



- (51) **International Patent Classification:**
H04W 16/18 (2009.01) *H04W 88/08* (2009.01)
- (21) **International Application Number:**
PCT/CN2016/071159
- (22) **International Filing Date:**
18 January 2016 (18.01.2016)
- (25) **Filing Language:** English
- (26) **Publication Language:** English
- (30) **Priority Data:**
201510022841.7 16 January 2015 (16.01.2015) CN
- (71) **Applicant:** **HANGZHOU H3C TECHNOLOGIES CO., LTD.** [CN/CN]; 466 Changhe Road, Binjiang District, Hangzhou, Zhejiang 310052 (CN).
- (72) **Inventors:** **FU, Jiajia**; Room 730, Oriental Electronic BLD., NO.2, Chuangye Road, Shangdi Information Industry Base, Haidian District, Beijing 100085 (CN). **Ji, Zhe**; Room 730, Oriental Electronic BLD., NO.2, Chuangye Road, Shangdi Information Industry Base, Haidian District, Beijing 100085 (CN).
- (74) **Agent:** **DEQI INTELLECTUAL PROPERTY LAW CORPORATION**; 7/F, Xueyuan International Tower, NO.1 Zhichun Road, Haidian District, Beijing 100083 (CN).

- (81) **Designated States** (*unless otherwise indicated, for every kind of national protection available*): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, 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).

Published:

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

(54) **Title:** ACCESS POINT MANAGEMENT

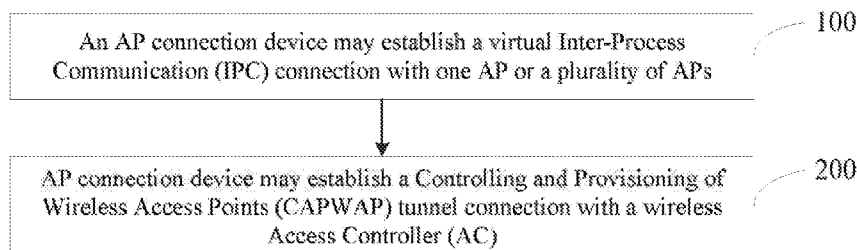


FIG. 2A

(57) **Abstract:** An Access Point (AP) connection device establishes a virtual Inter-Process Communication (IPC) connection with each of a plurality of APs. The AP connection device establishes a Controlling and Provisioning of Wireless Access Points (CAPWAP) tunnel connection with a wireless Access Controller (AC).

ACCESS POINT MANAGEMENT

BACKGROUND

[0001] A wireless Access Point (AP) is a common device in a wireless local area network (WLAN). The AP acts as a bridge connecting a wireless network to a wired network. The AP may allow a wireless network client to connect to a wired local area network, such as an Ethernet network. A wireless Access Controller (AC) is in charge of managing APs in a WLAN. The may handle tasks such as automatic adjustment of a basic wireless network and support advanced roaming service above the network. The AP and the AC may establish a connection via a Controlling And Provisioning of Wireless Access Points (CAPWAP) tunnel, and interact with each other through CAPWAP messages. A CAPWAP message may be encapsulated in a User Datagram Protocol (UDP) packet.

BRIEF DESCRIPTION OF THE DRAWINGS

[0002] For a better understanding of the present disclosure, reference should be made to the Detailed Description below, in conjunction with the following drawings in which like reference numerals refer to corresponding parts throughout the figures.

[0003] FIG. 1 is a schematic diagram illustrating a system for managing APs according to some examples of the present disclosure.

[0004] FIG. 2A is a flow diagram illustrating a method for managing APs according to some examples of the present disclosure.

[0005] FIG. 2B is a flow diagram illustrating a method for managing APs according to some examples of the present disclosure.

[0006] FIG. 3 is a flow diagram illustrating a method for establishing CAPWAP connections by an AP connection device and an AC according to some examples of the present disclosure.

[0007] FIG. 4 is a schematic diagram illustrating a device for managing APs according to some examples of the present disclosure.

[0008] FIG. 5 is a schematic diagram illustrating an AC connection module in the device for managing APs according to some examples of the present disclosure.

[0009] FIG. 6 is a schematic diagram illustrating an AP connection device according to some examples of the present disclosure.

DETAILED DESCRIPTION

[0010] In a typical WLAN system comprising an Access Controller (AC) controlling a plurality of Access Points (AP), certain local services may be performed by the APs. For example, the local services may include scanning scheduler, neighbor report connector, and so on. Performing these services places certain processing demands on the APs, so relatively expensive high performance APs may be used. As a wireless device, each AP covers a limited area and for large WLANs a large number of APs may be deployed. If all of the APs are high performance APs this can be relatively expensive.

[0011] In order to reduce costs, one approach is to have a hierarchical system with multiple ACs. A plurality of APs may connect to a first AC via respective CAPWAP tunnels and the first AC may connect to a second AC via a CAPWAP tunnel. In this arrangement the local service may be centrally processed by the first AC without being separately processed by each AP. This makes it possible to use lower performance APs, thus avoiding deployment of a large number of expensive high performance APs. However, in this approach the first AC still communicates with the APs through CAPWAP messages and the APs terminate the CAPWAP tunnel. After obtaining a CAPWAP message, the first AC parses the CAPWAP message to obtain a payload. So there is still a certain degree of performance demands on the memory and processors of the APs in order that they can handle the CAPWAP.

[0012] Furthermore, as mentioned above the CAPWAP is generally encapsulated in a User Datagram Protocol (UDP) packet. The format of a CAPWAP message may be: link header+ IP header+ UDP header+ CAPWAP header+ message element header+ payload. After receiving a CAPWAP message, both the AC and the AP may parse the CAPWAP message to obtain the payload in the CAPWAP message. The combination of CAPWAP and UDP may consume significant network bandwidth and in some cases may make it difficult to provide real time processing of local service and other functions.

[0013] In view of this, in an example of the present disclosure, an AP connection device is provided between the AC and the APs, and a virtual Inter-Process Communication (IPC)

connections are established between the AP connection device and the APs. The AC may connect to the AP connection device via a CAPWAP tunnel. In this way the CAPWAP tunnel terminates at the AP connection device. This may reduce the processing load on the APs and may reduce the consumption of network bandwidth in AC to AP communications.

[0014] A virtual IPC connection is a layer 2 virtual connection. The packet format supported by the IPC connection may be a packet comprising a layer 2 private protocol header and a payload. As such packets sent over an IPC connection may be at layer 2, rather than layer 3 which is used for a UDP encapsulated CAPWAP connection. Further, the structure of the IPC packets may be much simpler than a CAPWAP packet, for example the IPC packet may consist of just a layer 2 private protocol header and a payload. Thus the IPC connection may consume significantly less bandwidth and use less processing power than CAPWAP connections.

