



US009270551B2

(12) **United States Patent**
Kamal et al.

(10) **Patent No.:** **US 9,270,551 B2**
(45) **Date of Patent:** **Feb. 23, 2016**

(54) **DYNAMIC RECLASSIFICATION OF CLIENT DEVICES IN A NETWORK**

(71) Applicants: **CELLCO PARTNERSHIP**, Basking Ridge, NJ (US); **VERIZON PATENT AND LICENSING INC.**, Basking Ridge, NJ (US)

(72) Inventors: **Ashfaq Kamal**, Norristown, PA (US); **Jingyi Zhou**, Belle Mead, NJ (US); **Lily Hui Zhu**, Parsippany, NJ (US); **Robert Bruce Stansell**, Winston Salem, NC (US)

(73) Assignees: **Cellco Partnership**, Basking Ridge, NJ (US); **Verizon Patent and Licensing Inc.**, Basking Ridge, NJ (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 339 days.

(21) Appl. No.: **13/907,623**

(22) Filed: **May 31, 2013**

(65) **Prior Publication Data**
US 2014/0310387 A1 Oct. 16, 2014

Related U.S. Application Data
(60) Provisional application No. 61/810,999, filed on Apr. 11, 2013.

(51) **Int. Cl.**
G06F 15/177 (2006.01)
H04L 12/26 (2006.01)
H04L 12/24 (2006.01)

(52) **U.S. Cl.**
CPC **H04L 43/08** (2013.01); **H04L 41/0893** (2013.01); **H04L 41/085** (2013.01)

(58) **Field of Classification Search**
CPC H04L 43/08
USPC 709/221
See application file for complete search history.

(56) **References Cited**
U.S. PATENT DOCUMENTS

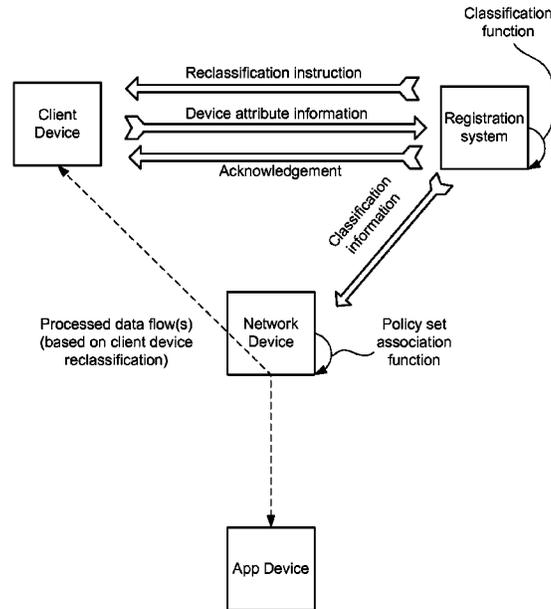
2005/0013316 A1* 1/2005 Liao H04L 12/5695
370/449
2012/0221955 A1* 8/2012 Raleigh H04M 15/00
715/736

* cited by examiner

Primary Examiner — Ario Etienne
Assistant Examiner — Sahera Halim

(57) **ABSTRACT**
One or more devices may store attribute information identifying multiple attributes associated with a client device that is associated with a particular classification; reclassify the client device based on the attribute information; and provide, based on reclassifying the client device, classification information to a network policy set, of multiple policy sets, with the client device. The classification information may identify an updated classification of the client device. The updated classification may be different from the particular classification. The particular policy set may be based on the updated classification of the client device. The particular policy set may include an instruction used to process a data flow provided to or provided from the client device.

