



(51) International Patent Classification:

G06F 15/00 (2006.01)

G06F 21/50 (2013.01)

(21) International Application Number:

PCT/CN2020/103338

(22) International Filing Date:

21 July 2020 (21.07.2020)

(25) Filing Language:

English

(26) Publication Language:

English

(71) Applicant: ARRIS ENTERPRISES LLC [US/US]; 3871

Lakefield Drive, Suwanee, Georgia 30024 (US).

(72) Inventors: WANG, Tao; F2 Building, FuTongCheng

Garden, Bao'an District, Shenzhen, Guangdong 518000

(CN). WANG, Tao; Hongjingyuan 1C-702, Baomin

Road of Bao'an District, Shenzhen, Guangdong 518000

(CN). WANG, Xin; Room 202, Building 1, Lizhiyuan,

Huaqiaocheng, Nanshan District, Shenzhen, Guangdong

518000 (CN). ZHAO, Wenji; South Second Lane No. 1

Room 803, Village of Pinus Tabulaeformis, Longhua Dis-

trict, Shenzhen, Guangdong 518000 (CN). YANG, Jin-

qing; Room 20E, Unit A, Building D, Xindejiayuan Gar-

den, Qianhai Road, Nanshan District, Shenzhen, Guang-

dong 518000 (CN).

(74) Agent: CHINA SINDA INTELLECTUAL PROPERTY

LIMITED; B11th Floor, Focus Place, 19 Financial Street,

Xicheng District, Beijing 100033 (CN).

(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, DJ, DK, DM, DO,

DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN,

HR, HU, ID, IL, IN, IR, IS, IT, JO, JP, KE, KG, KH, KN,

KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD,

ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO,

NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW,

SA, SC, SD, SE, SG, SK, SL, ST, SV, SY, TH, TJ, TM, TN,

TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, ZA, ZM, ZW.

(84) Designated States (unless otherwise indicated, for every

kind of regional protection available): ARIPO (BW, GH,

GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ,

UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ,

TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK,

EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV,

MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM,

TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW,

KM, ML, MR, NE, SN, TD, TG).

(54) Title: GENERATING AN AUDIO MESSAGE AT A NETWORK DEVICE IN RESPONSE TO DETECTION OF A NETWORK EVENT

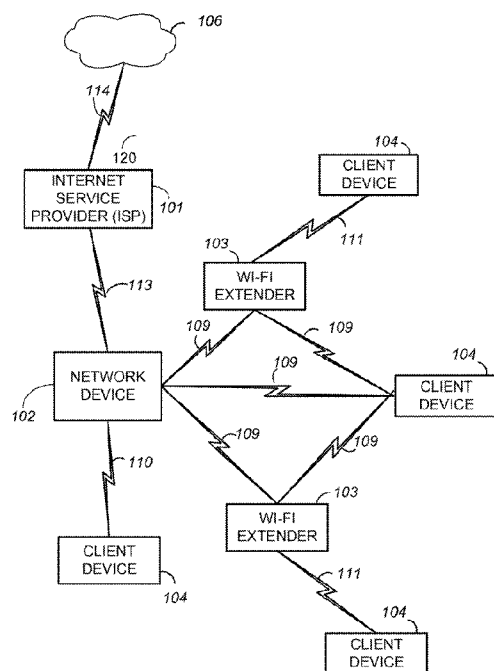


FIG. 1

(57) Abstract: A network device for providing an audio alarm by a network device. A user interface is used to configure the network device to generate an audio message associated with detection of an event. The network device using a management tool to detect the event. The management tool triggers generation of the audio message in response to detection of the event. An audio device that includes a speaker receives the audio message. The audio message is broadcast using the speaker.

**Published:**

- *with international search report (Art. 21(3))*
- *with amended claims (Art. 19(1))*

## GENERATING AN AUDIO MESSAGE AT A NETWORK DEVICE IN RESPONSE TO DETECTION OF A NETWORK EVENT

### BACKGROUND

[0001] The subject matter of the present disclosure relates generally to detecting a network event and generating an audio message at a network device in response to detecting the network event.

[0002] The difficulty of managing a network is directly proportional to its complexity. As networks grow in complexity, so too does the difficulty of managing the network. Alarms provide feedback that network processes or network elements themselves are not functioning as intended. However, alarms are communicated using LEDs, log files, or email. Such alarms are often missed by network managers responsible for maintaining the network the first time an alarm triggering event occurs.

### SUMMARY

[0003] An aspect of the present disclosure involves detecting a network event and generating an audio message at a network device in response to detecting the network event.

[0004] A network device is configured via a user interface to generate an audio message associated with detection of an event. A management tool monitors the network device to detect events. The management tool may include a network manager, a database of management information describing objects defining events of the network device, and a network agent. The network agent monitors the objects of the network device to detect an event based on the objects described in the database of management information. The network agent sends an indication of an event to the network manager. Events are entered into in the database of management information.

[0005] Upon receiving the indication of an event from the network agent, the network manager may trigger the generation of the audio message. The audio message is received at an audio device of the network device that includes a speaker and is broadcast using the speaker. The audio message may be an audio alarm message that indicates that an abnormal status of the network device was detected, that a parental control rule was triggered, or that an attempt was made by hackers to invade the network device. The audio message may also be an audible announcement of the service set identifier and password.

[0006] A firewall may be provided, wherein a firewall setting may be presented in a user interface. The user interface allows navigation to a speaker parameter selection page. On the speaker parameter page, an interface may be presented for enabling or disabling the audio alarm; and to select an audio message class, such as all, normal, or custom. The custom class allows the user to select the alarm type to use.

#### BRIEF SUMMARY OF THE DRAWINGS

[0007] The detailed description is set forth with reference to the accompanying figures. In the figures, the left-most digit(s) of a reference number identifies the figure in which the reference number first appears. The use of the same reference numbers in different figures indicates similar or identical items or features.

[0008] Fig. 1 is a schematic diagram of a system implementing the network device.

[0009] Fig. 2 illustrates a network device.

[0010] Fig. 3 is a diagram of a management tool.

[0011] Fig. 4 is a diagram illustrating a user interface to manage audio messages.

[0012] Fig. 5 illustrates a user interface to manage the audio message types provided to the speaker.

[0013] Fig. 6 is a flow chart illustrating generation of an audio message in response to detecting a network event.

[0014] While implementations are described herein by way of example, those skilled in the art will recognize that the implementations are not limited to the examples or figures described. It is understood that the figures and detailed description thereto are not intended to limit implementations to the particular form disclosed but, on the contrary, the intention is to cover modifications, equivalents, and alternatives falling within the spirit and scope as defined by the appended claims. The headings used herein are for organizational purposes and are not meant to be used to limit the scope of the description or the claims. As used throughout this application, the word “may” is used in a permissive sense (i.e., meaning having the potential to), rather than the mandatory sense (i.e., meaning must). Similarly, the words “include,” “including,” and “includes” mean including, but not limited to.

## DETAILED DESCRIPTION

[0015] Fig. 1 is a schematic diagram of a system implementing the network device.

[0016] As shown in Fig. 1, the main elements of the system include a network device 102 connected to the Internet 106 via an Internet Service Provider (ISP) 101 and also connected to different wireless devices such as wireless extenders 103 and client devices 104. The system shown in Fig. 1 includes wireless devices (e.g., wireless extenders 103 and client devices 104) that may be connected in one or more wireless networks (e.g., private, guest, iControl, backhaul network, or Internet of things (IoT) network) within the system. Additionally, there could be some overlap between wireless devices (e.g., wireless extenders 103 and client devices 104) in the different networks. That is, one or more network devices could be located in more than one network. For example, the wireless extenders 103 could be located both in a private network for providing content and information to a client device 104 and also included in a backhaul network or an iControl network.

[0017] Starting from the top of Fig. 1, the ISP 101 can be, for example, a streaming video provider or any computer for connecting the network device 102 to the Internet 106. The connection 114 between the Internet 106 and the ISP 101 and the connection 113 between the ISP 101 and the network device 102 can be implemented using a wide area network (WAN), a virtual private network (VPN), metropolitan area networks (MANs), system area networks (SANs), a DOCSIS network, a fiber optics network (e.g., FTTH (fiber to the home) or FTTX (fiber to the x), or hybrid fiber-coaxial (HFC)), a digital subscriber line (DSL), a public switched data network (PSDN), a global Telex network, or a 2G, 3G, 4G or 5G network, for example.

[0018] The connection 113 can further include as some portion thereof a broadband mobile phone network connection, an optical network connection, or other similar connections. For example, the connection 113 can also be implemented using a fixed wireless connection that operates in accordance with, but is not limited to, 3rd Generation Partnership Project (3GPP) Long Term Evolution (LTE) or 5G protocols. It is also contemplated by the present disclosure that connection 113 is capable of providing connections between the network device 102 and a WAN, a LAN, a VPN, MANs, PANs, WLANs, SANs, a DOCSIS network, a fiber optics network (e.g., FTTH, FTTX, or HFC), a PSDN, a global Telex network, or a 2G, 3G, 4G or 5G network, for example.