[0015] Reference will now be made in detail to examples, which are illustrated in the accompanying drawings. In the following detailed description, numerous specific details are set forth in order to provide a thorough understanding of the present disclosure. Also, the figures are illustrations of an example, in which modules or procedures shown in the figures are not necessarily essential for implementing the present disclosure. In other instances, well-known methods, procedures, components, and circuits have not been described in detail so as not to unnecessarily obscure aspects of the examples.

[0016] FIG. 1 is a schematic diagram illustrating a system for managing APs according to an example of the present disclosure. As shown in FIG.1, the system includes an AC, a plurality of APs and an AP connection device which is respectively connected with the AC and the APs. The AP connection device is a device that is to connect with the AC via a CAPWAP tunnel and connect with the APs via a plurality of virtual IPC connections.

[0017] The AC may access the public network, such as the Internet, and the AP connection device and the APs may form a local network, such as a LAN network.

[0018] The AC is to perform various functions, including for example any of the following: aggregating data from different APs and accessing the Internet, accomplishing the

configuration management of APs, the authentication and management of wireless user, broadband access, safety control, and the like.

[0019] The AP connection device is configured to establish a virtual IPC connection with an AP, and establish a CAPWAP tunnel connection with the AC; receive an IPC packet sent by a AP, forward the IPC packet in the local network or translate the IPC packet into a CAPWAP packet and send the CAPWAP packet to the AC; receive a CAPWAP packet sent by the AC, translate the CAPWAP packet into an IPC packet, and send the IPC packet to a corresponding AP.

[0020] In an example, the AP connection device may establish one CAPWAP tunnel connection with the AC, or establish multiple CAPWAP tunnel connections with the AC.

[0021] When establishing multiple CAPWAP tunnel connections with the AC, the AP connection device may establish one CAPWAP tunnel connection corresponding to the AP connection device itself between the AP connection device and the AC, and a CAPWAP tunnel connection corresponding to each AP between the AP connection device and the AC; or the AP connection device may establish a CAPWAP tunnel connection corresponding to each AP between the AP connection device and the AC, and not establish the CAPWAP tunnel connection corresponding to the AP connection device itself between the AP connection device and the AC.

[0022] In an example, the CAPWAP tunnel connection corresponding to the AP connection device itself between the AP connection device and the AC may be established according to a serial number or a MAC address of the AP connection device sent by the AP connection device. The CAPWAP tunnel connection corresponding to each AP between the AP connection device and the AC may be established according to a serial number or a MAC address of the corresponding AP sent by the AP connection device. In an example, the serial number may be a machine code or an identification number of the device, namely, the serial number is a unique identification of the device, and different devices have different serial numbers.

[0023] Because the serial number and the MAC address of each AP are packaged in the CAPWAP tunnel, and a unique source IP address+ a source port is used to identify a

corresponding AP at the outer layer of the CAPWAP tunnel, the same AP connection device may establish multiple CAPWAP tunnels. The source IP address is the same one, but the source ports are different, therefore there is no conflict between different CAPWAP tunnels.

[0024] In FIG.1, the solid lines depict the physical connections between the AC and the AP connection device, and the physical connections between the AP connection device and the APs; the dashed lines depict the virtual connections between the AC and the AP connection device, namely the CAPWAP tunnel connections, and the virtual connections between the AP connection device and the APs, namely the virtual IPC connections.

[0025] Each AP is configured to send an IPC packet to the AP connection device, and receive an IPC packet forwarded by the AP connection device.

[0026] In an example, the AC is further configured to send a latest version file to the AP connection device when determining that version information reported by the AP connection device is lower than the version information stored by the AC, namely, the version of the version file stored by the AP connection device is lower than the version of the version file stored by the AC. Correspondingly, the AP connection device is further configured to report version information of the AP connection device, receive the latest version file sent by the AC, and perform version update; send the latest version file to each AP to enable the AP to perform version update.

[0027] FIG. 2A and FIG. 2B are respectively a flow diagram illustrating a method for managing APs according to an example of the present disclosure. The method may be applied to the system for managing APs shown in FIG.1.

[0028] As shown in FIG.2A, the method may include the following processes.

[0029] An AP connection device may establish a virtual Inter-Process Communication (IPC) connection with one AP or a plurality of APs.

[0030] AP connection device may establish a Controlling and Provisioning of Wireless Access Points (CAPWAP) tunnel connection with a wireless Access Controller (AC).

[0031] As shown in FIG.2B, the method may include the following processes.

[0032] At block 101, the AP connection device is started, and the plurality of APs connected with the AP connection device are powered on.

[0033] In an example, when the AP connection device is started, the AP connection device may record locally stored configuration information including AC address first. For instance, the AP connection device may record locally stored configuration information including AC address into global information. The global information is relative to different AP information. Recording the configuration information including AC address into global information is for subsequent APs to connect the AC. In other words, each of subsequent APs may use the configuration information recorded in global information to establish a connection with the AC.

[0034] At block 102, when the APs are powered on, the AP connection device may establish a virtual IPC connection with each AP.

[0035] After a virtual IPC connection between the AP connection device and an AP is established, the AP connection device may receive a connection complete notification came from the AP.

[0036] In an example, the APs may be powered by the AP connection device. For example, after the AP connection device is started, the APs access the AP connection device and are started. In another example, the APs may be powered by a separate power supply system.

[0037] In an example, the process of establishing a virtual IPC connection between the AP connection device and an AP may include: the AP connection device sends a version file of the AP connection device to the AP to enable the AP to load the version file, and after the AP loads the version file, the AP connection device establishes the virtual IPC connection with the AP.

[0038] The version file of the AP connection device includes a version file of every AP. That is to say, at block 102, the AP connection device may obtain a version file corresponding to the AP from the version file of the AP connection device according to the type number of the AP, and download the obtained version file to the corresponding AP.

[0039] The type numbers of the APs may be different, or be the same, which will not be limited in the present disclosure.

[0040] By establishing the virtual IPC connections, services of APs may be centrally processed by the AP connection device, and be taken effect on the APs via the virtual IPC connections. It is not necessary for each AP to separately process the local service.

[0041] The virtual IPC connections are layer 2 virtual connections. The packet format supported by the IPC may be: layer 2 private protocol header+ payload. Namely, the payload may be packaged with a short packet header. Compared to the packet header of a CAPWAP message link header+ IP header+ UDP header+ CAPWAP header+ message element header, the virtual IPC connection may save the network bandwidth and CPU consumption of parsing and packaging. In addition, for the AP connection device, layer 2 virtual IPC connections can guarantee that the AP connection device possesses the function of setting APs similar as setting a local chip. On the basis of satisfying the functions of the AP connection device, the performance of the AP connection device may be guaranteed.

[0042] At block 103, the AP connection device may establish a CAPWAP tunnel connection with the AC. Thus, the CAPWAP tunnel between the APs and the AC may be terminated on the AP connection device.

