

(51) International Patent Classification:
H04L 12/28 (2006.01)(21) International Application Number:
PCT/CN2017/098293(22) International Filing Date:
21 August 2017 (21.08.2017)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
15/246,656 25 August 2016 (25.08.2016) US(71) Applicant: **HUAWEI TECHNOLOGIES CO., LTD.**
[CN/CN]; Huawei Administration Building, Bantian, Long-
gang District, Shenzhen, Guangdong 518129 (CN).(72) Inventors: **ZHANG, Tianhu**; 87 Jefferson Forest Dr.,
Richmond Hill, Ontario L4E 4J4 (CA). **POELUEV, Yuri**;
112 Woodridge Dr., Petersburg, Ontario N0B 2H0 (CA).(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, 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, SM, ST, SV, SY, TH, TJ, TM, TN,
TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.(84) Designated States (unless otherwise indicated, for every
kind of regional protection available): ARIPO (BW, GH,
GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ,
UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ,
TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK,
EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV,
MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM,

(54) Title: DEVICE AND METHOD FOR MANAGING A COMMUNICATION INTERFACE OF A COMMUNICATION DEVICE

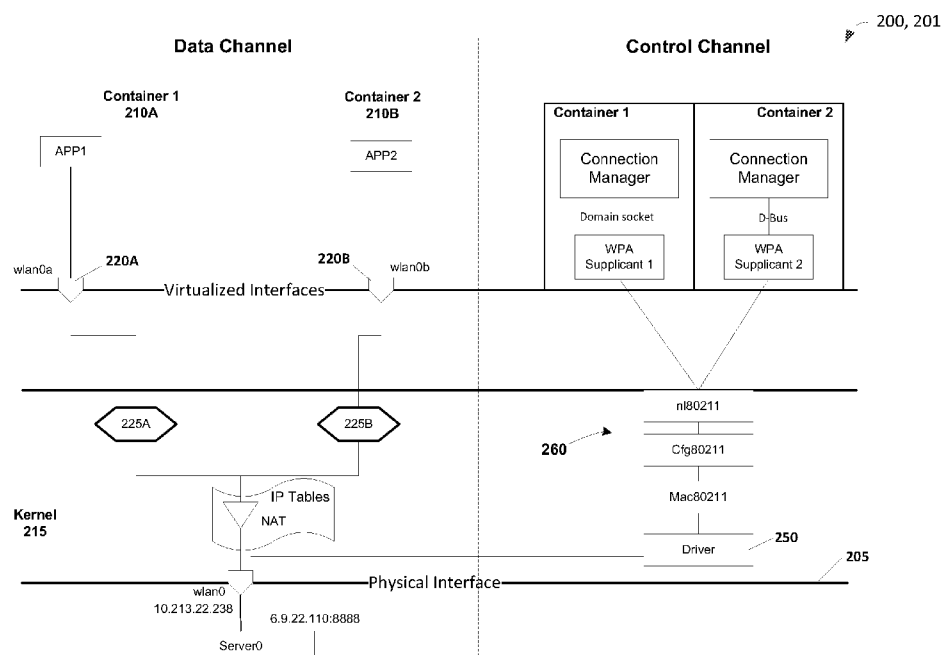


FIG. 2

(57) **Abstract:** Methods and devices for managing a physical communication interface can include operating a first communication interface management unit in a first container operating on the communication device, the first communication interface management unit managing a connection to a first virtual communication interface having a network connection with the physical communication interface; and concurrently with the operation of the first communication interface, operating a second communication interface management unit in a second container operating on the communication device, the second communication interface management unit managing a connection to a second virtual communication interface having a network connection with the physical communication interface.



TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW,
KM, ML, MR, NE, SN, TD, TG).

Declarations under Rule 4.17:

- *as to the applicant's entitlement to claim the priority of the earlier application (Rule 4.17(iii))*

Published:

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

DEVICE AND METHOD FOR MANAGING A COMMUNICATION INTERFACE OF A COMMUNICATION DEVICE

CROSS REFERENCE

[0001] The present application claims priority to U.S. Patent Application Serial No.
5 15/246,656, filed August 25, 2016, entitled "Device and Method for Managing a
Communication Interface of a Communication Device", the contents of which are
incorporated by reference herein in their entirety.

FIELD

[0002] Embodiments of this disclosure relate to the field of communication devices, and
10 more particularly to devices, methods and computer-readable media for managing a
communication interface.

BACKGROUND

[0003] Communication devices such as mobile phones are increasingly used for multiple
applications such as work activities, personal activities, or to access different external
15 systems. For security, privacy, permissions or other reasons, containers can be created on
the same device to isolate these applications.

[0004] It can be a challenge to manage device resources such as communication
interfaces between different containers while maintaining isolation between the containers.

SUMMARY

20 [0005] In some situations, some embodiments of the present disclosure may enable the
management of an external connection with a physical communication interface across
multiple containers operating on a single communication device.

[0006] In accordance with one aspect of the present disclosure, there is provided a
communication device including a physical communication interface; and at least one
25 processor. The at least one processor is configured to provide: a kernel configured for
operating first and second containers on the communication device; first and second network
nodes, the first network node providing a first virtual communication interface to the first
container, and the second network node providing a second virtual communication interface
to the second container; and a network controller configured to provide routing and a
30 network connection between the first network node and the physical communication
interface, and between the second network node and the physical communication interface;

the first container configured to operate a first communication interface management unit for managing a connection to the first virtual communication interface, and the second container configured to concurrently operate a second communication interface management unit for managing a connection to the second virtual communication interface.

- 5 [0007] Optionally, in any of the previous aspects, the at least one processor is configured to block direct network communications between the first network node and the second network node.

- [0008] Optionally, in any of the previous aspects, the first and the second communication interface management units concurrently manage access to the physical communication
10 interface for the respective first and second containers via the respective first and second virtual communication interfaces.

- [0009] Optionally, in any of the previous aspects, each of the first and the second communication interface management unit is configured to operate in a control mode in which the communication interface management unit controls a connection with the physical
15 communication interface, or to operate in a monitor mode in which the communication interface management unit monitors the connection with the physical communication interface.

- [0010] Optionally, in any of the previous aspects, the at least one processor is configured to provide a control management unit for managing the first and the second communication
20 interface management units such that only one of the first and the second communication management unit is operating in the control mode.

- [0011] Optionally, in any of the previous aspects, the control management unit identifies which of the first and the second communication interface management unit is to operate in the control mode based on communication interface profiles for the first and the second
25 containers, and based on available external connections for the physical communication interface.

- [0012] Optionally, in any of the previous aspects, when the first communication interface management unit is operating in the control mode, and a container focus switches from the first container to the second container, the first communication interface management unit
30 continues to operate in the control mode.

- [0013] Optionally, in any of the previous aspects, the communication interface manager is configured to manage a current connection to the physical communication interface when

the communication interface management unit operating in the control mode is changed from the first communication interface management unit to the second communication interface management unit.

5 [0014] Optionally, in any of the previous aspects, the at least one processor is configured to intercept messages sent to the kernel from the first and the second communication interface management units.

[0015] Optionally, in any of the previous aspects, the network controller is configured to hide the first and the second network nodes from an external connection with the physical communication interface.

10 [0016] In accordance with another aspect of the present disclosure there is provided a method for managing a physical communication interface on a communication device. The method includes: operating a first communication interface management unit in a first container operating on the communication device, the first communication interface management unit managing a connection to a first virtual communication interface having a
15 network connection with the physical communication interface; and concurrently with the operation of the first communication interface, operating a second communication interface management unit in a second container operating on the communication device, the second communication interface management unit managing a connection to a second virtual communication interface having a network connection with the physical communication
20 interface.

[0017] Optionally, in any of the previous aspects, the method further includes: blocking direct network communications between the first virtual communication interface and the second virtual communication interface.

25 [0018] Optionally, in any of the previous aspects, the method further includes: configuring the each of the first and the second communication interface management unit to operate in: a control mode in which the communication interface management unit controls a connection with the physical communication interface, or a monitor mode in which the communication interface management unit monitors the connection with the physical communication interface.

30 [0019] Optionally, in any of the previous aspects, the method further includes: managing the first and the second communication interface management units such that only one of the first and the second communication management unit is operating in the control mode.

[0020] Optionally, in any of the previous aspects, the method further includes: identifying which of the first and the second communication interface management unit is to operate in the control mode based on communication interface profiles for the first and the second containers, and based on available external connections for the physical communication interface.

[0021] Optionally, in any of the previous aspects, the method further includes: when the first communication interface management unit is operating in the control mode, and a container focus switches from the first container to the second container, continues to operate the first communication interface management unit in the control mode.

[0022] Optionally, in any of the previous aspects, the method further includes: managing a current connection to the physical communication interface when the communication interface management unit operating in the control mode is changed from the first communication interface management unit to the second communication interface management unit.

[0023] Optionally, in any of the previous aspects, the method further includes: intercepting messages sent to the kernel from the first and the second communication interface management units.

[0024] Optionally, in any of the previous aspects, the method further includes: hiding the first and the second virtual communication interfaces from an external connection with the physical communication interface.

[0025] In accordance with another aspect of the present disclosure there is provided a non-transitory, computer-readable medium or media having stored thereon computer-readable instructions. The instructions, which when executed by at least one processor, configure the at least one processor to operate a first communication interface management unit in a first container operating on the communication device, the first communication interface management unit managing a connection to a first virtual communication interface having a network connection with the physical communication interface; and concurrently with the operation of the first communication interface, operate a second communication interface management unit in a second container operating on the communication device, the second communication interface management unit managing a connection to a second virtual communication interface having a network connection with the physical communication interface.

[0026] Many further features and combinations thereof concerning the present improvements will appear to those skilled in the art following a reading of the instant disclosure.

DESCRIPTION OF THE FIGURES

5 [0027] FIG. 1 is a diagram showing an example operating system architecture for a communication device with multiple containers.

[0028] FIG. 2 is a diagram showing aspects of another example operating system architecture for a communication device with multiple containers.

10 [0029] FIG. 3 is a diagram showing data channel aspects of an example operating system architecture for a communication device.

[0030] FIG. 4 is a diagram showing control channel aspects of a first example operating system architecture for a communication device.