[0019] The network device 102 can be, for example, a hardware electronic device that may be a combination modem and gateway device that combines the functions of a modem, an access point, and/or a router for providing content received from the content provider 101 to network devices (e.g., wireless extenders 103 and client devices 104) in the system. It is also contemplated by the present disclosure that the network device 102 can include the function of, but is not limited to, an Internet Protocol/Quadrature Amplitude Modulator (IP/QAM) set-top box (STB) or smart media device (SMD) that is capable of decoding audio/video content, and playing over-the-top (OTT) or multiple system operator (MSO) provided content.

[0020] The connection 109 between the network device 102, the wireless extenders 103, and client devices 104 can be implemented using a wireless connection in accordance with any IEEE 802.11 Wi-Fi protocols, Bluetooth protocols, Bluetooth Low Energy (BLE), or other short range protocols that operate in accordance with a wireless technology standard for exchanging data over short distances using any licensed or unlicensed band such as the citizens broadband radio service (CBRS) band, 2.4 GHz bands, 5 GHz bands, or 6 GHz bands. Additionally, the connection 109 can be implemented using a wireless connection that operates in accordance with, but is not limited to, RF4CE protocol, ZigBee protocol, Z-Wave protocol, or IEEE 802.15.4 protocol. It is also contemplated by the present disclosure that the connection 109 can include connections to a media over coax (MoCA) network. One or more of the connections 109 can also be a wired Ethernet connection.

[0021] The wireless extenders 103 can be, for example, hardware electronic devices such as access points used to extend the wireless network by receiving the signals transmitted by the network device 102 and rebroadcasting the signals to, for example, client devices 104, which may out of range of the network device 102. The wireless extenders 103 can also receive signals from the client devices 104 and rebroadcast the signals to the network device 102, or other client devices 104.

[0022] The connection 111 between the wireless extenders 103 and the client devices 104 are implemented through a wireless connection that operates in accordance with any IEEE 802.11 Wi-Fi protocols, Bluetooth protocols, Bluetooth Low Energy (BLE), or other short range protocols that operate in accordance with a wireless technology standard for exchanging data over short distances using any licensed or unlicensed band such as the CBRS band, 2.4 GHz bands, 5 GHz bands, or 6 GHz bands. Additionally, the connection 111 can be implemented

using a wireless connection that operates in accordance with, but is not limited to, RF4CE protocol, ZigBee protocol, Z-Wave protocol, or IEEE 802.15.4 protocol. Also, one or more of the connections 111 can be a wired Ethernet connection.

[0023] The client devices 104 can be, for example, hand-held computing devices, personal computers, electronic tablets, smart phones, smart speakers, IoT devices, iControl devices, portable music players with smart capabilities capable of connecting to the Internet, cellular networks, and interconnecting with other devices via Wi-Fi and Bluetooth, or other wireless hand-held consumer electronic devices capable of executing and displaying content received through the network device 102. Additionally, the client devices 104 can be a TV, an IP/QAM STB or an SMD that is capable of decoding audio/video content and playing over OTT or MSO provided content received through the network device 102.

[0024] The connection 110 between the network device 102 and the client device 104 is implemented through a wireless connection that operates in accordance with, but is not limited to, any IEEE 802.11 protocols. Additionally, the connection 110 between the network device 102 and the client device 104 can also be implemented through a WAN, a LAN, a VPN, MANs, PANs, WLANs, SANs, a DOCSIS network, a fiber optics network (e.g., FTTH, FTTX, or HFC), a PSDN, a global Telex network, or a 2G, 3G, 4G or 5G network, for example.

[0025] The connection 110 can also be implemented using a wireless connection in accordance with Bluetooth protocols, Bluetooth Low Energy (BLE), or other short range protocols that operate in accordance with a wireless technology standard for exchanging data over short distances using any licensed or unlicensed band such as the CBRS band, 2.4 GHz bands, 5 GHz bands, or 6 GHz bands. One or more of the connections 110 can also be a wired Ethernet connection.

[0026] A detailed description of the exemplary internal components of the network device 102, the wireless extenders 103, and the client devices 104 shown in Fig. 1 will be provided in the discussion of Fig 2. However, in general, it is contemplated by the present disclosure that the network device 102, the wireless extenders 103, and the client devices 104 include electronic components or electronic computing devices operable to receive, transmit, process, store, and/or manage data and information associated with the system, which encompasses any suitable processing device adapted to perform computing tasks consistent with

the execution of computer-readable instructions stored in a memory or a computer-readable recording medium.

[0027] Further, any, all, or some of the computing components in the network device 102, the wireless extenders 103, and the client devices 104 may be adapted to execute any operating system, including Linux, UNIX, Windows, MacOS, DOS, and ChromOS as well as virtual machines adapted to virtualize execution of a particular operating system, including customized and proprietary operating systems. The network device 102, the wireless extenders 103, and the client devices 104 are further equipped with components to facilitate communication with other computing devices over the one or more network connections to local and wide area networks, wireless and wired networks, public and private networks, and any other communication network enabling communication in the system.

[0028] Fig. 2 illustrates a network device 200.

[0029] In Fig. 2, the network device 200 includes a user interface 210, a processor 220, an audio device 230, a network manager 240 (e.g., a management tool), and memory 250. The network device 200 also includes a network interface 260 for connecting one or more client device(s) 270, for example, using a wireless local area network 280, such as Wi-Fi.

[0030] The network manager 240 may be implemented using software elements (e.g., code embodied on a machine-readable medium) or hardware elements. For example, processor 220 may be configured to execute instructions 222 stored on said memory 250 to cause said network device 200 to provide the network manager 240 and user interface 210. The processor 220 may thus execute the processes carried out by the network manager 240. Communication between the components (e.g., 210, 220, 230, 240, 250, 260) of the network device 200 may be established using an internal bus 290.

[0031] Certain subject matter of the present disclosure is described herein as including logic or a number of components, units, elements, or mechanisms. The network device 200 may constitute either software elements (e.g., code embodied on a machine-readable medium) or hardware elements. A “hardware element” is a tangible unit capable of performing certain operations and may be configured or arranged in a certain physical manner. In various example, one or more computer systems (e.g., a standalone computer system, a client computer system, or a server computer system) or one or more hardware elements of a computer system (e.g., a processor or a group of processors) may be configured by software (e.g., an application or

application portion) as a hardware element that operates to perform certain operations as described herein.

[0032] The network manager 240 monitors the network 280 and connections by client device(s) 270. The network manager 240 detects an event 242 and generates an audio message 244. The audio message 244 may be selected by the network manager 240 from audio files 252 stored in memory 250. The network manager 240 selects an appropriate audio file 252 that is appropriate for the event 242 detected by the network manager 240. The audio message 244 is provided to audio device 230. Audio device 230 processes the audio message into an analog signal that may be emitted by speaker 232. For example, the audio message 244 may be a digital audio message that is converted into an analog signal 232 by signal processing 234, which may need to be amplified before transmitted to the speaker 236. Signal processing 234 may be implemented by processor 220. Speaker 236 receives the analog signal 232 and converts the analog signal to audio waves 238 that are perceptible by a user.

[0033] Audio message 244 may be an audio message that provides data to the user. Alternatively, or in addition to, the audio message 244 may provide warnings in the form of audio alarm messages. The speaker 236 may provide audio alarms that indicate an abnormal status of the network device 200, e.g., the network device 200 failed to start, an Internet connection was lost, a high temperature condition of processor 220 exist. The network manager 240 may also detect cyberattacks, such as a denial of service (DoS) attack and issue an alarm that indicates a particular cyberattack has taken place.

[0034] The audio message 244 may be a parental control violation audio alarm that indicates, for example, that a child tried to access some blocked websites, or tried to access the Internet during an unallowed period. The audio message 244 may be an audio alarm that indicates that someone has tried to hack into the home Wi-Fi network 260. For example, the network manager 240 may determine that multiple, different Wi-Fi passwords attempts have been made. Further, an authorize user may request identification of the name of the network, i.e., the service set identification (SSID) and password, and the network manager 240 may broadcast an audio message 244 that identifies the name of the network (SSID) and the password. Other features could also use the speaker 236 to perform other functions.

[0035] User interface 210 may include a graphic user interface (GUI) 212. The GUI 212 may be used to configure different settings for network manager 240. The configuration settings

accessible via the GUI 212 may be provided by files stored in memory 250. The configuration files stored in memory 250 may include an application 214, a Multiple System Operators (MSO) file 215, a Management Information Base (MIB) file 216, a Technical Report-069 (TR-069) file 217, etc. An application 214 may be downloaded and stored in memory 250. The application 214 may provide for network fault monitoring by network manager 240. MSO files 215 may be provided by one or more cable television systems to configure different components, such as network manager 240. MIBs 216 provide a database that is used for managing the entities in a network, such as network device 200 and client device(s) 270. MIBs 216 include information about standard network information, such as IP addresses, network interface settings, and Simple Network Management Protocol (SNMP) definitions. As one example, SNMP may be used to manage network resources. SNMP allows for creation of SNMP traps and conversion into alerts for managing the network device 200. Notifications, such as alert messages, are sent from a remote device, e.g., network device 200, client device(s) 270, to a central collector, such as network manager 240. TR-069 provides for the communication between a client device and an Auto-Configuration Server (ACS). The network manager 240 may also broadcast a SSID and password message 272 to client device 270 that is running a mobile application 274. For example, a guest may want to connect to the private SSID. Mobile application 274 may communicate with network manager 240, and if authorization is granted, the network manager 240 may cause the SSID and password message 272 to be sent to the mobile application 274.