[0043] In an example, the AP connection device may establish one CAPWAP tunnel with the AC, or establish parallel multiple CAPWAP tunnels with the AC. There is no difference between the depths of the packet parsing (link header, IP header, UDP header, CAPWAP header) whenever it is one CAPWAP tunnel or multiple CAPWAP tunnels. If only one CAPWAP tunnel is established, it is necessary to further distinguish information of different APs in the tunnel. If parallel multiple CAPWAP tunnels are established, due to the processing of one AP is not affected by the processing time of other APs, the processing efficiency of the whole system may be further increased.

[0044] FIG. 3 is a flow diagram illustrating a method for establishing CAPWAP connections by the AP connection device and the AC according to an example of the present disclosure. As shown in FIG.3, the method may include the following processes.

[0045] At block 1030, the AP connection device may send a first CAPWAP message to the AC, and establish a first CAPWAP tunnel connection with the AC.

[0046] There are the following two methods for establishing the first CAPWAP connection through the AP connection device.

[0047] The first method: the AP connection device may send the AC a first CAPWAP message carrying a serial number and a MAC address of the AP connection device. According to the first CAPWAP message, a CAPWAP tunnel connection corresponding the AP connection device itself is established between the AP connection device and the AC.

[0048] The second method: A CAPWAP tunnel connection corresponding to a first AP connected with the AP connection device rather than a CAPWAP tunnel connection corresponding the AP connection device itself is established between the AP connection device and the AC. Namely, it is not necessary for the AP connection device to establish a CAPWAP tunnel connection corresponding to the AP connection device itself between the AP connection device and the AC.

[0049] The AP connection device may send the AC a first CAPWAP message carrying a serial number and a MAC address of the first AP connected with the AP connection device. According to the first CAPWAP message, a CAPWAP tunnel connection corresponding to the first AP connected with the AP connection device is established between the AP connection device and the AC.

[0050] In an example, in above mentioned method for establishing the first CAPWAP connection, the AC may perform processing according to a normal AP access process without perceiving the existence of the AP connection device.

[0051] At block 1031, the AP connection device may report version information to the AC via the first CAPWAP tunnel connection, and trigger the AC to determine whether the version information reported by the AP connection device is not lower than the version information stored by the AC, when the version information reported by the AP connection device is not lower than the version information stored by the AC, namely, when the version of the version file stored by the AP connection device is not lower than the version of the version file stored by the AC, block 1034 is performed; otherwise, block 1032 is performed.

[0052] In an example, the AC may perform unified management on a version number and a type number of the AP connection device and a version number and a type number of each AP. The version file stored by the AC corresponds to the version file of the AP connection device, and has a latest version. The version file stored by the AC includes a version file of every AP. The version file of each AP may be obtained from the version file of the AP connection device.

[0053] The version information reported by the AP connection device includes: a type number and a version number of the AP connection device itself.

[0054] In an example, the AC stores a configuration file corresponding to each serial number or MAC address. In an example, when determining that the version information reported by the AP connection device is not lower than the version information stored by the AC, the AC may search for a configuration file matching the serial number or MAC address carried in the first CAPWAP message, and send a configuration file found out to the AP connection device.

[0055] The configuration file may include parameters with which an AP may associate with the AC, such as parameters with which the AP may provide wireless connection including Service Set Identifier (SSID) wireless service. The parameters may include timer configuration, a retransmission number, and so on. In another example, the AC may not send the configuration file, and the AP may use default values.

[0056] There may be two methods for sending the configuration file. The first method: based on each CAPWAP message, the AC sends a configuration file corresponding to a serial number or MAC address carried in the CAPWAP message. The second method: based on the first CAPWAP message carrying the serial number or MAC address of the AP connection device itself, the AC may send configuration files each of which corresponding to a serial number or MAC address of one of all APs connected with the AP connection device to the AP connection device, and then the AP connection device may in turn send each configuration file to the corresponding AP.

[0057] At block 1032, the AP connection device may receive the latest version file sent by the AC, and perform version update, after the version update is accomplished, block 1033 is performed.

[0058] In an example, when the version file is updated, the AP connection device will be restarted. When the APs are powered by the AP connection device, the APs will be restarted while the AP connection device is restarted. Therefore, when the AP connection device is restarted, it is not necessary for the AP connection device to notify the APs of being restarted.

[0059] At block 1033, the AP connection device may send the latest version file to each AP, to enable each AP to perform version update, and after the version update is accomplished, block 1034 is performed.

[0060] The AP connection device may obtain a version file corresponding to an AP from the latest version file according to a type number of the AP, and send the obtained version file to the corresponding AP.

[0061] At block 1034, for each AP, the AP connection device may respectively send a second CAPWAP message to establish a CAPWAP tunnel connection corresponding to the AP between the AP connection device and the AC. Each second CAPWAP message carries a serial number and a MAC address of an AP.

[0062] As for how a CAPWAP tunnel connection is established according to the serial number or a MAC address of the AP, those skilled in the art may obtain according to existing methods, no further descriptions will be given here.

[0063] In an example, corresponding to the first method for sending the configuration file, at block 1034, the AC may send a configuration file corresponding to the serial number or MAC address of the AP carried in the second CAPWAP message to the AP connection device, and the AP connection device may send the configuration file to corresponding AP.

[0064] If the total number of APs is N, when adopting the first method for establishing the first CAPWAP tunnel connection, after block 1034 is performed, N+1 CAPWAP tunnel connections will be established, that is to say, N CAPWAP tunnel connections each of which corresponds to one of APs connected with the AP connection device are established, and one CAPWAP tunnel connection corresponding to the AP connection device is established. when adopting the second method for establishing the first CAPWAP tunnel connection, after block 1034 is performed, N CAPWAP tunnel connections will be established, that is to say, N CAPWAP tunnel connections each of which corresponds to one of APs connected with the

AP connection device are established, and no CAPWAP tunnel connection corresponding to the AP connection device is established.

[0065] At block 104, the AP connection device may receive an IPC packet sent by an AP, and forward the IPC packet in local network, or translate the IPC packet into a CAPWAP packet and send the CAPWAP packet to the AC; receive a CAPWAP packet sent by the AC, and translate the CAPWAP packet into an IPC packet, and send the IPC packet to a corresponding AP.

[0066] In an example, receiving an IPC packet sent by an AP, and forwarding the IPC packet in local network, or translating the IPC packet into a CAPWAP packet and sending the CAPWAP packet to the AC, may include: the AP connection device receives an IPC packet sent by an AP, parses the IPC packet and obtains a data packet, according to content of a specified field in the data packet, determines the destination receiver of the IPC packet, if the destination receiver is a local AP, forwards the data packet to the destination AP; if the destination receiver is the AC, packages the data packet into a CAPWAP packet, and sends the CAPWAP packet to the AC; if the destination receiver is a local wired connecting party, forwards the data packet to a corresponding destination port.