[0031] FIG. 5A is a diagram showing control channel aspects of a second example operating system architecture for a communication device.

15 [0032] FIG. 5B is a diagram showing an example mechanism for filtering messages.

[0033] FIG. 6 is a diagram showing aspects of an example communication device.

[0034] FIG. 7 is a flowchart showing aspects of an example method for managing a physical communication interface.

20 [0035] FIGS. 8A and 8B are diagrams showing example before and after states of a control channel when a change of container focus occurs.

[0036] FIGS. 9A and 9B are diagrams showing example before and after states of another control channel when a change of container focus occurs.

[0037] FIGS. 10A and 10B are diagrams showing example before and after states of a control channel when there is a change in available external connections.

25 [0038] FIGS. 11A and 11B are diagrams showing example before and after states of another control channel when there is a change in available external connections.

[0039] These drawings depict aspects of example embodiments for illustrative purposes. Variations, alternative configurations, alternative components and modifications may be made to these example embodiments.

DETAILED DESCRIPTION

5 [0040] The use of virtualization or multiple containers operating on a communication device can, in some instances, help to isolate different applications, for example, separating work and personal activities, or limiting access to data, instructions or communication messages between different user profiles.

10 [0041] In some applications, the use of multiple containers on a single physical device can be applicable to bring-your-own-device programs within an enterprise to provide device flexibility to both employees and the enterprise while addressing privacy concerns for the user and meeting security requirements for the enterprise.

15 [0042] Although data and applications may be separated through the use of different containers (e.g. a first container for personal applications and data, and a second container for work applications and data), challenges may arise when resources such as communication interfaces are shared between the containers.

20 [0043] FIG. 1 shows an example operating system architecture 100 for a communication device 101. In this architecture 100, the communication device 101 is operating two separate containers 110A, 110B which may require access to a WiFi interface 105. Container 1 is currently in focus (as indicated by the bold outline) on the communication device 101. In some embodiments, a container is considered to be in focus when it is actively displayed on a display device. For example, a user interface showing aspects of a first container can include windows, desktops, pages, menus, command prompts, applications, etc. for the first container. In some examples, the user interface showing only aspects of the in-focus first container can fill the entire area of the display device.

25 [0044] In another embodiment, a user interface may show aspects of multiple containers. For example, windows corresponding to applications running on different containers may be displayed on different portions of the user interface. In some such examples, a first container may be in focus when at least one or its windows or other visual aspects of its application(s) are displayed more prominently than windows or other visual aspects of the second container's applications. For example, a first container's visual aspects may be displayed more prominently when they appear to be on top or unobstructed (i.e., the entire window

is visible), or when the visual aspects are displayed more boldly (e.g. window frame/title bar is bold, or is not greyed out/muted).

[0045] In another embodiment where a user interface may show aspects of both containers, a particular container may be considered to be in focus when any input received
5 from an input device such as a keyboard or touchscreen will be applied to an application running in the particular container.

[0046] In this state, the wlan0 interface is moved 150 from the host WiFi interface 105 to Container 1, and the WPA (WiFi Protected Access) Supplicant (which may be referred to as “wpa_supplicant”) 130A for Container 1 is running and controlling aspects of the WiFi driver
10 155. In other words, when in focus, Container 1 has a network connection with the WiFi Interface 105 and has control of the WiFi connection via its connection manager 120A and WPA Supplicant 130A.

[0047] In this state, Container 2, which is not in focus, does not have access to the wlan0 interface or the physical WiFi interface 105, and its WPA Supplicant 130B is terminated or
15 inactive.

[0048] In the operating system architecture 100 illustrated in FIG. 1, the container not in focus does not have access to the network connection, and any applications which may be running in the container that is not in focus (e.g. APP2 140B) will not have access to the network. If the application receives updates from the network (e.g. a messaging application),
20 the application will not receive updates while its container is not in focus.

[0049] When the focus switches from Container 1 to Container 2, Container 1 terminates or suspends its WPA Supplicant 130A, losing its WiFi connection. Container 2 starts its WPA Supplicant 130B and the wlan0 interface is moved from Container 1 to Container 2. When the focus is on Container 2, applications such as APP1 140A running in Container 1 will
25 have no WiFi access.

[0050] Switching between containers in this manner involves the termination and starting of different WiFi processes, which requires processing time and power consumption. Also, during the switchover, there may be a period during which the WiFi interface may be unavailable while the appropriate supplicants and other related processes are initiated.
30 During this period, the communication device 101 may not be connected to any WiFi network, and applications 140A, 140B will lose WiFi access.

[0051] For the architecture 100 illustrated in FIG. 1, in some instances, switching focus from a first container 110A to a second container 110B may cause the communication device 101 to connect to a different WiFi connection if the connection manager 120B of the second container has different permissions and/or WiFi profile data than the connection manager 120A of the first container. In other instances, switching focus from a first container 110A to a second container 110B may cause the communication device 101 to lose WiFi connectivity completely if the connection manager 120B of the second container does not have permissions and/or WiFi profile data for any available network.

[0052] FIG. 2 shows aspects of an example operating system architecture 200 for a communication device 201. For illustrative purposes, the architecture 200 has been logically divided into a data channel and a control channel.

[0053] The communication device 201 includes one or more physical communication interfaces 205. In some embodiments, the physical communication interfaces 205 can include one or more wireless communication interfaces such as wireless local area network (WLAN) interfaces and/or mobile/cellular data network interfaces. Example interfaces include, but are not limited to, IEEE 802.11 (WiFi) interfaces, Bluetooth™, Global System for Mobile Communications (GSM), Code Division Multiple Access (CMDA), Long-Term Evolution (LTE), and the like.

[0054] A kernel 215 is configured to operate two or more containers on the communication device 201. Each container 210A, 210B has its own respective virtual communication interface 220A, 220B which connects to the physical communication interface 205 via a respective communication node 225A, 225B. In some embodiments, these virtual communication interfaces 220A, 220B are managed irrespective of whether the corresponding container is in focus or not.

[0055] Although the examples illustrated herein show two containers operating on the device 201, in other embodiments, three, four, five, or any other number of containers can be operating on the device 201.

[0056] In some embodiments, a container can be an operating system container such as a Google Android™ operating system. In some embodiments, a container can be a mobile operating system or a virtual phone.

[0057] In some embodiments, a container can be associated with one or more profiles. In one example, a container can be associated with a personal profile for personal applications,

permissions and/or data. In another example, a container can be associated with an enterprise or work profile for enterprise/work applications, permissions and/or data. Any other profile or set of applications, permissions and/or data can be associated with a container.

- 5 [0058] In some embodiments, two or more containers can be operating on the device such that applications on each container can communicate over, or otherwise have access to, the physical interface concurrently.

[0059] In some embodiments, the data channel can be concurrently accessed by any number of containers on the device 201. A network node 225A, 225B is created for each
10 container having access to the physical interface of the data channel. In some embodiments, the network nodes 225A, 225B can be network bridges. In some embodiments, the network nodes 225A, 225B can be any virtual or physical network device which creates a separate sub-network for its respective container.

[0060] In some instances, each network node provides a dedicated communication
15 interface (e.g. WLAN interface) 220A, 220B for its corresponding container. The network nodes can be created and/or managed by the kernel, for example through the use of a software bridge.

[0061] The control channel of the architecture 200 governs which container is currently in
20 full control of the physical interface. In some embodiments, the other containers not in full control can receive and/or request information from the physical interface. The control channel can include a driver 250 for the physical interface and interface subsystems 260.

[0062] FIG. 3 shows aspects of an example operating system architecture for a
communication device which can, in some situations, represent a data channel 300 for a wireless local area network interface 205. In this example, network bridge Br0 is attached to
25 Container 1 and provides a corresponding sub-network 192.168.200.0. Similarly, network bridge Br1 is attached to Container 2 and provides a corresponding sub-network 192.168.100.0. The WiFi interface, wlan0, in the kernel is mapped to wlan0a in Container 1, and to wlan0b in Container 2.

[0063] In some embodiments, applications running in Container 1 (e.g. APP1) interact
30 with the virtual interface wlan0a as if it were physical interface 205. Similarly, applications running in Container 2 (e.g. APP2) interact with the virtual interface for Container 2 wlan0b as if it were physical interface 205. In some embodiments, applications running in a

container are unaware of the physical interface 205 or any network aspects outside their own network node.

[0064] In some embodiments, the operating system architecture 200 includes one or more network controllers 330. The network controller 330 is configured to provide routing and a network connection between the network nodes 225A, 225B and the physical communication interface 205. In some embodiments, the network controller 330 is configured to provide internet protocol (IP) forwarding and/or network address transaction (NAT) functionality. The network controller 330 may store, manage and/or otherwise have access to IP and/or other routing tables to route packets between the external interface and the virtual interfaces.

[0065] In some embodiments, the network controller 330 is configured to isolate the internal network 192.168.0.0 from the external network. In some situations, the internal network and/or the different containers will not be visible to the external network. In some embodiments, the network controller 330 can include a firewall or other component(s) to prevent attacks on the containers from outside the device 201. In some instances, this may provide greater security than the architecture 100 in FIG. 1 in which the wlan0 interface is moved from the host WiFi interface to the container.

[0066] In some embodiments, the network controller 330 is configured to disable communication between containers. In some instances, the isolation of the different internal networks may provide security and/or privacy between different containers. In some embodiments, a routing table used by the network controller includes entries or is otherwise configured to disable communication between containers. In some embodiments, an application running in a container is unaware of the physical interface sharing and/or of the container and network isolation mechanisms outside its container.

[0067] FIG. 4 shows aspects of an example operating system architecture for a communication device which can, in some situations, represent a control channel 400 for a wireless local area network interface 205.

[0068] Each container 210A, 210B has its own interface authentication unit 450A, 450B for authenticating access to an external connection over the physical communication interface 205. In some embodiments, the interface management unit 450A, 450B can be a supplicant such as a WPA Supplicant which may be used for WiFi authentication. In some embodiments, the interface management unit 450A, 450B can be another supplicant or other management unit used to authenticate access to a Bluetooth™ connection, a GSM or CDMA

connection, or the like. In some embodiments, the interface management units 450A, 450B can operate as daemons.

