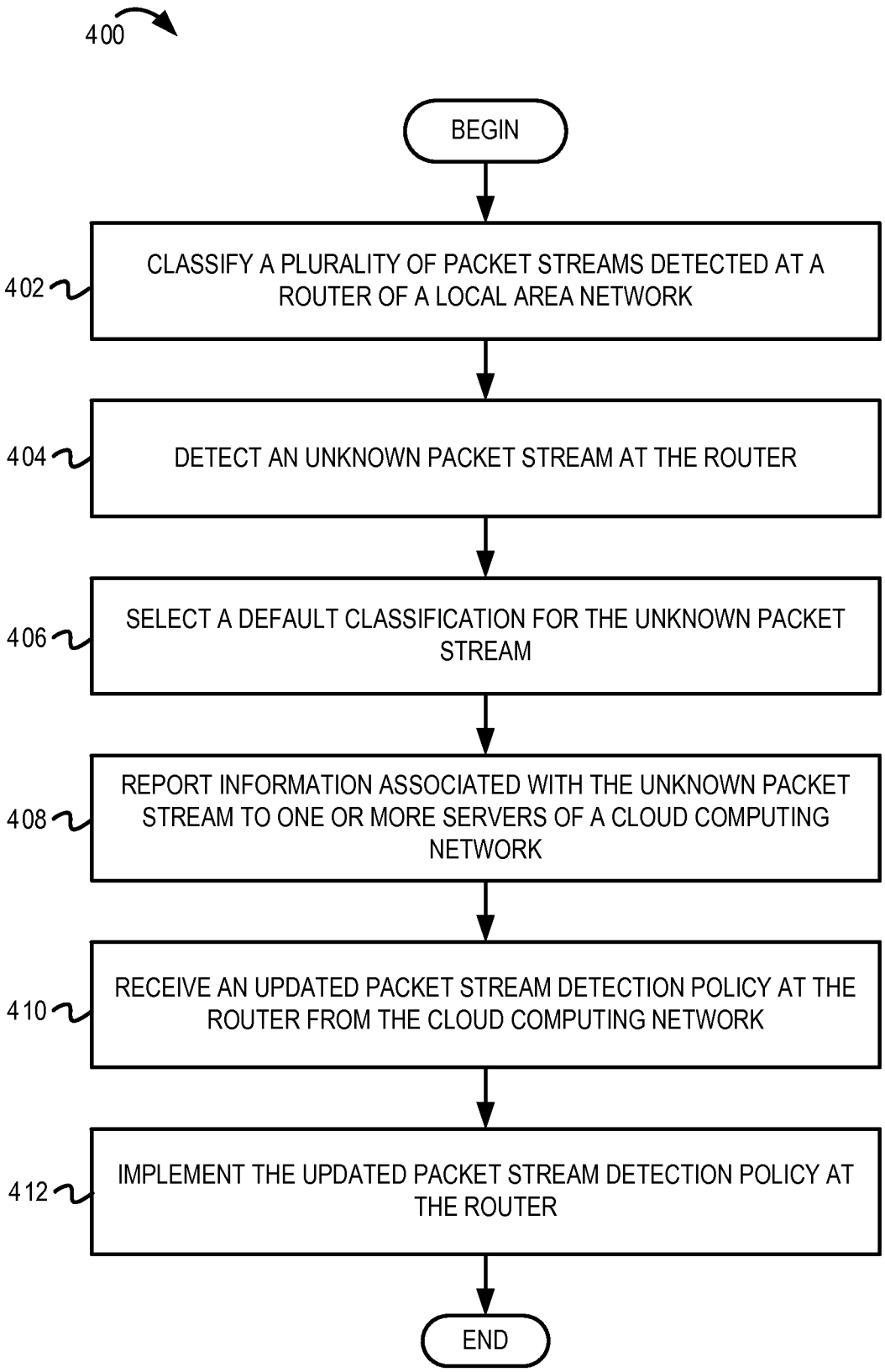
400
BEGIN
402
CLASSIFY A PLURALITY OF PACKET STREAMS DETECTED AT A ROUTER OF A LOCAL AREA NETWORK
404
DETECT AN UNKNOWN PACKET STREAM AT THE ROUTER
406
SELECT A DEFAULT CLASSIFICATION FOR THE UNKNOWN PACKET STREAM
408
REPORT INFORMATION ASSOCIATED WITH THE UNKNOWN PACKET STREAM TO ONE OR MORE SERVERS OF A CLOUD COMPUTING NETWORK
410
RECEIVE AN UPDATED PACKET STREAM DETECTION POLICY AT THE ROUTER FROM THE CLOUD COMPUTING NETWORK
412
IMPLEMENT THE UPDATED PACKET STREAM DETECTION POLICY AT THE ROUTER
END