20 Claims, 6 Drawing Sheets



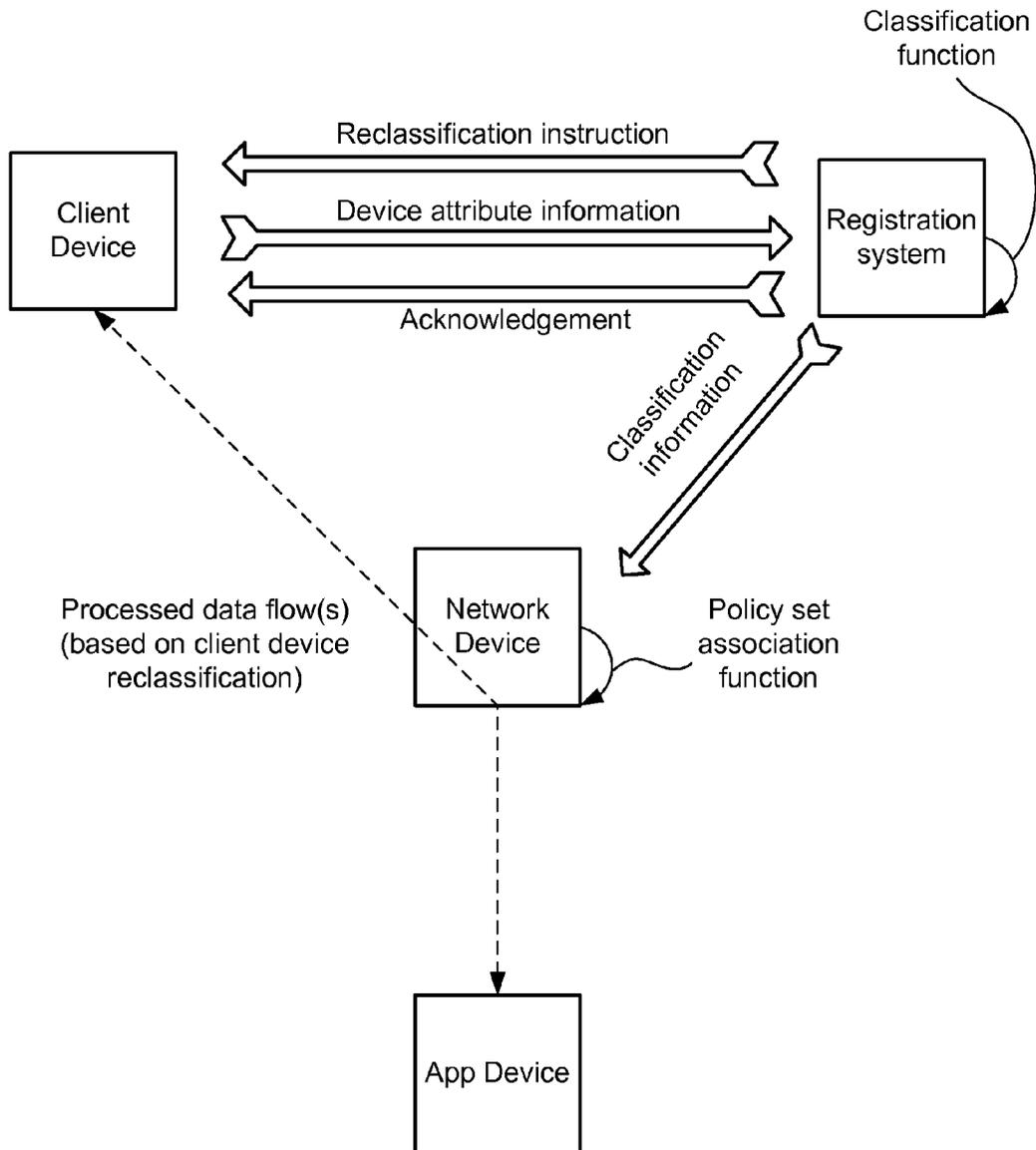


Fig. 1

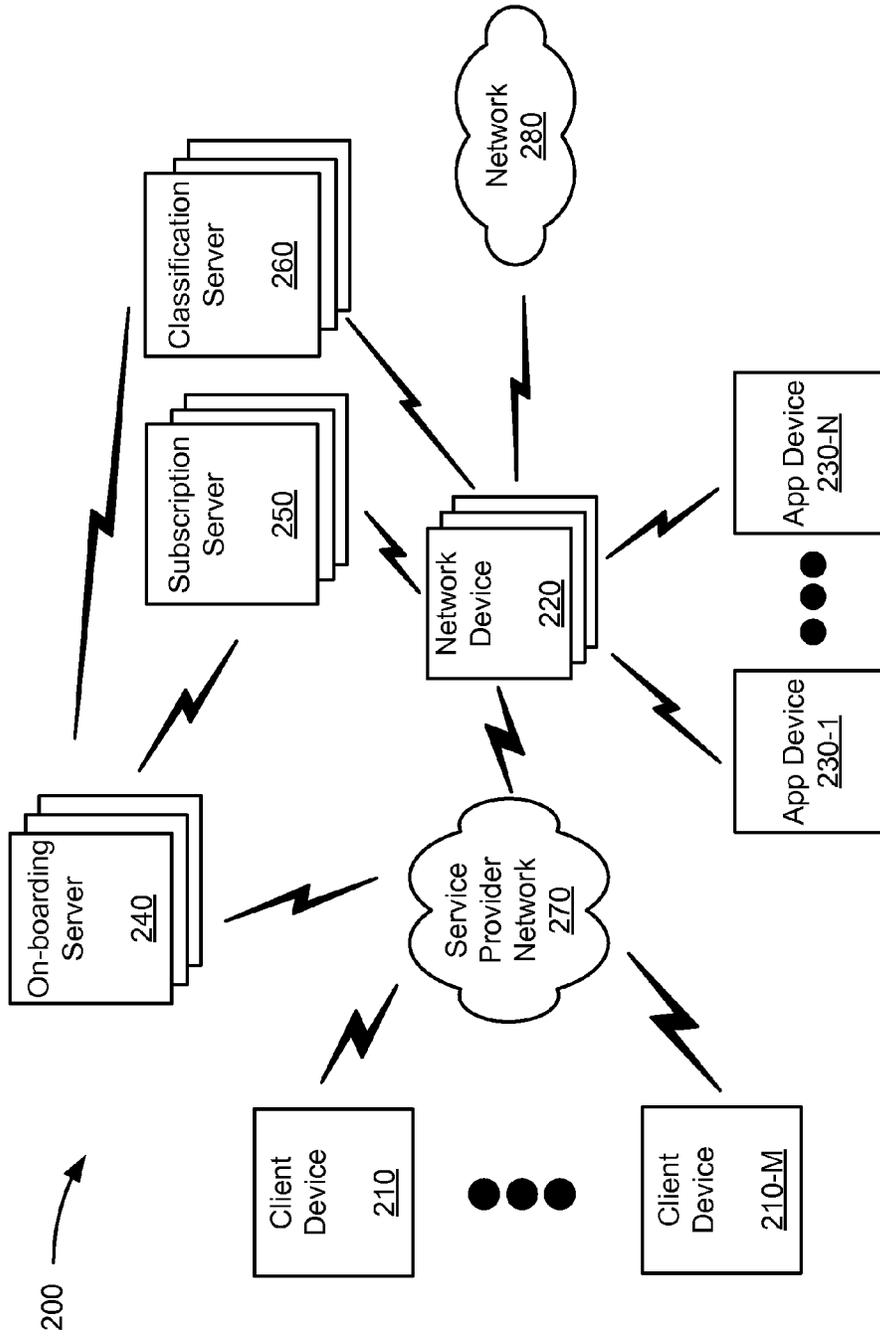


Fig. 2

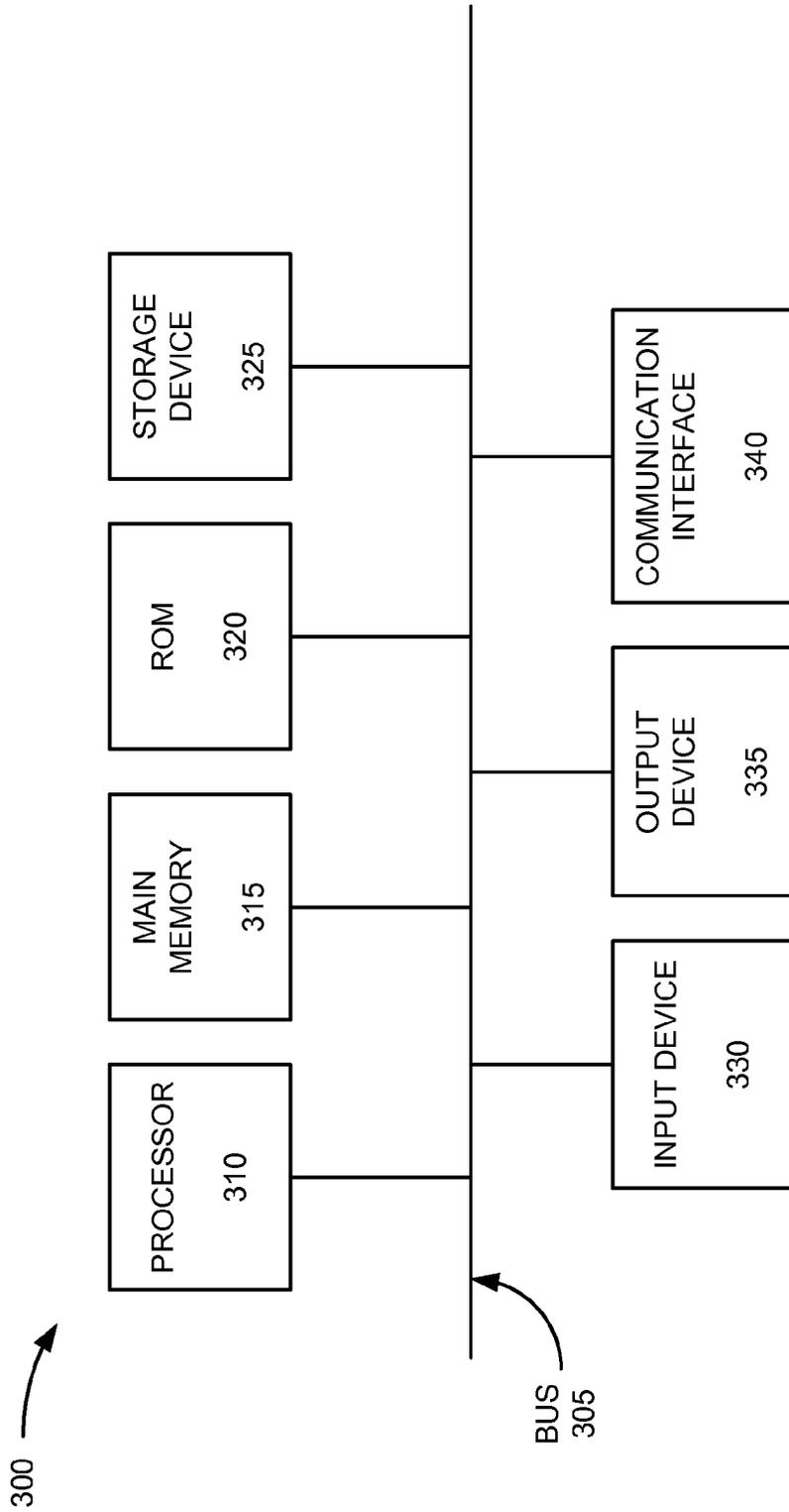


Fig. 3

400 →

Classification Matrix 410				
Device attributes	Classification			
	Type 1	Type 2	Type 3	Type N
LAN Connectivity Management	Client support	Client + Access point Support	Access point Support	
Data Collection Function	X	X		●
Control Function			X	●
Device Management	X			
Security Management	X		X	
Function AA				