5 [0069] In some embodiments, each container 210A, 210B has a separate namespace, such as a Linux namespace, which is separate from a host or parent namespace for the device 201. In some examples, these namespaces may include a communication interface namespace or network namespace.

10 [0070] Each interface management unit 450A, 450B can concurrently manage its connection with the physical interface 205 via the interface management unit's respective virtual interface (e.g. wlan0a, wlan0b). In some embodiments, each interface management unit 450A, 450B interacts with or otherwise utilizes one or more drivers 460, firmware or other device or process to interact with the physical interface 205.

15 [0071] In some embodiments, an interface management unit 450A, 450B is configured to operate in a control mode or a monitor mode. In the control mode, an interface management unit 450A, 450B is configured to have full control of the physical communication interface 205. In some examples, an interface management unit operating in a control mode can query information about the physical interface and/or to configure or otherwise control the operation of the physical interface. For example, in some instances, an interface management unit operating in a control mode can send "set", "get" and/or "configure" commands to the physical interface device 205.

20 [0072] In some embodiments, the interface management unit operating in the control mode can set permissions or otherwise control whether other interface management units operating in the monitor mode and/or operating on a container not in focus can connect to the physical interface. In some instances, the interface management unit operating in the control mode can block or otherwise prevent other interface management units from
25 accessing the physical interface.

[0073] In the monitor mode, an interface management unit 450A, 450B is configured to monitor the physical communication interface 205. In some examples, an interface management unit operating in a monitor mode can query information about the physical interface but cannot configure or otherwise control the operation of the physical interface.
30 For example, in some instances, an interface management unit operating in a monitor mode can send "get" and/or "query" commands to the physical interface device 205.

[0074] Unless explicitly blocked by the interface management unit operating in the control mode, interface management units operating in the monitor mode can be configured to manage a connection between the physical interface and the corresponding virtual communication interface.

5 [0075] In some embodiments, an interface management unit 450A, 450B may be aware of the virtual environment and may be configured not to conflict with another interface management unit. In some embodiments, an interface management unit 450A, 450B may know which interface management unit operating on the device is currently operating in the control mode.

10 [0076] In some embodiments, the interface management units 450A, 450B can be configured to operate in a control mode or a monitor mode based on policy data and/or instructions from a control management unit 470. In some embodiments, the control management unit 470 is configured to provide policy data and/or instructions to ensure that only one container's interface management unit is operating in a control mode, and the
15 interface management units for all other containers are operating in a monitor mode.

[0077] In some embodiments, the control management unit 470 can be a system process or other application operating on the device that is configured to provide data and/or instructions as to whether a container's interface management unit is operating in a control mode or a monitor mode. In some embodiments, the control management unit 470 is
20 configured to determine the appropriate mode for a container based on a number of factors. In some examples, these factors can include: available interface connections (e.g. available WiFi networks), an interface currently connected to the physical interface (e.g. a WiFi network to which the device is currently connected), a current container in focus, a container to which the focus is to be shifted, connection profiles/authorized connections of the
25 container in focus (e.g. the container's stored WiFi profiles), connection profiles/authorized connections of the container to be put into focus, connection characteristics (e.g. signal strength, encryption modes, etc.), and/or any other relevant factor.

[0078] In some embodiments, the control management unit 470 can have access to and/or manage connection profiles and/or authorized connections for a container. For
30 example, for a WiFi interface, connection profiles can include WiFi profile information such as a WiFi service set identifiers (SSID) and credentials or other login information. Authorized connections can include, for example, whitelists or blacklists of SSIDs which a contained is permitted or restricted from accessing. In some embodiments, connection profiles and/or

authorized connection data can be stored on a storage device for access by one or more applications of the container.

[0079] In some embodiments, the control management unit 470 can be a set of policies and/or data which is accessed, referenced or otherwise utilized by an interface management unit 450A, 450B. For example, the control management unit 407 can be a set of data and/or instructions stored on a storage device for access by the interface management unit 450A, 450B of a container.

[0080] In some embodiments, the control management unit 470 may be part of an interface management unit 450A, 450B. For example, the control management unit 470 may be a subroutine or other process, and/or a set of instructions and/or data, which is logically or structurally part of the interface management unit 450A, 450B.

[0081] In some embodiments, the control management unit 470 and/or its associated functions can be provided by the physical interface manager 480.

[0082] In some embodiments, control management unit policies, instructions, and/or data may be common between different containers. For example, in some embodiments, policies implemented based on instructions and/or data from a control management unit may be common across all containers to ensure that only one container is operating in a control mode at a time.

[0083] In some embodiments, one or more containers may include a connection manager 420A, 420B. A connection manager can, in some instances, be an application or process which provides a user interface for configuring interface connection services. For example, in some embodiments involving a WiFi physical interface, a connection manager can provide an interface to receive inputs for selecting an available WiFi SSID, entering WiFi connection credentials, updating WiFi profile information, displaying available networks, displaying connection signal strength, etc.

[0084] In some embodiments, interface management units 450A, 450B are compatible with multiple operating system connection managers. In some embodiments, interface management units 450A, 450B modified to handle different operating systems but are still coordinated in their control/monitor modes of operation by the control management unit(s).

[0085] In some embodiments, the interface management units 450A, 450B communicate with their respective connection managers 420A, 420B and/or other units using different inter-process communications. For example, in some embodiments, interface management

units 450A can communication via domain sockets 475A. In some embodiments, interface management units 450B can communicate via D-Bus communication mechanisms 475B. In some embodiments, the communication mechanism between a connection manager 420A, 420B and its corresponding interface management unit 450A, 450B can be container operating system-specific or implementation-specific. In some embodiments, the interface management units can be configured to support any type of top layer protocol such as wpa_ctl or D-Bus. In some embodiments, a connection manager 420A, 420B can select any compatible top layer protocol.

[0086] In some embodiments, the control channel 400 includes a physical interface manager 480. The physical interface manager can, in some embodiments, be instructed to scan which connections (e.g. WiFi networks) are available via the physical interface 205, to associate or otherwise connect to a particular connection, and/or to authenticate with the particular connection. In some embodiments, the physical interface manager 480 communicates with the interface management units 450A, 450B to receive instructions and/or communicate statuses, available connections, etc.

[0087] In some embodiments, the physical interface manager is configured to operate at a host level (e.g. in a host namespace). In some embodiments, the architecture includes an interceptor mechanism 490 for filtering, intercepting or otherwise controlling the messages sent to the kernel 215 from the interface management units 450A, 450B.

[0088] FIG. 5A shows a schematic showing aspects of an example namespace architecture 500 for a control channel for a WiFi physical interface. As illustrated, in some embodiments, aspects of an interface management unit 450 can be positioned within a container network namespace 510, a host network namespace 520, and a container UNIX Time Sharing (UTS)/Unix System Resources (USR)/Interprocess Communication (IPC)/mount (MNT)/Process ID (PID) namespace 530. In other embodiments, as suitable, any number of namespaces and/or architectures may be used including others which may not be explicitly mentioned herein.

[0089] References A, B and C show example points in the processes at which messages sent to the kernel 215 from the interface management units 450 can be intercepted.

[0090] FIG. 5B shows an example mechanism for filtering messages at C in FIG. 5A. In this example embodiment, a Netlink libnl library is used to silently intercept netlink messages before they are sent through the socket to the kernel 215. Before the message is sent 585, the libnl library call nl_sendmsg 580 passes the message to NL_CB_MSG_OUT 590.

NL_CB_MSG_OUT 590 is a callback function configured to inspect the message, modify the message, discard the message, and/or return an error code.

[0091] FIG. 6 shows a schematic diagram showing aspects of an example communication device 600. In some embodiments, the communication device 500 may include one or more processors 601, memory devices 620, communication interfaces 205, input and/or output devices 640, and/or any other components or mechanisms suitable for or involved in performing aspects of the methods and functions described herein.

[0092] In some embodiments, an example communication device 500 may be a mobile device such as a smartphone, tablet computer, laptop, wearable device or other computing device.

[0093] Each processor 601 may be, for example, any type of general-purpose microprocessor or microcontroller, a central or graphics processing unit, a digital signal processing (DSP) processor, an integrated circuit, a field programmable gate array (FPGA), a reconfigurable processor, or any combination thereof.

[0094] Memory or storage devices 620 may include one or a combination of any type of computer memory that is located either internally or externally, for example, hard drives, flash memory, solid state memory, network storage devices, random-access memory (RAM), cache memory, read-only memory (ROM), electro-optical memory, magneto-optical memory, erasable programmable read-only memory (EPROM), and electrically-erasable programmable read-only memory (EEPROM), Ferroelectric RAM (FRAM), non-transitory computer readable media or the like.

[0095] In some examples, memory or storage devices 620 may include data or instruction sets for configuring the one or more processors to implement, control and/or instruct a kernel, containers, interface management units, control management units, physical interface managers, connection managers, network nodes, network controllers and any other suitable application or process. Although there may be a distinction between processes and applications operating at a kernel level and those operating at a container level, all such processes and applications at both levels can be interpreted as being provided through the operations of the processor(s) 501. The memory devices 520 may also include instructions or code for configuring one or more processors and other components of the communication device 500 to perform any of the methods and functions described herein.

[0096] In some embodiments, the communication device 600 may include input or output devices 640 such as keyboard, mouse, camera, touch screen, microphone, displays, or other integrated, peripheral or linked input or output device. The input devices may be configured to receive instructions to select or change connection profile information. The output devices may be configured to display or otherwise communicate connection information, etc.

[0097] In some examples, the communication device 600 includes one or more physical communication interfaces 205. In some embodiments, the physical communication interfaces can include radios, antennae, circuits, and any other hardware, device or module for providing an aspect of a communication interface. In some embodiments, the one or more communication interfaces 205 can be configured to communications using IEEE 802.11 (WiFi), Bluetooth™, Global System for Mobile Communications (GSM), Code Division Multiple Access (CDMA), Long-Term Evolution (LTE), and/or the like.

[0098] FIG. 7 is a flowchart showing aspects of an example method 700 for managing a physical communication interface on a communication device 500.

