Office de la Propriété Intellectuelle du Canada
Un organisme d'Industrie Canada

Canadian Intellectual Property Office
An agency of Industry Canada

CA 2523915 A1 2005/04/28

(21) 2 523 915

(12) DEMANDE DE BREVET CANADIEN
CANADIAN PATENT APPLICATION

(13) A1

(86) Date de dépôt PCT/PCT Filing Date: 2004/10/20
(87) Date publication PCT/PCT Publication Date: 2005/04/28
(85) Entrée phase nationale/National Entry: 2005/10/26
(86) N° demande PCT/PCT Application No.: CN 2004/001191
(87) N° publication PCT/PCT Publication No.: 2005/039110
(30) Priorité/Priority: 2003/10/22 (200310104527.0) CN

(51) Cl.Int.^{7}/Int.Cl.^{7} H04L 12/28

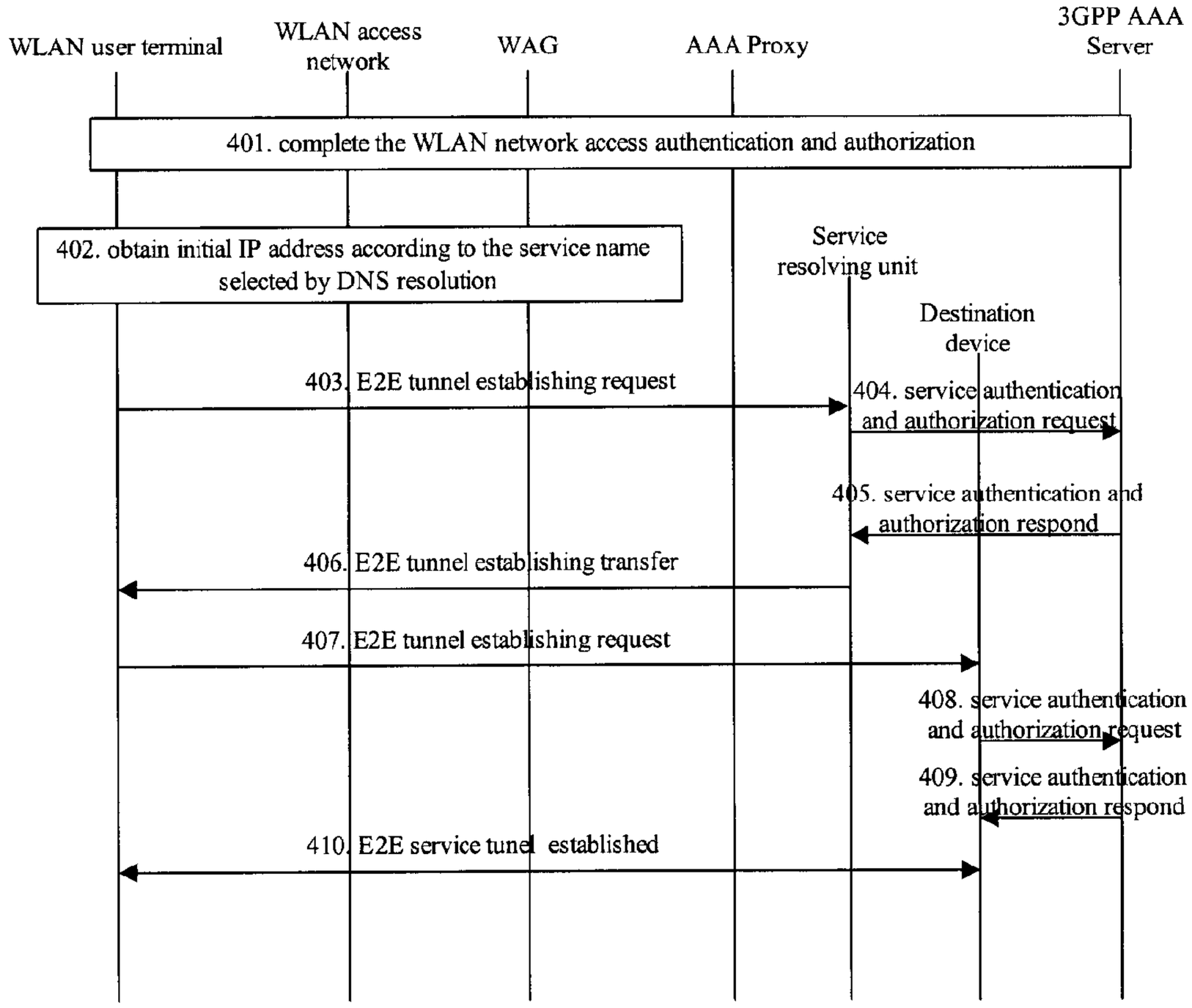
(71) Demandeur/Applicant:
HUAWEI TECHNOLOGIES CO., LTD., CN

(72) Inventeur/Inventor:
ZHANG, WENLIN, CN

(74) Agent: GOWLING LAFLEUR HENDERSON LLP

(54) Titre : METHODE POUR RESOUDRE ET ACCEDER A UN SERVICE SELECTIONNE DANS UN RESEAULOCAL SANS FILS

(54) Title: METHOD FOR RESOLVING AND ACCESSING SELECTED SERVICE IN WIRELESS LOCAL AREA NETWORK



(57) Abrégé/Abstract:
This invention discloses a method of analyzing the accessing process of the selected service in the Wireless Local Area Network, wherein: preset a service analyzing unit to initiate the accessing process, the method includes: the user terminal of the WLAN

(21) 2 523 915

(13) A1

(57) Abrégé(suite)/Abstract(continued):
sends a request of setting the service to the service analyzing unit; the service analyzing unit sends a service authentication and authorization request which contains a user signing information to the service authentication and authorization unit after it receives the request, the service authentication and authorization unit attests and authorizes the user terminal which sent the request based on the signing information of the WLAN user terminal which sent the request; then determines whether the authentication and authorization are successful , if they are successful , the service authentication and authorization unit sends back the authorized destination of the device to the user terminal which sent the request, the user terminal sets the service link to the destination device; otherwise, service authentication and authorization unit responds a unsuccessful information to the service setting request. This method can simplify the accessing process of the selected service, and at the same time, it can improve the safe reliability of the network greatly.

Abstract

The present invention discloses a method for resolving and accessing a selected service in a Wireless Local Area Network (WLAN), wherein a service resolving unit is preconfigured for initial access, the method comprising: a WLAN user terminal sending a service establishing request to the service resolving unit; after receiving the service establishing request, the service resolving unit sending a service authentication and authorization request containing the user's subscription information to the service authentication authorization unit, which performs authentication and authorization to the requesting WLAN user terminal; then judging whether the authentication and authorization is successful, if yes, the service authentication authorization unit returning the address of the authorized destination device to the requesting WLAN user terminal so as to establish a service connection between the WLAN user terminal and the destination device; otherwise, the service authentication authorization unit returning the failure information of the service establishing request. With this method, the analytical access processing of the selected service can be simplified while the security and reliability of the network greatly enhanced.

Method for Resolving and Accessing Selected Service in Wireless Local Area Network

Field of the Technology

The present invention relates to service accessing technique, more particularly to a method for resolving and accessing services selected by users in Wireless Local Area Network (WLAN).

Background of the Invention

As users' demands for an increasingly high rate of wireless access, there emerges the WLAN, which is able to provide high-rate wireless data access in a relatively small area. Various techniques have been used in WLAN, among which a technical standard with more applications is IEEE 802.11b. This standard involves the frequency band of 2.4GHz with a data transmission rate up to 11 Mbps. Other technical standards involving the same frequency band include IEEE 802.11g and the Bluetooth, where the data transmission rate of IEEE 802.11g is up to 54Mbps. There are other new standards such as IEEE 802.11a and ETSI BRAN Hiperlan2, which use the frequency band of 5GHz with the transmission rate up to 54 Mbps as well.

Although there are various techniques for wireless access, most WLANs are utilized to transfer IP data packets. The specific WLAN access technique adopted by a wireless IP network is usually transparent to the upper IP layer. Such a network is usually configured with Access Points for providing wireless access to a user terminal and with controlling and connecting devices for implementing IP transmission.

Along with the rising and developing of WLAN, focus of research is shifting to the inter-working of WLAN with various mobile communications networks, such as GSM, CDMA, WCDMA, TD-SCDMA, and CDMA2000. In accordance with the 3GPP standards, a user terminal is able to connect to Internet and Intranet via the WLAN access network and also connect to a user's home network and visited networks of a 3GPP system via the WLAN access network. To be specific, when accessing locally, a WLAN user terminal will get connected to the 3GPP home network via the WLAN access network, as shown in Figure 2; when roaming, it will get connected to the 3GPP visited network via the WLAN access network. Some

entities of the 3GPP visited network are connected with corresponding entities of the 3GPP home network, for instance, the 3GPP Authentication, Authorization and Accounting (AAA) Proxy in the visited network is connected with the 3GPP AAA Server in the home network, the WLAN Access Gateway (WAG) in the visited network is connected with the Packet Data Gateway (PDG) in the home network, as shown in Figure 1. Figure1 and Figure 2 are the schematic diagrams illustrating the networking architectures of a WLAN inter-working with a 3GPP system with and without roaming facilities, respectively.