[0067] In an example, the content of the specified field in the data packet may be a type of the data packet, an address of the data packet, a VLAN identification of the data packet, and the like.

[0068] In an example, the AP connection device may establish an Access Control List (ACL) according to the configuration file sent by the AC, and determines the destination receiver of the IPC packet according to a set condition in the ACL.

[0069] In an example, receiving a CAPWAP packet sent by the AC, and translating the CAPWAP packet into an IPC packet, and sending the IPC packet to a corresponding AP, may include: the AP connection device receives the CAPWAP packet sent by the AC, parses the CAPWAP packet and obtains the payload, namely a data packet, repackages the data packet into an IPC packet, and sends the IPC packet to the AP.

[0070] Examples of the present disclosure also provide a device for managing APs, and the device may execute the method for managing APs shown in FIG.2. Some details undisclosed in the device examples may refer to the descriptions in the method examples.

[0071] FIG. 4 is a schematic diagram illustrating a device for managing APs according to some examples of the present disclosure. The device for managing APs may be applied to the AP connection device in the system for managing APs shown in FIG.1. As shown in FIG.4, the device may include a starting module 201, an AP connecting module 202, an AC connecting module 203 and a packet sending module 204.

[0072] The starting module 201 is configured to, after the AP connection device is started, notify a plurality of APs connected with the AP connection device of being powered on.

[0073] In an example, when the AP connection device is started, the AP connection device may record locally stored configuration information including AC address first. For instance, the AP connection device may record locally stored configuration information including AC address into global information.

[0074] The AP connecting module 202 is configured to, when the APs are powered on, establish a virtual IPC connection with each of a plurality of APs. After the virtual IPC connection is established, the AP connecting module 202 may indicate the AC connecting module 203 to perform operations, namely, indicate the AC connecting module 203 to establish a CAPWAP tunnel connection with the AC. In an example, after the virtual IPC connection is established, the AP connecting module 202 may receive a connection complete notification sent by the AP, and then the AP connecting module 202 may indicate the AC connecting module 203 to perform operations.

[0075] In an example, the APs may be powered by the AP connection device. For example, after the AP connection device is started, the APs access the AP connection device and are started. In another example, the APs may be powered by a separate power supply system.

[0076] In an example, the AP connecting module 202 may send a version file of the AP connection device to the AP to enable the AP to load the version file, and after the AP loads the version file, establish the virtual IPC connection with the AP.

[0077] By establishing the virtual IPC connections, services of APs may be centrally processed by the AP connection device, and be taken effect on the APs via the virtual IPC connections. It is not necessary for each AP to separately process the local service.

[0078] The virtual IPC connections are layer 2 virtual connections. The packet format supported by the IPC may be: layer 2 private protocol header+ payload. Namely, the payload may be packaged with a short packet header. Compared to the packet header of a CAPWAP message link header+ IP header+ UDP header+ CAPWAP header+ message element header, the virtual IPC connection may save the network bandwidth and CPU consumption of parsing and packaging. In addition, for the AP connection device, layer 2 virtual IPC connections can guarantee that the AP connection device possesses the function of setting APs similar as setting a local chip. On the basis of satisfying the functions of the AP connection device, the performance of the AP connection device may be guaranteed.

[0079] The AC connecting module 203 is configured to establish a CAPWAP tunnel connection with the AC. Thus, the CAPWAP tunnel between the APs and the AC may be terminated on the AP connection device.

[0080] In an example, the AP connecting module 203 may establish one CAPWAP tunnel with the AC, or establish parallel multiple CAPWAP tunnels with the AC. There is no difference between the depths of the packet parsing (link header, IP header, UDP header, CAPWAP header) whenever it is one CAPWAP tunnel or multiple CAPWAP tunnels. If only one CAPWAP tunnel is established, it is necessary to further distinguish information of different APs in the tunnel. If parallel multiple CAPWAP tunnels are established, due to the processing of one AP is not affected by the processing time of other APs, the processing efficiency of the whole system may be further increased.

[0081] In the example, it is taken as an example that parallel multiple CAPWAP tunnels are established. If the total number of APs is N, in an example, N+1 CAPWAP tunnel connections will be established, that is to say, N CAPWAP tunnel connections each of which corresponds to one of APs connected with the AP connection device are established, and one CAPWAP tunnel connection corresponding to the AP connection device is established. In another example, N CAPWAP tunnel connections will be established, that is to say, N CAPWAP tunnel connections each of which corresponds to one of APs connected with the

AP connection device are established, and no CAPWAP tunnel connection corresponding to the AP connection device is established.

[0082] The AC connecting module 203 may have multiple implementation structures. FIG. 5 is a schematic diagram illustrating an AC connection module in the device for managing APs according to some examples of the present disclosure. As shown in FIG.5, the AC connecting module may include a first tunnel establishing module 2031, a version information reporting module 2032, a version updating module 2033, a version file sending module 2034 and a second tunnel establishing module 2035.

[0083] The first tunnel establishing module 2031 is configured to send a first CAPWAP message to the AC, and establish a first CAPWAP tunnel connection with the AC.

[0084] There are the following two methods for establishing the first CAPWAP connection through the first tunnel establishing module 2031.

[0085] The first tunnel establishing module 2031 may send the AC a first CAPWAP message carrying a serial number and a MAC address of the AP connection device. According to the first CAPWAP message, a CAPWAP tunnel connection corresponding to the AP connection device itself is established between the AP connection device and the AC.

[0086] The second method: A CAPWAP tunnel connection corresponding to a first AP connected with the AP connection device rather than a CAPWAP tunnel connection corresponding to the AP connection device itself is established. Namely, it is not necessary for the AP connection device to establish a CAPWAP tunnel connection corresponding to the AP connection device itself between the AP connection device and the AC.

[0087] The first tunnel establishing module 2031 may send the AC a first CAPWAP message carrying a serial number and a MAC address of the first AP connected with the AP connection device. According to the first CAPWAP message, a CAPWAP tunnel connection corresponding to the first AP connected with the AP connection device is established between the AP connection device and the AC.

[0088] The version information reporting module 2032 is configured to report version information to the AC, and trigger the AC to determine whether the version information

reported by the version information reporting module is not lower than the version information stored by the AC, when the version information reported by the version information reporting module is not lower than the version information stored by the AC, namely, when the version of the version file stored by the AP connection device is not lower than the version of the version file stored by the AC, indicate the second tunnel establishing module 2035 to perform operations, namely, indicate the second tunnel establishing module 2035 to respectively establish a CAPWAP tunnel connection corresponding to each of APs between the device and the AC; otherwise, indicate the version updating module 2033 to perform operations, namely, indicate the version updating module 2033 to perform version update according to the latest version file sent by the AC.