[0099] At 710, processor(s) of the communication device 500 operate a first communication interface management unit in a first container operating on the communication device 500. In some embodiments, the first communication interface management unit manages 715 a connection to a first virtual communication interface having a network connection with the physical communication interface. In some instances, the first virtual communication interface is provided by a first network node positioned between the first container and the physical communication interface.

[00100] At 720, the processor(s) of the communication device 500 operate a second communication interface management unit in a second container operating on the communication device 500. In some embodiments, the second communication interface management unit manages 725 a connection to a second virtual communication interface having a network connection with the physical communication interface. In some instances, the second virtual communication interface is provided by a second network node positioned between the second container and the physical communication interface.

[00101] In some embodiments, the processors similarly operate any number of communication interface management units for a corresponding number of containers operating on the communication device.

[00102] In some embodiments, the second communication interface management unit operates concurrently with the operation of the first communication interface. In some instances, the concurrent operation provides both containers with access to the physical communication interface.

5 [00103] In some embodiments, the processor(s) block direct network communications between the first communication interface and the second communication interface. In some embodiments, the processors hide the virtual communication interfaces from an external connection with the physical communication interface. In some embodiments, the processors block direct network communications between virtual communication interfaces
10 and/or hide the virtual communication interfaces with a networking controller.

[00104] As described herein or otherwise, in some embodiments, the processors configure each of the communication interface management units to operate in a control mode or a monitor mode. In some embodiments, the processors configure the communication interface management units such that only one of the communication interface management units
15 operate in a control mode at a time.

[00105] As described herein or otherwise, in some embodiments, the processors identify which communication interface management unit is to operate in the control mode based on communication interface profiles for the containers, and based on available external connections for the physical communication interface.

20 [00106] FIGS. 8A and 8B illustrate before and after states for a control channel for an example architecture 800 operating two containers 210A, 210B when a focus shifts from the first container 210A to the second container 210B. In both states, WiFi network SSID 1 is available.

[00107] In the before state in FIG. 8A, the first container 210A is in focus (indicated by the
25 bold outline), and the communication interface management unit 450A in the first container is operating in a control mode (also indicated by a bold outline). Referring again to FIG. 8A, the first container 210A has a profile for authenticating/authorizing access to SSID 1, and the first communication interface management unit 450A is in a control mode and connects to the SSID 1 network.

30 [00108] When a change of focus to the second container 210B is triggered as illustrated in FIG. 8B, the control management unit(s) are used to check and compare the WiFi profiles of the containers and any policies. Because the profiles of the second container 210B permit

access to SSID 2 but not SSID 1, the device processor(s) keep the first communication interface management unit 450A operating in a control mode, and the second communication interface management unit 450B operates in a monitor mode and can, in some embodiments, provide a notification of such to the second container's connection manager 420B.

[00109] In some embodiments, this assignment of modes may permit the second container 210B which is now in focus to have network communications even though its profile information does not have the credentials for access the network. In some instances, this may improve usability by not disconnecting the communication device from the network simply because of a change of container focus. In some instances, this behavior may be overridden by policy data which may prevent the first container from sharing its SSID profile, or policy data which may prevent the second container from accessing a SSID of another profile. Other variations and considerations are possible.

[00110] FIGS. 9A and 9B illustrate before and after states for a control channel for an example architecture 900 operating two containers 210A, 210B when a focus shifts from the first container 210A to the second container 210B. In both states, WiFi network SSID 1 is available. When a change of focus to the second container 210B is triggered as illustrated in FIG. 9B, the control management unit(s) are used to check and compare the WiFi profiles of the containers and any policies.

[00111] Because the profiles of the second container 210B also has access to SSID 1, the device processor(s) configured the second communication interface management unit 450B to operate in the control mode, and the first communication interface management unit 450A to operating in the monitor mode. Because the driver and physical interface is already connected to SSID 1, there is no interruption of the network connection when control is shifted from one container to another.

[00112] FIGS. 10A and 10B illustrate before and after states for a control channel for an example architecture 1000 operating two containers 210A, 210B when an available external connection changes. When a change in external network availability is detected, the processors check the policy data and WiFi profiles. Because the new and only available network connection is SSID 2 which matches a WiFi profile of the second container 210B, control is shifted to the second communication interface management unit 450B even though the focus continues to be on the first container 210A. In some instances, this may provide for

network access even though no available network connections match any profiles for the first container 210A.

[00113] FIGS. 11A and 11B illustrate before and after states for a control channel for an example architecture 1100 operating two containers 210A, 210B when available external connections changes. When a change in external network availability is detected, the processors check the policy data and WiFi profiles. Even though a new network connection SSID 2 is available which may have a higher priority for the second container 210B, the processors may not shift control. In some instances, this may prevent the temporary loss of network connectivity that would be caused by disconnecting from SSID 1 and connecting to SSID 2 with the second communication interface management unit 450B. In some instances, this behavior may be overridden by policy data which may prioritize the second container's profiles when the second container is in focus despite any potential temporary loss of connection. Other variations and considerations are possible.

[00114] Embodiments disclosed herein may be implemented using hardware, software or some combination thereof. Based on such understandings, the technical solution may be embodied in the form of a software product. The software product may be stored in a non-volatile or non-transitory storage medium, which can be, for example, a compact disk read-only memory (CD-ROM), USB flash disk, a removable hard disk, flash memory, hard drive, or the like. The software product includes a number of instructions that enable a computing device (computer, server, mainframe, or network device) to execute the methods provided herein.

[00115] Program code may be applied to input data to perform the functions described herein and to generate output information. The output information is applied to one or more output devices. In some embodiments, the communication interface may be a network communication interface. In embodiments in which elements are combined, the communication interface may be a software communication interface, such as those for inter-process communication. In still other embodiments, there may be a combination of communication interfaces implemented as hardware, software, and/or combination thereof.

[00116] Each computer program may be stored on a storage media or a device (e.g., ROM, magnetic disk, optical disc), readable by a general or special purpose programmable computer, for configuring and operating the computer when the storage media or device is read by the computer to perform the procedures described herein. Embodiments of the system may also be considered to be implemented as a non-transitory computer-readable

storage medium, configured with a computer program, where the storage medium so configured causes a computer to operate in a specific and predefined manner to perform the functions described herein.

5 [00117] Furthermore, the systems and methods of the described embodiments are capable of being distributed in a computer program product including a physical, non-transitory computer readable medium that bears computer usable instructions for one or more processors. The medium may be provided in various forms, including one or more diskettes, compact disks, tapes, chips, magnetic and electronic storage media, volatile memory, non-volatile memory and the like. Non-transitory computer-readable media may include all
10 computer-readable media, with the exception being a transitory, propagating signal. The term non-transitory is not intended to exclude computer readable media such as primary memory, volatile memory, RAM and so on, where the data stored thereon may only be temporarily stored. The computer useable instructions may also be in various forms, including compiled and non-compiled code.

15 [00118] The present disclosure may make numerous references to servers, services, interfaces, portals, platforms, or other systems formed from hardware devices. It should be appreciated that the use of such terms is deemed to represent one or more devices having at least one processor configured to execute software instructions stored on a computer readable tangible, non-transitory medium. One should further appreciate the disclosed
20 computer-based algorithms, processes, methods, or other types of instruction sets can be embodied as a computer program product comprising a non-transitory, tangible computer readable media storing the instructions that cause a processor to execute the disclosed steps.

[00119] Various example embodiments are described herein. Although each embodiment
25 represents a single combination of inventive elements, the inventive subject matter is considered to include all possible combinations of the disclosed elements. Thus, if one embodiment comprises elements A, B, and C, and a second embodiment comprises elements B and D, then the inventive subject matter is also considered to include other remaining combinations of A, B, C, or D, even if not explicitly disclosed.

30 [00120] The embodiments described herein are implemented by physical computer hardware embodiments. The embodiments described herein provide useful physical machines and particularly configured computer hardware arrangements of computing devices, servers, processors, memory, networks, for example. The embodiments described

herein, for example, are directed to computer apparatuses, and methods implemented by computers through the processing and transformation of electronic data signals.

[00121] The embodiments described herein may involve computing devices, servers, receivers, transmitters, processors, memory(ies), displays, networks particularly configured to implement various acts. The embodiments described herein are directed to electronic machines adapted for processing and transforming electromagnetic signals which represent various types of information. The embodiments described herein pervasively and integrally relate to machines and their uses; the embodiments described herein have no meaning or practical applicability outside their use with computer hardware, machines, a various hardware components.

[00122] Substituting the computing devices, servers, receivers, transmitters, processors, memory, display, networks particularly configured to implement various acts for non-physical hardware, using mental steps for example, may substantially affect the way the embodiments work.

[00123] Such hardware limitations are clearly essential elements of the embodiments described herein, and they cannot be omitted or substituted for mental means without having a material effect on the operation and structure of the embodiments described herein. The hardware is essential to the embodiments described herein and is not merely used to perform steps expeditiously and in an efficient manner.

[00124] Although the present invention and its advantages have been described in detail, it should be understood that various changes, substitutions and alterations can be made herein without departing from the invention as defined by the appended claims.

[00125] Moreover, the scope of the present application is not intended to be limited to the particular embodiments of the process, machine, manufacture, composition of matter, means, methods and steps described in the specification. As one of ordinary skill in the art will readily appreciate from the disclosure of the present invention, processes, machines, manufacture, compositions of matter, means, methods, or steps, presently existing or later to be developed, that perform substantially the same function or achieve substantially the same result as the corresponding embodiments described herein may be utilized according to the present invention. Accordingly, the appended claims are intended to include within their scope such processes, machines, manufacture, compositions of matter, means, methods, or steps.