As shown in Figure 1 and Figure 2, a 3GPP system primarily comprises Home Subscriber Server (HSS)/ Home Location Register (HLR), 3GPP AAA Server, 3GPP AAA Proxy, WAG, PDG, Offline Charging System and Online Charging System (OCS). User terminals, WLAN access network, and all the entities of the 3GPP system together constitute a 3GPP-WLAN inter-working network, which can be used as a WLAN service system. In this service system, 3GPP AAA Server is in charge of the authentication, authorization and accounting of a user, collecting the charging information sent from the WLAN access network and transferring the information to the charging system; PDG is in charge of the transmission of the user's data from the WLAN access network to the 3GPP network or other packet networks; and the charging system receives and records the subscribers' charging information transferred from the network. OCS instructs the network transmit the online charging information periodically in accordance with the expense state of the online charged subscribers and makes statistics and conducts control.

In the non-roaming case, when a WLAN user terminal desires to access directly the Internet/Intranet, the user terminal can access Internet/Intranet via WLAN access network after it passes authentication and authorization of AAA server (AS) via WLAN access network. If the WLAN user terminal desire to access services of 3GPP packet switching (PS) domain as well, it may further request the services of Scenario 3 from the 3GPP home network. That is, the WLAN user terminal initiates a authorization request for the services of Scenario 3 to the AS of the 3GPP home network, which will carry out service authentication and authorization for that request; if it succeeds, AS will send an access accept message to the user terminal and assign a corresponding PDG for the user terminal. When a tunnel is established between the

user terminal and the assigned PDG, the user terminal will be able to access to the services of the 3GPP PS domain. Meanwhile, the offline charging system and OCS records the charging information in accordance with the user terminal's occupation of network resources. In the roaming case, when a WLAN user terminal desires to access directly the Internet/Intranet, it may make a request to the 3GPP home network by way of the 3GPP visited network for access to the Internet/Intranet. If the user terminal also desires to request the services of Scenario 3 to access the services of the 3GPP PS domain, the user terminal needs to initiate via the 3GPP visited network a service authorization process at the 3GPP home network. The authorization is carried out likewise between the user terminal and AS of the 3GPP home network. After the authorization succeeds, AS assigns the corresponding home PDG for the user terminal, then the user terminal will be able to access the services of 3GPP PS domain of the home network after it establishes a tunnel with the assigned PDG via the WAG of the 3GPP visited network.

At present, after a user selects an Access Point Name (APN) of a service, there are two implementing schemes to obtain the address of corresponding service providing unit according to the service name after authentication and authorization of the AAA server,:

One scheme is: the user terminal directly obtains the address of final service providing unit, namely destination PDG address, through a public Domain Name Server (DNS), wherein the destination PDG is usually located in home network of current user terminal. In this case, user terminal sends a tunnel establishing request to the destination PDG, the PDG authenticates current user terminal on AAA server after receiving the request. If the authentication is successful, the destination PDG directly establishes a tunnel between itself and User Terminal (UE). Disadvantage of this scheme lies in: it is difficult for visited network to judge whether to allow the user to visit destination address and make control, so that illegal data may be transmitted among networks. Because inter-network traffic is usually long-distance traffic, transmission cost is pretty high and inter-network balance is required. Therefore, it's better to avoid transmitting unauthenticated information. In addition, in terms of security, if all PDGs in a network of an operator are exposed in DNS system and any Internet users can get them, there will be great potential trouble for network security.

The other scheme is: the user terminal obtains through by private DNS resolving the WAG which covers it currently and service authentication and authorization is performed through interaction between the WAG and AAA server. After the authorization is successful, the WAG obtains the address of final service providing unit from AAA server, namely address of PDG, and then current user terminal sends a tunnel establishing request to the destination PDG to establish a tunnel between UE and destination PDG. However, as a user's request is directly handled by WAG in this scheme, a WAG detecting mechanism, like DNS or DHCP, is needed to inquire and resolve WAG's address, accordingly new protocol needs to be added for interaction. Besides, since there is repeated interaction between PDG and AAA server for APN authentication and authorization, this scheme through WAG becomes more complicated. Moreover, there are much more WAGs than PDGs in a visited network. All this leads to a greater demand for WAG in the visited network, which has to provide sufficient WAGs so as to guarantee the service interaction. What's more, as a large number of WAGs in other networks will interact with AAA server, the core device in the home network, a great threat is posed for the security of AAA server, thus bringing difficulty to the roaming of services.

Therefore, there are obvious disadvantages in the above two schemes, so it is difficult to put them into use. The main reason is that neither of the schemes adopts proper resolution strategy according to different capabilities of visited networks. In one scheme, the visited network is required to have strong capability, leading to problems like complicated network implementation and potential trouble for inter-network security, so that roaming scope is restricted. With the other scheme, although public DNS resolution is pretty easy, inter-network data cannot be effectively controlled and public DNS must be relied on, which brings potential security problem and consequently confines the application of this scheme.

Summary of the Invention

Therefore, the main object of the present invention is to provide a method for resolving and accessing selected services in Wireless Local Area Network, to simplify the resolution and access processing by the network for a selected service, and meanwhile to greatly enhance network security and reliability.

To attain the above object, technical scheme of the present invention is implemented as follows:

A method for resolving and accessing selected services in WLAN, wherein a service resolving unit is pre-configured for initial access processing, the method comprising:

a. A WLAN user terminal sending a service establishing request to the said service resolving unit;

b. After receiving the service establishing request, the service resolving unit sending to service authentication authorization unit a service authentication and authorization request that comprises user subscription information extracted from the service establishing request, according to subscription information of the WLAN user terminal initiating the request, the service authentication authorization unit performing service authentication and authorization of the WLAN user terminal initiating the request;

c. The service authentication authorization unit judging whether authentication and authorization is successful, if yes, the service authentication authorization unit returning the addresses of destination devices authorized to handle the selected services to the WLAN user terminal initiating the request via the service resolving unit, the WLAN user terminal establishing a service connection with the said destination devices; otherwise, the service authentication authorization unit returning failure information of the service establishing request.

The said WLAN user terminal sending a request to the service resolving unit in step a comprises: the WLAN user terminal sending a request to the service resolving unit according to the local network address obtained through private DNS resolution or according to a public IP address; or the WLAN user terminal sending a request to the service resolving unit according to the public IP address obtained through public network DNS resolution; or the WLAN user terminal sending a request to the service resolving unit according to a preset IP address or any address in an address list; or the WLAN user terminal sending a request to the service resolving unit according to the last visited IP address.

The said judging whether authentication and authorization is successful in step c further comprises: judging whether the routing between current authorized destination

device and the WLAN access gateway to which the requesting WLAN user terminal belongs is opened to the requesting WLAN user terminal, if the routing is opened, the service authentication and authorization is successful; otherwise, the service authentication authorization unit sending an open route notification to the WLAN access gateway to which the requesting WLAN user terminal belongs to instruct the WLAN access gateway to open the route between the authorized destination device and itself, then judging whether the route is successfully opened, if yes, the service authentication and authorization is successful, otherwise unsuccessful.

The said service resolving unit is the destination device authorized to process the selected services, then said step c comprises: after the service authentication authorization unit sending the destination device address to the service resolving unit, the service resolving unit directly sending service establish response to the requesting WLAN user terminal, and starting a process of establishing service connection with the requesting WLAN user terminal.

The said process of establishing a service connection between the WLAN user terminal and the destination device in step c further comprises: after receiving the address of destination device authorized to process the selected service, the requesting device sending a service establishing request to the destination device once again; after receiving the service establishing request, the destination device performing authentication and authorization to the current requesting WLAN user terminal through interaction with the service authentication authorization unit, if the authorization is successful, the destination device establishing a service connection with the requesting WLAN user terminal.

In step c, while returning address of the destination device authorized to process the selected service to the requesting WLAN user terminal, the service authentication authorization unit sending a service authorization notification that carries information of the requesting WLAN user terminal to the destination device. The process of establishing a service connection between the WLAN user terminal and the destination device in step c further comprising: after receiving the address of destination device authorized to process the selected service, the requesting WLAN user terminal sending a service establishing request to the destination device once again; after receiving the service establishing request, the destination device

performing authentication and authorization to the requesting WLAN user terminal according to the information in the service authorization notification, if the authorization is successful, establishing a service connection with current requesting WLAN user terminal.