[0089] The version information reported by the version information reporting module 2032 includes: a type number and a version number of the AP connection device itself.

[0090] The version updating module 2033 is configured to receive the latest version file sent by the AC, and perform version update, after the version update is accomplished, indicate the version file sending module 2034 to perform operations, namely, indicate the version file sending module 2034 to send the latest version file to each AP.

[0091] In an example, when the version updating module 2033 performs the version update, the AP connection device will be restarted. When the APs are powered by the AP connection device, the APs will be restarted while the AP connection device is restarted. Therefore, when the AP connection device is restarted, it is not necessary for the AP connection device to notify the APs of being restarted.

[0092] The version file sending module 2034 is configured to send the latest version file received by the version updating module 2033 to each AP to enable each AP to perform version update, and after the version update is accomplished, indicate the second tunnel establishing module 2035 to perform operations, namely, indicate the second tunnel establishing module 2035 to, for each AP, send a second CAPWAP message to the AC to establish a CAPWAP tunnel connection between the AP and the AC.

[0093] The second tunnel establishing module 2035 is configured to, for each AP, send a second CAPWAP message to the AC to establish a CAPWAP tunnel connection corresponding to the AP between the AP connection device and the AC.

[0094] Each second CAPWAP message carries a serial number and a MAC address of the AP.

[0095] As for how a CAPWAP tunnel connection is established according to the serial number or a MAC address of the AP, those skilled in the art may obtain according to existing methods, no further descriptions will be given here.

[0096] In an example, the AC stores a configuration file corresponding to each serial number or MAC address. In an example, when determining that the version information reported by the AP connection device is not lower than the version information stored by the AC, the AC may search for a configuration file matching the serial number or the MAC address according to the serial number or the MAC address carried in the CAPWAP message, and send a configuration file found out to the AP connection device.

[0097] There may be two methods for sending the configuration file. The first method: based on each CAPWAP message, the AC sends a configuration file corresponding to a serial number or MAC address carried in the CAPWAP message. The second method: based on the first CAPWAP message carrying the serial number or MAC address of the AP connection device itself, the AC may send configuration files each of which corresponding to a serial number or MAC address of one of all APs connected with the AP connection device to the AP connection device, and then the AP connection device may in turn send each configuration file to the corresponding AP.

[0098] The packet sending module 204 is configured to receive an IPC packet sent by an AP, and forward the IPC packet in local network, or translate the IPC packet into a CAPWAP packet and send the CAPWAP packet to the AC; receive a CAPWAP packet sent by the AC, and translate the CAPWAP packet into an IPC packet, and send the IPC packet to a corresponding AP.

[0099] In an example, the packet sending module 204 may receive the IPC packet sent by an AP, parse the IPC packet and obtain a data packet, according to content of a specified field in

the data packet, determine the destination receiver of the IPC packet, if the destination receiver is a local AP, forward the data packet to the destination AP; if the destination receiver is the AC, package the data packet into a CAPWAP packet, and send the CAPWAP packet to the AC; if the destination receiver is a local wired connecting party, forward the data packet to a corresponding destination port.

[00100] The IPC packet includes: layer 2 private protocol header+ payload. The CAPWAP packet includes: link header+ IP header+ UDP header+ CAPWAP header+ message element header+ payload.

[00101] In an example, the packet sending module 204 may receive the CAPWAP packet sent by the AC, parse the CAPWAP packet and obtain the payload, namely a data packet, repackages the data packet into an IPC packet, and send the IPC packet to the AP

[00102] FIG. 6 is a schematic diagram illustrating an AP connection device according to some examples of the present disclosure. As shown in FIG.6, the AP connection device may include: a processor 61, a non-transitory machine readable storage medium 62, and program modules stored in the non-transitory machine readable storage medium 62 and executable by the processor 61. The program models may include: a starting module 621, an AP connecting module 622, an AC connecting module 623, and a packet sending module 624.

[00103] The functions of each of above mentioned modules may be the same as that described in FIG.4, and no further descriptions will be given here.

[00104] In the method, device and system for managing APs provided by examples of the present disclosure, an AP connection device is configured between the AC and the APs, and a virtual Inter-Process Communication (IPC) connection is established between the AP connection device and the APs for replacing the CAPWAP tunnel connection. Thus the CAPWAP tunnels between the AC and the APs are terminated at the AP connection device, and the communication consumption between services may be reduced.

[00105] In addition, due to the CAPWAP tunnel connection between the APs and the first AC is cancelled, the processing of the APs is simplified, and the requirement for AP performance and memory is reduced. That is to say, in an actual application, APs with low-

end model may satisfy the user requirement, thus the deployment costs of the whole network may be reduced.

[00106] The foregoing description, for purpose of explanation, has been described with reference to specific examples. However, the illustrative discussions above are not intended to be exhaustive or to limit the present disclosure to the precise forms disclosed. Many modifications and variations are possible in view of the above teachings. The examples were chosen and described in order to best explain the principles of the present disclosure and its practical applications, to thereby enable others skilled in the art to best utilize the present disclosure and various examples with various modifications as are suited to the particular use contemplated.

[00107] The above examples may be implemented by hardware, software, firmware, or a combination thereof. For example the various methods, processes and functional modules described herein may be implemented by a processor (the term processor is to be interpreted broadly to include a CPU, processing unit/module, ASIC, logic module, or programmable gate array, etc.). The processes, methods and functional modules may all be performed by a single processor or split between several processors; reference in this disclosure or the claims to a 'processor' should thus be interpreted to mean 'one or more processors'. The processes, methods and functional modules are implemented as machine readable instructions executable by one or more processors, hardware logic circuitry of the one or more processors or a combination thereof. The modules, if mentioned in the aforesaid examples, may be combined into one module or further divided into a plurality of sub-modules. Further, the examples disclosed herein may be implemented in the form of a software product. The computer software product is stored in a non-transitory storage medium and comprises a plurality of instructions for making an electronic device implement the method recited in the examples of the present disclosure.

CLAIMS

WHAT IS CLAIMED IS:

1. A method for managing wireless Access Point (AP)s, comprising:
establishing, by an AP connection device, a virtual Inter-Process Communication (IPC) connection with an AP; and
establishing, by the AP connection device, a Controlling and Provisioning of Wireless Access Points (CAPWAP) tunnel connection with a wireless Access Controller (AC).
2. The method according to claim 1, there are a plurality of APs, wherein establishing, by the AP connection device, a CAPWAP tunnel connection with the AC, comprises:
establishing, by the AP connection device, one CAPWAP tunnel connection with the AC, or
establishing, by the AP connection device, multiple CAPWAP tunnel connections with the AC.
3. The method according to claim 2, wherein establishing, by the AP connection device, multiple CAPWAP tunnel connections with the AC, comprises:
establishing, by the AP connection device, one CAPWAP tunnel connection corresponding to the AP connection device itself between the AP connection device and the AC, and a CAPWAP tunnel connection corresponding to each of the plurality of APs between the AP connection device and the AC; or
establishing, by the AP connection device, a CAPWAP tunnel connection corresponding to each of the plurality of APs between the AP connection device and the AC.
4. The method according to claim 2, wherein establishing, by the AP connection device, a CAPWAP tunnel connection with the AC, further comprises:
after determining that version information of the AP connection device is lower than version information stored by the AC, receiving, by the AP connection device, a latest version file sent by the AC, and performing version update;

sending, by the AP connection device, the latest version file to each of the plurality of APs to enable each of the plurality of APs to perform version update.