FIG. 4

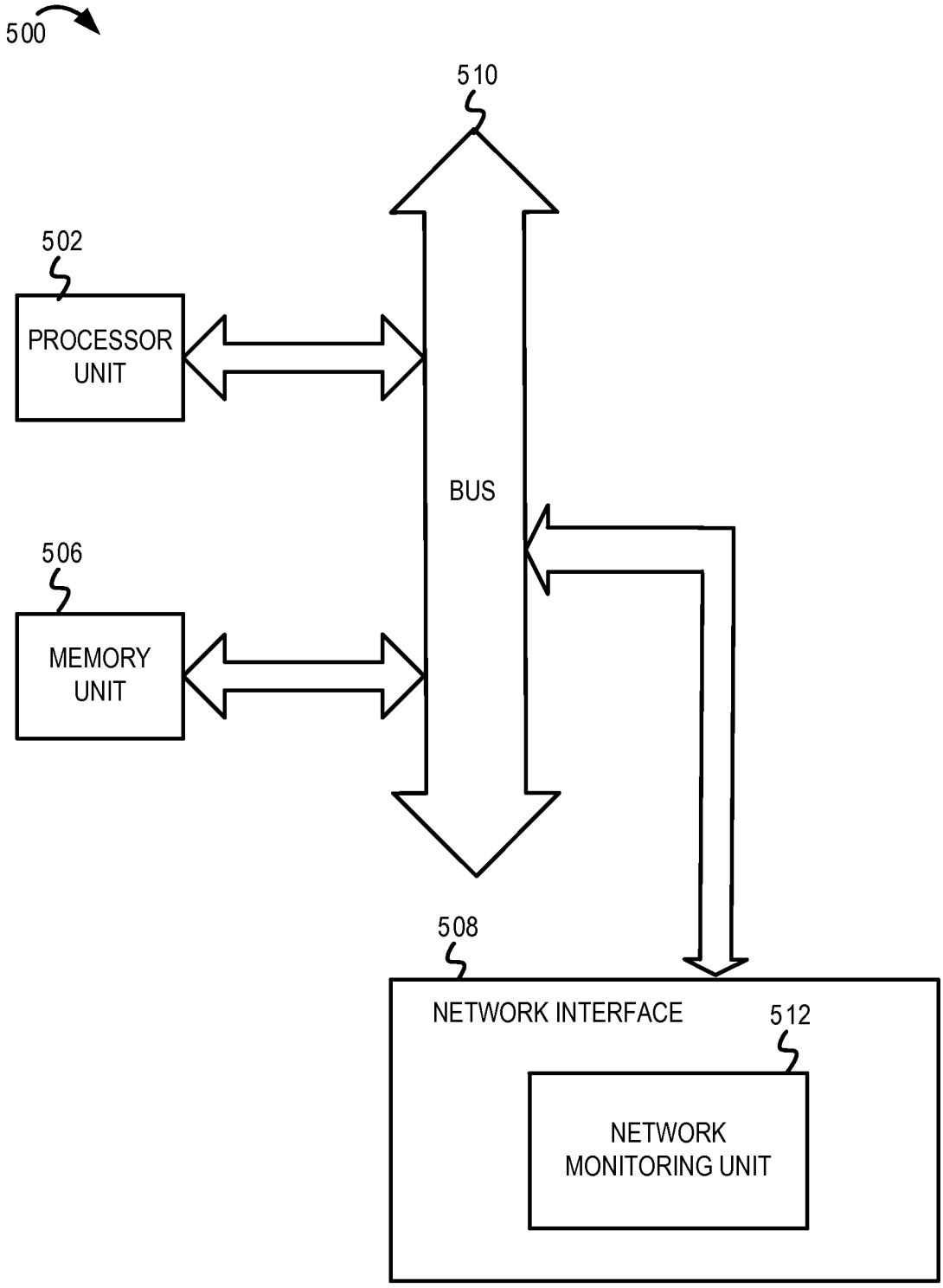
500
510
502
PROCESSOR UNIT
BUS
506
MEMORY UNIT
508
NETWORK INTERFACE
512
NETWORK MONITORING UNIT