The said user subscription information at least comprises: user identity of the requesting WLAN user terminal and service name of the selected service that the WLAN user terminal requests to access. The service establishing request is included in a tunnel establish request signaling provided by the standard. The service resolving unit is configured inside the visited network or inside the home network of the requesting WLAN user terminal.

The service authentication authorization unit is an Authentication Authorization and Accounting (AAA) server. The service authentication authorization unit is a 3GPP AAA Server. The destination device authorized to process the selected service is a PDG device specified by 3GPP standards or a General Package Radio Service (GPRS) Gateway Support Node (GGSN).

The method further comprises: after the selected service is successfully accessed, the requesting WLAN user terminal storing corresponding relation between the selected service name and the address of destination device authorized to process the selected service.

The method further comprises: after the selected service is successfully accessed, the requesting WLAN user terminal storing corresponding relation between the selected service name and the service resolving unit.

The method further comprises: after current access to selected service is over, closing the route between the WLAN access gateway device and the authorized destination device, wherein the route is provided for the requesting WLAN user terminal.

In the above scheme, the WLAN access gateway device is a WLAN Access Gateway (WAG).

The user identity is Network Access Identity (NAI) or user IP or International

Mobile Subscriber Identity (IMSI) or TEMPID or Session Initialization Protocol-Uniform Resource Locator Identity (SIP-URL) of the requesting WLAN user terminal.

Step c further comprises: while returning failure information to the requesting WLAN user terminal, indicating corresponding error information to the requesting WLAN user terminal.

In accordance with the method for resolving and accessing selected service in WLAN provided by the present invention, one or more than one service resolving unit specially used for initial access processing is configured, and user terminals will send all service access requests to the service resolving unit, which controls the subsequent procedures of authentication, authorization and service connection establishment. This method has the following advantages and features:

1) The present invention can furthest implement resolution and access procedure of the selected WLAN service according to the capabilities and structure of a practical network.

2) When using a public DNS, there is only a few devices acting as service resolving unit, like PDG, whose addresses is to be found in the public DNS while other common service access devices that provide services, e.g. PDG, do not have to be disclosed in the public DNS, so security of gateway devices that provide services, e.g. PDG, is guaranteed, preventing the users without authentication or authorization from directly visited the gateway device that provide services, e.g. PDG. As for service resolving units that can be found in public DNS, the security and reliability thereof can be improved by enhancing security protection and the processing capability thereof.

3) For a visited network with strong capabilities and allowed to visit home network user data and/or allowed to interact with home network AAA server, resolution and authorization operations can be performed by devices in visited networks; for a visited network with weak capabilities, resolution and authorization operations can be forwarded to home network through specified route and destination address, so as to avoid roaming scope restriction. However, as far as the user terminal is concerned, the above-mentioned two approaches are both invisible and with

completely the same interactive modes, which can guarantee simplicity and consistency of the user terminal.

4) VPLMN/WLAN operators decide whether to adopt private or public DNS resolution method to obtain the address of the service resolving unit, which may be located in VPLMN or HPLMN without the need of differentiating between PDG and WAG.

5) The requesting WLAN user terminal and the destination device make interaction by means of existing signaling for establishing End-to-End (E2E) tunnel so as to avoid adding new interactive protocols. The service resolving unit interacts with AAA server to perform authentication and authorization of the user terminal, the authorization result of which will lead to the actual PDG for processing the service.

Brief Description of the Drawings

Figure 1 is a schematic diagram illustrating network structure of inter-working WLAN system and 3GPP system in the roaming case;

Figure 2 is a schematic diagram illustrating network structure of inter-working WLAN system and 3GPP system in the non-roaming case;

Figure 3 is a flowchart illustrating access authorization procedure;

Figure 4 is a flowchart illustrating the basic processing in accordance with the present invention;

Figure 5 is a flowchart of the processing in the first embodiment according to the method of the present invention;

Figure 6 is a flowchart of the processing in the second embodiment according to the method of the present invention;

Figure 7 is a flowchart of the processing in the third embodiment according to the method of the present invention;

Figure 8 is a flowchart of the processing in the forth embodiment according to the method of the present invention;

Figure 9 is a flowchart of the processing in the fifth embodiment according to the method of the present invention;

Figure 10 is a flowchart of the processing in the sixth embodiment according to the method of the present invention;

Figure 11 is a flowchart of the processing in the seventh embodiment according to the method of the present invention.

Detailed Description of the Invention

The rationale of the present invention is: adopting two-step resolution, that is, presetting one or more than one service resolving unit used for initial access processing. These service resolving units receive users' requests, perform authentication and authorization with a service authorization unit, and then return to the requesting user terminal the address of the device authorized by the service authorization unit to process the selected services, wherein the authorized device can also provide some simple services. That is to say, User terminals will send all the service access requests to the service resolving units, which control subsequent operations like authentication, authorization and address returning.

The service resolving unit can be set inside the home network or visited network of the requesting user terminal, which is determined by operator of the visited network according to predefined roaming agreement. The service resolving unit can be located in WAG or PDG. The service authentication authorization unit can be an AAA server or a 3GPP AAA Server in a 3G system. The device authorized to process selected services can be PDG, GGSN or other gateway devices for service connection.

In the present invention, one or more than one service resolving unit is to be set in advance. Multi service resolving units can be differentiated based on the differences among services to be processed. All service resolving units are connected with the service authentication authorization unit. Figure 4 is a flowchart illustrating the basic processing in accordance with the present invention. As shown in figure 4, the access processing of selected services in accordance with the present invention mainly comprises the flowing steps:

Step 401: when a WLAN user terminal requests to access 3GPP-WLAN

inter-working network through WLAN, the WLAN user terminal or the network initiates an access authentication procedure and the network side performs authentication to this WLAN user terminal. Specifically speaking, the access authentication authorization unit at the network side performs legality authentication between the user terminal and the network through an access control unit. Here, the access control unit can be Access Controller (AC) in WLAN access network or WAG in operational network or combination of the two; the access authentication authorization unit can be a 3GPP AAA Server.

As shown in step 301~step 306 in figure 3, the access authentication and authorization procedure between WLAN user terminal and 3GPP AAA Server comprises: WLAN user terminal transmitting authentication information needed for authentication to the access authentication authorization unit through the access control unit; after receiving relevant information of the user terminal, the access authentication authorization unit performing access authentication in itself, if the authentication is successful, authorizing the user's access scope according to the subscription information and continuing with subsequent operations; otherwise, notifying the user terminal about failure of the access authentication and ending the current access authorization procedure.

The said subscription information concerning access scope means that the user terminal has to be authorized for access when initially accessing WLAN. At this moment, it will be determined whether the user data can be allowed to pass WAG. After the access is authorized, the user terminal can access the Internet and Local Area Network but cannot access 3GPP packet services, i.e. cannot access various 3G network services provided through PDG.

If a certain terminal is able to access a 3G service and has subscribed to this service, the PDG providing the service may still be closed to this user terminal, therefore routing the user data to the PDG will be forbidden at WAG. But in order to let the request of this user terminal pass WAG, this user terminal will be authorized at WAG to visit the initial resolution device. Obviously, the route to the PDG providing the service can be opened to the user terminal during access authorization so that the signaling of the user terminal's request can pass, but it is still needed to perform service authorization by interacting with the PDG during service access procedure.

Some low-cost user terminals, which has not subscribed to the services requiring interaction with a 3G network, will only be allowed to directly access the Internet through WLAN, but permanently forbidden to access such a 3G core-network device as PDG through WLAN, then any data of this kind of users will be forbidden to pass at WAG.

Step 402: after passing the access authentication, WLAN user terminal, by interacting with a public or private DNS, obtains the IP address of the service resolving unit according to the service name of the selected service.

Here, there are many ways for a WLAN user terminal to obtain the IP address of the service resolving unit: obtaining the local network address or public IP address according to the resolution in a private DNS; or obtaining the public IP address according to resolution in a public DNS; or obtaining the IP address of the service resolving unit according to a preconfigured IP address or any address in the address list; or obtaining the IP address of the service resolving unit according to the IP address obtained by resolution performed in the last access.

Step 403: according to the address obtained in step 402, the requesting WLAN user terminal sends a service establishing request to the service resolving unit. In this embodiment, the End-to-End tunnel establish request in the existing standard signaling can be adopted to bear this service establishing request, or the service establishing request can be made by signaling independently set. In this embodiment, the service resolving unit is an independent device.

Relevant subscription information of current WLAN user terminal carried in this request mainly comprises: user identity of current WLAN user terminal and name of service selected by current WLAN user terminal, wherein the user identity can be Network Access Identity (NAI), user IP, International Mobile Subscriber Identity (IMSI), TEMP ID or Session Initialization Protocol-Uniform Resource Locator Identity (SIP-URL). In this embodiment, the selected services may comprise short message service, multimedia short message service, location service, IP Multimedia Subsystem (IMS) services, and so on.

