

(51) International Patent Classification:

H04L 12/24 (2006.01) H04L 12/28 (2006.01)

(21) International Application Number:

PCT/US2015/018137

(22) International Filing Date:

27 February 2015 (27.02.2015)

(25) Filing Language:

English

(26) Publication Language:

English

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

(72) Inventors: **DELGADO CAMPOS, Allan**; UltraPark, La Aurora, Heredia, Building 8, San Jose, 40104 (CR). **MAGALLON GHERARDELLI, Marcelo Eduardo**; UltraPark, La Aurora, Heredia, Building 8, San Jose, 40104 (CR).

(74) Agents: **BELL, Scott** et al.; Hewlett Packard Enterprise, 3404 E. Harmony Road, Mail Stop 79, Fort Collins, CO 80528 (US).

(81) Designated States (unless otherwise indicated, for every kind of national protection available): AE, AG, AL, AM,

AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

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

Declarations under Rule 4.17:

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

[Continued on next page]

(54) Title: CLOUD NETWORK MANAGEMENT

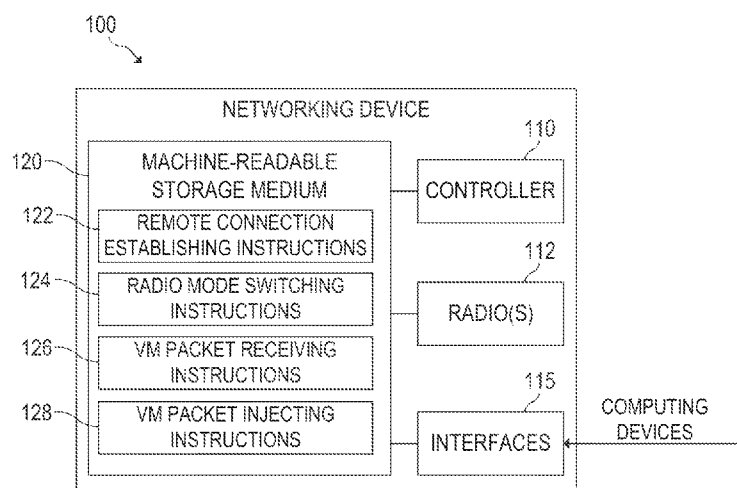


FIG. 1

(57) Abstract: Examples relate to enabling cloud network management. In some examples, a remote connection is established with a remote computing device, where the remote computing device is configured to execute a remote virtual machine. In response to a network virtualization request, a radio is switched to a client station mode. Next, a virtual machine network packet is received from the remote computing device, and the radio is used to inject the virtual machine network packet into a local network as local traffic for the remote virtual machine.



Published:

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

CLOUD NETWORK MANAGEMENT

BACKGROUND

[0001] Cloud network management often involves administrators that configure devices (e.g., switches, access points, etc.) located on unreachable networks (i.e., administrator is off-premise). Such administrators should verify that configuration changes have the desired effect on network clients' connectivity. For example, an administrator may request that a user that is on-premise perform connectivity tests and report back with the results. In another example, a virtual private network (VPN) can be established by the administrator so that the connectivity tests can be performed over a secure channel to the unreachable network.

BRIEF DESCRIPTION OF THE DRAWINGS

[0002] The following detailed description references the drawings, wherein:

[0003] FIG. 1 is a block diagram of an example networking device for cloud network management;

[0004] FIG. 2 is a block diagram of an example system for cloud network management;

[0005] FIG. 3 is a flowchart of an example method for execution by a networking device for cloud network management; and

[0006] FIG. 4 is a flowchart of an example method for execution by a remote computing device for cloud network management.

DETAILED DESCRIPTION

[0007] As described above, cloud network management can involve an on-premise user to coordinate with an administrator or a VPN. Cloud-managed network devices (e.g., switches, access points, etc.) can establish full-duplex communication channels (i.e., Web Socket) to a cloud management device. In examples described herein, a communication channel is used as a tunnel for network traffic (i.e., packet captures (PCAPs)) that originate off-premise. In these examples, a virtual machine is created, where network traffic of this off-premise

virtual machine can be redirected to the on-premise network using the communication channel.