Classification Policies 420		
Classification	Policy Set	Client Device IDs
Type 1	Policy Set 1	ID 1, ID 2, ID 3
Type 2	Policy Set 2	ID 4, ID 5
Type 3	Policy Set 3	ID 6
Type 4	Policy Set 4	ID 7, ID 8...
	●	●
Type BB	Policy Set CC	

Fig. 4

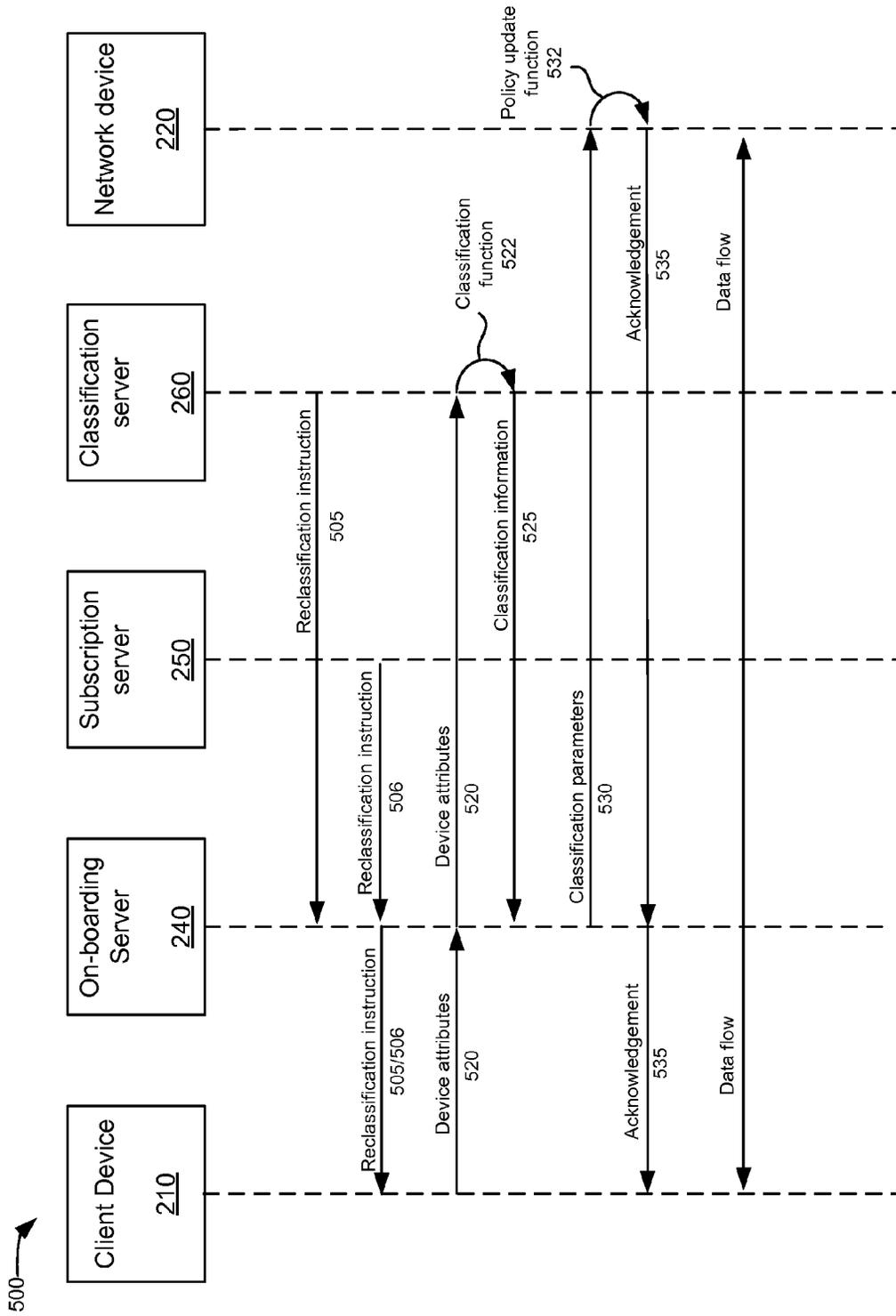


Fig. 5

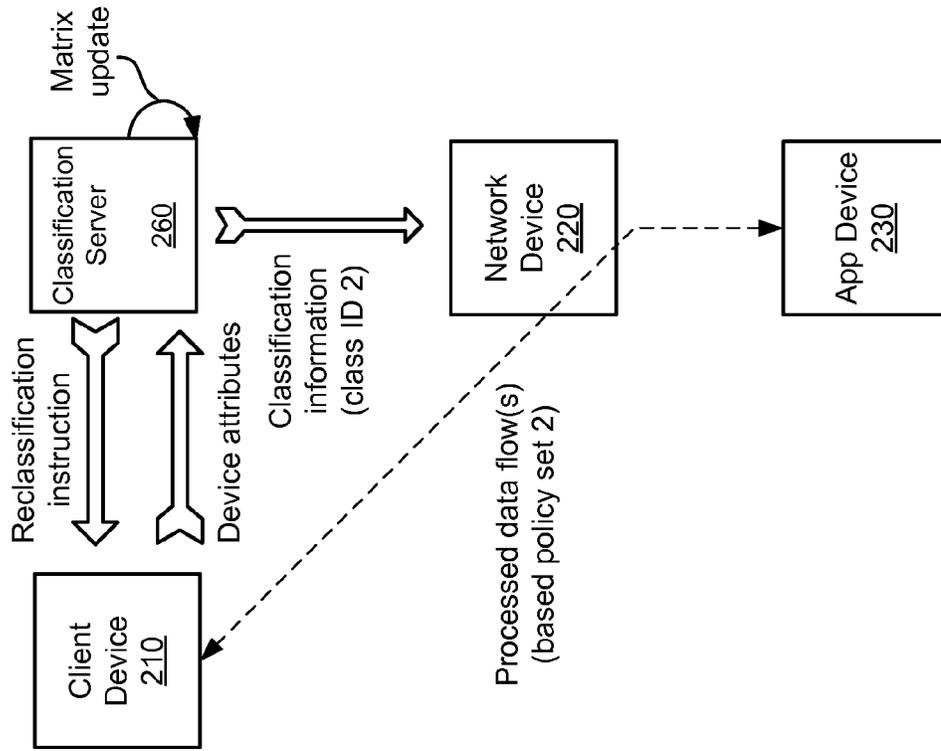


Fig. 6A

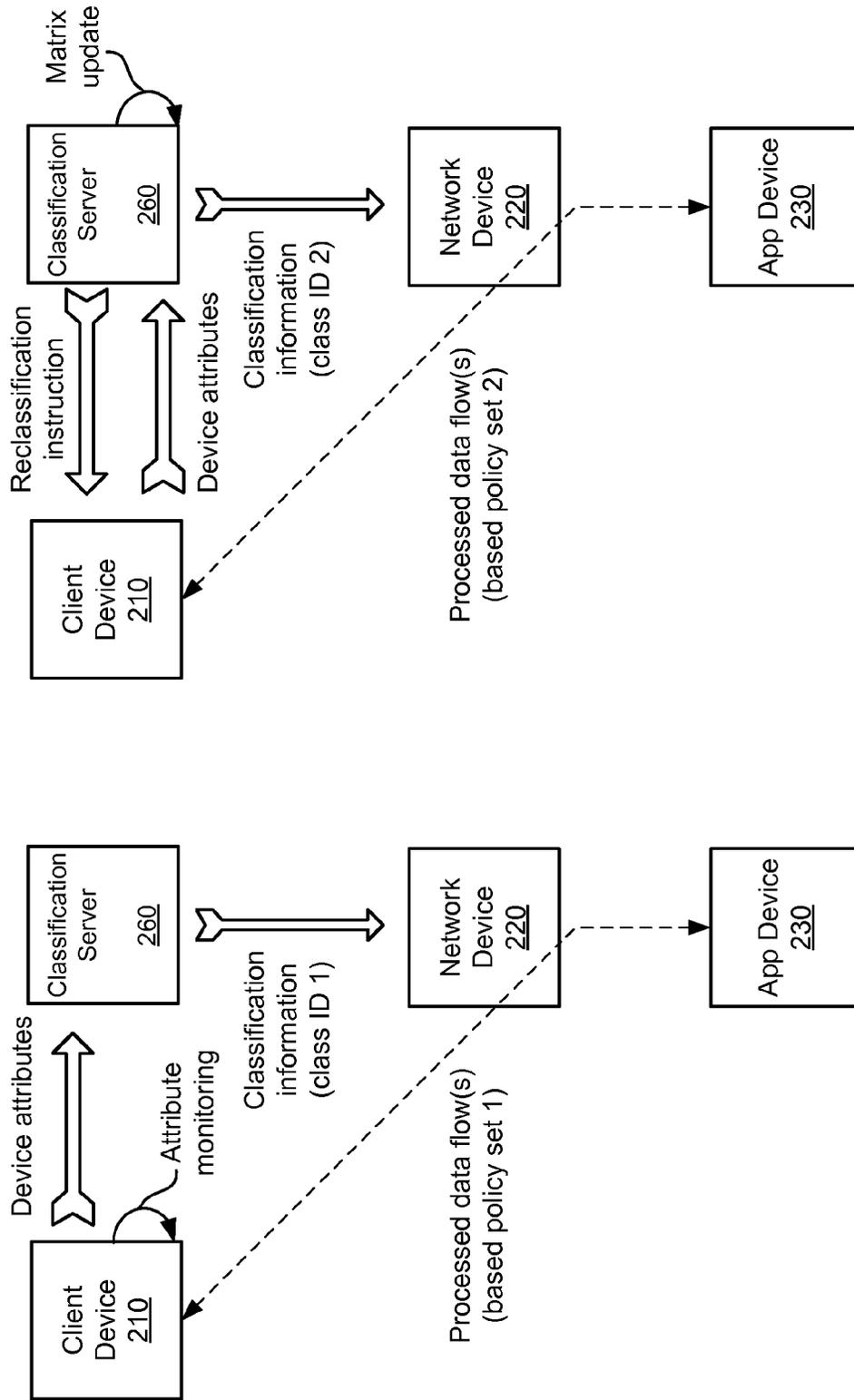


Fig. 6B

DYNAMIC RECLASSIFICATION OF CLIENT DEVICES IN A NETWORK

RELATED APPLICATION

This application claims priority to U.S. Provisional Patent Application No. 61/810,999, filed Apr. 11, 2013, the disclosure of which is incorporated by reference herein.

BACKGROUND

Client devices sometimes communicate with applications (e.g., via a network device) to process data gathered by the client device. A data flow, provided to/from a client device, may be in need of more network resources than another data flow, provided to/from another client device. As such, the network device may overcompensate and provide some data flows with more network resources than needed (thereby increasing network traffic), or undercompensate by providing other data flows with insufficient network resources (thereby causing performance problems in a communication between the client device and an application).

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1 illustrates an example overview of an implementation described herein;

FIG. 2 illustrates an example environment in which systems and/or methods, described herein, may be implemented;

FIG. 3 illustrates example components of a device that may be used within the environment of FIG. 2;

FIG. 4 illustrates an example data structure that may be stored by one or more devices in the environment of FIG. 2;

FIG. 5 illustrates a call flow diagram of example operations capable of being performed by an example portion of the environment of FIG. 2; and

FIGS. 6A and 6B illustrate an example implementation as described herein.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

The following detailed description refers to the accompanying drawings. The same reference numbers in different drawings may identify the same or similar elements.

Systems and/or methods, as described herein, may provide a technique to dynamically reclassify a client device (e.g., a machine-to-machine (M2M) device, or some other type of device) in order to facilitate a communication between the client device and an application device (hereinafter referred to as an “app device”) via a network device. For example, the network device may process a data flow, provided to/from the client device, based on a particular data flow policy set that is selected based on a classification of the client device (e.g., in order to provide the data flow with sufficient network resources without providing the data flow with additional network resources that the data flow may not need).

In some implementations, the client device may be reclassified as part of a design decision to modify how data flows, provided to/from the client device, are processed. As an example, the design decision may be based on a performance study that identifies that a reclassification of the client device may lead to an increase in data flow processing efficiency.

FIG. 1 illustrates an example overview of an implementation described herein. In FIG. 1, assume that a network device stores information that identifies a classification of a client device. Further, assume that the network device stores a par-

particular data flow policy set (hereinafter referred to as a “policy set”), of multiple policy sets, for the client device and that the particular policy set is based on a classification of the client device. Further, assume that the classification is based on attributes of the client device. The particular policy set may be used, by the network device, to process a data flow provided to/from the client device (e.g., provide the data flow with a particular network resource). For example, a network resource may include a particular protocol with which to transmit the data flow, a particular Quality of Service (QoS), a particular bit rate, a particular latency value, a particular jitter value, a particular network service (e.g., a firewall service, a packet-inspection service, a virus-scanning service, etc.), and/or some other network resource.