Step 404~step 405: after receiving the service establishing request, the service resolving unit sends a service authentication and authorization request to the service

authentication authorization unit, wherein the request carries the user's subscription information. The service authentication authorization unit performs authentication and authorization to the requesting WLAN user terminal according to the received user's subscription information and then returns a service authentication and authorization response to the service resolving unit, wherein the response carries the result of authentication and authorization. In this embodiment, the service authentication authorization unit is a 3GPP AAA Server.

If the authentication and authorization is successful, the service authentication authorization unit will return the address of the device authorized to process selected services and the name of the authorized service to the service resolving unit; if unsuccessful, the service authentication authorization unit will return failure information to the requesting WLAN user terminal by way of service resolving unit and end the current access procedure. While returning failure information, the service resolving unit can provide the corresponding error information for WLAN user terminal. The subsequent steps are described by taking example of successful authentication and authorization.

While the said service authentication authorization unit authenticates the WLAN user terminal, 3GPP AAA Server will try to identify the requesting WLAN user terminal, if the identification is successful, it will be checked whether the requested service matches the service subscription information thereof, if they do not match, return failure information directly or return the information of a possible substitute service, for instance, replacing multimedia short message service by short message service. In this case, if the user terminal accepts the new substitute service, subsequent operations will be executed; otherwise, current procedure will be ended. If the identification is unsuccessful, user identification failure information will be directly returned and new procedures like user identity re-synchronization or re-authentication will be initiated.

Step 406: after receiving the address of destination device and authorized service names, the service resolving unit will forward the received information to the requesting WLAN user terminal. In this embodiment, the existing standard End-to-End tunnel establishing transfer signaling is adopted to transmit information like the address of destination device and authorized service names.

Step 407: after receiving the address of destination device, the requesting WLAN user terminal sends a service establishing request to the destination device once again according to the received address thereof to request for establishing service connection. In this embodiment, this service establishing request can be borne by existing standard End-to-End tunnel establishing transfer signaling.

Step 408~409: after the destination device receives the service establishing request, the service authentication authorization unit will authenticate the requesting WLAN user terminal. Because the destination device does not know that the requesting WLAN has passed the authentication, the requesting WLAN user terminal will be processed as a terminal initiating a new request.

Step 410: after the authentication is successful, the destination device will return a service establish response and interact with the requesting WLAN user terminal to establish a service tunnel. Since this requesting WLAN user terminal has passed an authentication, it can pass this authentication usually. Here, standard End-to-End tunnel establish interactive procedure can be adopted to implement the interactive procedure of establishing service tunnel.

Usually, data transmission between the destination device authorized by the service authentication authorization unit to process selected services and the intermediate route control device, such as WAG, is configured as enabled in advance. In another word, the address of destination device is an address allowed to route via the WAG, namely, there will be an open route between the WAG and destination device such that they can interact with each other. Specifically speaking, data of the requesting user terminal are allowed to arrive at the authorized destination device via WAG. There are two schemes to implement configuration in advance: The first scheme is that, the allowed address scope is sent to the devices like WAG during access authorization, for instance, a certain IP address may be opened for all subscribers whose home network operator is CMCC, allowing them to visit the network; or all devices are only allowed to access a certain device in the local network; the other scheme is that, after the access, AAA server issues to the relevant visited networks the instruction about the opened IP addresses in the local network, or the IP addresses that every subscriber is allowed to visit.

However, sometimes there is no allowed route preset between the destination device and intermediate route control device. In this case, after having determined the authorized destination device, the service authentication authorization unit will check its own record and judge whether there is an authorization allowed route between the WAG to which requesting WLAN user terminal currently belongs and the destination device, wherein this judgment is based on whether the service authentication authorization unit has previously sent relevant authorization of route opening or closing to WAG or AAA proxy, if not yet, it is needed to notify the relevant WAG. As shown in figure 5, this embodiment comprises the following steps:

Step 501~504: completely the same as step 401~404. In this embodiment, the intermediate control device is WAG, and the service authentication authorization unit is 3GPP AAA Server.

Step 505~506: after determining the authorized destination device, 3GPP AAA Server sends an open route notification to the WAG to which requesting WLAN user terminal belongs, wherein the notification carries the information of the destination device; after receiving the open route notification, WAG will open corresponding routes according to the address of the destination device and then return an open route notification acknowledgment to 3GPP AAA Server.

Obviously, after receiving the open route notification, WAG may judge whether it is allowed to open the corresponding routes, if not allowed or the route opening fails due to other reasons, the returned open route notification acknowledgment will carry failure information. Meanwhile, current access procedure for the selected service will be ended.

Step 507~512: completely the same as step 405~410.

In case that a route is successfully opened, WAG can close the opened route after access of the selected service is ended.

In terms of the scheme shown in figure 4, after determining the destination device to process the selected service, the service authentication authorization unit, while sending service authentication and authorization response to the service resolving unit, sends a service authorization notification to the destination device to

notify the device that it has been authorized to process a certain selected service requested by a certain WLAN user terminal. In this way, re-authentication procedure in step 408 and 409 can be skipped. The specific process is as shown in figure 6, comprising the following steps:

Step 601~604: completely the same as step 401~404. In this embodiment, the intermediate route control device is WAG and the service authentication authorization unit is 3GPP AAA Server.

Step 605~606: completely the same as step 505~506, but these two steps can be skipped. In case that steps 605 and 606 are included, the embodiment shown in figure 5 can also adopt the scheme of sending authorization notification to the destination device.

Step 607: completely the same as step 405.

Step 608: after determining the destination device authorized to process selected services, 3GPP AAA Server, while sending service authentication and authorization response to the service resolving unit, sends a service authorization notification to the destination device.

Step 609~611: the same as steps 406~407 and step 410, respectively. Since the destination device has learned in advance which user terminal sends the request as well as the request is for which service, after receiving the End-to-End tunnel establish request from the user terminal, the destination device will only compare the pre-received authorization notification with this received request, if they are from the same user terminal and are the same service, service connection can be directly established without making authentication again.

In this invention, the service resolving unit may act as the destination device. In this case, the corresponding procedure is as shown in figure 7, comprising the following steps:

Step 701~704: completely the same as step 401~404. In this embodiment, the intermediate route control device is WAG and the service authentication authorization unit is 3GPP AAA Server.

Step 705: after determining the destination device authorized to process selected services, 3GPP AAA Server sends service authentication and authorization response to the service resolving unit, indicating that this service resolving unit has been authorized as the destination device to process the service selected by the current user terminal.

Step 706: after receiving the service authentication and authorization response, the service resolving unit directly responds to the establishment of a service connection so that the WLAN user terminal performs subsequent interaction directly to establish the service connection without the need of sending an End-to-End tunnel establish request to the service resolving unit according to the received address.

There are two ways of setting the service resolving unit: setting the service resolving unit inside a visited network or a home network. Procedure of resolution implemented by a service resolving unit in a visited network is as follows:

Figure 8 illustrates an embodiment where the service resolving unit is set inside a visited network. As shown in figure 8, in this embodiment, a PDG in the visited network is taken as the service resolving unit, which can be called R-PDG. An IP address should be allocated by the visited network. The address of the service resolving unit that user terminal accesses is placed in a private DNS system, and an R-PDG address of the visited network can be obtained by resolving any service name. During access authorization this R-PDG address will be allowed to be accessed through WAG.

Figure 9 illustrates another embodiment when the service resolving unit is set inside the visited network. As shown in figure 9, in this embodiment, a WAG in the visited network acts as the service resolving unit. The visited network takes this WAG address as the initial resolution result of any user service, and the WAG should be able to interact with 3GPP AAA Server to perform service authentication and authorization while the signaling can be transmitted through AAA proxy. In case that the WAG is unable to interact with 3GPP AAA Server, the WAG acting as the service resolving unit can be taken as an R-PDG, wherein the network structure thereof is essentially the same as that shown in figure 8. As a result, there is the case when the two schemes as shown in figures 8 and 9 co-exist in merged applications.

Procedure of resolution implemented by the service resolving unit in the home network comprises the following steps:

Figure 10 illustrates an embodiment when the service resolving unit is set inside a home network. As shown in figure 10, in the present embodiment, a PDG in the home network acts as the service resolving unit, which can be called R-PDG. When access authorization is required, the access rule sent by home network is implemented to allow users of the home network to route to an address or address segment of the R-PDG that can be taken as a service resolving unit.