[0008] In some examples, a remote connection is established with a remote computing device, where the remote computing device is configured to execute a remote virtual machine. In response to a network virtualization request, a radio is switched to a client station mode. Next, a virtual machine network packet is received from the remote computing device, and the radio is used to inject the virtual machine network packet into a local network as local traffic for the remote virtual machine.

[0009] Referring now to the drawings, FIG. 1 is a block diagram of an example networking device 100 for cloud network management. The example networking device 100 may be a switch, an access point, a wireless router, a repeater, a bridge, or any other electronic device suitable for cloud network management. In the embodiment of FIG. 1, networking device 100 includes controller 110, interfaces 115, and machine-readable storage medium 120.

[0010] Controller 110 may be one or more central processing units (CPUs), microprocessors, and/or other hardware devices suitable for retrieval and execution of instructions stored in machine-readable storage medium 120. Controller 110 may fetch, decode, and execute instructions 122, 124, 126, 128 to enable cloud network management, as described below. As an alternative or in addition to retrieving and executing instructions, controller 110 may include one or more electronic circuits comprising a number of electronic components for performing the functionality of one or more of instructions 122, 124, 126, 128.

[0011] Radio(s) 112 may include wireless interface(s) for communicating with other computing devices via radio frequencies. Radio(s) 112 can be configured to facilitate wireless networks that allow for wireless communication between computing devices. Radio(s) 112 may support an alternative operating mode such as client station mode. When a radio 112 is switched to client station mode, the networking device 100 can use the radio 112 to behave like a client and join wireless networks provided by other networking devices. In other examples where

networking device 100 is a switch, radio(s) 112 are not included in the networking device 100.

[0012] Interfaces 115 may include a number of electronic components for communicating with end devices. For example, interfaces 115 may be wireless interfaces such as wireless local area network (WLAN) interfaces and/or physical interfaces such as Ethernet interfaces, Universal Serial Bus (USB) interfaces, external Serial Advanced Technology Attachment (eSATA) interfaces, or any other physical connection interface suitable for communication with end devices. In operation, as detailed below, interfaces 115 may be used to send and receive data to and from other computing devices.

[0013] Machine-readable storage medium 120 may be any electronic, magnetic, optical, or other physical storage device that stores executable instructions. Thus, machine-readable storage medium 120 may be, for example, Random Access Memory (RAM), Content Addressable Memory (CAM), Ternary Content Addressable Memory (TCAM), an Electrically-Erasable Programmable Read-Only Memory (EEPROM), flash memory, a storage drive, an optical disc, and the like. As described in detail below, machine-readable storage medium 120 may be encoded with executable instructions for enabling cloud network management.

[0014] Remote connection establishing instructions 122 establish a connection with a remote computing device such as a cloud management server. The connection may be a full-duplex communication channel over the Internet, where the remote computing device is on a different local area network than networking device 100. In some cases, the communication channel may also involve other networking devices such as switches and/or routers.

[0015] Radio mode switching instructions 124 modify a mode of the radio 112 based on requests from the remote computing device. Specifically, if a virtualization request is received from the remote computing device, the mode of the radio 112 can be switched to client station mode, which allows the networking device 100 to connect to other wireless networks. In some cases, computing device 100 includes multiple radios 112 so that one radio can be switched to client

station mode while the other radios continue to operate in a normal operating mode that continues to provide wireless network(s). Alternatively, if the networking device 100 is a switch, radio mode switching instructions 124 are not included in machine-readable storage medium 120.

[0016] VM packet receiving instructions 126 receive virtual machine packets from a virtual machine of the remote computing device. In this example, the remote computing device initiates the virtual machine and uses the connection established above to send packets from the virtual machine. Networking device 100 identifies the virtual machine packets as originating from the remote computing device and, accordingly, processes them as described below.