5. The method according to claim 2, wherein, the AP connection device and the AP form a local network; after establishing, by the AP connection device, a CAPWAP tunnel connection with the AC, further comprising:

receiving, by the AP connection device, an IPC packet sent by an AP, forwarding the IPC packet in the local network or translating the IPC packet into a CAPWAP packet and sending the CAPWAP packet to the AC;

receiving, by the AP connection device, a CAPWAP packet sent by the AC, translating the CAPWAP packet into an IPC packet, and sending the IPC packet to a corresponding AP.

6. The method according to claim 5, wherein receiving, by the AP connection device, an IPC packet sent by an AP, forwarding the IPC packet in the local network or translating the IPC packet into a CAPWAP packet and sending the CAPWAP packet to the AC, comprises:

receiving, by the AP connection device, the IPC packet sent by an AP, parsing the IPC packet and obtaining a data packet, according to content of a specified field in the data packet, determining the destination receiver of the IPC packet, if the destination receiver is a local AP, forwarding the data packet to the destination AP; if the destination receiver is the AC, packaging the data packet into a CAPWAP packet, and sending the CAPWAP packet to the AC; if the destination receiver is a local wired connecting party, forwarding the data packet to a corresponding destination port.

7. The method according to claim 1, wherein establishing, by an AP connection device, a virtual IPC connection with the AP, comprises:

sending, by the AP connection device, a version file of the AP connection device to the AP to enable the AP to load the version file, and after the AP loads the version file, establishing, by the AP connection device, the virtual IPC connection with the AP.

8. A device for managing wireless Access Point (AP)s, comprising:
an AP connecting module to establish a virtual Inter-Process Communication (IPC) connection with an AP; and
an AC connecting module to establish a Controlling and Provisioning of Wireless Access Points (CAPWAP) tunnel connection with a wireless Access Controller (AC).
9. The device according to claim 8, wherein, the device and the AP form a local network; the device further comprises:
a packet sending module to receive an IPC packet sent by an AP, and forward the IPC packet in the local network, or translate the IPC packet into a CAPWAP packet and send the CAPWAP packet to the AC; receive a CAPWAP packet sent by the AC, and translate the CAPWAP packet into an IPC packet, and send the IPC packet to a corresponding AP.
10. The device according to claim 9, there are a plurality of APs; wherein the AC connecting module is to establish one CAPWAP tunnel connection corresponding to the device itself between the device and the AC, and a CAPWAP tunnel connection corresponding to each of the plurality of APs between the device and the AC; or
the AC connecting module is to establish a CAPWAP tunnel connection corresponding to each of the plurality of APs between the device and the AC.
11. The device according to claim 10, wherein the AC connecting module comprises:
a first tunnel establishing module to send a first CAPWAP message to the AC, and establish a CAPWAP tunnel connection between the device itself and the AC or establish a CAPWAP tunnel connection between the AC and an AP connected with the device;
a version information reporting module to report version information to the AC, and trigger the AC to determine whether the version information reported by the version information reporting module is not lower than the version information stored by the AC; and
a second tunnel establishing module to when the version information reported by the version information reporting module is not lower than the version

information stored by the AC, for each of the plurality of APs each of which has not a corresponding CAPWAP tunnel connection, send a second CAPWAP message to the AC to establish a CAPWAP tunnel connection corresponding to the AP between the device and the AC.

12. The device according to claim 11, wherein the AC connecting module further comprises:

a version updating module to receive a latest version file sent by the AC, and perform version update, after the version update is accomplished, indicate a version file sending module to perform operations; and

the version file sending module to send the latest version file received by the version updating module to each of the plurality of APs to enable each of the plurality of APs to perform version update.

13. The device according to claim 9, wherein the packet sending module is to parse the IPC packet and obtain a data packet, according to content of a specified field in the data packet, determines the destination receiver of the IPC packet, if the destination receiver is a local AP, forward the data packet to the destination AP; if the destination receiver is the AC, package the data packet into a CAPWAP packet, and send the CAPWAP packet to the AC; if the destination receiver is a local wired connecting party, forward the data packet to a corresponding destination port.

14. The device according to claim 8, wherein the AP connecting module is to send a version file of the device to each AP to enable the AP to load the version file, and after the AP loads the version file, establish the virtual IPC connection with the AP.