As shown in FIG. 1, a registration system may provide a reclassification instruction to the client device to cause the client device to provide device attribute information, used to reclassify the client device, to the registration system. For example, the registration system may provide the reclassification instruction when receiving an update to a classification matrix used to classify the client device based on attributes of the client device. In some implementations, the client device may provide device attribute information without receiving the reclassification instruction. For example, the client device may provide the device attribute information when one or more attributes of the client device changes, thereby potentially impacting the classification of the client device.

In some implementations, the registration system may receive the device attribute information and may perform a classification function to reclassify the client device based on the device attribute information. As shown in FIG. 1, the registration system may provide classification information to the network device. For example, the registration system may provide a classification identifier (ID) and/or some other information that identifies how the client device is reclassified. In some implementations, the network device may receive the classification information and may associate an updated policy set for the client device based on the reclassification of the client device.

As shown in FIG. 1, the registration system may provide an acknowledgement to the client device (e.g., when the network device associates an updated policy set with the client device) to indicate that the client device and the app device may communicate via the network device. For example, the client device may provide a data flow destined for the app device (or the app device may provide a data flow destined for the client device). In some implementations, the network device may receive the data flow and may process the data flow based on the updated policy set associated with the client device.

As described above, a particular policy set may be based on a particular classification of the client device and may be used to process a data flow provided to/from the client device. As a result, the network device may process data flows based on a policy set that is particular to the classification of the client device, thereby increasing efficiency in facilitating communication between the client device and the app device and increasing efficiency in processing data flows. Further, the client device may be dynamically reclassified such that the network device associates an updated policy set with the client device.

As used herein, the term “classify” may be used interchangeably with the term “reclassify.” That is, when describing an example for classifying a client device, the same example may apply to reclassifying a client device that includes an existing classification.

FIG. 2 is a diagram of an example environment 200 in which systems and/or methods described herein may be

implemented. As shown in FIG. 2, environment 200 may include client devices 210-1, . . . , 210-M (where $M \geq 1$), network device 220, app devices 230-1 through 230-N (where $N \geq 1$), on-boarding server 240, subscription server 250, classification server 260, service provider network 270, and network 280.

Client device 210 may include one or more machine-to-machine (M2M) devices capable of communicating via service provider network 270 and/or network 280. For example, client device 210 may include a network device (e.g., a modem, a switch, a gateway, etc.), a sensing device, a processing device, and/or some other type of device. In some implementations, client device 210 may include a sensing or metering device to gather data (e.g., temperature measurements, resource usage measurements, motion detection, object detection, etc.), a processing device to process the data to form processed data (e.g., via an application implemented on client device 210), and/or a network device to provide a data flow (including the processed data) towards app device 230 (e.g., via network device 220). In some implementations, client device 210 may provide a data flow including a control instruction to another client device 210 (e.g., an instruction to adjust a sensor position/configuration and/or some other type of instruction). In some implementations, client device 210 may include another type of device that gathers, stores, processes, and/or transmits data via service provider network 270 and/or network 280.