[0036] GUI 212 may be used to implement firewall level settings. GUI 212 may display a page that allows navigation to a page for configuration of the speaker 236. The GUI 212 may then be used to enable/disable audio messages by the speaker 236. In addition, the GUI 212 may be used to select which class to use: All/Normal/Custom. The default value may be chosen to be the normal configuration and alarm types selected for the normal configuration may be used. Selection of custom class allows the user may select the alarm type to use for any particular event 242.

[0037] Fig. 3 is a diagram of a management tool 300.

[0038] In Fig. 3, the management tool 300 includes a network manager 310, database of management information 320, e.g., MIB, and network agents 330. The network manager 310 manages the client devices by accessing the database of management information 320, e.g., MIB. The database of management information 320 includes a collection of managed objects that may

be accessed using network-management protocols, e.g., SNMP. A network agent 330 monitors objects included in the database of management information 320. The network agent 330 detects events associated with the objects and sends notifications and data to the network manager 310. The events are logged by the network agent 330 into the database of management information 320. The network manager 310 receives the notifications and collects data from the network agents 330. The network agent 330 sends alerts called traps and answers requests that were sent by the network manager 310. The network manager 310 captures and decodes the traps. The network manager 310 may also request specific information from the network agent 330. Information is passed through requests and replies with the use of the MIB 320. The network manager 310 is responsible for decoding the packets and providing an interface to an administrator. The GUI 212 may be used to provide an interface for managing and configuring the management tool 300.

**[0039]** Fig. 4 is a diagram illustrating a user interface 400 to manage audio messages

**[0040]** In Fig. 4, the user interface 400 includes an area for page navigation 410. A main web page 410 for configuration of a network device is provided. The main web page provides firewall settings 412 and a selection 414 for navigating to a hardware parameter selection page 420. The hardware parameter selection page 420 includes selections for hardware choices 422 and a selection 424 for navigating to a speaker parameter selection page 430. Speaker parameter selection page 430 include options for setting speaker parameters 432.

**[0041]** User interface 400 also includes a sub-interface for controlling audio messages 440. The user may select to enable audio messages 442 or may select to disable audio messages 444. User interface further includes a sub-interface for selecting a speaker class to use 450. The user may select All 452, Normal 454, and Custom 456. The default value may be chosen to be the normal configuration 454 where alarm types selected for the normal configuration may be used. The user selects custom class 456, which allows the user may to select the alarm type to use for any particular event. Once a selection is made, the audio message types may be selected, as described in further detail with reference to Fig. 5

**[0042]** Fig. 5 illustrates a user interface 500 to manage the audio message types provided to the speaker.

**[0043]** In Fig. 5, four different audio message types 510, 520, 530, 540 are shown. The first message type 510 is for an audio alarm message indicating an abnormal status of the

network device. Under the first audio alarm message type 510, the user may select to generate an audio alarm message reporting the system failed to start via checking the status for system key interfaces of the network device (e.g., eRouter/eCM) 512. The user may generate an audio alarm message reporting that an Internet connection was lost 514 as determined, for example, by pinging the WAN side of an eRouter and determining that the WAN side is not responding. Also, the first audio alarm message type 510 may include an audio alarm message reporting a high temperature once the CPU temperature exceeds a predetermined value 516.

[0044] The second type of audio alarm message 520 includes audio alarm messages that indicate parental control rules have triggered an alarm. The second type of audio alarm message 520 may include an audio alarm message that is triggered by a child trying to access some blocked websites or by a child trying to access the Internet during an unallowed time 522. The second type of audio alarm message 520 may also include an audio alarm message stating that the firewall logs should be checked to detect whether rules have been triggered and reporting the status 524.

[0045] The third type of audio message 530 includes audio alarm messages that indicate hackers have attempted to invade the network. The third type of audio alarm message 530 may include an audio alarm message warning that someone has been continuously trying different Wi-Fi passwords to attempt to connect to a private SSID 532. The third type of audio alarm message 530 may also include an audio alarm message stating that DoS attacks have been detected by the firewall 534.

[0046] The fourth type of audio message 540 includes audio messages that broadcast the SSID/password for the network. The fourth type of audio message 540 may include an audio message announcing the SSID and password for the network 542 that is generated by a guest requesting connection to the network and the system determines the guest is authorized to access the network. The SSID and password for the network may be broadcast to the network device and/or to a mobile application 542. This message type 540 is enabled by the owner of the network.

[0047] Fig. 6 is a flow chart 600 illustrating generation of an audio message in response to detecting a network event.

[0048] In Fig. 6, it is assumed that the network device includes software stored in memory, which when executed perform functions and operations of the subject matter of the

present disclosure. In Fig. 6, method 600 starts (S602), and the network device is configured via a user interface to generate an audio message associated with detection of an event (S610). Referring to the description of the network device 200 in Fig. 2, user interface 210 may include a graphic user interface (GUI) 212. The GUI 212 may be used to configure different settings for network manager 240. The configuration settings accessible via the GUI 212 may be provided by files stored in memory 250. The network manager 240 monitors the network to detect an event 242 and generates an audio message 244. The audio message 244 may be selected by the network manager 240 from audio files 252 stored in memory 250.

[0049] Management commands are initiated by the network manager (S614). For example, referring again to the description of the network device 200 in Fig. 2, the network manager 240 may begin to monitor the network 280 and connections by client device(s) 270. The network manager 240 may detect an event 242 and generates an audio message 244. Monitoring notifications are received by the network manager from an object of the network device (S618). A network agent 330 monitors objects and sends notifications to the network manager 310. The network manager 310 collects data sent from the network agents 330.

[0050] Events of the network device are described by objects stored in the database of management information (S622). Referring to the description of management tool 300 in Fig. 3, the database of management information 320 includes a collection of managed objects that may be accessed using network-management protocols, e.g., SNMP.

[0051] The objects of the network device are monitored by a network agent to detect events based on the objects described in the database of management information (S626). Referring to the description of management tool 300 in Fig. 3, the network agent 330 monitors objects included in the database of management information 320.

[0052] An indication of the event is sent by the network agent to the network manager (S630). The network agent 330 detects events associated with the objects and sends notifications and data to the network manager 310. The network manager 310 receives the notifications and collects data from the network agents 330.

[0053] The events are logged by the network agent into the database of management information (S634). Referring again to the description of management tool 300 in Fig. 3, the events are logged by the network agent 330 into the database of management information 320.

[0054] An audio message is generated by the network manager upon receiving the indication of the event is received from the network agent (S638). Referring again to the description of the network device 200 in Fig. 2, the network manager 240 detects an event 242 and generates an audio message 244. The audio message 244 may be selected by the network manager 240 from audio files 252 stored in memory 250. The network manager 240 selects an appropriate audio file 252 that is appropriate for the event 242 detected by the network manager 240.

[0055] The audio message is received at an audio device (e.g., a network device 200 and/or client device 270 running a mobile application 274) (S642). The audio message is played using the speaker (S646). Referring again to the description of the network device 200 in Fig. 2, speaker 236 receives the analog signal 232 and converts the analog signal to audio waves 238 that are perceptible by a user.

[0056] The processes discussed in this disclosure may be implemented in hardware, software, or a combination thereof. In the context of software, the described operations represent computer-executable instructions stored on one or more non-transitory computer readable recording medium that, when executed by one or more hardware processors, perform the recited operations. Generally, computer-executable instructions include routines, programs, objects, components, data structures, and the like that perform particular functions or implement particular abstract data types. Those having ordinary skill in the art will readily recognize that certain steps or operations illustrated in the figures above may be eliminated, combined, or performed in an alternate order. Any steps or operations may be performed serially or in parallel. Furthermore, the order in which the operations are described is not intended to be construed as a limitation.

[0057] Subject matter of the present disclosure may be provided as a computer program product including one or more non-transitory computer readable recording medium having stored thereon instructions (in compressed or uncompressed form) that may be used to program a computer (or other electronic device) to perform processes or methods described herein. The computer-readable storage media may include one or more of an electronic storage medium, a magnetic storage medium, an optical storage medium, a quantum storage medium, or the like. For example, the computer-readable storage media may include, but are not limited to, hard drives, floppy diskettes, optical disks, read-only memories (ROMs), random access memories

(RAMs), erasable programmable ROMs (EPROMs), electrically erasable programmable ROMs (EEPROMs), flash memory, magnetic or optical cards, solid-state memory devices, or other types of physical media suitable for storing electronic instructions. Further, subject matter of the present disclosure may also be provided as a computer program product including a transitory machine-readable signal (in compressed or uncompressed form). Examples of machine-readable signals, whether modulated using a carrier or unmodulated, include, but are not limited to, signals that a computer system or machine hosting or running a computer program may be configured to access, including signals transferred by one or more networks. For example, a transitory machine-readable signal may comprise transmission of software by the Internet.