[0017] VM packet injecting instructions 128 use the radio 112 in client station mode to inject the virtual machine packets into a network of networking device 100. In this manner, the virtual machine packets from the off-premise virtual machine can be treated as if they originated from a computing device that is on-premise. The remote computing device can request that the wireless networks accessible to the radio 112 be discovered, where one of the wireless networks can then be selected for joining by the virtual machine. The virtual machine can then be configured to remotely join the network of networking device 100 using network association parameters (e.g., internet protocol address, subnet mask, gateways, etc.) obtained by the radio 112. Because the virtual machine packets are tunneled through the established connection, the virtual machine is able to join the wireless network even though remote computing device is off-premise. Alternatively, if networking device 100 is a switch with no radio, the virtual machine packets can be injected into the network using a port of the switch.

[0018] FIG. 2 is a block diagram of an example system 200 including a remote computing device 216 interacting with computing devices of an off-premise network 201. Network 201 includes switch 202, access points 204A, 204N, and client computing devices 212A, 212N. The components of access points 204A, 204N may be similar to the corresponding components of networking device 100 described above with respect to FIG. 1.

[0019] As illustrated, access point A 204A includes radios 206A, 206N and controller 208. Controller 208 can be associated with firmware that includes instructions similar to as discussed above with respect to FIG. 1. Each of the radios 206A, 206N is configured to provide wireless networks of network 201. For example, the radios 206A, 206N can broadcast service set identifications (SSID's) that identify wireless networks that can be joined by client computing devices 212A, 212N. In this example, the wireless networks can be secured with encryption for preventing access by unauthorized devices.

[0020] Each of the radios 206A, 206N can also be configured to operate in a client station mode. When in client station mode, a radio 206A, 206N can be used to join wireless networks as if the corresponding access point 204A, 204N was a client device. For example, radio A 206A can be switched to client station mode while radio N 206N continues to operate in an access point mode (i.e., providing access to wireless networks). Access point N 204N does not show components in order to simply FIG. 2; however, access point N 204N can include similar components as described above with respect to access point A 204A.

[0021] Client computing devices 212A, 212N use access points 204A, 204N to access wireless networks of network 201. For example, client computing device A 212A can use access point A 204A to discover and join a wireless network. In this example, packets from client computing device A 212 can then be accepted by access point A 204A and routed through switch 202 to provide client computing device 212A with access to the Internet or other client computing devices 212N on network 201.

[0022] Remote computing device 216 is an off-premise device for managing components of network 201 such as switch 202 and access points 204A, 204N. Remote computing device 216 may be configured to access and reconfigure components such as switch 202 and access points 204A, 204N over the Internet. Because remote computing device 216 is off-premise, it cannot normally verify the reconfiguration of the components.

[0023] Remote computing device 216 includes virtual machine(s) 218 that are configured to verify the reconfiguration of the components. Remote computing

device 216 can instantiate a virtual machine 218 and then use a connection with an access point 204A, 204N to tunnel virtual machine packets between the remote computing device 216 and network 201. In this example, the initial connection between remote computing device 216 and the access point 204A, 204N allow the virtual machine 218 to behave as if it was on-premise. Accordingly virtual machine 218 can access and join wireless networks provided by access points 204A, 204N to verify a reconfiguration of the components of network 201.

[0024] In some cases, remote computing device 216 may instantiate multiple virtual machines 218, where packets from each machine are tunneled through a different radio (e.g., radio A 206A, radio N 206N) of an access point (e.g., access point A 204A, access point N 204N). In this case, remote computing device 216 can use the virtual machines 218 to confirm that the reconfigured components of network 201 still allow for communication between different client devices.

[0025] FIG. 3 is a flowchart of an example method 300 for execution by a networking device 100 for cloud network management. Although execution of method 300 is described below with reference to networking device 100 of FIG. 1, other suitable devices for execution of method 300 may be used such as access point 204A, 204N of FIG. 2. Method 300 may be implemented in the form of executable instructions stored on a machine-readable storage medium, such as computer readable medium 120 of FIG. 1, and/or in the form of electronic circuitry.