In some implementations, client device 210 may include a monitoring function to identify when an attribute (e.g., functionality, hardware/software configurations, data flow transmission protocols, etc.) changes for client device 210. In some implementations, client device 210 may provide a reclassification request to on-boarding server 240 in order to reclassify client device 210.

Network device 220 may include one or more network devices, such as a gateway, a router, a modem, a switch, a firewall, a network interface card (NIC), a hub, a bridge, a proxy server, an optical add-drop multiplexer (OADM), or some other type of device that processes and/or transfers traffic. Network device 220 may, for example, provide connectivity of client device 210 to external packet data networks by being a traffic exit/entry point from/to service provider network 270 for client device 210. Network device 220 may perform policy enforcement, packet filtering, charging support, lawful intercept, and/or packet screening. In some implementations, network device 220 may store one or more policy sets for corresponding classifications of client device 210 and may associate a particular network device 220 with a particular policy set. In some implementations, network device 220 may facilitate communication between client device 210 and app device 230 by processing data flows in accordance with a policy set associated with client device 210 (e.g., based on the classification of client device 210).

In some implementations, network device 220 may perform data proxy communication functions (real time and scheduled) device and application management functions, policy filter provisioning functions, subscriber provisioning functions, application provisioning functions, user subscriber provisioning functions, application name provisioning functions, device hardware ID provisioning functions, classification provisioning functions, and/or some other type of provisioning function. In some implementations, network device 220 may also perform internal query/validation functions, such as user subscription validation, client device 210 class validation, application data transmission state tracking, and/or some other type of network related function.

App device 230 may include a computing device, such as a server device, a desktop computing device, a portable computing device (e.g., a laptop, a tablet, a mobile phone, etc.), an M2M device, and/or some other type of computing device. In some implementations, app device 230 may include one or more applications that receive a data flow, originated from client device 210 (e.g., a data flow having data gathered by a sensor device of client device 210), and may perform a task based on the data flow. For example, app device 230 may perform a data analysis based on the data flow, such as a temperature trends analysis, an inventory analysis, a sales trend analysis, etc. In some implementations, app device 230 may provide a control instruction to client device 210 (e.g., an instruction to adjust a sensor position/configuration and/or some other type of instruction).

On-boarding server 240 may include one or more computing devices, such as a server device or a collection of server devices. In some implementations, on-boarding server 240 may receive a reclassification request (e.g., from client device 210, subscription server 250, and/or classification server 260) and may transmit information regarding the reclassification request to/from network device 220, subscription server 250, and/or classification server 260 in order to reclassify client device 210 (e.g., to allow network device 220 to associate a particular policy set with a particular network device 220). In some implementations, on-boarding server 240 may provide an acknowledgement to client device 210 when client device 210 has been reclassified to allow client device 210 and app device 230 to communicate via network device 220.

Subscription server 250 may include one or more computing devices, such as a server device or a collection of server devices. In some implementations, subscription server 250 may store subscription information for client devices 210. For example, subscription server 250 may store information that uniquely identifies client devices 210 that are subscribed to service provider network 270 and/or authorized to access network device 220. For example, subscription server 250 may store a hardware identifier (ID), a network access ID, and/or some other information to uniquely identify client device 210. In some implementations, subscription server 250 may validate an ID of client device 210 (e.g., when subscription server 250 stores the ID of client device 210) in order to authorize client device 210 to access network device 220.

Classification server 260 may include one or more computing devices, such as a server device or a collection of server devices. In some implementations, classification server 260 may store one or more classification matrices and/or classification rules. In some implementations, classification server 260 may classify client device 210 based on a classification profile (e.g., attributes) associated with client device 210. In some implementations, classification server 260 may provide information identifying a classification of client device 210 to network device 220 (e.g., via on-boarding server 240) to allow network device 220 to associate a policy set with client device 210 based on the classification of client device 210.

In some implementations, classification server 260 may receive an update to a classification matrix, thereby impacting a classification of client device 210. Based on receiving an update to the classification matrix, classification server 260 may provide a reclassification instruction to client device 210 in order to reclassify client device 210.

Service provider network 270 may include one or more wired and/or wireless networks via which client devices 210 and/or app devices 230 communicate and/or receive content. For example, service provider network 270 may include a

cellular network, the Public Land Mobile Network (PLMN), a second generation (2G) network, a third generation (3G) network, a fourth generation (4G) network (e.g., a long term evolution (LTE) network), a fifth generation (5G) network, and/or another type of network. Additionally, or alternatively, service provider network **260** may include a wide area network (WAN), a metropolitan area network (MAN), an ad hoc network, an intranet, a fiber optic-based network, and/or a combination of these or other types of networks.

Network **280** may include one or more wired and/or wireless networks. For example, network **280** may include a cellular network, a public land mobile network (PLMN), a second generation (2G) network, a third generation (3G) network, a fourth generation (4G) network, a fifth generation (5G) network, and/or another network. Additionally, or alternatively, network **280** may include a local area network (LAN), a wide area network (WAN), a metropolitan network (MAN), a telephone network (e.g., the Public Switched Telephone Network (PSTN)), an ad hoc network, a managed IP network, a virtual private network (VPN), an intranet, the Internet, a fiber optic-based network, and/or a combination of these or other types of networks.

The quantity of devices and/or networks, illustrated in FIG. 2, is not limited to what is shown. In practice, there may be additional devices and/or networks; fewer devices and/or networks; different devices and/or networks; or differently arranged devices and/or networks than illustrated in FIG. 2. Also, in some implementations, one or more of the devices of environment **200** may perform one or more functions described as being performed by another one or more of the devices of environment **200**. Devices of environment **200** may interconnect via wired connections, wireless connections, or a combination of wired and wireless connections. In some implementations, functions described as being performed by one device may be performed by multiple devices (e.g., to meet capacity demands). Also, devices in environment **200** may be implemented in various geographic locations (e.g., to comply with regulatory requirements/laws associated with a geographic location).

FIG. 3 illustrates example components of a device **300** that may be used within environment **200** of FIG. 2. Device **300** may correspond to client device **210**, network device **220**, app device **230**, on-boarding server **240**, subscription server **250**, and/or classification server **260**. Each of client device **210**, network device **220**, app device **230**, on-boarding server **240**, subscription server **250**, and/or classification server **260** may include one or more devices **300** and/or one or more components of device **300**.

As shown in FIG. 3, device **300** may include a bus **305**, a processor **310**, a main memory **315**, a read only memory (ROM) **320**, a storage device **325**, an input device **330**, an output device **335**, and a communication interface **340**.

Bus **305** may include a path that permits communication among the components of device **300**. Processor **310** may include a processor, a microprocessor, an application specific integrated circuit (ASIC), a field programmable gate array (FPGA), or another type of processor that interprets and executes instructions. Main memory **315** may include a random access memory (RAM) or another type of dynamic storage device that stores information or instructions for execution by processor **310**. ROM **320** may include a ROM device or another type of static storage device that stores static information or instructions for use by processor **310**. Storage device **325** may include a magnetic storage medium, such as a hard disk drive, or a removable memory, such as a flash memory.

Input device **330** may include a component that permits an operator to input information to device **300**, such as a control button, a keyboard, a keypad, a sensor, or another type of input device. Output device **335** may include a component that outputs information to the operator, such as a light emitting diode (LED), a display, or another type of output device. Communication interface **340** may include any transceiver-like component that enables device **300** to communicate with other devices or networks. In some implementations, communication interface **340** may include a wireless interface, a wired interface, or a combination of a wireless interface and a wired interface.