Figure 11 illustrates another embodiment when the service resolving unit is set inside home network. As shown in figure 11, in the present embodiment, WAGs in the home network act as the service resolving unit. These WAGs should be able to interact with 3GPP AAA Server to perform service authentication and authorization. When the user is covered by the home network, the procedure hereby is the same as that of the embodiment shown in figure 9. When the user is roaming, these WAGs are equivalent to the R-PDGs in the embodiment shown in figure 10, wherein the home network will, as pre-arranged or dynamically, notify the visited network about these addresses. When resolving a service request of the user terminal by DNS, the visited network directly notifies the user terminal about the addresses of these R-PDGs as DNS resolution results, in this way, the user terminal can obtain the addresses of service resolving units in the home network.

The above mentioned interaction procedures for resolution and access of a selected service can be applied in any combination in practical networks. In terms of a home network, this capability can be easily provided by using PDG as the service resolving unit, so can it by using WAG, both will attain the object of centralized management, but the latter will cost more than the former. Therefore, ordinary roaming partners are only required to be able to return the requested route obtained through initial resolution of DNS mechanism to some devices allowed by the home network.

In the above mentioned different embodiments, in case of services that are successfully accessed, the requesting WLAN user terminal can store the service names of the selected services and addresses of the corresponding destination devices

so that the stored information can be used when establishing services once again. For instance, when establishing a service once again, if the service name is the same as the successfully accessed one and the stored association is still available, or if it is determined according to the special rules that the stored association can be tried, then the user terminal can directly send a service connection establish request to the stored address of the destination device that has once been authorized, and perform End-to-End (E2E) tunnel establishing to leave out the resolution procedure and access directly. Of course, if the stored address of destination device can not be reached or is rejected, resolution has to be performed once again.

Likewise, successfully accessed services mean that the service resolving unit succeeds in resolution, thus the requesting WLAN user terminal can store the service names of the selected services and addresses of corresponding destination devices such that the stored information can be used when establishing services once again. For instance, when establishing a service once again, if the service name is the same as the successfully accessed one and the stored association is still available, or if it is determined according to the special rules that the stored association can be tried, the user terminal can directly send a service establishing request to the stored address of service resolving unit to skip initial resolution, namely, procedure of finding the service resolving unit is the procedure of obtaining the address of the service resolving unit by DNS resolution. Of course, if the stored address of the service resolving unit can not be reached or is rejected, resolution has to be performed once again.

In the above scheme, the service resolving unit can also act as the service authentication authorization unit at the same time, or the service resolving unit and service authentication authorization unit are implemented by the same device. In this case, the authentication and authorization process can be implemented directly by the service resolving unit. Specifically speaking, after receiving a tunnel establish request, the service resolving unit extracts the user identity of the WLAN user terminal and the name of the service that the WLAN user terminal requests to access; meanwhile, the service resolving unit obtains the subscription information of the requesting WLAN user terminal from HSS/HLR according to the user identity, and then compares the obtained subscription information with the extracted information, if they match, the

authentication is successful; otherwise, the authentication is unsuccessful.

The above description only shows preferable embodiments of the present invention, and is not used to confine the protection scope of the present invention.

Claims

1. A method for resolving and accessing selected services in Wireless Local Area Network (WLAN), wherein a service resolving unit is configured for initial access processing, the method comprising the steps of:

a. A WLAN user terminal sending a service establishing request to the said service resolving unit;

b. After receiving the service establishing request, the service resolving unit sending a service authentication and authorization request that contains the user's subscription information extracted from the service establishing request to a service authentication authorization unit; the service authentication authorization unit performing service authentication and authorization to the WLAN user terminal that initiates the request according to the subscription information of the WLAN user terminal;

c. The service authentication authorization unit judging whether the authentication and authorization is successful, if yes, the service authentication authorization unit returning via the service resolving unit the address of a destination device authorized to process the selected service to the WLAN user terminal that initiates the request, and the WLAN user terminal establishing a service connection with the said destination device; otherwise, the service authentication authorization unit responding to the service establishing request with the failure information.

2. A method according to claim 1, wherein said step a comprises: the WLAN user terminal sending the service establishing request to the service resolving unit according to the local network address or public IP address obtained through a private Domain Name Server (DNS) resolution; or the WLAN user terminal sending the service establishing request to the service resolving unit according to the public IP address obtained through a public network DNS resolution; or the WLAN user terminal sending the service establishing request to the service resolving unit according to a preconfigured IP address or any address in a preconfigured IP address list; or the WLAN user terminal sending the service establishing request to the service resolving unit according to the IP address obtained by resolution in the last access.

3. A method according to claim 1, wherein said judging whether the

authentication and authorization is successful in step c further comprises: judging whether a route between the current authorized destination device and the WLAN access gateway device serving the WLAN user terminal that initiates the request is opened to the said WLAN user terminal, if opened, the service authentication and authorization is successful; otherwise, the service authentication authorization unit sending an open route notification to the WLAN access gateway device serving the WLAN user terminal that initiates the request so as to instruct the WLAN access gateway device to open the route to the authorized destination device; then judging whether the route is successfully opened, if yes, the service authentication and authorization is successful; otherwise, the service authentication and authorization failing.

4. A method according to claim 1 or claim 3, wherein said service resolving unit is the destination device authorized to process the selected service, then in step c, after the service authentication authorization unit sends the address of the destination device to the service resolving unit, the service resolving unit sends a service establishing response directly to the WLAN user terminal that initiates the request, and starts the process of establishing a service connection with the WLAN user terminal that initiates the request.

5. A method according to claim 1 or claim 3, wherein said process of establishing a service connection between the WLAN user terminal and the destination device in step c further comprises: after receiving the address of the destination device authorized to process the selected service, the WLAN user terminal that initiates the request sending the service establishing request to the destination device once again; after receiving the service establishing request, the destination device performing authentication and authorization to the current WLAN user terminal that initiates the request through interaction with the service authentication authorization unit, if the authorization is successful, establishing a service connection with the current WLAN user terminal that initiates the request.

6. A method according to claim 1 or claim 3, wherein in step c, while returning the address of the destination device authorized to process the selected service to the WLAN user terminal that initiates the request, the service authentication authorization unit sending a service authorization notification that carries information of the said

WLAN user terminal to the said destination device.

7. A method according to claim 6, wherein said process of establishing a service connection between the WLAN user terminal and the destination device in step c further comprises: after receiving the address of the destination device authorized to process the selected service, the WLAN user terminal that initiates the request sending a service establishing request to the destination device once again; after receiving the service establishing request, the destination device performing authentication and authorization to the said WLAN user terminal according to the information in the service authorization notification, if the authentication is successful, the destination device establishing a service connection with the current WLAN user terminal that initiates the request.

8. A method according to claim 1, wherein said user subscription information at least comprises the user identity of the WLAN user terminal that initiates the request and the service name of the selected service which the WLAN user terminal requests to access.

9. A method according to claim 1 or claim 3, wherein said service establishing request is included in the signaling of tunnel establishing request defined in the standard.

10. A method according to claim 1, wherein said service resolving unit is set in a visited network or set in the home network of the WLAN user terminal that initiates the request.

11. A method according to claim 1, wherein said service authentication authorization unit is an Authentication Authorization and Accounting (AAA) server.

12. A method according to claim 11, wherein said service authentication authorization unit is a 3GPP AAA Server.

13. A method according to claim 1, claim 11 or claim 12, wherein said destination device authorized to process the selected service is a PDG device as defined by the 3GPP standard or is a General Package Radio Service (GPRS) Gateway Support Node (GGSN).

14. A method according to claim 1, further comprising: after the selected service is successfully accessed, the WLAN user terminal that initiates the request storing the corresponding relationship between the service name of the selected service and the address of the destination device authorized to process the selected service.

15. A method according to claim 1, further comprising: after the selected service is successfully accessed, the WLAN user terminal that initiates the request storing the corresponding relationship between the service name of the selected service and the said service resolving unit.

16. A method according to claim 3, further comprising: after the access to the current selected service is over, closing the route between the WLAN access gateway device and the authorized destination device provided for the WLAN user terminal that initiates the request.

17. A method according to claim 3 or claim 16, wherein said WLAN access gateway device is a WLAN Access Gateway (WAG).

18. A method according to claim 1, wherein said user identity is the Network Access Identity (NAI), or user IP, or International Mobile Subscriber Identity (IMSI), or TEMP ID, or Session Initialization Protocol-Uniform Resource Locator (SIP-URL) Identity of the WLAN user terminal that initiates the request.

19. A method according to claim 17, wherein said user identity is the Network Access Identity (NAI), or user IP, or International Mobile Subscriber Identity (IMSI), or TEMP ID, or Session Initialization Protocol-Uniform Resource Locator (SIP-URL) Identity of the WLAN user terminal that initiates the request.

20. A method according to claim 1, wherein said step c further comprises: while returning the failure information to the WLAN user terminal that initiates request, indicating the appropriate error information to the WLAN user terminal that initiates the request.