[0058] Separate instances of these programs can be executed on or distributed across any number of separate computer systems. Thus, although certain steps have been described as being performed by certain devices, software programs, processes, or entities, this need not be the case. A variety of alternative implementations will be understood by those having ordinary skill in the art.

[0059] Use of the phrases “capable of,” “capable to,” “operable to,” or “configured to”, refers to some apparatus, logic, hardware, and/or element designed in such a way to enable use of the apparatus, logic, hardware, and/or element in a specified manner. The subject matter of the present disclosure is provided as examples of apparatus, systems, methods, and programs for performing the features described in the present disclosure. However, further features or variations are contemplated in addition to the features described above. It is contemplated that the implementation of the components and functions of the present disclosure can be done with any newly arising technology that may replace any of the above implemented technologies.

[0060] Additionally, those having ordinary skill in the art readily recognize that the techniques described above can be utilized in a variety of devices, environments, and situations. Although the subject matter has been described in language specific to structural features or methodological acts, it is to be understood that the subject matter defined in the appended claims is not necessarily limited to the specific features or acts described. Rather, the specific features and acts are disclosed as exemplary forms of implementing the claims.

## CLAIMS

What is claimed is:

1. A network device, comprising:
  - a user interface for configuring the network device to generate an audio message associated with detection of an event;
  - a memory;
  - a speaker; and
  - a processor configured to execute instructions stored on said memory to cause said network device to:
    - monitor the network device to detect the event;
    - trigger generation of the audio message in response to the detecting of the event;and
  - broadcast the audio message using the speaker.
2. The network device of claim 1, wherein:
  - the memory has stored thereon a database of management information describing objects defining events of the network device;
  - the processor is further configured to execute the instructions stored on said memory to cause said network device to:
    - initiate management commands and receive monitoring notifications from an object of the network device;
    - monitor the objects of the network device to detect the event based on the objects described in the database of management information;
    - send an indication of the event to the network manager;
    - log the events in the database of management information, and
    - generate the audio upon receiving the indication of the network event.

3. The network device of claim 1, wherein the processor is further configured to execute the instructions stored on said memory to cause said network device to broadcast an audio message indicating at least one of:

- an abnormal status of the network device was detected,
- a parental control rule was triggered,
- an attempt by hackers to invade the network device, and
- the service set identifier and password, wherein the broadcast of the audio message further comprises broadcasting the service set identifier and password to a mobile application.

4. The network device of claim 3, wherein the broadcast of the audio message comprises broadcast of an audio alarm message indicating the abnormal status of the network device was detected, wherein the broadcast of the audio alarm message indicating the abnormal status of the network further comprises broadcasting an audio alarm message indicating at least one of the network device failed to start based on a key system interface status, an IP connection was lost once a ping of a WAN side of the network device fails, and the temperature of the processor exceeds a predetermine high temperature level.

5. The network device of claim 3, wherein the broadcast of the audio message comprises broadcast of an audio alarm message indicating the parental control rule was triggered, wherein the broadcast of the audio alarm message indicating the parental control rule was triggered further comprises broadcasting at least one of an audio alarm message that an attempt to access a block website was detected, an audio alarm message that an attempt to access the Internet occurred at a blocked time, and an audio alarm message that a firewall logs indicate at least one rule were violated.

6. The network device of claim 3, wherein the broadcast of the audio message comprises broadcast of an audio alarm message indicating an attempt by hackers to invade the network device, wherein the broadcast of the audio alarm message indicating an attempt by hackers to invade the network device further comprises broadcasting an audio alarm message indicating that attempts to connect to a private service set identifier using a plurality of different

incorrect passwords or broadcasting an audio alarm message indicating a denial of service (DoS) attack detected by a firewall.

7. The network device of claim 1 further comprising a firewall setting presented through accessing a web page associated with the user interface, and navigating from a main web page to hardware parameter selection page and then to a speaker parameter selection page, wherein the speaker parameter selection page includes an interface for enabling or disabling the audio alarm, and an interface to select one of all, normal, or custom class, wherein the custom class allows the user to select the alarm type to use.

8. The network device of claim 1, wherein the user interface is provided by at least one selecting from the group consisting of an audio alarm application, a network management tool, a configuration file, and TR-069, the user interface further comprising a graphical user interface (GUI) for management of the audio messages.

9. The network device of claim 1, wherein the audio message broadcast using the speaker comprises a voice speaking at least one word.

10. A method for providing an audio alarm by a network device, comprising:  
configuring the network device via a user interface to generate an audio message associated with detection of an event;  
monitoring the network device, using a management tool, to detect the event;  
triggering, by the management tool, generation of the audio message in response to the detecting of the event;  
receiving the audio message at an audio device of the network device that includes a speaker; and  
broadcasting the audio message using the speaker.

11. The method of claim 10, wherein the management tool comprises a network manager, a database of management information describing objects defining events of the network device, and a network agent, wherein the method further comprises:

- initiating, by the network manager, management commands;
- receiving, by the network manager, monitoring notifications from an object of the network device;
- describing, by objects stored in the database of management information, events of the network device;
- monitoring, by a network agent, the objects of the network device to detect the event based on the objects described in the database of management information;
- sending, by the network agent, an indication of the event to the network manager;
- logging, by the network agent, the events in the database of management information;

and

generating, by the network manager upon receiving the indication of the event, the audio message.

12. The method of claim 10, wherein the broadcasting the audio message using the speaker further comprises broadcasting the audio message indicating at least one of:

- an abnormal status of the network device was detected,
- a parental control rule was triggered,
- an attempt by hackers to invade the network device, and
- the service set identifier and password, wherein the broadcast of the audio message further comprises broadcasting the service set identifier and password to a mobile application.

13. The method of claim 12, wherein the broadcasting the audio message comprises broadcasting an audio alarm message indicating the abnormal status of the network device was detected, wherein the broadcasting the audio alarm message indicating the abnormal status of the network further comprises broadcasting an audio alarm message indicating at least one of the network device failed to start based on a key system interface status, an IP connection was lost once a ping of a WAN side of the network device fails, and the temperature of the processor exceeds a predetermine high temperature level.

14. The method of claim 12, wherein the broadcasting the audio message comprises broadcast of an audio alarm message indicating the parental control rule was triggered, wherein the broadcasting the audio alarm message indicating the parental control rule was triggered further comprises broadcasting at least one of an audio alarm message that an attempt to access a block website was detected, an audio alarm message that an attempt to access the Internet occurred at a blocked time, and an audio alarm message that a firewall logs indicate at least one rule were violated, and wherein the broadcasting the audio message comprises broadcasting an audio alarm message indicating an attempt by hackers to invade the network device, the broadcasting of the audio alarm message indicating an attempt by hackers to invade the network device further comprises broadcasting an audio alarm message indicating that attempts to connect to a private service set identifier using a plurality of different incorrect passwords or broadcasting an audio alarm message indicating a denial of service (DoS) attack detected by the firewall.

15. The method of claim 10 further comprising:

- presenting a firewall setting by accessing a web page associated with the user interface and navigating from a main web page to hardware parameter selection page and then to a speaker parameter selection page; and
- providing on the speaker parameter selection page:
  - an interface for enabling or disabling the audio alarm; and
  - an interface to select one of all, normal, or custom classes, wherein the custom class allows the user to select the alarm type to use.

16. A non-transitory, computer-readable media having computer-readable instructions stored thereon, the computer-readable instructions being capable of being read by a network device, wherein the computer-readable instructions are capable of instructing the network device to perform a method for providing an audio alarm, the method comprising:

configuring the network device via a user interface to generate an audio message associated with detection of an event;

monitoring the network device, using a management tool, to detect the event;

triggering, by the management tool, generation of the audio message in response to the detecting of the event;

receiving the audio message at an audio device of the network device that includes a speaker; and

broadcasting the audio message using the speaker.

17. The non-transitory, tangible, computer-readable media of claim 16, wherein the management tool comprises a network manager, a database of management information describing objects defining events of the network device, and a network agent, wherein the method further comprises:

initiating, by the network manager, management commands;

receiving, by the network manager, monitoring notifications from an object of the network device;

describing, by objects stored in the database of management information, events of the network device;

monitoring, by a network agent, the objects of the network device to detect the event based on the objects described in the database of management information;

sending, by the network agent, an indication of the event to the network manager;

logging, by the network agent, the events in the database of management information; and

generating, by the network manager upon receiving the indication of the event, the audio message.