1/4

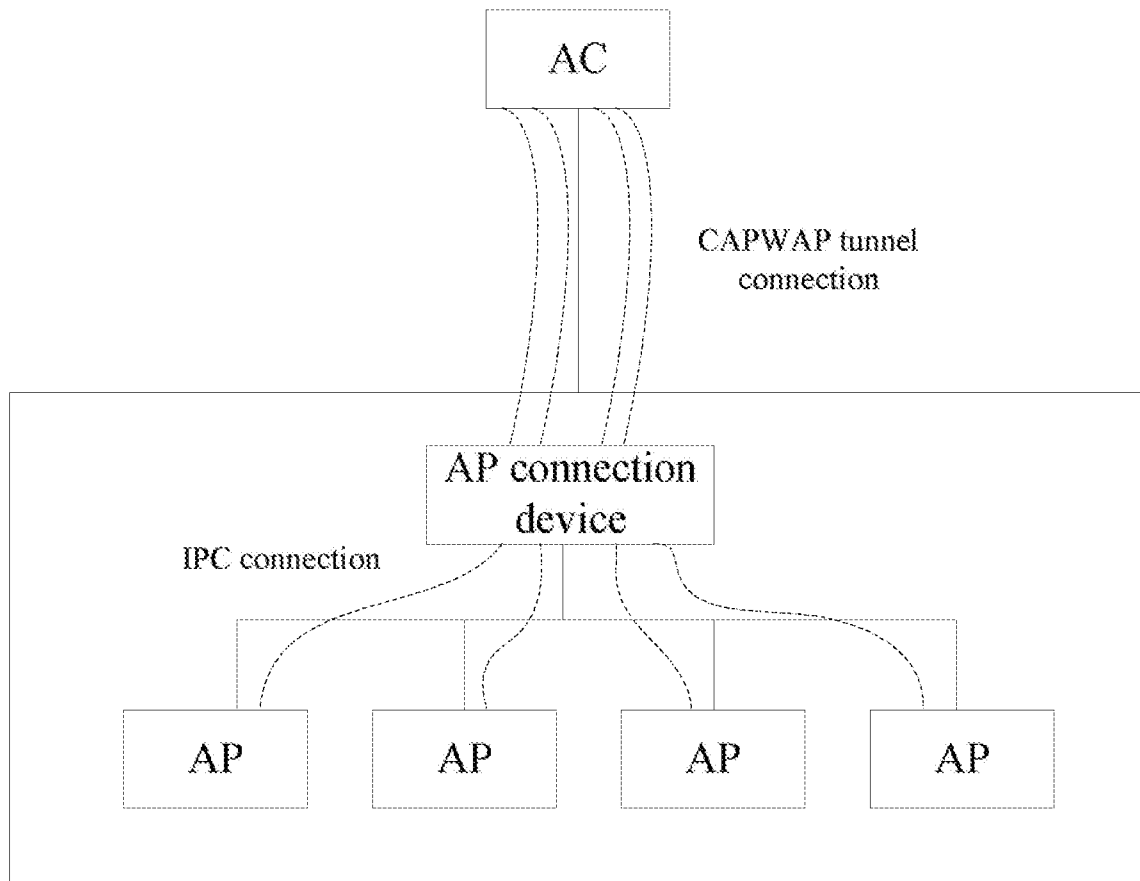


FIG. 1

2/4

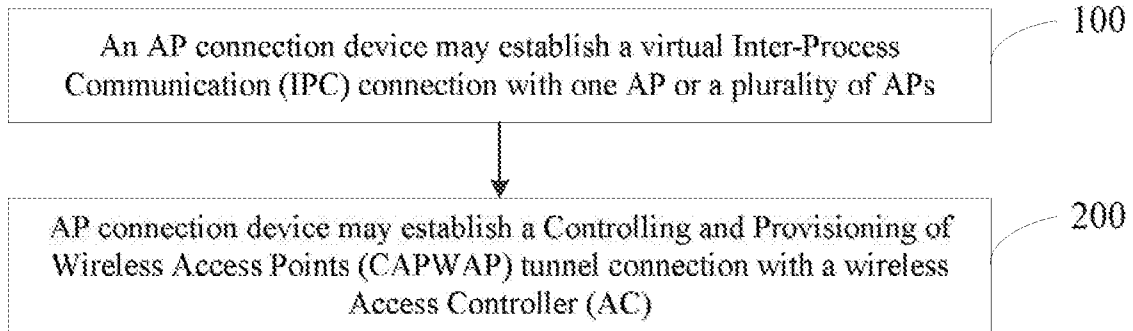


FIG. 2A

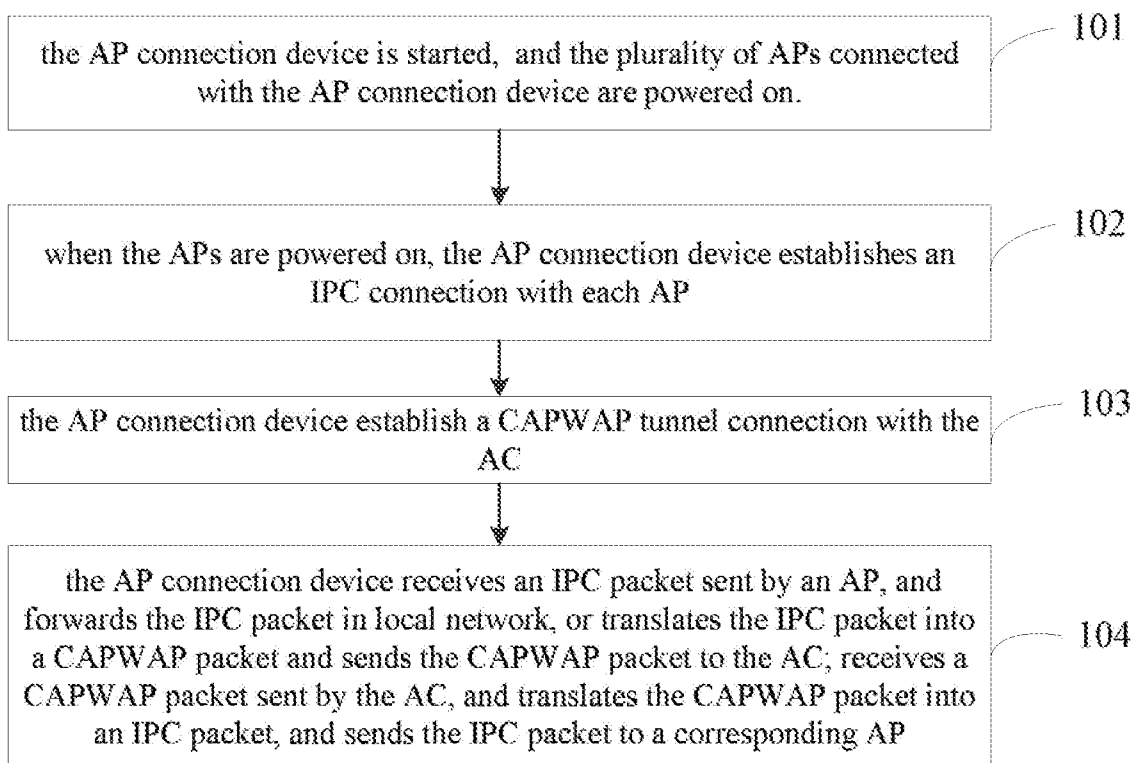


FIG. 2B

3/4

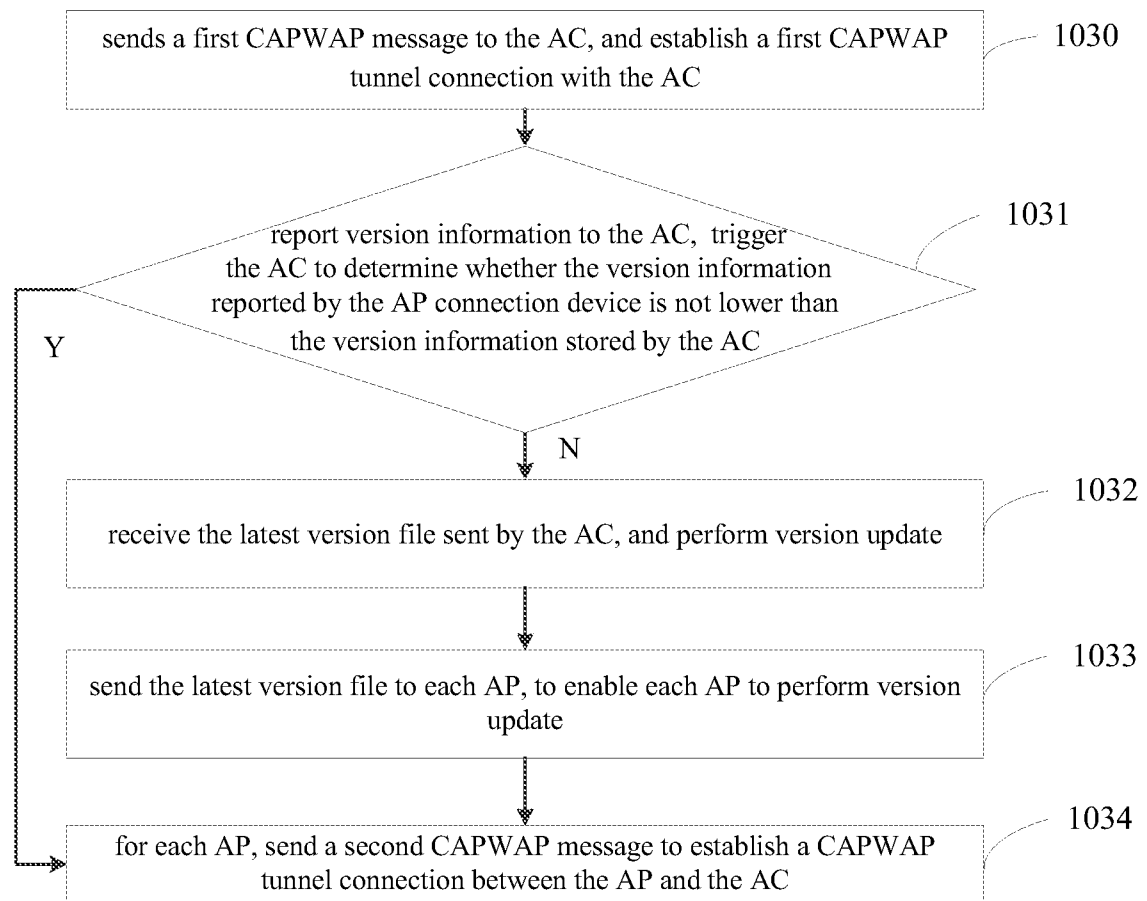


FIG. 3

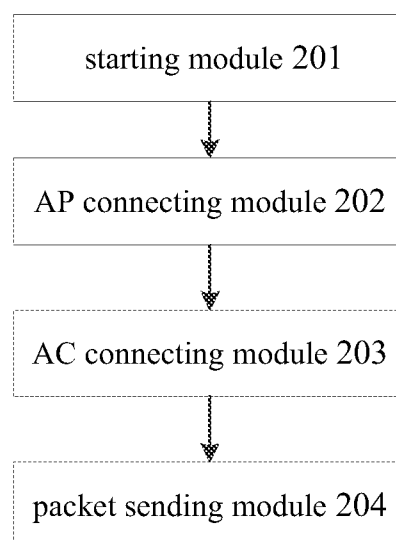


FIG. 4

4/4

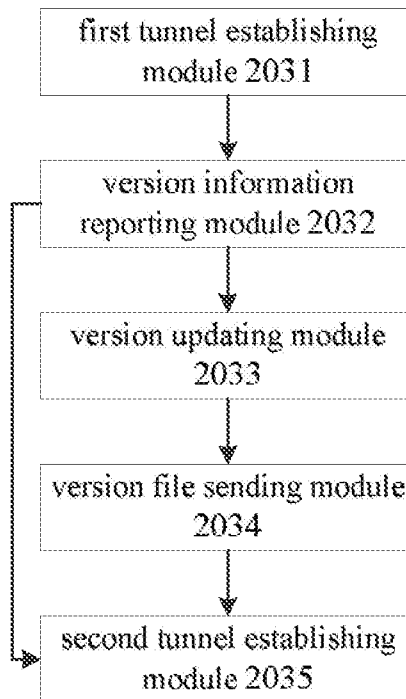


FIG. 5

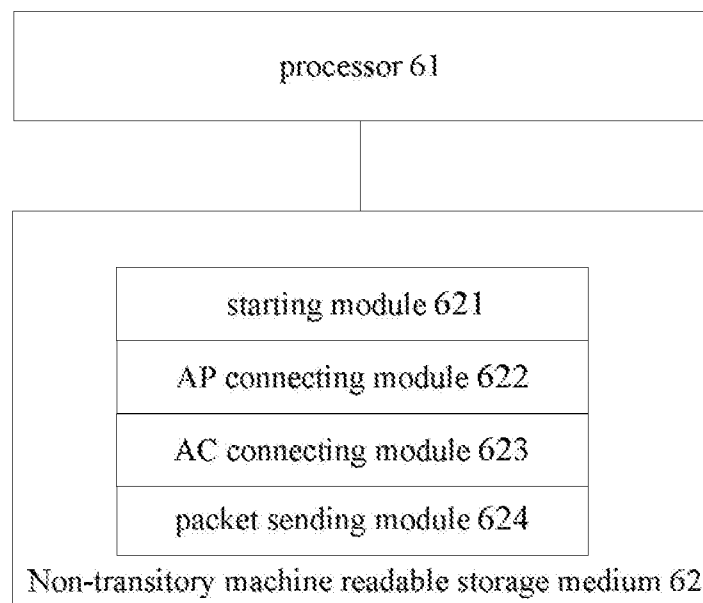


FIG. 6

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2016/071159

A. CLASSIFICATION OF SUBJECT MATTER

H04W 16/18(2009.01)i; H04W 88/08(2009.01)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)

H04W; H04Q

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)

WPI, EPODOC, CNPAT, CNKI: IPC, AC, AP, CAPWAP, inter process communication, access point?, access controller, virtual, layer 2, L2, version

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	CN 103546915 A (HANGZHOU H3C TECHNOLOGIES CO., LTD.) 29 January 2014 (2014-01-29) abstract, description, paragraphs [0058]-[0065]	1-14
A	CN 102595463 A (BEIJING AUTELAN TECHNOLOGY CO., LTD.) 18 July 2012 (2012-07-18) the whole document	1-14
A	CN 102143045 A (HUAWEI TECHNOLOGIES CO., LTD.) 03 August 2011 (2011-08-03) the whole document	1-14
A	US 2012127903 A1 (ESTEVEZ, LEONARDO WILLIAM ET AL.) 24 May 2012 (2012-05-24) the whole document	1-14



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

16 March 2016

Date of mailing of the international search report

24 March 2016

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,Puxin

Telephone No. (86-10)62413345

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.

PCT/CN2016/071159

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)			Publication date (day/month/year)
CN	103546915	A	29 January 2014	None			
CN	102595463	A	18 July 2012	None			
CN	102143045	A	03 August 2011	WO	2011140879	A1	17 November 2011
US	2012127903	A1	24 May 2012	US	2014146808	A1	29 May 2014