Application number/numéro de demande: CN2004/001191

Figures: 1, 2, 6-11

Pages:

DRW-IP

Unscannable items
received with this application
(Request original documents in File Prep. Section on the 10th Floor)

Documents reçus avec cette demande ne pouvant être balayés
(Commander les documents originaux dans la section de préparation des dossiers au 10ième étage)

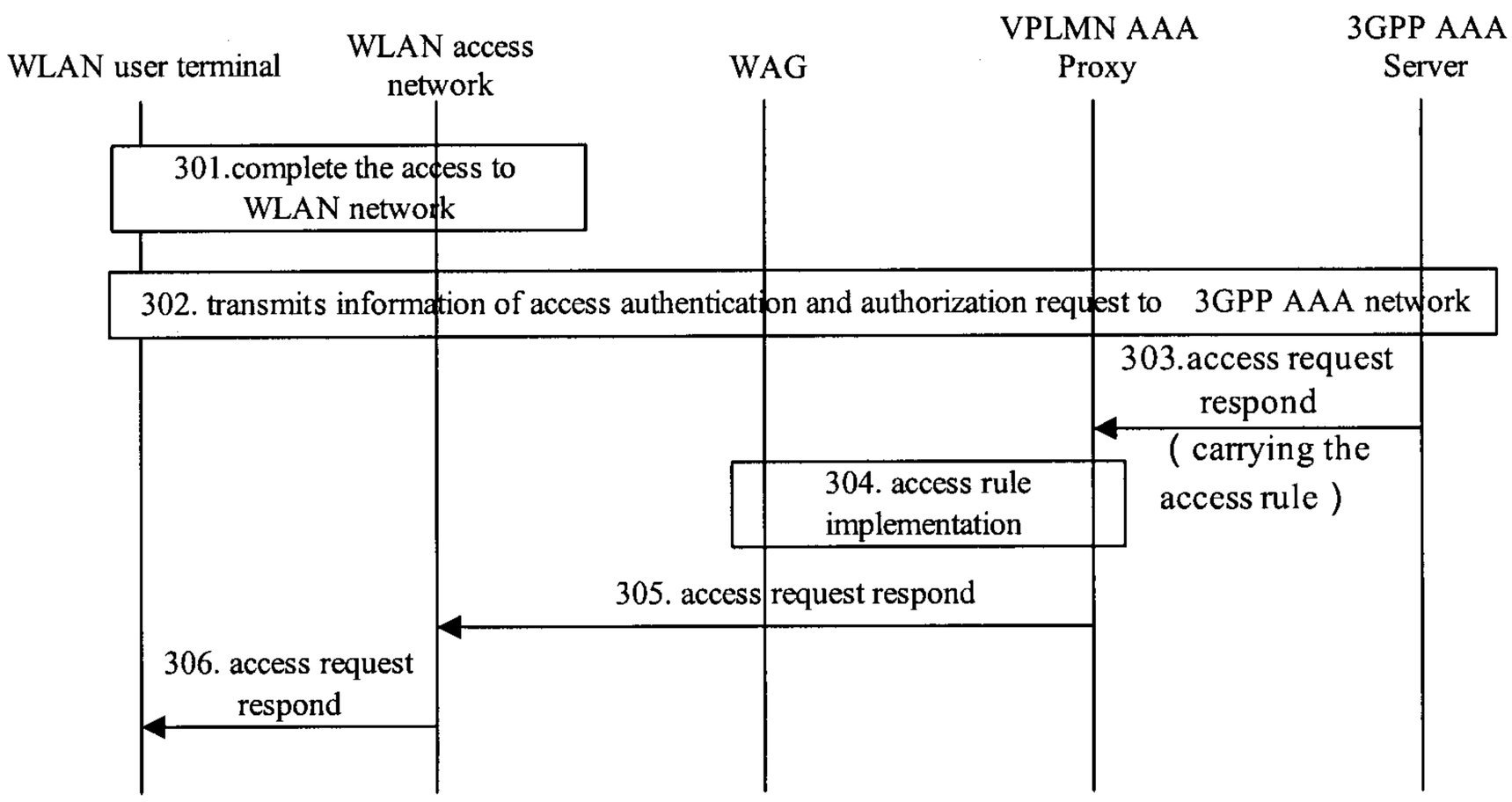

WLAN user terminal
WLAN access network
WAG
VPLMN AAA Proxy
3GPP AAA Server
301.complete the access to WLAN network
302. transmits information of access authentication and authorization request to 3GPP AAA network
303.access request respond
(carrying the access rule)
304. access rule implementation
305. access request respond
306. access request respond

Figure 3

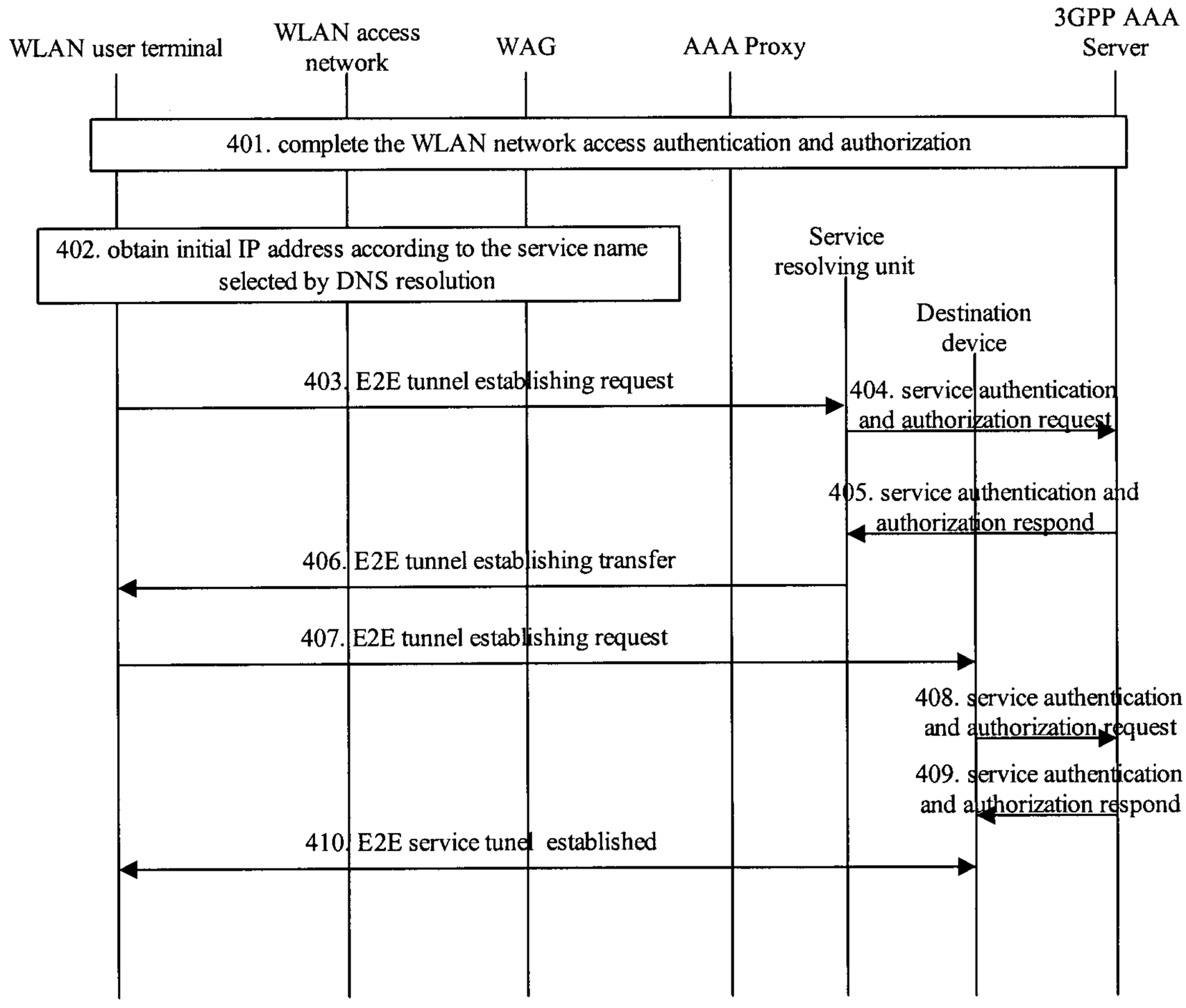

WLAN user terminal
WLAN access network
WAG
AAA Proxy
3GPP AAA Server
401. complete the WLAN network access authentication and authorization
402. obtain initial IP address according to the service name selected by DNS resolution
Service resolving unit
Destination device
403. E2E tunnel establishing request
404. service authentication and authorization request
405. service authentication and authorization respond
406. E2E tunnel establishing transfer
407. E2E tunnel establishing request
408. service authentication and authorization request
409. service authentication and authorization respond
410. E2E service tunel established