Device **300** may perform certain operations, as described in detail below. Device **300** may perform these operations in response to processor **310** executing software instructions contained in a computer-readable medium, such as main memory **315**. A computer-readable medium may be defined as a non-transitory memory device. A memory device may include memory space within a single physical storage device or memory space spread across multiple physical storage devices.

The software instructions may be read into main memory **315** from another computer-readable medium, such as storage device **325**, or from another device via communication interface **340**. The software instructions contained in main memory **315** may direct processor **310** to perform processes that will be described later. Alternatively, hardwired circuitry may be used in place of or in combination with software instructions to implement processes described herein. Thus, implementations described herein are not limited to any specific combination of hardware circuitry and software.

In some implementations, device **300** may include additional components, fewer components, different components, or differently arranged components than are shown in FIG. 3.

FIG. 4 illustrates an example data structure **400** that may be stored by one or more devices in environment **200**. In some implementations, data structure **400** may be stored in a memory of network device **220** and/or classification server **260**. In some implementations, data structure **400** may be stored in a memory separate from, but accessible by network device **220** and/or classification server **260**. In some implementations, data structure **400** may be stored by some other device in environment **200**, such as app device **230**, on-boarding server **240**, and/or subscription server **250**.

A particular instance of data structure **400** may contain different information and/or fields than another instance of data structure **400**. In some implementations, classification server **260** may classify client device **210** based on information stored by data structure **400**. Additionally or alternatively, network device **220** may identify a policy set to associate with client device **210** based on information stored by data structure **400**.

As shown in FIG. 4, data structure **400** may include classification matrix field **410** and classification policies field **420**.

Classification matrix field **410** may store information that identifies one or more classifications associated with corresponding device attributes. For example, classification matrix field **410** may store a classification, such as a "type 1" classification. Further, classification matrix field **410** may store attributes that define the "type 1" classification for client devices **210**. As shown in FIG. 4, client devices **210** having the "type 1" classification may have particular attributes, such as client support LAN connectivity management, data collection functionality, device management functionality, and

security management functionality. As shown in FIG. 4, other classifications may be associated with a different set of attributes.

In some implementations, classification server 260 may classify client device 210 based on receiving information identifying attributes of client device 210 and based on information stored by classification matrix field 410. For example, assume that client device 210 has particular attributes, such as client support LAN connectivity management, data collection functionality, device management functionality, and security management functionality. Further, assume that classification matrix field 410 identifies a “type 1” classification for client devices 210 having a client support LAN connectivity management attribute, a data collection functionality attribute, a device management functionality attribute, and a security management functionality attribute. Further, assume that classification server 260 receives information identifying the attributes of client device 210. Given these assumptions, classification server 260 may classify client device 210 as a “type 1” classification device.

While a particular list of attributes is illustrated in classification matrix field 410, in practice, classification matrix field 410 may store additional or fewer attributes. For example, classification matrix field 410 may store attributes that identify functions, hardware configurations, software configurations, IP addresses, geographic locations, and/or some other attribute associated with a particular classification. Also, classification matrix field 410 may store attributes that identify subscription information of client device 210. Thus, a classification of client device 210 may be based on subscription information stored by subscription server 250.

Classification policies field 420 may store information that identifies policy sets corresponding to classification types. As described above, network device 220 may associate a policy set with client device 210 based on a classification of client device 210. In some implementations, network device 220 may identify a particular policy set to associate with client device 210 having a particular classification based on information stored by classification policies field 420. As shown in FIG. 4, classification policies field 420 may store information that identifies particular client devices 210 associated with a particular classification type and a particular policy set. For example, classification policies field 420 may store an identifier of client device 210 (and/or some other information to uniquely identify client device 210) in connection with a corresponding classification and/or a corresponding policy set.

In some implementations, network device 220 may determine a policy set to use when processing a data flow provided to/from client device 210 based on information stored by classification policies field 420. For example, network device 220 may determine an ID of client device 210 based on a session between client device 210 and network device 220 and may determine a corresponding policy set for the ID. In some implementations, a policy set may be based on some other factor (e.g., instead of or in addition to being based on a classification of client device 210), such as a geographic location and/or an IP address associated with client device 210.

In some implementations, a policy set may identify a network resource to provide to a data flow. For example, the policy set may include a quality of service (QoS) policy, such as a guaranteed bit rate (GBR), a latency value, a jitter value. Additionally or alternatively, the policy set may include an instruction to provide a particular service to a data flow (e.g., a firewall service, a routing service, a packet-inspection service, a virus scanning service, etc.). Additionally or alterna-

tively, the policy set may include an instruction to provide a data flow to client device 210 via a particular network interface or via a particular network protocol (e.g., via a particular routing protocol and/or a particular security protocol). Additionally or alternatively, the policy set may include one or more protocols that network device 220 may use to transmit the data flow. Additionally or alternatively, the policy set may include a resource and/or a particular app device 230 that client device 210 may access. Additionally or alternatively, the policy set may include another type of policy or instruction.

As described above, a particular policy set may be associated with a particular client device 210 based on the classification of client device 210. The particular policy set may be particular to the classification such that data flows, provided to/from client device 210, are processed in accordance with the particular policy set (e.g., to increase efficiency in facilitating communication between client devices 210 and app devices 230). For example, a policy set for a type 1 type client device 210 (e.g., a client device that includes a video camera and a single application to capture audio/video data) may include policies that direct network device 220 to process data flows provided to/from client device 210 more efficiently than if network device 220 were to process the data flows using a policy set for a type 2 type client device 210 (e.g., a client device that includes multiple applications, multiple network interfaces, and/or multiple sensors).

In some implementations, information stored by classification matrix and/or class policies field 420 may be modified, for example, as a result of a design decision. For example, the design decision may be based on a decision to modify how client device 210 is classified, thereby modifying how data flows, provided to/from client device 210 are processed. As an example, the design decision may be based on a performance study that identifies that a reclassification of client device 210 may lead to an increase in data flow processing efficiency. Additionally, or alternatively, the design decision may be based on a performance study that identifies that a modification in a policy set for a particular classification may lead to an increase in data flow processing efficiency.

While particular fields are shown in a particular format in data structure 400, in practice, data structure 400 may include additional fields, fewer fields, different fields, or differently arranged fields than are shown in FIG. 4. Also, FIG. 4 illustrates examples of information stored by data structure 400. In practice, other examples of information stored by data structure 400 are possible.

FIG. 5 illustrates a call flow diagram of example operations capable of being performed by an example portion 500 of environment 200. As shown in FIG. 5, portion 500 may include client device 210, network device 220, on-boarding server 240, subscription server 250, and/or classification server 260. Client device 210, network device 220, on-boarding server 240, subscription server 250, and/or classification server 260 may include components and/or perform functions described above in connection with, for example, one or more of FIGS. 1-3. FIG. 5 may correspond to example operations to reclassify client device 210. In FIG. 5, assume that client device 210 includes a classification and that network device 220 stores information that identifies the classification of client device 210.

In some implementations, classification server 260 may provide reclassification instruction 505 towards client device 210. For example, classification server 260 may provide reclassification instruction 505 based on receiving an update to a classification matrix stored by classification server 260

(e.g., from an operator of classification server 260 and/or based on a design decision to modify how client device 210 is classified).

In some implementations, subscription server 250 may provide reclassification instruction 506, for example, based on an update to subscription information stored by subscription server 250 and associated with client device 210. As described above, client device 210 may be classified based on attributes of client device 210. The attributes of client device 210 may include subscription information associated with client device 210 (e.g., information that identifies applications/services that client device 210 may access and/or information that relates to processing instructions for data flows provided to/from client device 210). Thus, client device 210 may be reclassified when the subscription information is modified.