18. The non-transitory, tangible, computer-readable media of claim 16, wherein the broadcasting the audio message using the speaker further comprising broadcasting an audio message indicating at least one of:

- an abnormal status of the network device was detected,
- a parental control rule was triggered,
- an attempt by hackers to invade the network device, and
- the service set identifier and password, wherein the broadcast of the audio message further comprises broadcasting the service set identifier and password to a mobile application.

19. The non-transitory, tangible, computer-readable media of claim 18, wherein the broadcasting the audio message comprises broadcasting an audio alarm message indicating the abnormal status of the network device was detected, wherein the broadcasting the audio alarm message indicating the abnormal status of the network further comprises broadcasting an audio alarm message indicating at least one of the network device failed to start based on a key system interface status, an IP connection was lost once a ping of a WAN side of the network device fails, and the temperature of the processor exceeds a predetermine high temperature level.

20. The non-transitory, tangible, computer-readable media of claim 18, wherein the broadcasting the audio message comprises broadcast of an audio alarm message indicating the parental control rule was triggered, wherein the broadcasting the audio alarm message indicating the parental control rule was triggered further comprises broadcasting at least one of an audio alarm message that an attempt to access a block website was detected, an audio alarm message that an attempt to access the Internet occurred at a blocked time, and an audio alarm message that a firewall logs indicate at least one rule were violated, and wherein the broadcasting the audio message comprises broadcasting an audio alarm message indicating an attempt by hackers to invade the network device, the broadcasting of the audio alarm message indicating an attempt by hackers to invade the network device further comprises broadcasting an audio alarm message indicating that attempts to connect to a private service set identifier using a plurality of different incorrect passwords or broadcasting an audio alarm message indicating a denial of service (DoS) attack detected by the firewall.

**AMENDED CLAIMS**  
**received by the International Bureau on 13 October 2021 (13.10.2021)**

1. (Currently Amended) A network device, comprising:
  - a user interface for configuring the network device to manage a network and to generate an audio message associated with a detected network event;
  - a memory storing a database of managed network objects defining network events for the network device;
  - a speaker; and
  - a processor configured to execute instructions stored on said memory to cause said network device to:
    - execute a network manager for managing the network based on the database of the managed network objects;
    - monitor the network using the managed network objects in the database of the managed network objects to detect the network event using the network manager;
    - trigger generation of the audio message associated with the network event in response to the detecting of the network event; and
    - broadcast the audio message associated with the network event using the speaker.
2. (Currently Amended) The network device of claim 1, wherein:
  - the processor is further configured to execute the instructions stored on said memory to cause said network device to:
    - in response to detecting the network event, initiate management commands and receive monitoring notifications from an object of the network device;
    - send an indication of the network event to the network manager; and
    - log the events in the database of the managed network objects.
3. (Currently Amended) The network device of claim 1, wherein the processor is further configured to execute the instructions stored on said memory to cause said network device to broadcast the audio message associated with the network event indicating at least one of:
  - an abnormal status of the network device was detected,

a parental control rule was triggered.  
an attempt by hackers to invade the network device, and  
the service set identifier and password, wherein the broadcast of the audio message  
further comprises broadcasting the service set identifier and password to a mobile application.

4. (Currently Amended) The network device of claim 3, wherein the processor is further configured to broadcast of an audio alarm message indicating the abnormal status of the network device was detected, wherein the audio alarm message further comprises an audio alarm message indicating at least one of the network device failed to start based on a key system interface status, an IP connection was lost once a ping of a WAN side of the network device fails, and the temperature of the processor exceeds a predetermine high temperature level.

5. (Currently Amended) The network device of claim 3, wherein the processor is further configured to broadcast of an audio alarm message indicating the parental control rule was triggered, wherein the audio alarm message further comprises at least one of an audio alarm message that an attempt to access a block website was detected, an audio alarm message that an attempt to access the Internet occurred at a blocked time, and an audio alarm message that a firewall logs indicate at least one rule were violated.

6. (Currently Amended) The network device of claim 3, wherein the processor is further configured to broadcast of an audio alarm message indicating an attempt by hackers to invade the network device, wherein the audio alarm message further comprises an audio alarm message indicating that attempts to connect to a private service set identifier using a plurality of different incorrect passwords or broadcasting an audio alarm message indicating a denial of service (DoS) attack detected by a firewall.

7. (Currently Amended) The network device of claim 1 further comprising a firewall presenting a firewall setting in a web page accessed through the user interface, and navigating from a main web page to hardware parameter selection page and then to a speaker parameter selection page, wherein the speaker parameter selection page includes an interface for enabling or disabling the audio alarm, and an interface to select one of all, normal, or custom class, wherein the custom class allows the user to select the alarm type to use.

8. (Currently Amended) The network device of claim 1, wherein the user interface is provided by at least one selected from the group consisting of an audio alarm application, a network management tool, a configuration file, and TR-069, the user interface further comprising a graphical user interface (GUI) for management of the audio messages.

9. (Original) The network device of claim 1, wherein the audio message broadcast using the speaker comprises a voice speaking at least one word.

10. (Currently Amended) A method for providing an audio alarm by a network device, comprising:
- storing, in memory, a database of managed network objects defining network events for the network device;
  - executing a management tool for managing the network based on the database of the managed network objects;
  - configuring the network device via a user interface to generate an audio message associated with detection of a network event;
  - monitoring the network, using the management tool, to detect the network event;
  - triggering, by the management tool, generation of the audio message in response to the detecting of the network event;
  - receiving the audio message at an audio device of the network device that includes a speaker; and
  - broadcasting the audio message using the speaker.

11. (Currently Amended) The method of claim 10, wherein the management tool comprises a network manager, and a network agent, wherein the method further comprises:

- initiating, by the network manager, management commands;
- receiving, by the network manager, monitoring notifications from at least one of the management network objects in the database of the managed network objects;
- describing, by objects stored in the database of the managed network objects, network events of the network device;
- monitoring, by a network agent, the managed network objects of the network device to detect the network event based on the objects described in the database of the managed network objects;
- sending, by the network agent, an indication of the network event detected by the network agent to the network manager;
- logging, by the network agent, the network event detected by the network agent in the database of the managed network objects; and
- generating, by the network manager upon receiving the indication of the network event detected by the network agent, the audio message.

12. (Original) The method of claim 10, wherein the broadcasting the audio message using the speaker further comprises broadcasting the audio message indicating at least one of:

- an abnormal status of the network device was detected,
- a parental control rule was triggered.
- an attempt by hackers to invade the network device, and
- the service set identifier and password, wherein the broadcast of the audio message further comprises broadcasting the service set identifier and password to a mobile application.

13. (Original) The method of claim 12, wherein the broadcasting the audio message comprises broadcasting an audio alarm message indicating the abnormal status of the network device was detected, wherein the broadcasting the audio alarm message indicating the abnormal status of the network further comprises broadcasting an audio alarm message indicating at least one of the network device failed to start based on a key system interface status, an IP connection was lost once a ping of a WAN side of the network device fails, and the temperature of the processor exceeds a predetermine high temperature level.

14. (Original) The method of claim 12, wherein the broadcasting the audio message comprises broadcast of an audio alarm message indicating the parental control rule was triggered, wherein the broadcasting the audio alarm message indicating the parental control rule was triggered further comprises broadcasting at least one of an audio alarm message that an attempt to access a block website was detected, an audio alarm message that an attempt to access the Internet occurred at a blocked time, and an audio alarm message that a firewall logs indicate at least one rule were violated, and wherein the broadcasting the audio message comprises broadcasting an audio alarm message indicating an attempt by hackers to invade the network device, the broadcasting of the audio alarm message indicating an attempt by hackers to invade the network device further comprises broadcasting an audio alarm message indicating that attempts to connect to a private service set identifier using a plurality of different incorrect passwords or broadcasting an audio alarm message indicating a denial of service (DoS) attack detected by the firewall.

15. (Currently Amended) The method of claim 10 further comprising:  
presenting a firewall setting by accessing a web page associated with the user interface and navigating from a main web page to a hardware parameter selection page and then to a speaker parameter selection page; and  
providing on the speaker parameter selection page:  
an interface for enabling or disabling the audio alarm; and  
an interface to select one of all, normal, or custom classes, wherein the custom class allows the user to select the alarm type to use.

16. (Currently Amended) A non-transitory, computer-readable media having computer-readable instructions stored thereon, the computer-readable instructions being capable of being read by a network device, wherein the computer-readable instructions are capable of instructing the network device to perform a method for providing an audio alarm, the method comprising:

storing, in memory, a database of managed network objects defining network events for the network device;

executing a management tool for managing the network based on the database of the managed network objects;

configuring the network device via a user interface to generate an audio message associated with detection of a network event;

monitoring the network, using the management tool, to detect the network event;

triggering, by the management tool, generation of the audio message associated with the network event in response to the detecting of the network event;

receiving the audio message at an audio device of the network device that includes a speaker; and

broadcasting the audio message using the speaker.