Figure 4

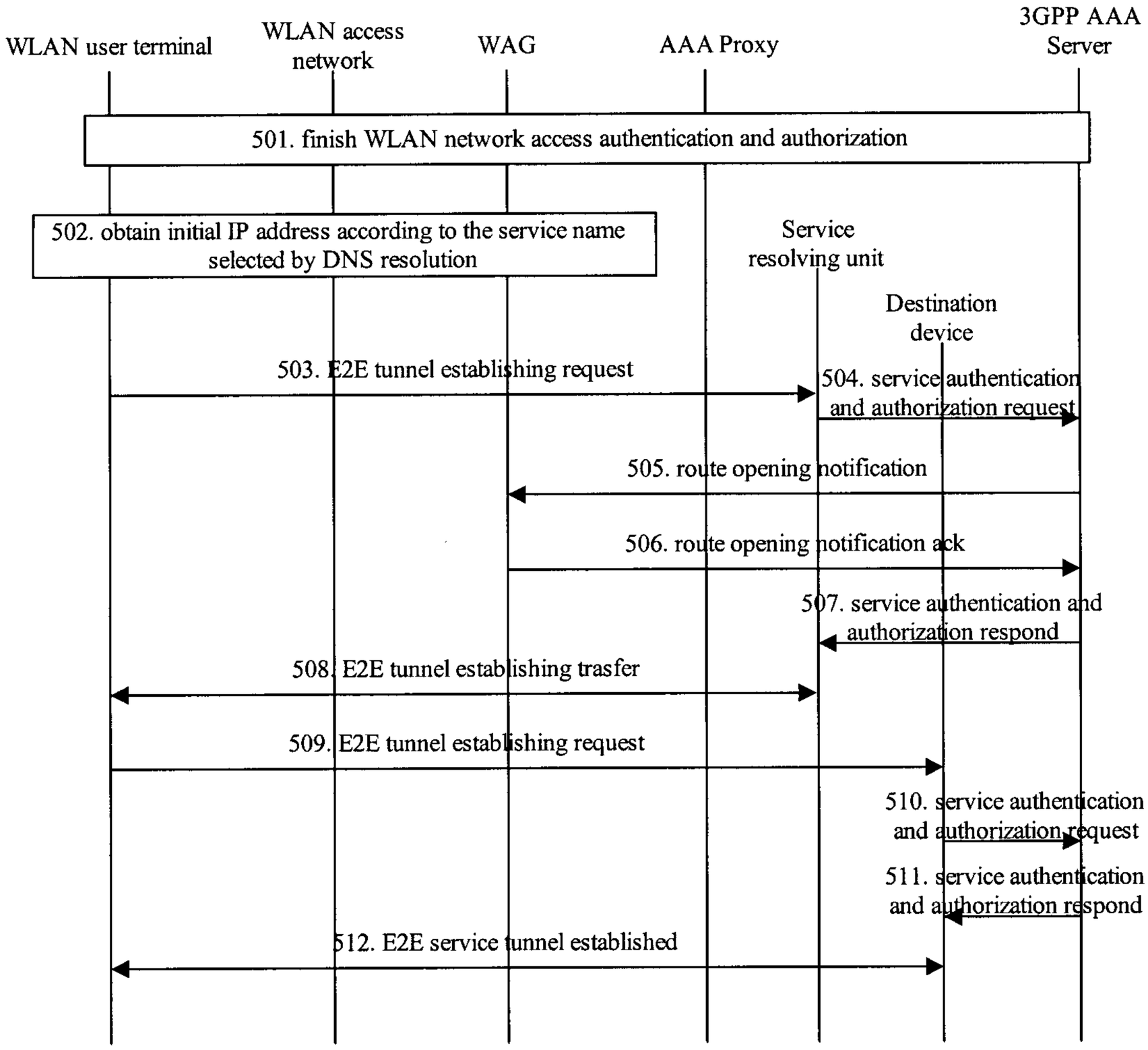

WLAN user terminal
WLAN access network
WAG
AAA Proxy
3GPP AAA Server
501. finish WLAN network access authentication and authorization
502. obtain initial IP address according to the service name selected by DNS resolution
Service resolving unit
Destination device
503. E2E tunnel establishing request
504. service authentication and authorization request
505. route opening notification
506. route opening notification ack
507. service authentication and authorization respond
508. E2E tunnel establishing trasfer
509. E2E tunnel establishing request
510. service authentication and authorization request
511. service authentication and authorization respond
512. E2E service tunnel established

Figure 5

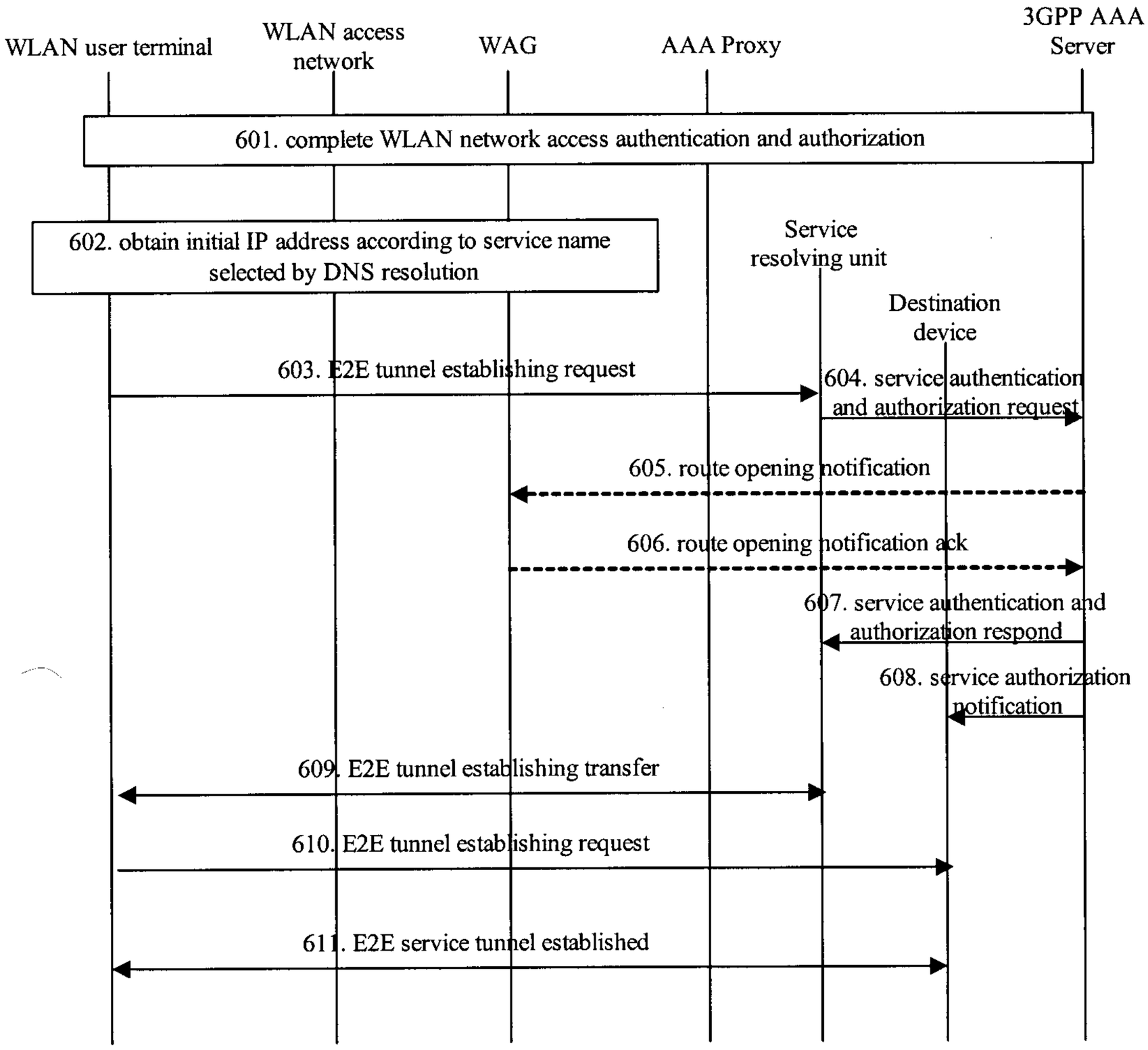

WLAN user terminal
WLAN access network
WAG
AAA Proxy
3GPP AAA Server
601. complete WLAN network access authentication and authorization
602. obtain initial IP address according to service name selected by DNS resolution
Service resolving unit
Destination device
603. E2E tunnel establishing request
604. service authentication and authorization request
605. route opening notification
606. route opening notification ack
607. service authentication and authorization respond
608. service authorization notification
609. E2E tunnel establishing transfer
610. E2E tunnel establishing request
611. E2E service tunnel established