In some implementations, on-boarding server 240 may provide reclassification instruction 505 and/or reclassification instruction 506 to client device 210 on behalf of subscription server 250 and/or classification server 260. Based on receiving reclassification instruction 505 and/or reclassification instruction 506, client device 210 may provide device attributes 520 to on-boarding server 240. In some implementations, client device 210 may provide device attributes 520 without receiving reclassification instruction 505 and/or reclassification instruction 506. For example, client device 210 may include a monitoring function that monitors attributes of client device 210 (e.g., functions, hardware/software configurations, data usage, applications/services implemented or accessed by client device 210, etc.). In some implementations, client device 210 may provide device attributes 520 when an attribute of client device 210 is modified. In some implementations, device attributes 520 may include a request to reclassify client device 210 based on the attributes of client device 210.

In some implementations, device attributes 520 may include an identifier (ID) of client device 210, such as a device ID, a media access control (MAC) address, a network access ID, a telephone number, and/or some other information that uniquely identifies client device 210. In some implementations, device attributes 520 may include information that identifies hardware, software, functions, and/or network interfaces implemented by client device 210. For example, attributes 520 may include a hardware profile that identifies hardware components implemented by client device 210 (e.g., processor information, storage information, memory information, sensor information, etc.). Additionally or alternatively, device attributes 520 may include a software profile that identifies software implemented by client device 210 (e.g., software/application information, middleware information, etc.).

Additionally or alternatively, device attributes 520 may include information identifying functions performed by client device 210 (e.g., connection management functions, data collection functions, control functions, device management functions, security management functions, etc.). Additionally or alternatively, device attributes 520 may include information identifying applications with which client device 210 communicates (e.g., applications implemented by app device 230). Additionally or alternatively, device attributes 520 may include an IP address and/or a geographic location associated with client device 210. Additionally or alternatively, device attributes 520 may include usage information of client device 210 (e.g., an amount of network resources used by client device 210). Additionally or alternatively, device attributes 520 may include subscription information of client device 210. Additionally or alternatively, device attributes 520 may

include some other information that identifies features, functions, components, and/or elements of client device 210.

As shown in FIG. 5, on-boarding server 240 may receive device attributes 520 and validate device attributes 520. As an example, assume that device attributes 520 include information identifying a geographic location of client device 210. Given this assumption, on-boarding server 240 may validate the geographic location information based on IP address information received via a session with client device 210. In some implementations, on-boarding server 240 may validate another device attribute, identified by device attributes 520, based on some other technique. In some implementations, on-boarding server 240 may provide device attributes 520 to classification server 260 based on validating device attributes 520.

As shown in FIG. 5, classification server 260 may receive device attributes 520 and may perform classification function 522 to reclassify client device 210 based on device attributes 520. For example, classification server 260 may store a classification matrix and may apply device attributes 520 to the classification matrix to reclassify client device 210. Examples of reclassifying client device 210 based on the classification matrix and based on device attributes 520 are described above with respect to classification matrix field 410. In some implementations, classification server 260 may provide classification information 525 to on-boarding server 240 based on performing classification function 522 to reclassify client device 210. In some implementations, classification information 525 may identify a classification of client device 210. For example, classification information 525 may include a classification ID that corresponds to a particular classification (e.g., a “type 1” classification, a “type 2 classification”, a “multiple application” classification, a “single application” classification, a “sensor-specific” classification, and/or some other type of classification).

In some implementations, on-boarding server 240 may receive classification information 525 and may provide classification parameters 530 to network device 220. In some implementations, classification parameters 530 may include classification information 525 in addition to an ID of client device 210. As shown in FIG. 5, network device 220 may receive classification parameters 530 and may perform policy update function 532 to associate an updated policy set with client device 210. For example, as described above with respect to classification policies field 420, network device 220 may store information that identifies a policy set to associate with client device 210 based on the classification of client device 210. In some implementations, network device 220 may identify a particular policy set, associated with the classification of client device 210 (e.g., based on information included in classification parameters 530), and may associate the ID of client device 210 with the particular policy set. For example, network device 220 may store the ID of client device 210 in a row of classification policies field 420 corresponding to the particular policy set and/or corresponding to the classification of client device 210. In some implementations, network device 220 may provide acknowledgement 535 to client device 210 (e.g., via on-boarding server 240) to indicate that client device 210 has been reclassified and that client device 210 may communicate with app device 230 via network device 220.

As shown in FIG. 5, network device 220 may provide a data flow (e.g., a data flow associated with a communication between client device 210 and app device 230) to/from client device 210 based on performing policy update function 532. In some implementations, network device 220 may process the data flow in accordance with the policy set associated with

client device 210. For example, network device 220 may determine an ID of client device 210, based on a session between client device 210 and network device 220, and may determine a corresponding policy set for the ID (e.g., based on information stored by classification policies field 420). As a result, network device 220 may process data flows based on a policy set that is particular to the classification of client device 210, thereby increasing efficiency in facilitating communication between client device 210 and app device 220 and increasing efficiency in processing data flows.

While a particular series of operations and/or data flows have been described above with regards to FIG. 5, the order of the operations and/or data flows may be modified in other implementations. Further, non-dependent operations may be performed in parallel. Also, in some implementations, some of the operations and/or data flows may be omitted. For example, on-boarding server 240 may store device attributes 520 and may provide device attributes 520 without receiving device attributes 520 from client device 210. Additionally, or alternatively, classification server 260 may store the device attributes of client device 210 and may reclassify client device 210 without involving client device 210 and/or on-boarding server 240.

FIGS. 6A-6B illustrate an example implementation as described herein. In FIG. 6A, assume that network device 220 stores classification information to identify a classification of client device 210. As described above, client device 210 may include an attribute monitoring function to monitor device attributes of client device 210. In FIG. 6A, assume that client device 210 identifies an update to a device attribute associated with client device 210. Given this assumption, client device 210 may provide device attributes to classification server 260 (e.g., via on-boarding server 240). As described above, the device attributes may include a request to reclassify client device 210. Based on receiving device attributes, classification server 260 may reclassify client device 210 and may provide, to network device 220, classification information that identifies the classification of client device 210. For example, classification server 260 may provide a classification ID (e.g., classification ID 1) and/or some other information that identifies the classification of client device 210. In some implementations, network device 220 may associate a particular policy set based on classification ID 1 (e.g., policy set 1) and may process a data flow provided to/from client device 210 using policy set 1. At a later point in time, classification server 260 may reclassify client device 210 based on an update to a classification matrix stored by classification server 260.

For example, referring to FIG. 6B, classification server 260 may receive an update to a classification matrix (e.g., from an operator of classification server 260) to reclassify client device 210. As shown in FIG. 6B, classification server 260 may provide a reclassification instruction to client device 210 (e.g., via on-boarding server 240). In some implementations, client device 210 may provide, to classification server 260, device attributes of client device 210 based on receiving the reclassification instruction. Additionally, or alternatively, on-boarding server 240 may provide the device attributes of client device 210 without involving client device 210. In some implementations, classification server 260 may reclassify client device 210 based on the device attributes of client device 210 and may provide a classification ID (e.g., classification ID 2), corresponding to the reclassification of client device 210, to network device 220. In some implementations, network device 220 may associate a particular policy set based on classification ID 2 (e.g., policy set 2) and may process a data flow provided to/from client device 210 using policy set

2. As a result, client device 210 may be reclassified at different points in time based on an update to device attributes of client device 210 and/or based on an update to classification matrix stored by classification server 260 (e.g., based on a design decision).

While a particular example is shown in FIGS. 6A-6B, it will be apparent that the above description is merely an example implementation. Other examples are possible from what is shown in FIGS. 6A-6B.