17. (Currently Amended) The non-transitory, tangible, computer-readable media of claim 16, wherein the management tool comprises a network manager, and a network agent, wherein the method further comprises:

initiating, by the network manager, management commands;

receiving, by the network manager, monitoring notifications from at least one of the management network objects in the database of the managed network objects;

describing, by objects stored in the database of the managed network objects, network events of the network device;

monitoring, by a network agent, the managed network objects of the network device to detect the network event based on the managed network objects described in the database of the managed network objects;

sending, by the network agent, an indication of the network event detected by the network agent to the network manager;

logging, by the network agent, the network event detected by the network agent in the database of the managed network objects; and

generating, by the network manager upon receiving the indication of the network event detected by the network agent, the audio message.

18. (Original) The non-transitory, tangible, computer-readable media of claim 16, wherein the broadcasting the audio message using the speaker further comprising broadcasting an audio message indicating at least one of:

an abnormal status of the network device was detected,

a parental control rule was triggered.

an attempt by hackers to invade the network device, and

the service set identifier and password, wherein the broadcast of the audio message further comprises broadcasting the service set identifier and password to a mobile application.

19. (Original) The non-transitory, tangible, computer-readable media of claim 18, wherein the broadcasting the audio message comprises broadcasting an audio alarm message indicating the abnormal status of the network device was detected, wherein the broadcasting the audio alarm message indicating the abnormal status of the network further comprises broadcasting an audio alarm message indicating at least one of the network device failed to start based on a key system interface status, an IP connection was lost once a ping of a WAN side of the network device fails, and the temperature of the processor exceeds a predetermine high temperature level.

20. (Original) The non-transitory, tangible, computer-readable media of claim 18, wherein the broadcasting the audio message comprises broadcast of an audio alarm message indicating the parental control rule was triggered, wherein the broadcasting the audio alarm message indicating the parental control rule was triggered further comprises broadcasting at least one of an audio alarm message that an attempt to access a block website was detected, an audio alarm message that an attempt to access the Internet occurred at a blocked time, and an audio alarm message that a firewall logs indicate at least one rule were violated, and wherein the broadcasting the audio message comprises broadcasting an audio alarm message indicating an attempt by hackers to invade the network device, the broadcasting of the audio alarm message indicating an attempt by hackers to invade the network device further comprises broadcasting an audio alarm message indicating that attempts to connect to a private service set identifier using a plurality of different incorrect passwords or broadcasting an audio alarm message indicating a denial of service (DoS) attack detected by the firewall.