[0026] Method 300 may start in block 305 and continue to block 310, where networking device 100 establishes a connection with a remote computing device such as a cloud management server. The communication channel may also involve other networking devices such as switches and/or routers. Remote computing device may use the communication channel to reconfigure networking device 100 or other components on the same network. In block 315, networking device 100 modifies a mode of one of its radios in response to a virtualization request from remote computing device. The virtualization request may notify networking device 100 that remote computing device will be initiating a virtual machine to verify the reconfiguration of the network.

[0027] In block 320, networking device 100 receives virtual machine packets from a virtual machine of the remote computing device. The virtual machine packets are sent from the virtual machine of remote computing device. In block 325, networking device 100 uses its radio in client station mode to inject the virtual machine packets into the network, which allows for the virtual machine to behave as if it is on-premise. Because the virtual machine packets are tunneled through the established connection, the virtual machine is able to join a wireless network as described below and verify the reconfiguration. Packets from the network can also be received by radio and then tunneled in the opposite direction to the virtual machine. Method 300 may then continue block 330, where method 300 may stop.

[0028] FIG. 4 is a flowchart of an example method 400 for execution by a remote computing device 216 for cloud network management. Although execution of method 400 is described below with reference to remote computing device 216 of FIG. 2, other suitable devices for execution of method 400 may be used. Method 400 may be implemented in the form of executable instructions stored on a machine-readable storage medium and/or in the form of electronic circuitry.

[0029] Method 400 may start in block 405 and continue to block 410, where remote computing device 216 establishes a remote connection to an access point in a different network than remote computing device 216. The communication channel may also involve other networking devices such as switches and/or routers. Remote computing device 216 may use the communication channel to reconfigure the access point or other components in the access point's network. In block 415, remote computing device 216 creates a virtual machine that is configured to join the remote network.

[0030] In block 420, remote computing device 216 sends a virtualization request to the access point, where the remote connection is used as a tunnel for subsequent requests from the remote computing device 216. In block 425, remote computing device 216 sends a request to access point for the available wireless networks of the remote network. A radio of the access point in client station mode is used by access points to discover the available wireless networks,

which are sent back to the remote computing device 216. In block 430, remote computing device 216 selects and joins one of the wireless networks through the tunnel. Specifically, remote computing device 216 uses the radio to obtain network association parameters and then uses the network association parameters to join the selected wireless network. Method 400 may then continue to block 435, where method 400 may stop.

[0031] The foregoing disclosure describes a number of examples for enabling cloud network management. In this manner, the examples disclosed herein facilitate cloud network management by using a radio of an access point that is in client station mode as a tunnel for a remote virtual machine executed by a remote management device.

CLAIMSWe claim:

1. A networking device for enabling cloud network management, comprising:
 - a radio that supports a client station mode;
 - an interface to receive communications from a remote computing device;
 - and
 - a controller operatively connected to the radio, the controller to:
 - establish a remote connection with the remote computing device, wherein the remote computing device is configured to execute a remote virtual machine;
 - in response to a network virtualization request, switch the radio to the client station mode;
 - receive a virtual machine network packet from the remote computing device; and
 - use the radio to inject the virtual machine network packet into a local network as local traffic for the remote virtual machine.
2. The networking device of claim 1, further comprising a second radio that operates in an access point mode while the radio is in the client station mode.
3. The networking device of claim 1, wherein the controller is further to:
 - use the radio to discover a plurality of wireless networks in the local network; and
 - send a list of the plurality of wireless networks to the remote computing device.
4. The networking device of claim 3, wherein the controller is further to:
 - receive a join request from the remote computing device that specifies a selected wireless network of the plurality of wireless networks, wherein the join request is injected into the local network by the radio; and

send network association parameters to the remote virtual machine, wherein the remote virtual machine uses the network association parameters to join the selected wireless network.

5. The networking device of claim 1, wherein a second virtual machine of the remote computing device joins the local network using a second radio.

6. The networking device of claim 1, wherein the remote computing device modifies a network configuration of the local network, and wherein the remote virtual machine uses the radio to verify the network configuration.