WHAT IS CLAIMED IS:

1. A communication device comprising:

a physical communication interface; and

at least one processor configured to provide:

a kernel configured for operating first and second containers on the communication device;

first and second network nodes, the first network node providing a first virtual communication interface to the first container, and the second network node providing a second virtual communication interface to the second container; and

a network controller configured to provide routing and a network connection between the first network node and the physical communication interface, and between the second network node and the physical communication interface;

the first container configured to operate a first communication interface management unit for managing a connection to the first virtual communication interface, and the second container configured to concurrently operate a second communication interface management unit for managing a connection to the second virtual communication interface.
2. The communication device of claim 1, wherein the at least one processor is configured to block direct network communications between the first network node and the second network node.
3. The communication device of any of claims 1 to 2, wherein the first and the second communication interface management units concurrently manage access to the physical communication interface for the respective first and second containers via the respective first and second virtual communication interfaces.
4. The communication device of any of claims 1 to 3, wherein each of the first and the second communication interface management unit is configured to operate in a control mode in which the communication interface management unit controls a connection with the physical communication interface, or to operate in a monitor mode in which the communication interface management unit monitors the connection with the physical communication interface.
5. The communication device of claim 4, wherein the at least one processor is configured to provide a control management unit for managing the first and the second communication interface management units such that only one of the first and the second communication management unit is operating in the control mode.

6. The communication device of claim 5 wherein the control management unit identifies which of the first and the second communication interface management unit is to operate in the control mode based on communication interface profiles for the first and the second containers, and based on available external connections for the physical communication interface.

7. The communication device of claim 5 wherein when the first communication interface management unit is operating in the control mode, and a container focus switches from the first container to the second container, the first communication interface management unit continues to operate in the control mode.

8. The communication device of claim 5 wherein the communication interface manager is configured to manage a current connection to the physical communication interface when the communication interface management unit operating in the control mode is changed from the first communication interface management unit to the second communication interface management unit.

9. The communication device of any of claims 1 to 8 wherein the at least one processor is configured to intercept messages sent to the kernel from the first and the second communication interface management units.

10. The communication device of any of claims 1 to 9 wherein the network controller is configured to hide the first and the second network nodes from an external connection with the physical communication interface.

11. A method for managing a physical communication interface on a communication device, the method comprising:

operating a first communication interface management unit in a first container operating on the communication device, the first communication interface management unit managing a connection to a first virtual communication interface having a network connection with the physical communication interface; and

concurrently with the operation of the first communication interface, operating a second communication interface management unit in a second container operating on the communication device, the second communication interface management unit managing a connection to a second virtual communication interface having a network connection with the physical communication interface.

12. The method of claim 11, comprising: blocking direct network communications between the first virtual communication interface and the second virtual communication interface.

13. The method of any of claims 11 to 12, comprising: configuring the each of the first and the second communication interface management unit to operate in:

a control mode in which the communication interface management unit controls a connection with the physical communication interface, or

a monitor mode in which the communication interface management unit monitors the connection with the physical communication interface.

14. The method of claim 13, comprising: managing the first and the second communication interface management units such that only one of the first and the second communication management unit is operating in the control mode.

15. The method of claim 14, comprising: identifying which of the first and the second communication interface management unit is to operate in the control mode based on communication interface profiles for the first and the second containers, and based on available external connections for the physical communication interface.

16. The method of claim 14, comprising: when the first communication interface management unit is operating in the control mode, and a container focus switches from the first container to the second container, continues to operate the first communication interface management unit in the control mode.

17. The method of claim 14, comprising: managing a current connection to the physical communication interface when the communication interface management unit operating in the control mode is changed from the first communication interface management unit to the second communication interface management unit.

18. The method of any of claims 11 to 17, comprising: intercepting messages sent to the kernel from the first and the second communication interface management units.

19. The method of any of claims 11 to 18, comprising: hiding the first and the second virtual communication interfaces from an external connection with the physical communication interface.

20. A computer-readable medium or media having stored thereon computer-readable instructions which when executed by at least one processor configure the at least one processor to

operate a first communication interface management unit in a first container operating on the communication device, the first communication interface management unit managing a connection to a first virtual communication interface having a network connection with the physical communication interface; and

concurrently with the operation of the first communication interface, operate a second communication interface management unit in a second container operating on the communication device, the second communication interface management unit managing a connection to a second virtual communication interface having a network connection with the physical communication interface.