Figure 6

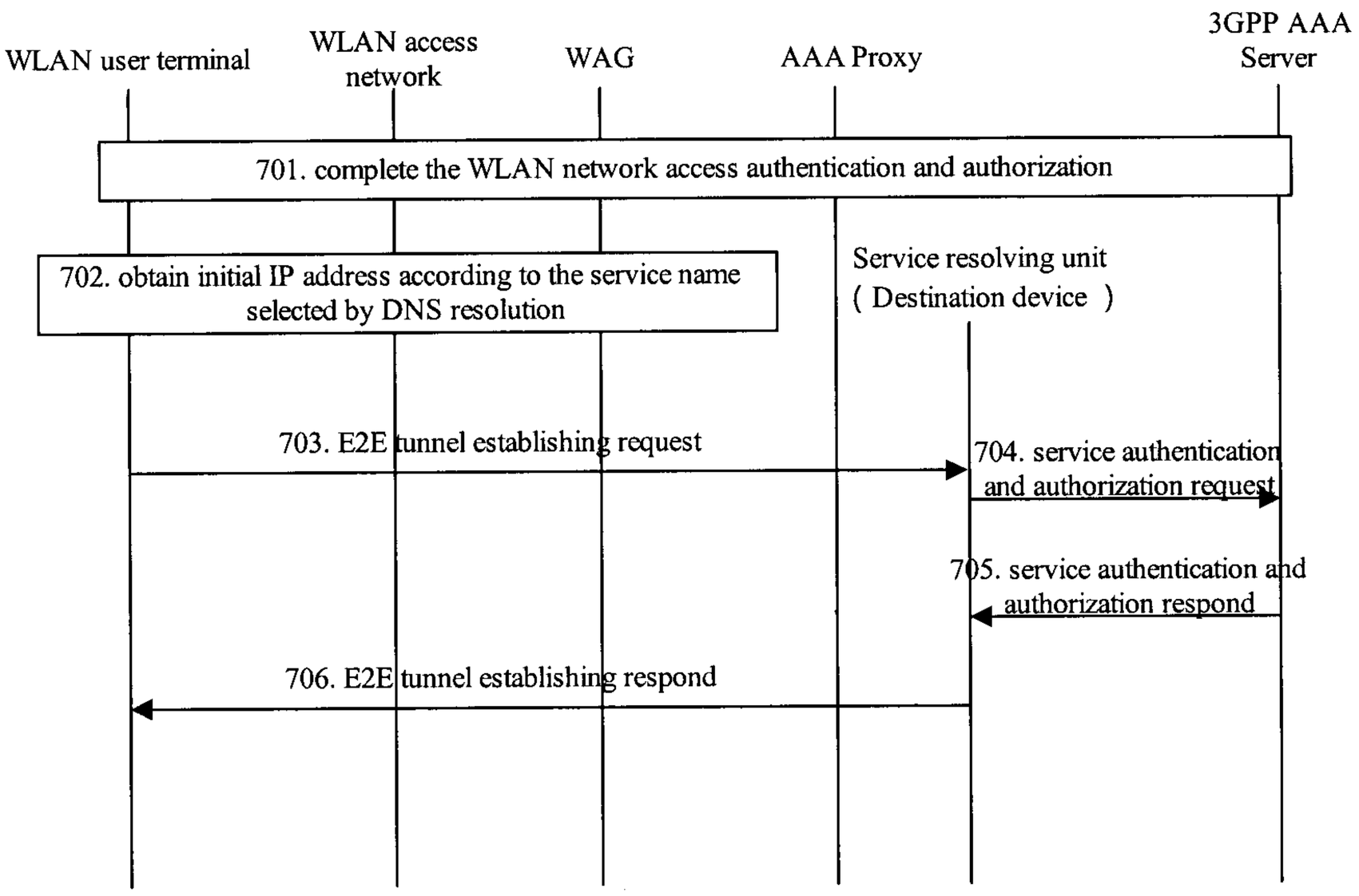
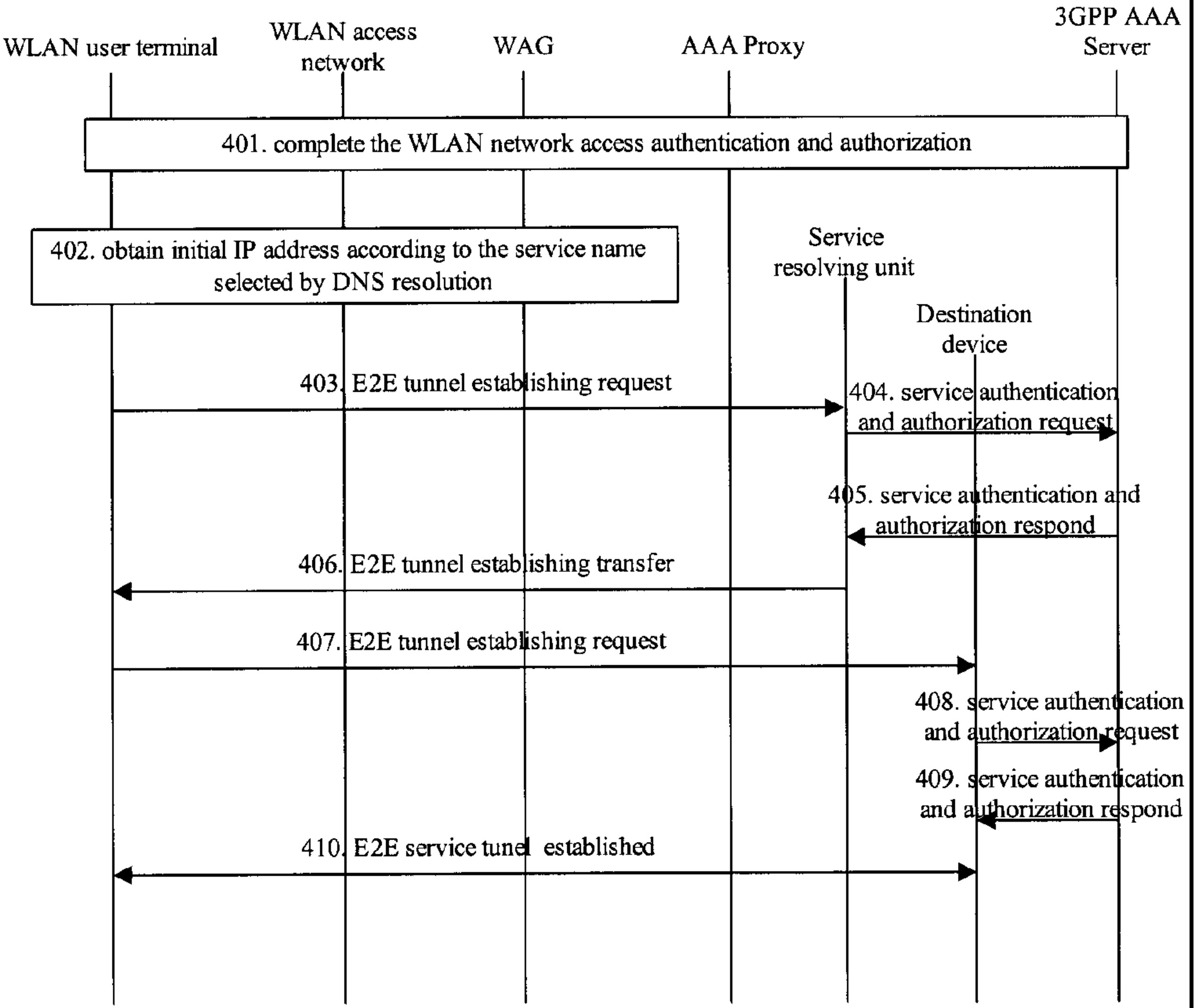

WLAN user terminal
WLAN access network
WAG
AAA Proxy
3GPP AAA Server
701. complete the WLAN network access authentication and authorization
702. obtain initial IP address according to the service name selected by DNS resolution
Service resolving unit
(Destination device)
703. E2E tunnel establishing request
704. service authentication and authorization request
705. service authentication and authorization respond
706. E2E tunnel establishing respond

Figure 7


WLAN user terminal
WLAN access network
WAG
AAA Proxy
3GPP AAA Server
401. complete the WLAN network access authentication and authorization
402. obtain initial IP address according to the service name selected by DNS resolution
Service resolving unit
Destination device
403. E2E tunnel establishing request
404. service authentication and authorization request
405. service authentication and authorization respond
406. E2E tunnel establishing transfer
407. E2E tunnel establishing request
408. service authentication and authorization request
409. service authentication and authorization respond
410. E2E service tunel established