7. A method for enabling cloud network management, comprising:
establishing a remote connection with a networking device in a remote network;
creating a virtual machine that is configured to join the remote network;
sending a network virtualization request to the networking device; and
sending a virtual machine network packet to the access point, wherein the remote networking device injects the virtual machine network packet into the remote network as local traffic for the virtual machine.

8. The method of claim 7, wherein the networking device is an access point, and wherein the access point switches a radio to a client station mode in response to the network virtualization request.

9. The method of claim 8, further comprising:
sending a request for available wireless networks to the access point, wherein the access point uses the radio to discover a plurality of wireless networks in the local network; and
receiving a list of the plurality of wireless networks from the access point.

10. The method of claim 9, further comprising:

sending a join request to the access point that specifies a selected wireless network of the plurality of wireless networks, wherein the access point uses the radio to inject join request into the remote network; and
receiving network association parameters from the access point; and
using the network association parameters and the radio to join the selected wireless network.

11. The method of claim 8, further comprising:
creating a second virtual machine that joins the remote network using a second radio; and
verifying that the virtual machine can communicate with the second virtual machine.

12. The method of claim 8, further comprising:
modifying a network configuration of the remote network; and
using the virtual machine and the radio to verify the network configuration.

13. A non-transitory machine-readable storage medium encoded with instructions executable by a processor for cloud network management, the machine-readable storage medium comprising instructions to:

establish a remote connection with a remote computing device, wherein the remote computing device is configured to execute a remote virtual machine, and wherein the remote computing device modifies a network configuration of a local network;

in response to a network virtualization request, switch a radio to a client station mode;

receive a virtual machine network packet from the remote computing device; and

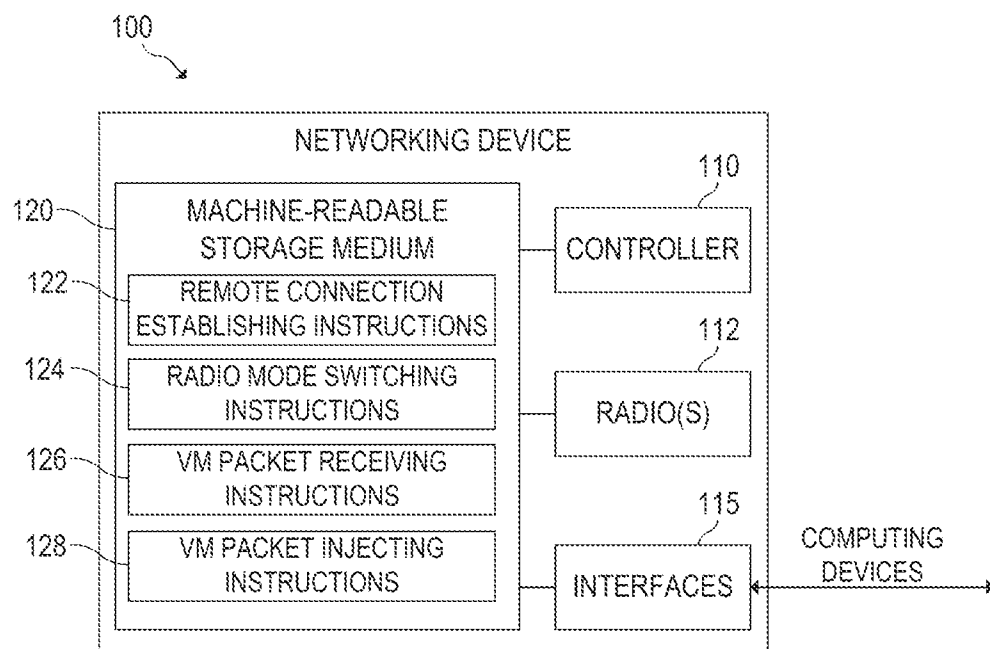
use the radio to inject the virtual machine network packet into the local network as local traffic for the remote virtual machine, wherein the remote virtual machine uses the radio to verify the network configuration.