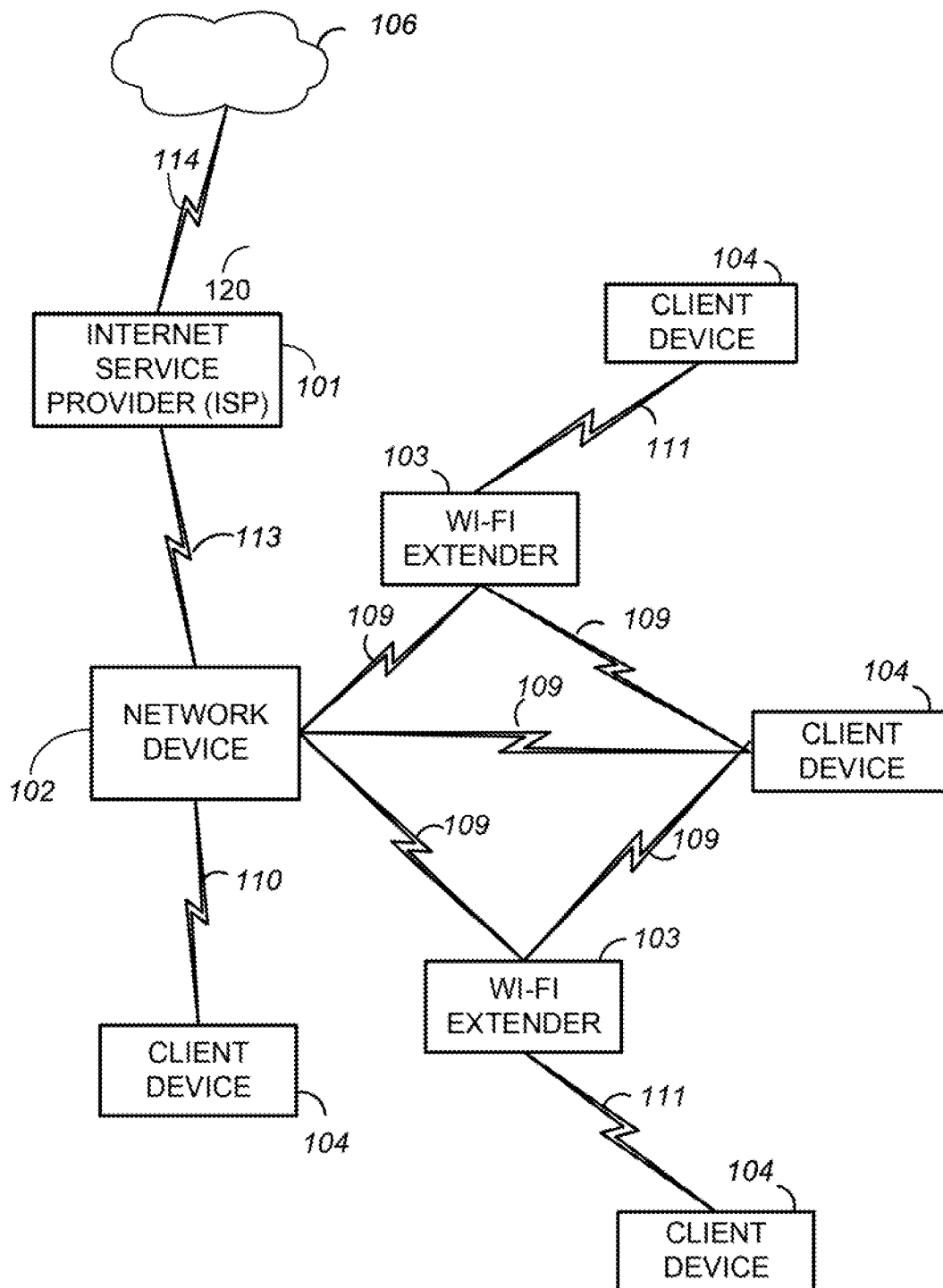


FIG. 1

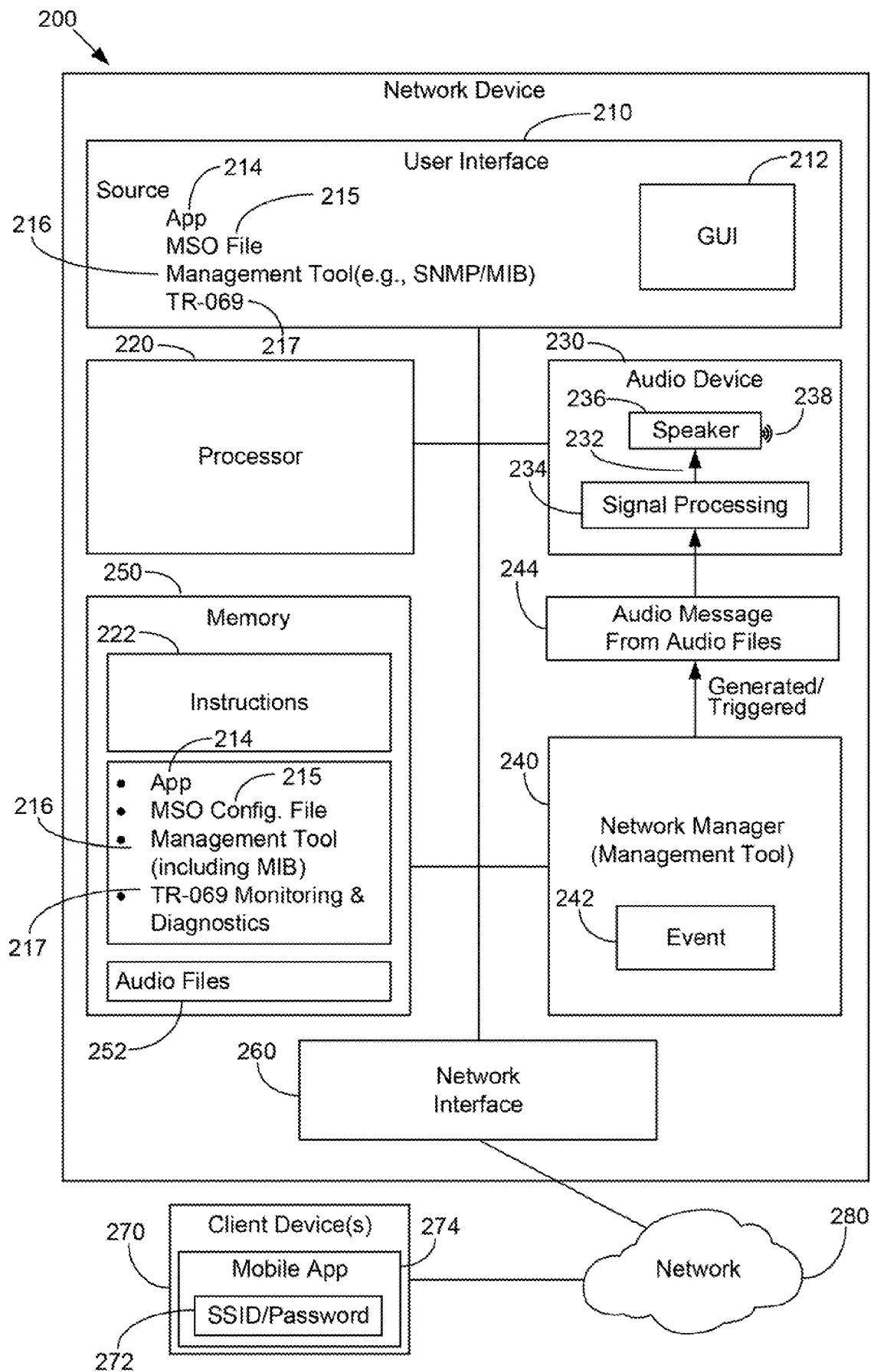


FIG. 2

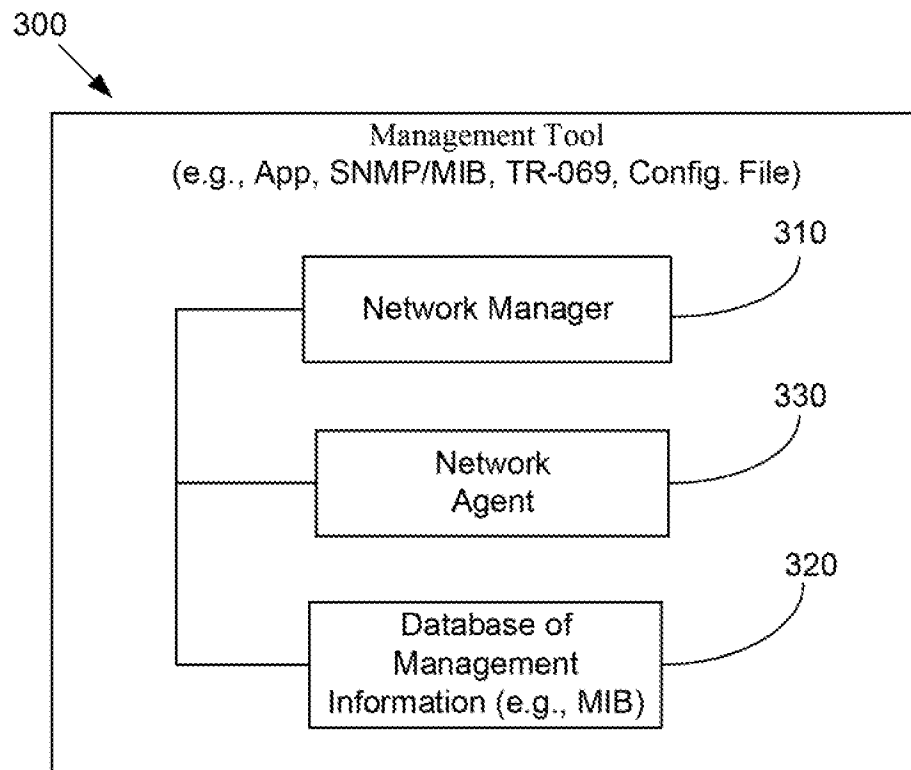


FIG. 3

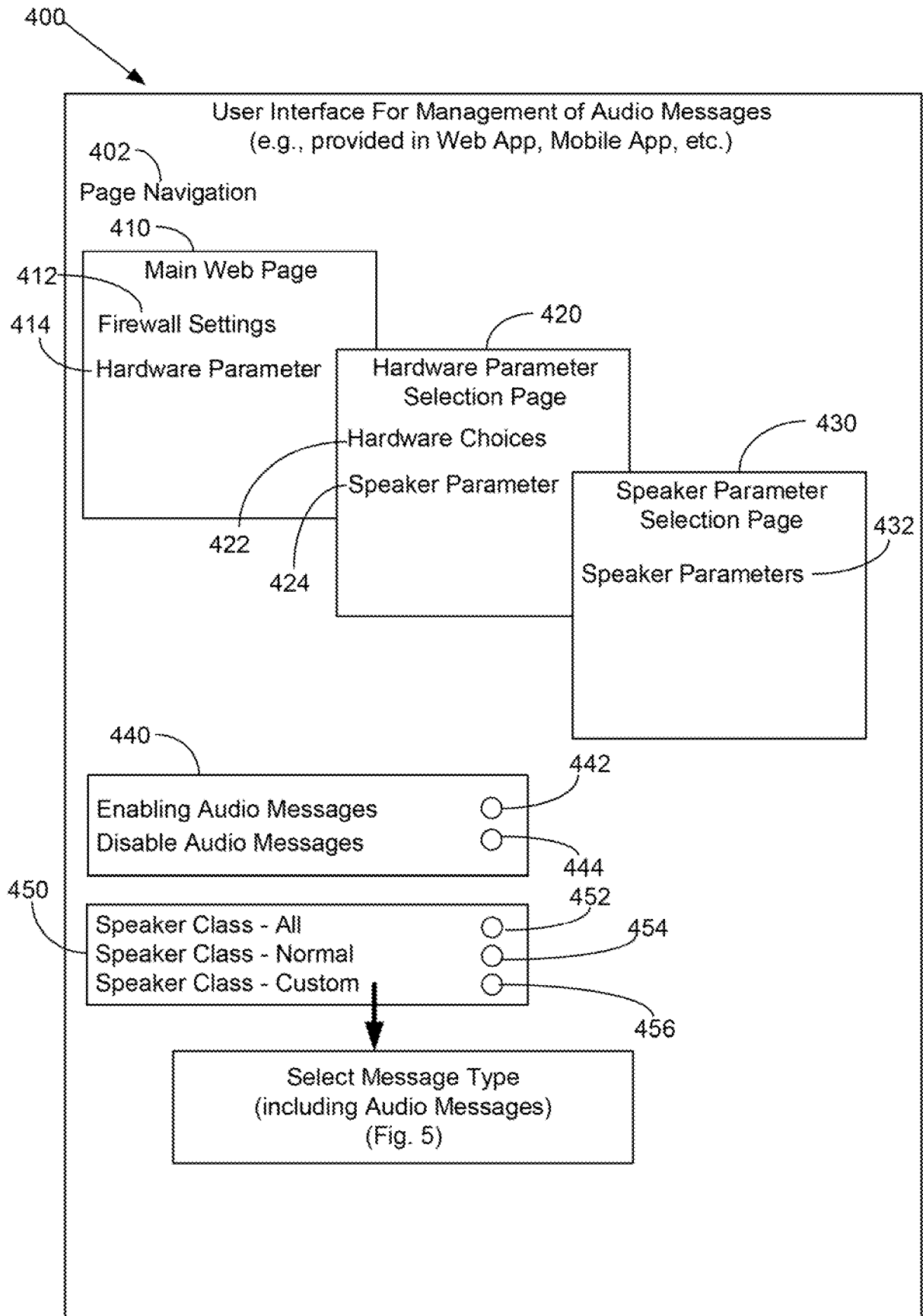


FIG. 4

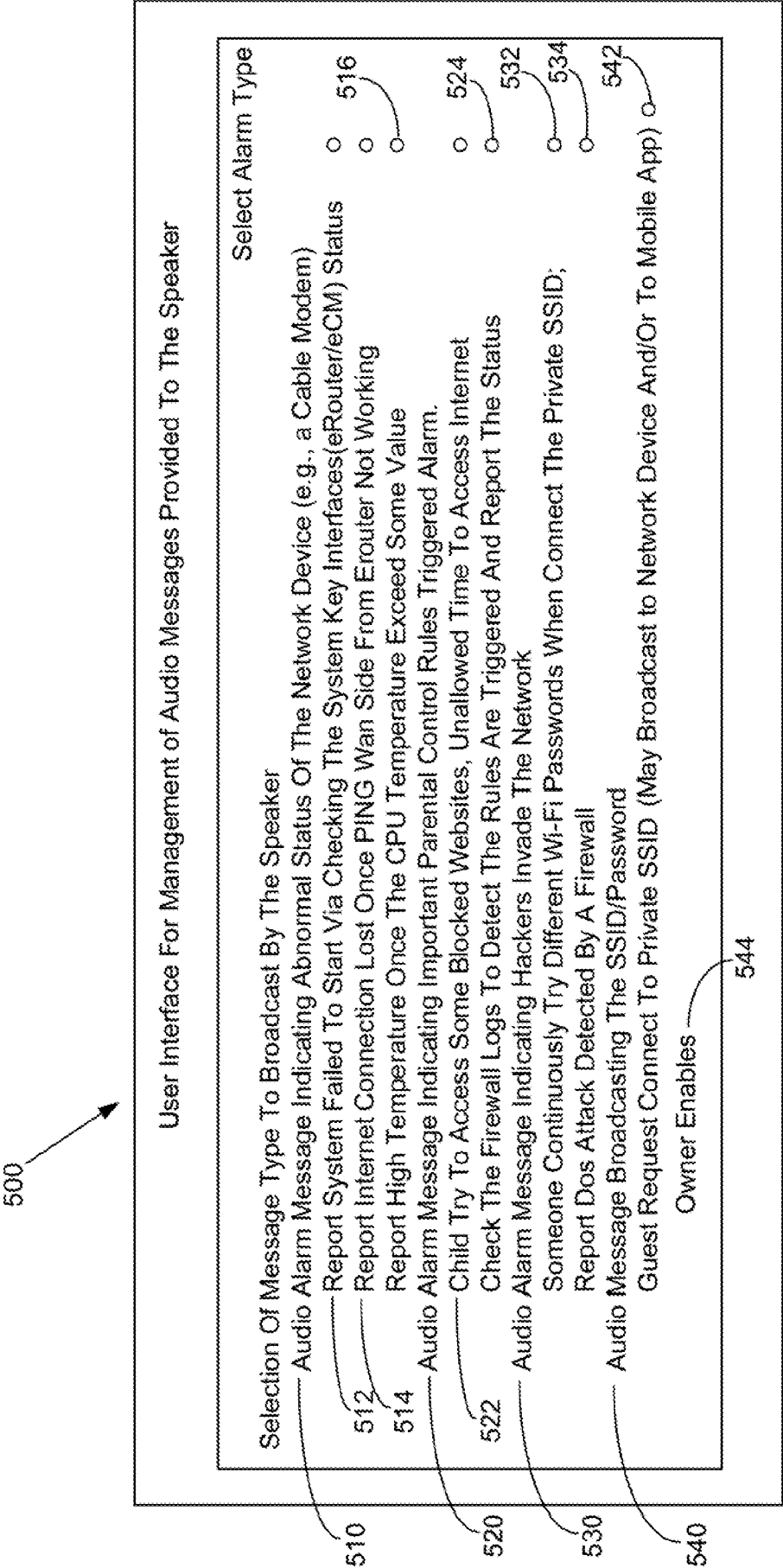


FIG. 5

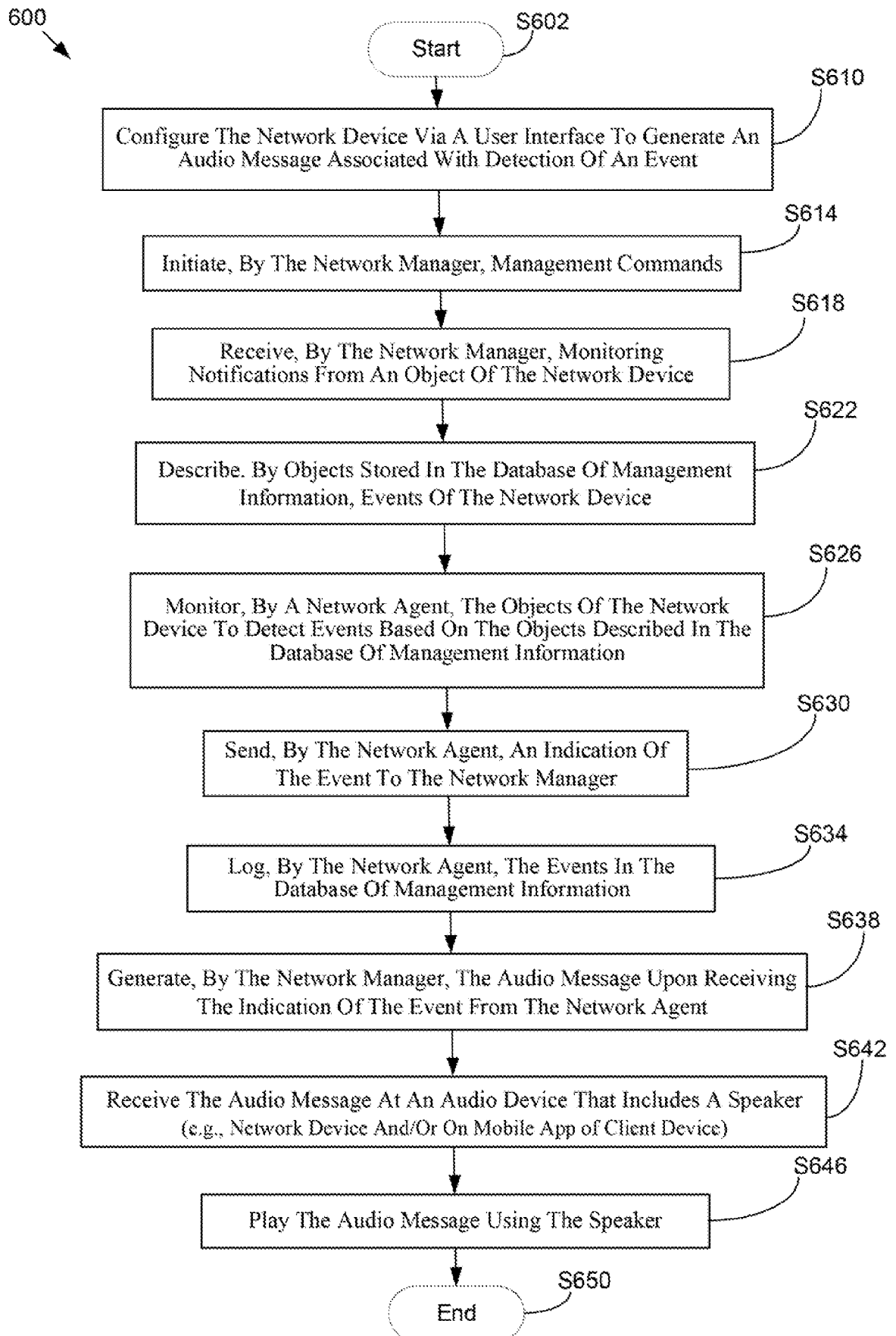


FIG. 6

## INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2020/103338

**A. CLASSIFICATION OF SUBJECT MATTER**

G06F 15/00(2006.01)i; G06F 21/50(2013.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

**B. FIELDS SEARCHED**

Minimum documentation searched (classification system followed by classification symbols)

G06F; 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)

CNPAT, CNKI, WPI, EPODOC:network, audio, message, detection, event, speaker, monitor, detect, trigger, broadcast, interface

**C. DOCUMENTS CONSIDERED TO BE RELEVANT**

| Category* | Citation of document, with indication, where appropriate, of the relevant passages                                                 | Relevant to claim No. |
|-----------|------------------------------------------------------------------------------------------------------------------------------------|-----------------------|
| X         | US 2005068567 A1 (HULL, Jonathan J. et al.) 31 March 2005 (2005-03-31)<br>description, paragraphs [0023]-[0076]                    | 1-20                  |
| X         | US 2003217110 A1 (WEISS, Eugene S.) 20 November 2003 (2003-11-20)<br>description, paragraphs [0054]-[0099]                         | 1-20                  |
| A         | US 2012084857 A1 (VERIZON PATENT AND LICENSING INC.) 05 April 2012<br>(2012-04-05)<br>the whole document                           | 1-20                  |
| A         | CN 109447048 A (SUZHOU SHANCHI NUMERICAL CONTROL SYSTEM<br>INTEGRATION CO., LTD.) 08 March 2019 (2019-03-08)<br>the whole document | 1-20                  |

☐ Further documents are listed in the continuation of Box C.☒ See patent family annex.

\* Special categories of cited documents:

“A” document defining the general state of the art which is not considered to be of particular relevance