100, 101

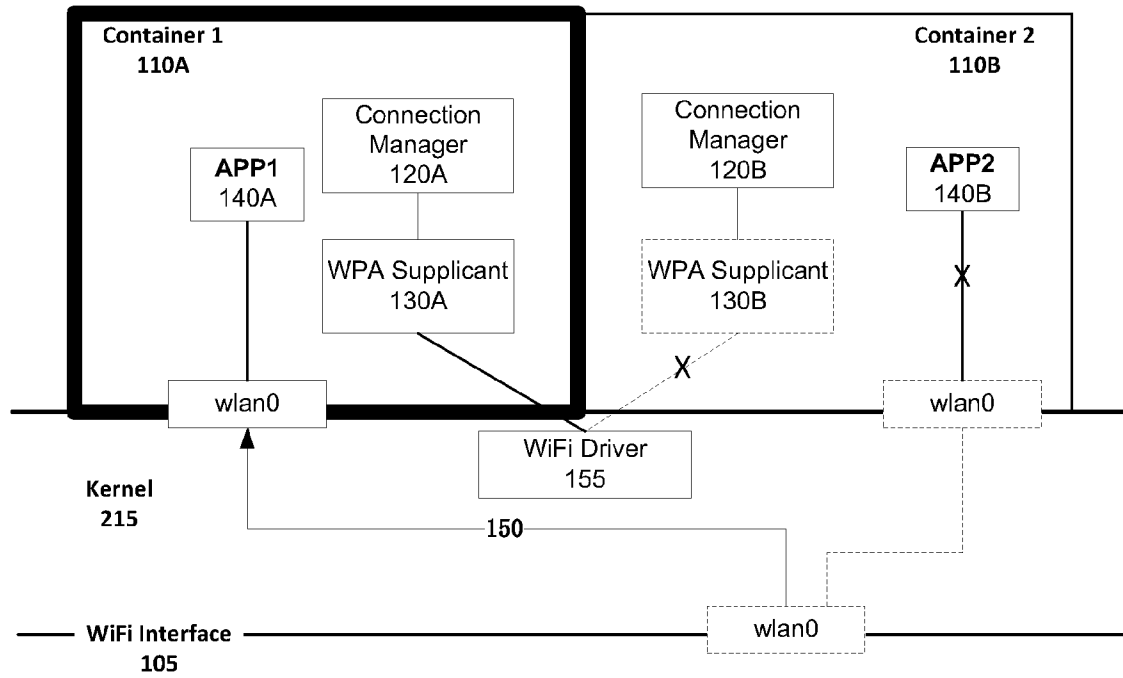


FIG. 1

200, 201

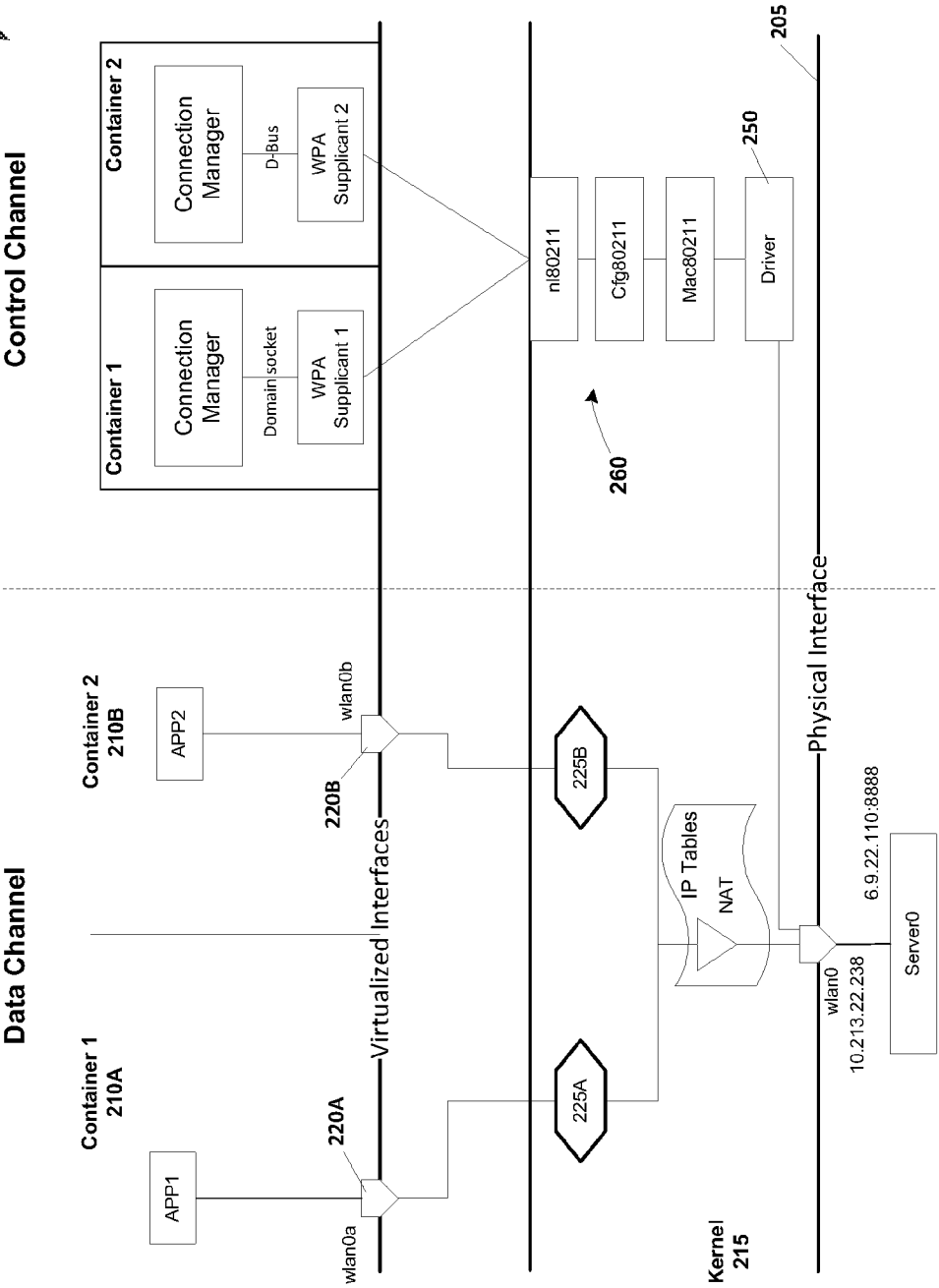


FIG. 2

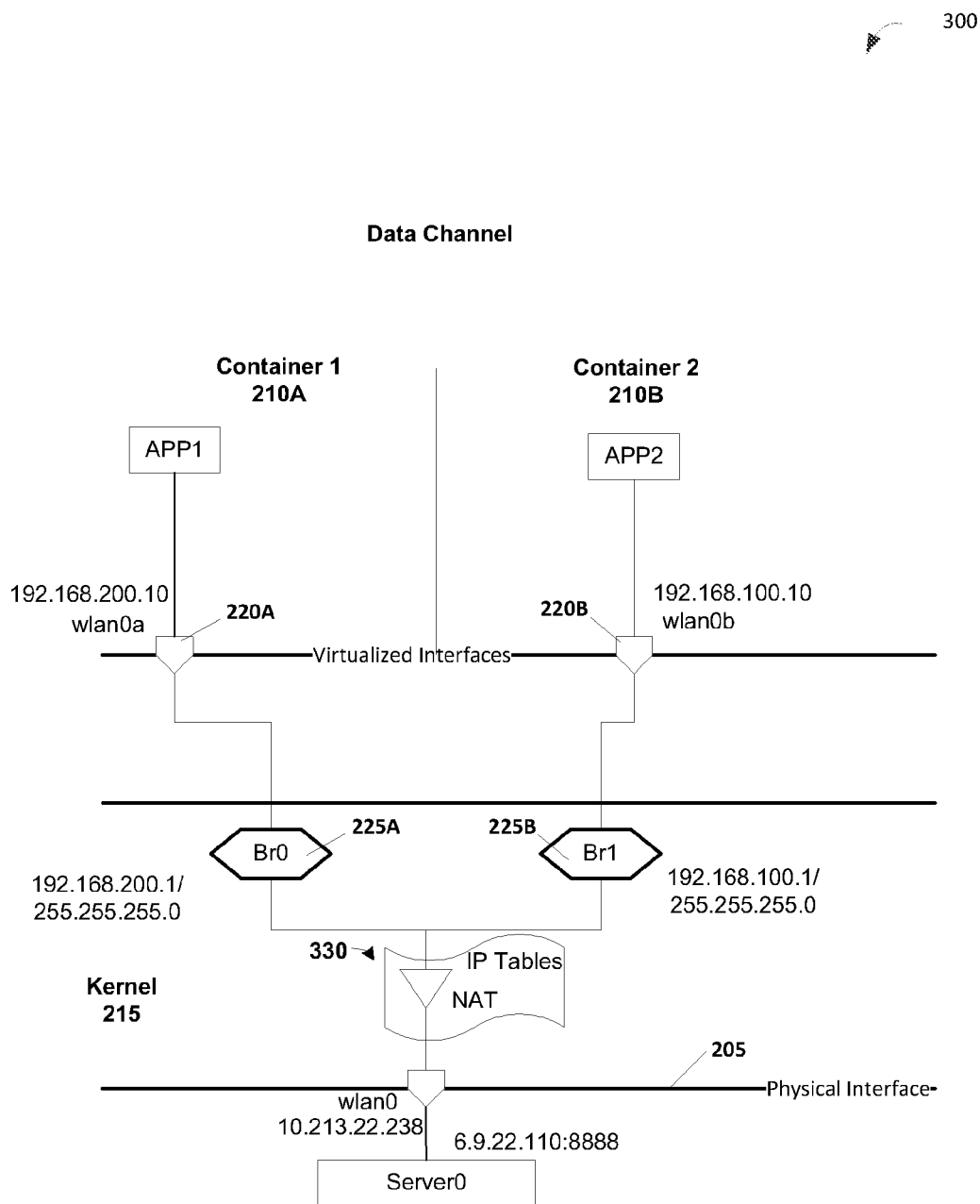


FIG. 3

400

Control Channel

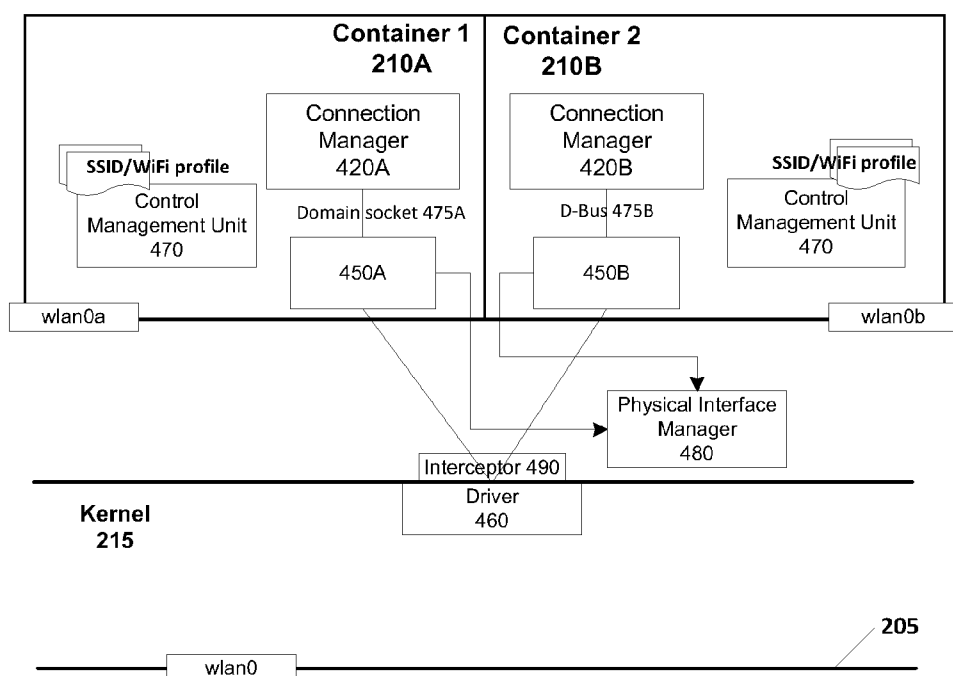


FIG. 4

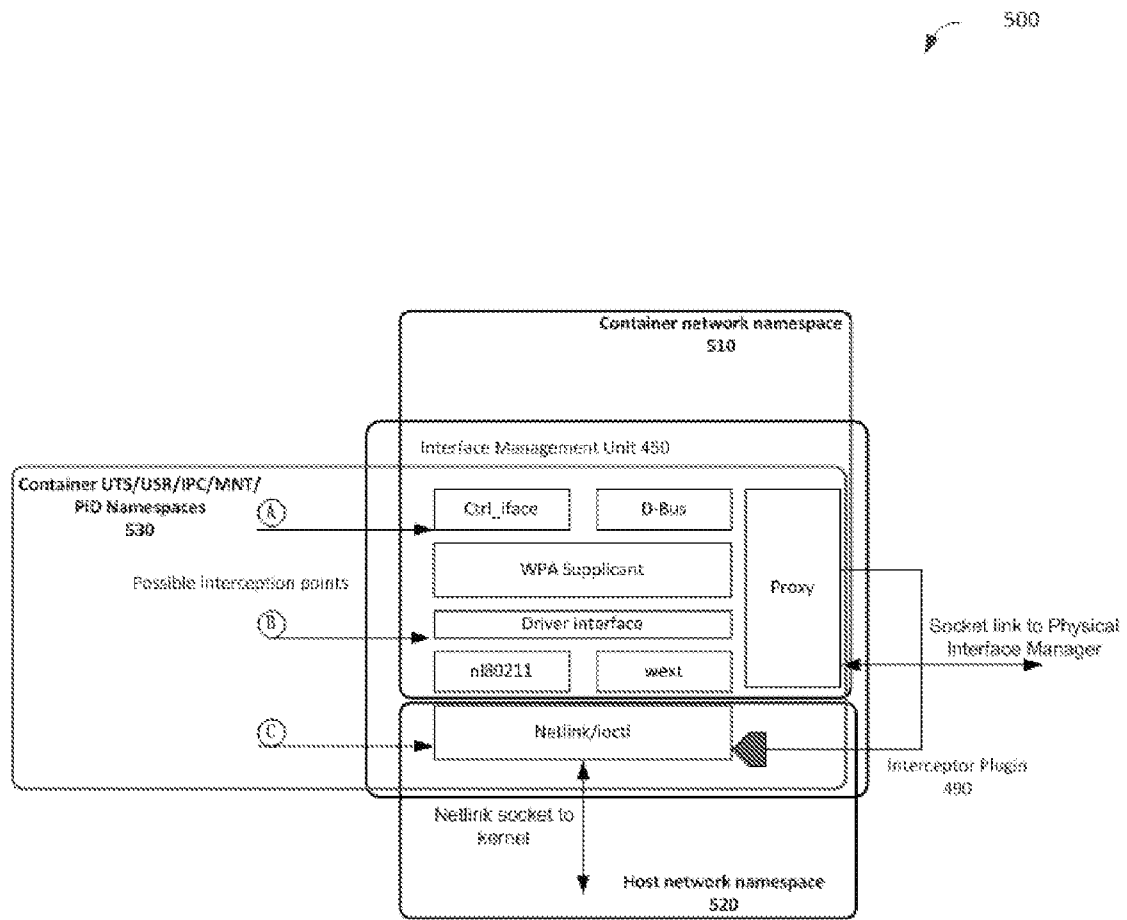


FIG. 5A

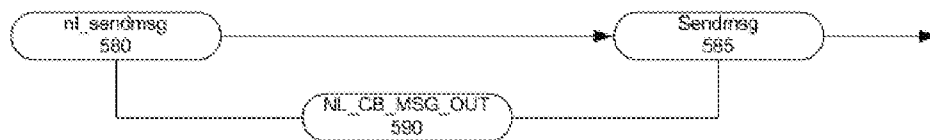


FIG. 5B

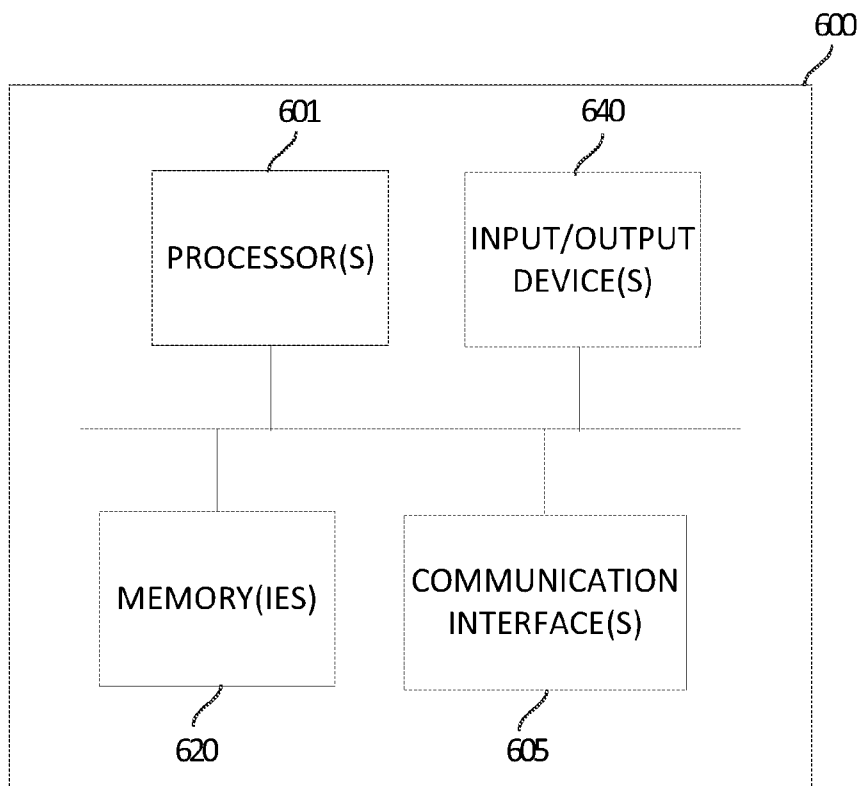


FIG. 6

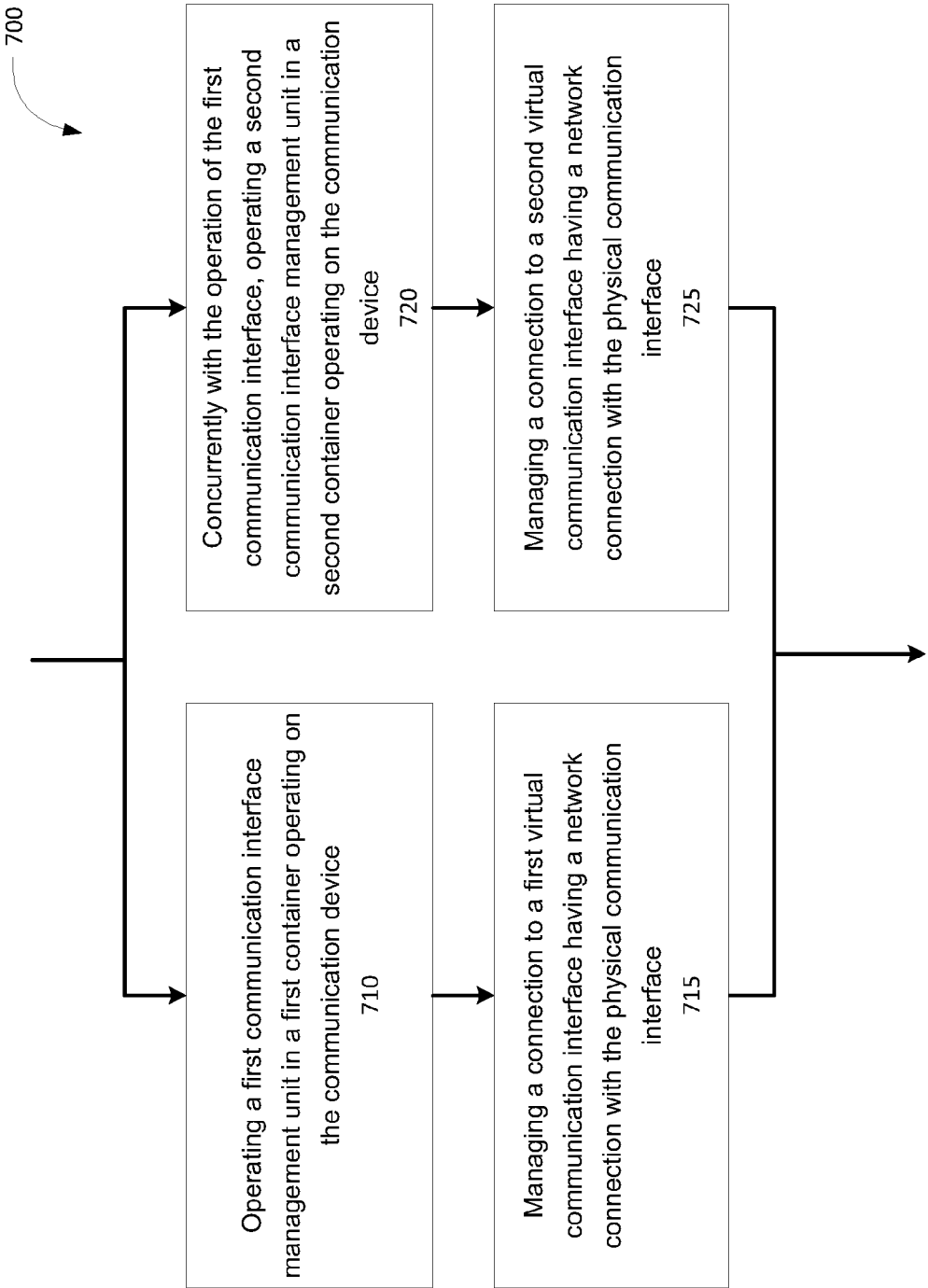


FIG. 7

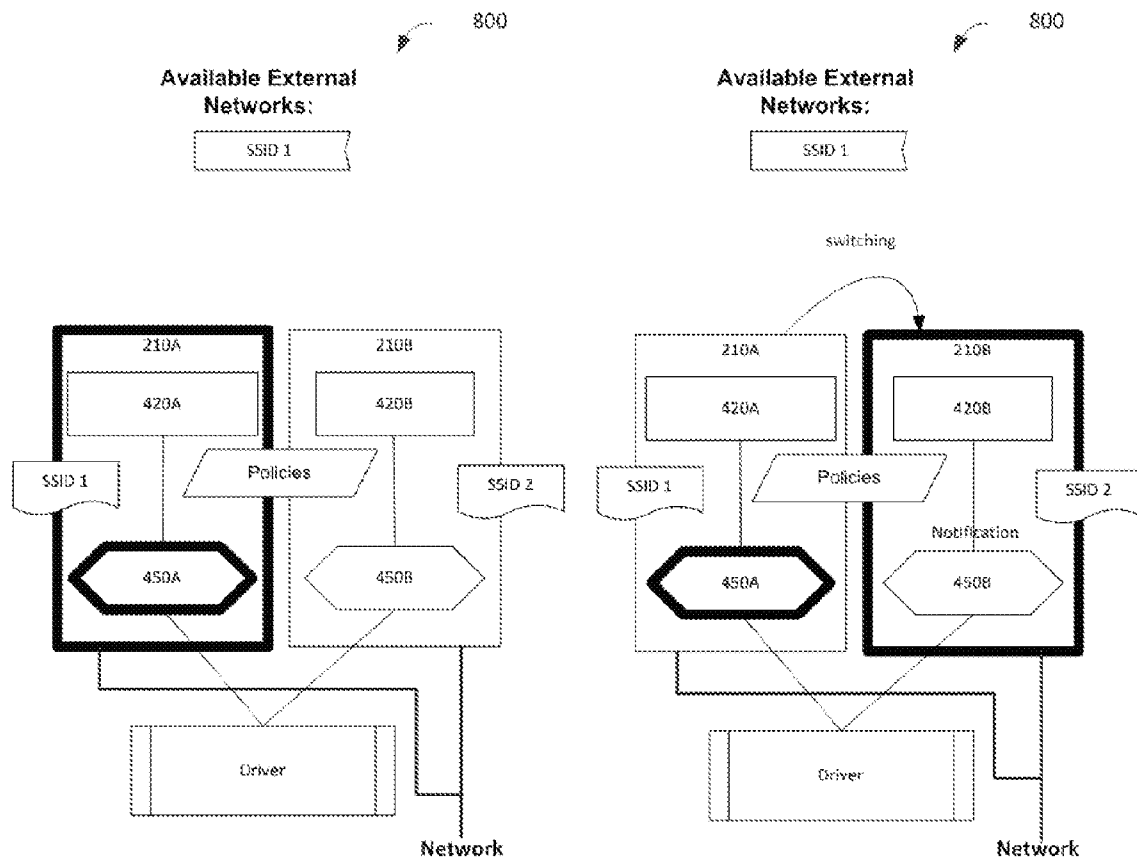


FIG. 8A

FIG. 8B

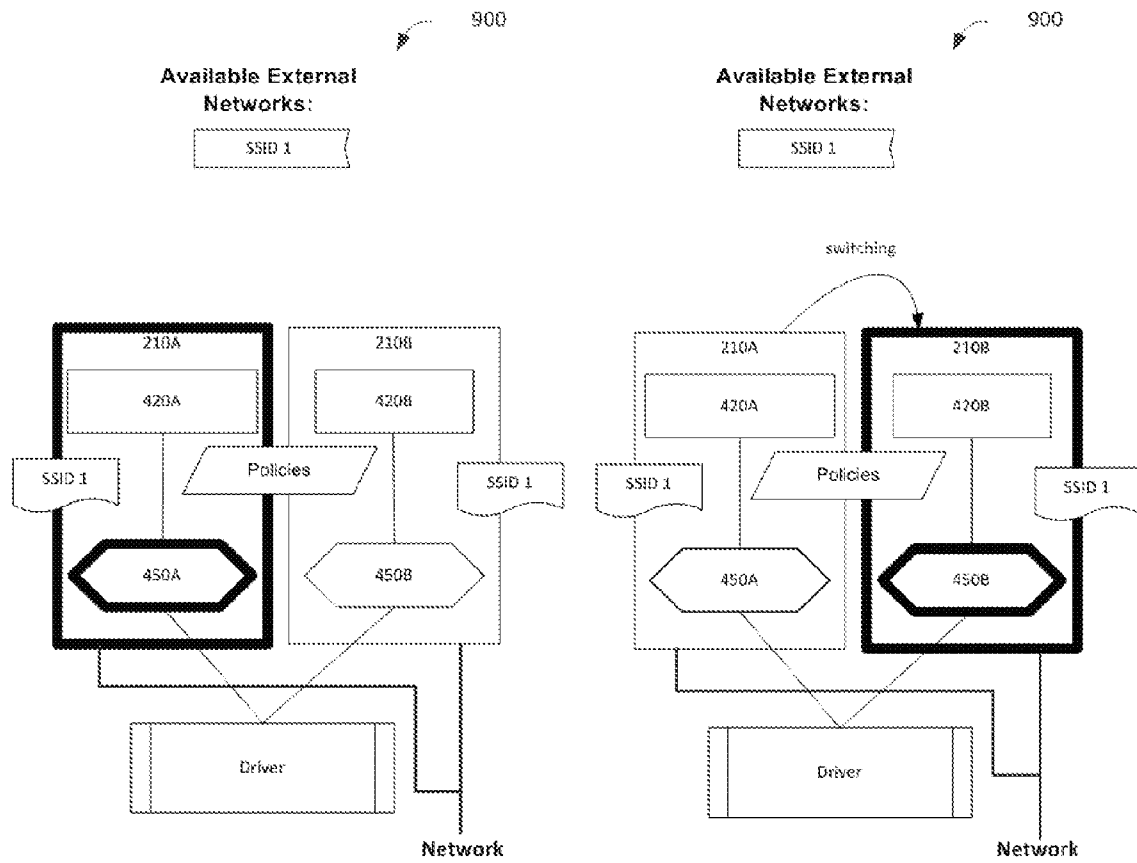


FIG. 9A

FIG. 9B

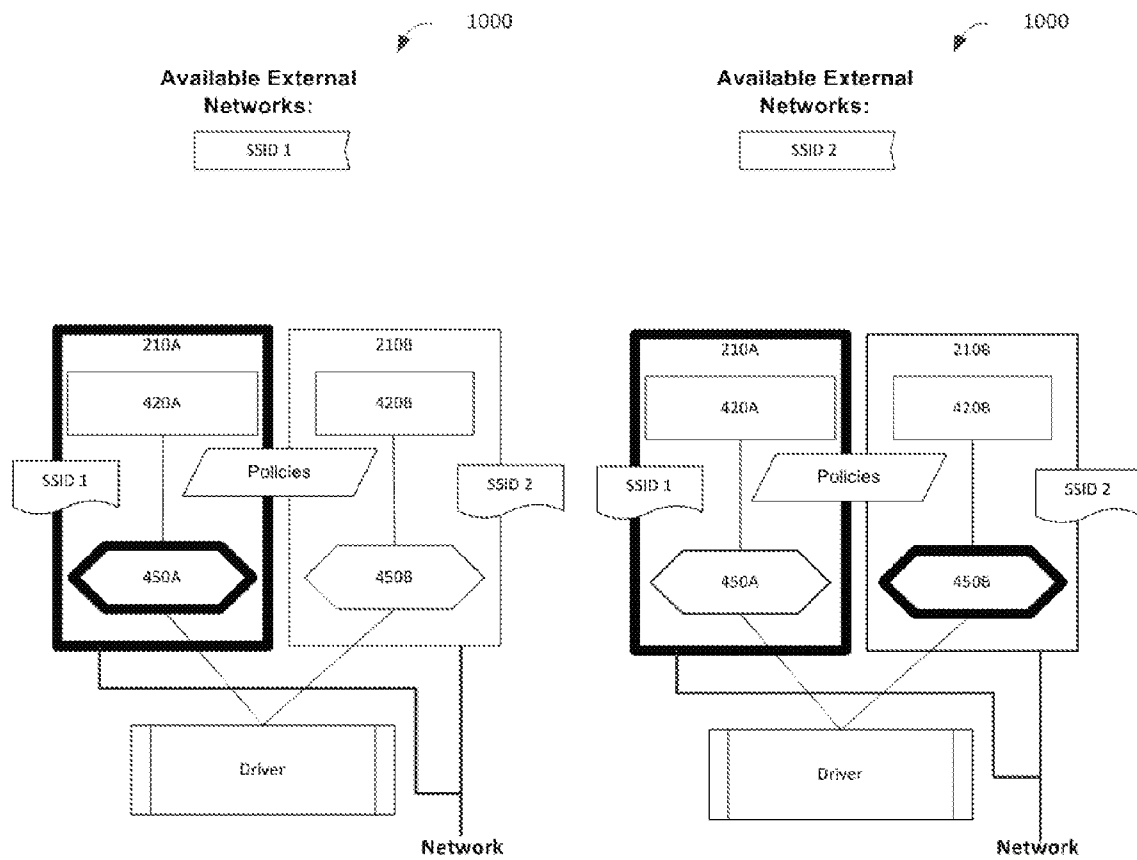


FIG. 10A

FIG. 10B

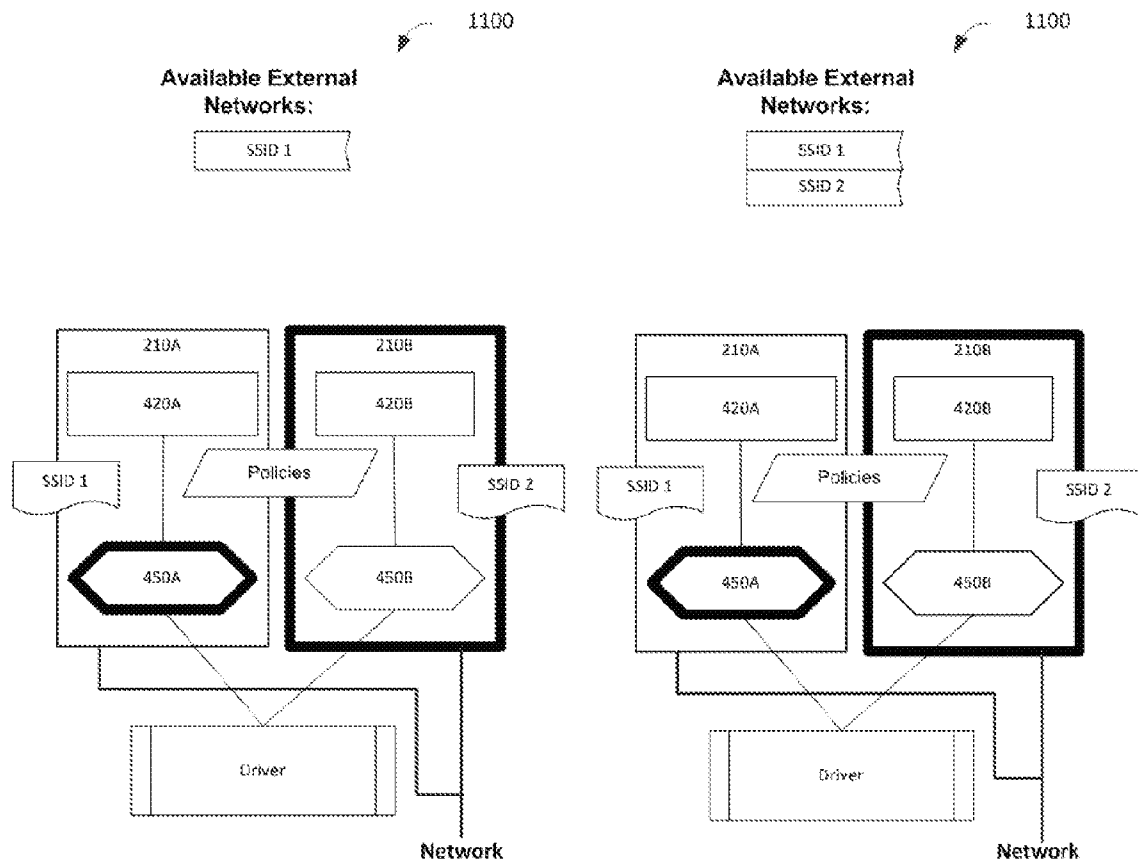


FIG. 11A

FIG. 11B

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2017/098293

A. CLASSIFICATION OF SUBJECT MATTER