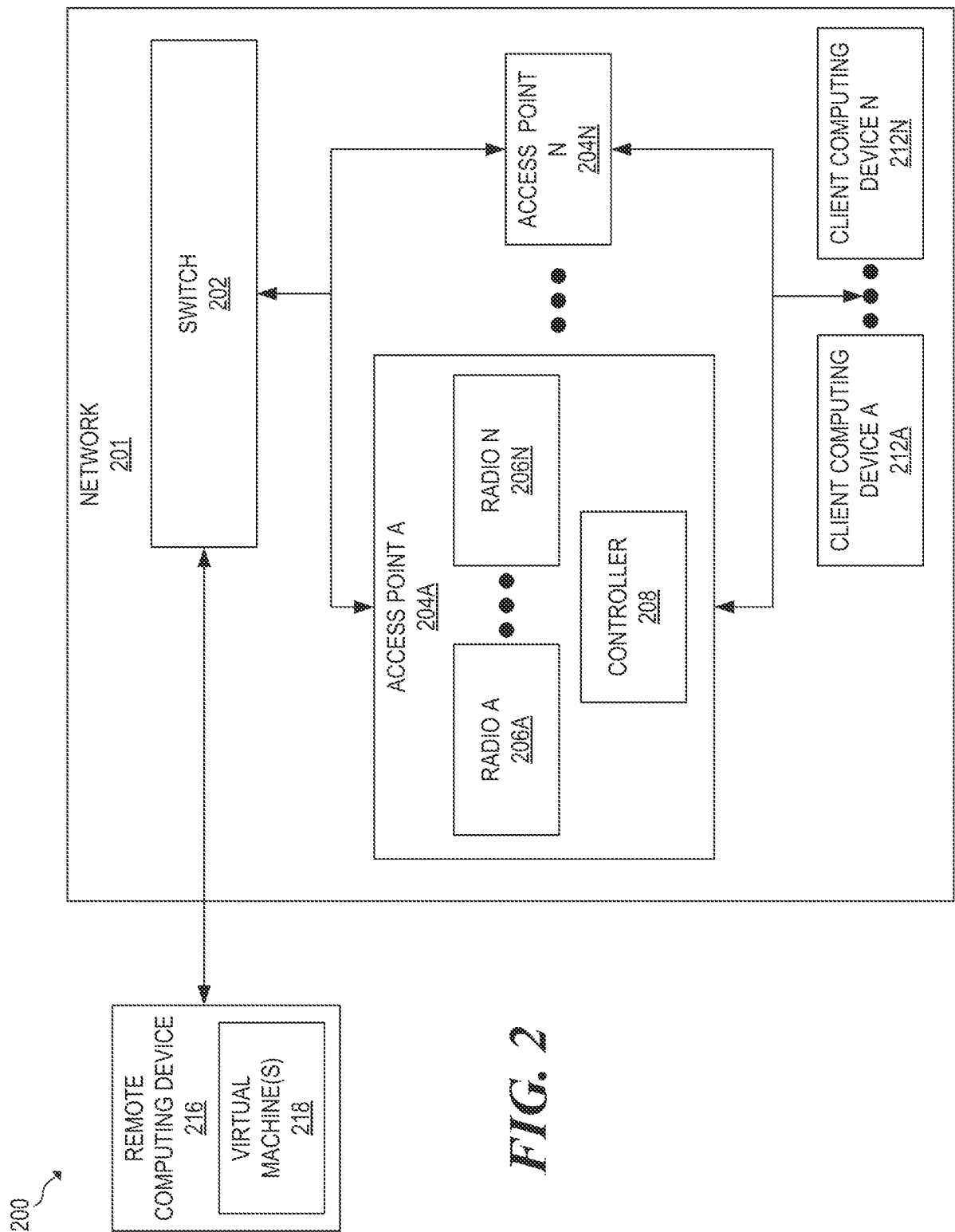
14. The non-transitory machine-readable storage medium of claim 13, wherein the instructions are further to tunnel network packets from the local network to the remote virtual machine.