“E” earlier application or patent but published on or after the international filing date

“L” document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

“O” document referring to an oral disclosure, use, exhibition or other means

“P” document published prior to the international filing date but later than the priority date claimed

“T” later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

“X” document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

“Y” document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

“&” document member of the same patent family

Date of the actual completion of the international search

26 March 2021

Date of mailing of the international search report

22 April 2021

Name and mailing address of the ISA/CN

National Intellectual Property Administration, PRC  
6, Xitucheng Rd., Jimen Bridge, Haidian District, Beijing  
100088  
China

Authorized officer

CHANG, Jiaofa

Facsimile No. (86-10)62019451

Telephone No. 86-(10)-53961735

**INTERNATIONAL SEARCH REPORT**  
**Information on patent family members**

International application No.

**PCT/CN2020/103338**

| Patent document<br>cited in search report |            |    | Publication date<br>(day/month/year) | Patent family member(s) |            | Publication date<br>(day/month/year) |
|-------------------------------------------|------------|----|--------------------------------------|-------------------------|------------|--------------------------------------|
| US                                        | 2005068567 | A1 | 31 March 2005                        | JP                      | 2005100414 | A 14 April 2005                      |
| US                                        | 2003217110 | A1 | 20 November 2003                     | None                    |            |                                      |
| US                                        | 2012084857 | A1 | 05 April 2012                        | None                    |            |                                      |
| CN                                        | 109447048  | A  | 08 March 2019                        | None                    |            |                                      |