H04L 12/28(2006.01)i

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

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H04L

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)

CNABS, CNPAT, WPI, EPODOC, 3GPP, IEEE: virtual+, VM, container, first, second, kernel, network, rout+, connect+, interface, physical, concurrent+

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2008151779 A1 (SUN MICROSYSTEMS INC.) 26 June 2008 (2008-06-26) description, paragraphs [0020]-[0037]	1-20
A	US 2008123536 A1 (SUN MICROSYSTEMS INC.) 29 May 2008 (2008-05-29) the whole document	1-20
A	US 2008151893 A1 (SUN MICROSYSTEMS INC.) 26 June 2008 (2008-06-26) the whole document	1-20
A	CN 104506404 A (H3C TECHNOLOGIES CO., LTD.) 08 April 2015 (2015-04-08) the whole document	1-20
A	CN 105808320 A (SICHUAN ANQIAN TECHNOLOGY CO., LTD.) 27 July 2016 (2016-07-27) 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

27 October 2017

Date of mailing of the international search report

21 November 2017

Name and mailing address of the ISA/CN

STATE INTELLECTUAL PROPERTY OFFICE OF THE
P.R.CHINA
6, Xitucheng Rd., Jimen Bridge, Haidian District, Beijing
100088
China

Facsimile No. (86-10)62019451

Authorized officer

LI,Yan

Telephone No. (86-10)61648550

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.

PCT/CN2017/098293

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
US	2008151779	A1	26 June 2008	None	
US	2008123536	A1	29 May 2008	None	
US	2008151893	A1	26 June 2008	None	
CN	104506404	A	08 April 2015	None	
CN	105808320	A	27 July 2016	None	