As described above, a policy set may be based on a classification of client device 210. In some implementations, the policy set may be predetermined for each classification to facilitate data flows provided to/from client devices 210. As a result, network device 220 may process data flows based on a policy set that is particular to the classification of client device 210, thereby increasing efficiency in facilitating communication and processing a data flow between client device 210 and app device 230. Further, client device 210 may be reclassified at different points in time based on an update to device attributes of client device 210 and/or based on an update to classification matrix stored by classification server 260 (e.g., based on a design decision). For example, the design decision may be based on a performance study that identifies that a reclassification of the client device may lead to an increase in data flow processing efficiency.

The foregoing description provides illustration and description, but is not intended to be exhaustive or to limit the possible implementations to the precise form disclosed. Modifications and variations are possible in light of the above disclosure or may be acquired from practice of the implementations.

It will be apparent that different examples of the description provided above may be implemented in many different forms of software, firmware, and hardware in the implementations illustrated in the figures. The actual software code or specialized control hardware used to implement these examples is not limiting of the implementations. Thus, the operation and behavior of these examples were described without reference to the specific software code—it being understood that software and control hardware can be designed to implement these examples based on the description herein.

Even though particular combinations of features are recited in the claims and/or disclosed in the specification, these combinations are not intended to limit the disclosure of the possible implementations. In fact, many of these features may be combined in ways not specifically recited in the claims and/or disclosed in the specification. Although each dependent claim listed below may directly depend on only one other claim, the disclosure of the possible implementations includes each dependent claim in combination with every other claim in the claim set.

No element, act, or instruction used in the present application should be construed as critical or essential unless explicitly described as such. Also, as used herein, the article “a” is intended to include one or more items and may be used interchangeably with “one or more.” Where only one item is intended, the term “one” or similar language is used. Further, the phrase “based on” is intended to mean “based, at least in part, on” unless explicitly stated otherwise.

What is claimed is:

1. A method comprising:

determining, by one or more devices of a network, one or more attributes of a client device that is associated with a particular classification;

determining, by the one or more devices, subscription information associated with the client device;

13

reclassifying, by the one or more devices, the client device based on the one or more attributes of the client device and based on the subscription information associated with the client device,
 the one or more attributes including at least one of a hardware profile, a software profile, a function, a geographic location, or a subscription profile;
 determining, by the one or more devices, classification information based on reclassifying the client device; and
 providing, by the one or more devices and to a network device of the network, the classification information to cause the network device to associate a particular policy set, of a plurality of policy sets, with the client device, the classification information identifying an updated classification of the client device,
 the updated classification being different from the particular classification,
 the particular policy set being based on the updated classification of the client device, and
 the particular policy set including an instruction used to process a data flow provided to or provided from the client device.

2. The method of claim 1, further comprising:
 receiving an update to a classification matrix used to reclassify the client device,
 where reclassifying the client device comprises:
 reclassifying the client device based on the one or more attributes of the client device, based on the subscription information associated with the client device, and based on receiving the update to the classification matrix.

3. The method of claim 1,
 where determining the subscription information comprises:
 receiving, from a subscription server, an update to the subscription information associated with the client device, and
 where reclassifying the client device comprises:
 reclassifying the client device based on the one or more attributes of the client device and based on receiving the update to the subscription information.

4. The method of claim 1, further comprising:
 receiving, from the client device, updated attribute information that includes information identifying the one or more attributes of the client device,
 where reclassifying the client device comprises:
 reclassifying the client device based on the updated attribute information and based on the subscription information associated with the client device.

5. The method of claim 1, where the one or more attributes further include an internet protocol (IP) address of the client device.

6. The method of claim 1, where the instruction used to process the data flow causes the network device to provide the data flow with a particular network resource.

7. The method of claim 1,
 where the classification information includes an identifier of the client device, and
 where the network device associates the client device with the particular policy set based on the identifier of the client device.

8. The method of claim 1, further comprising:
 receiving an acknowledgement from the network device after the network device associates the particular policy set with the client device; and

14

providing the acknowledgement to the client device to cause the client device to provide or receive the data flow.

9. The method of claim 1, where the client device is a machine-to-machine (M2M) device that includes at least one of a sensor or an application.

10. A system comprising:
 one or more devices to:
 determine a plurality of attributes of a client device that is associated with a particular classification;
 determine subscription information associated with the client device;
 reclassify the client device based on the plurality of attributes of the client device and based on the subscription information associated with the client device,
 the plurality of attributes including at least one of a hardware profile, a software profile, a function, a geographic location, or a subscription profile;
 determine classification information based on reclassifying the client device; and
 provide, to a network device of a network, the classification information to cause the network device to associate a particular policy set, of a plurality of policy sets, with the client device,
 the classification information identifying an updated classification of the client device,
 the updated classification being different than the particular classification,
 the particular policy set being based on the updated classification of the client device, and
 the particular policy set including an instruction used to process a data flow provided to or provided from the client device.

11. The system of claim 10,
 where the one or more devices are further to:
 receive an update to a classification matrix used to reclassify the client device, and
 where, when reclassifying the client device, the one or more devices are to:
 reclassify the client device based on the plurality of attributes of the client device, based on the subscription information associated with the client device, and based on receiving the update to the classification matrix.

12. The system of claim 10,
 where, when determining the subscription information, the one or more devices are to:
 receive an update to the subscription information associated with the client device, and
 where, when reclassifying the client device, the one or more devices are to:
 reclassify the client device based on the one or more attributes of the client device and based on receiving the update to the subscription information.

13. The system of claim 10,
 where the one or more devices are further to:
 receive updated attribute information that includes information identifying the plurality of attributes of the client device, and
 where, when reclassifying the client device, the one or more devices are to:
 reclassify the client device based on the updated attribute information and based on the subscription information associated with the client device.

15

14. The system of claim 10, where the plurality of attributes further include an internet protocol (IP) address of the client device.

15. The system of claim 10, where the instruction used to process the data flow causes the network device to provide the data flow with a particular network resource.

16. The system of claim 10, where the client device is a machine-to-machine (M2M) device that includes at least one of a sensor or an application.

17. A non-transitory computer-readable medium for storing instructions, the instructions comprising:

a plurality of instructions which, when executed by one or more processors, cause the one or more processors to:

determine a plurality of attributes of a client device that is associated with a particular classification;

determine subscription information associated with the client device;

reclassify the client device based on the plurality of attributes of the client device and based on the subscription information associated with the client device,

the plurality of attributes including at least one of a hardware profile, a software profile, a function, a geographic location, or a subscription profile;

determine classification information based on reclassifying the client device; and

provide, to a network device of a network, the classification information to a network device to cause the network device to associate a particular policy set, of a plurality of policy sets, with the client device, the classification information identifying an updated classification of the client device,

the updated classification being different than the particular classification;

the particular policy set being based on the updated classification of the client device,

16

the particular policy set including an instruction used to process a data flow provided to or provided from the client device, and

the instruction to process the data flow causing the network device to provide the data flow with a particular network resource.

18. The non-transitory computer-readable medium of claim 17,

where the plurality of instructions further cause the one or more processors to:

receive an update to a classification matrix used to reclassify the client device; and

where one or more instructions, of the plurality of instructions, to reclassify the client device, cause the one or more processors to:

reclassify the client device further based on the plurality of attributes of the client device, based on the subscription information associated with the client device, and base on receiving the update to the classification matrix.

19. The non-transitory computer-readable medium of claim 17,

where the plurality of instructions further cause the one or more processors to:

receive updated attribute information that includes information identifying the plurality of attributes of the client device, and

where one or more instructions, of the plurality of instructions, to reclassify the client device, further cause the one or more processors to:

reclassify the client device based on the updated attribute information and based on the subscription information associated with the client device.

20. The non-transitory computer-readable medium of claim 17, where the plurality of attributes further include an internet protocol (IP) address of the client device.

* * * * *