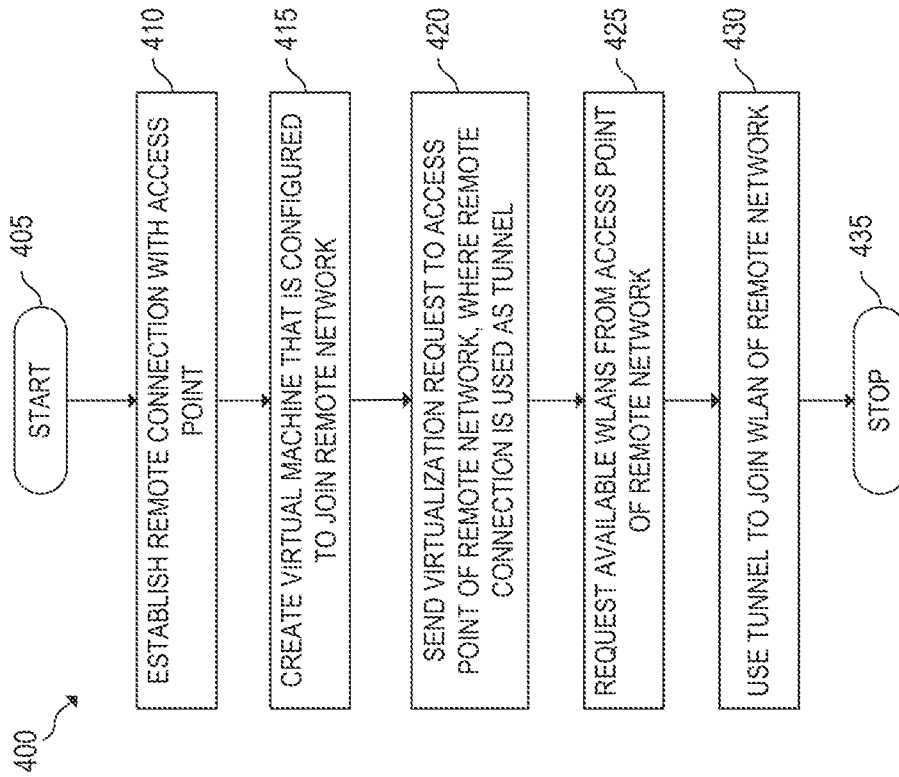
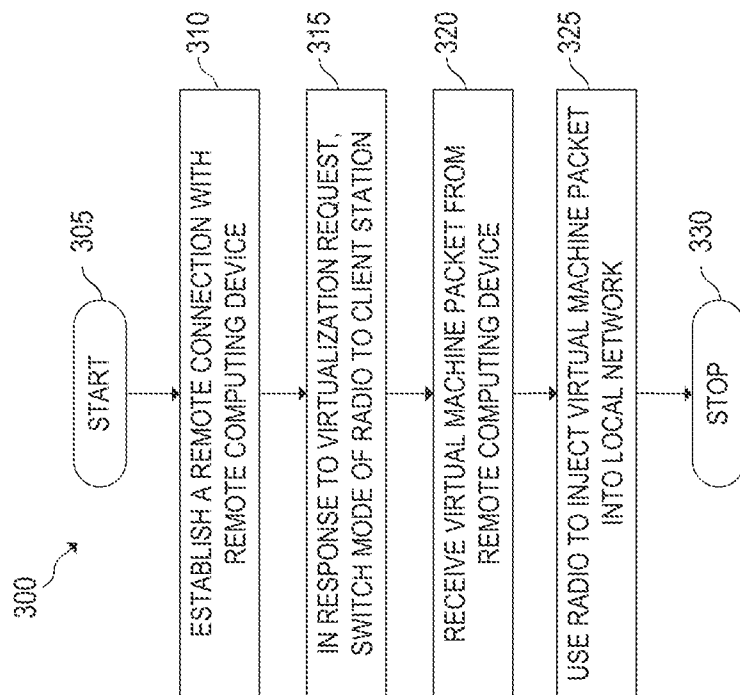
15. The non-transitory machine-readable storage medium of claim 13, wherein the instructions are further to:

use the radio to discover a plurality of wireless networks in the local network; and

send a list of the plurality of wireless networks to the remote computing device.