FIG. 5

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2012/061216

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04L12/24 H04L12/851
ADD. H04L12/859

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

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

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	EP 1 750 394 A2 (NOVELL INC [US]) 7 February 2007 (2007-02-07) paragraphs [0001], [0011], [0016] - [0028], [0049] - [0054] -----	1-9, 18-25
X	US 2010/023604 A1 (VERMA DINESH [US] ET AL) 28 January 2010 (2010-01-28) paragraphs [0020] - [0028], [0031] - [0036], [0042] -----	1-9, 18-25
A	US 7 043 659 B1 (KLEIN GARY R [US] ET AL) 9 May 2006 (2006-05-09) column 3, line 36 - column 4, line 38 column 9, line 66 - column 10, line 60 column 13, line 23 - column 15, line 16 ----- -/--	1-9, 18-25

[X] Further documents are listed in the continuation of Box C.

[X] 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	Date of mailing of the international search report
13 March 2013	21/03/2013

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Itani, Maged

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2012/061216

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 2006/068548 A1 (ERICSSON TELEFON AB L M [SE]; LINDHOLM FREDRIK [SE]; BASILIER HENRIK [] 29 June 2006 (2006-06-29) abstract page 7, line 17 - page 8, line 28 page 10, lines 16-33 page 20, line 26 - page 21, line 18 page 30, line 9 - page 31, line 23	10-17, 26-36
A	US 2005/114541 A1 (GHETIE ANDREI [US] ET AL) 26 May 2005 (2005-05-26) paragraphs [0005], [0050] - [0052], [0060]	10-17, 26-36
A	US 7 664 048 B1 (YUNG WENG-CHIN [US] ET AL) 16 February 2010 (2010-02-16) column 9, line 32 - column 13, line 39	10-17, 26-36

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US2012/061216

Box No. II Observations where certain claims were found unsearchable (Continuation of item 2 of first sheet)

This international search report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:

2. ☐ Claims Nos.:
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:

3. ☐ Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box No. III Observations where unity of invention is lacking (Continuation of item 3 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

see additional sheet

1. ☒ As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.

2. ☐ As all searchable claims could be searched without effort justifying an additional fees, this Authority did not invite payment of additional fees.

3. ☐ As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:

4. ☐ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

Remark on Protest

☐ The additional search fees were accompanied by the applicant's protest and, where applicable, the payment of a protest fee.

☐ The additional search fees were accompanied by the applicant's protest but the applicable protest fee was not paid within the time limit specified in the invitation.

☒ No protest accompanied the payment of additional search fees.

FURTHER INFORMATION CONTINUED FROM PCT/ISA/ 210

This International Searching Authority found multiple (groups of) inventions in this international application, as follows:

1. claims: 1-9, 18-25

A method for correlating network events

---

2. claims: 10-17, 26-36

A method for data traffic classification

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/US2012/061216

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 1750394 A2	07-02-2007	EP 1750394 A2	07-02-2007
		US 2007033636 A1	08-02-2007
US 2010023604 A1	28-01-2010	NONE	
US 7043659 B1	09-05-2006	NONE	
WO 2006068548 A1	29-06-2006	AT 443955 T	15-10-2009
		CA 2591222 A1	29-06-2006
		CN 101088256 A	12-12-2007
		EP 1829295 A1	05-09-2007
		JP 2008524916 A	10-07-2008
		US 2008002579 A1	03-01-2008
		WO 2006068548 A1	29-06-2006
US 2005114541 A1	26-05-2005	US 2005114541 A1	26-05-2005
		US 2010095017 A1	15-04-2010
US 7664048 B1	16-02-2010	NONE	