**FIG. 1**



**FIG. 4****FIG. 3**

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US2015/018137**A. CLASSIFICATION OF SUBJECT MATTER****H04L 12/24(2006.01)i, 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 12/24; G06F 15/16; G06F 9/445; H04W 88/08; H04W 48/16; G06F 9/44; G06F 9/455; H04L 12/28

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

Korean utility models and applications for utility models

Japanese utility models and applications for utility models

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

eKOMPASS(KIPO internal) & Keywords: wireless, network, management, remote, virtual, machine, access, point, station, and similar terms.

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 2010-0042988 A1 (CHRISTER LUNDIN et al.) 18 February 2010 See paragraphs [0007], [0036], [0050]-[0051]; figure 1; and claims 7, 10.	1-15
Y	US 2014-0269257 A1 (HONEYWELL INTERNATIONAL INC.) 18 September 2014 See paragraphs [0032], [0041], [0048]; and figures 1-2.	1-15
A	US 2014-0204797 A1 (ACCTON TECHNOLOGY CORP.) 24 July 2014 See paragraphs [0041]-[0079]; and figures 3A-5.	1-15
A	US 2011-0239210 A1 (SEIGO KOTANI et al.) 29 September 2011 See paragraphs [0020]-[0054]; and figures 1-3.	1-15
A	US 2010-0299387 A1 (GEORGE RUNCIE et al.) 25 November 2010 See paragraphs [0013]-[0025]; and figures 1-5.	1-15



Further documents are listed in the continuation of Box C.



See patent family annex.

* Special categories of cited documents:

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

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

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

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

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

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

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

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

"&" document member of the same patent family

Date of the actual completion of the international search

27 October 2015 (27.10.2015)

Date of mailing of the international search report

21 December 2015 (21.12.2015)

Name and mailing address of the ISA/KR

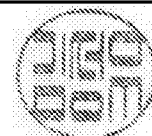
International Application Division
Korean Intellectual Property Office
189 Cheongsu-ro, Seo-gu, Daejeon Metropolitan City, 35208,
Republic of Korea

Facsimile No. +82-42-472-7140

Authorized officer

KIM, Seong Woo

Telephone No. +82-42-481-3348



INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.

PCT/US2015/018137

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2010-0042988 A1	18/02/2010	None	
US 2014-0269257 A1	18/09/2014	EP 2779733 A1	17/09/2014
US 2014-0204797 A1	24/07/2014	CN 103945394 A TW 201431418 A	23/07/2014 01/08/2014
US 2011-0239210 A1	29/09/2011	CN 102404312 A CN 102859935 A CN 102870093 A CN 103154966 A EP 2550595 A1 EP 2550596 A2 EP 2550768 A1 EP 2550768 B1 EP 2550769 A1 JP 2012-059270 A JP 2013-522793 A JP 2013-522794 A JP 2013-522795 A JP 2013-532394 A JP 5516821 B2 JP 5522307 B2 US 09059978 B2 US 2011-0238260 A1 WO 2011-119297 A1 WO 2011-119298 A1 WO 2011-119299 A1 WO 2011-119300 A2	04/04/2012 02/01/2013 09/01/2013 12/06/2013 30/01/2013 30/01/2013 30/01/2013 25/03/2015 30/01/2013 22/03/2012 13/06/2013 13/06/2013 13/06/2013 15/08/2013 11/06/2014 18/06/2014 16/06/2015 29/09/2011 29/09/2011 29/09/2011 29/09/2011 29/09/2011
US 2010-0299387 A1	25/11/2010	US 08438216 B2 US 08849906 B2 US 2013-227570 A1 US 2015-135180 A1	07/05/2013 30/09/2014 29/08/2013 14/05/2015