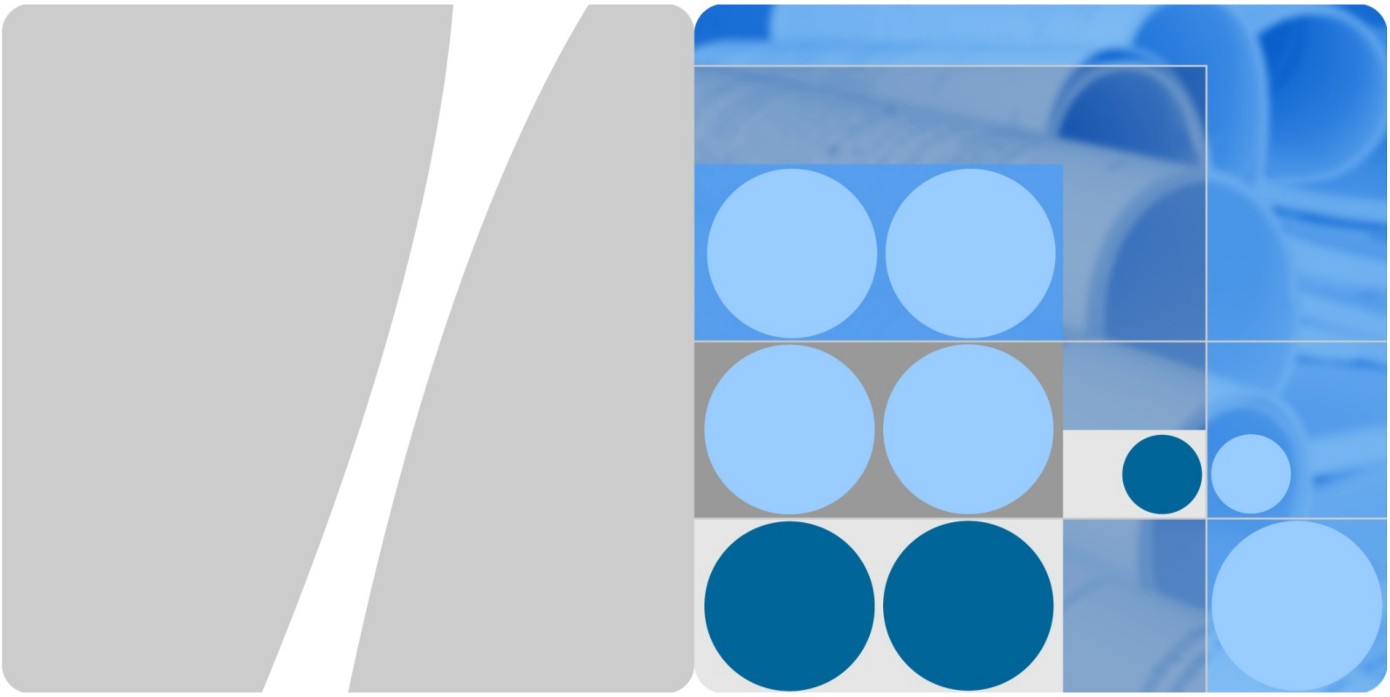


Public Wi-Fi Technology White Paper for Carriers

Issue	**1.0**
Date	

HUAWEI TECHNOLOGIES CO., LTD.

Trademarks and Permissions

Notice

The purchased products, services and features are stipulated by the contract made between Huawei and the customer. All or part of the products, services and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, all statements, information, and recommendations in this document are provided "AS IS" without warranties, guarantees or representations of any kind, either express or implied.

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.

Huawei Technologies Co., Ltd.

Address: Huawei Industrial Base
Bantian, Longgang
Shenzhen 518129
People's Republic of China

Website: http://www.huawei.com

Email: support@huawei.com

About This Document

Overview

This document describes service background and currently main issues of carriers' public Wi-Fi networks, and the major functions, service processes, application scenarios, and deployment suggestions of Huawei WLAN Solution.

NOTE

This document provides customers with the benefits, concepts, and commercial deployment suggestions of Huawei WLAN Solution. It is used for communication with customers and is not an official commitment to customers.

Intended Audience

This document is intended for the following engineers related to the lifecycle WLAN products:

- Marketing engineers
- Technical sales engineers
- Chief marketing engineers
- Product management personnel

Symbol Conventions

The symbols that may be found in this document are defined as follows.

Symbol	Description
⚠ DANGER	Indicates an imminently hazardous situation which, if not avoided, will result in death or serious injury.
⚠ WARNING	Indicates a potentially hazardous situation which, if not avoided, could result in death or serious injury.
⚠ CAUTION	Indicates a potentially hazardous situation which, if not avoided, may result in minor or moderate injury.

Symbol	Description
⚠ NOTICE	Indicates a potentially hazardous situation which, if not avoided, could result in equipment damage, data loss, performance deterioration, or unanticipated results. NOTICE is used to address practices not related to personal injury.
🕮 NOTE	Calls attention to important information, best practices and tips. NOTE is used to address information not related to personal injury, equipment damage, and environment deterioration.

Contents

1 Overview

This chapter describes the network architecture that converges Huawei WLANs with cellular networks, as well as the service process. It also provides features of Huawei WLAN Solution.

1.1 Network Convergence

With popularity and upgrade of smartphones, declining of communications costs, and increasingly diversified Internet and multimedia applications, the number of users and mobile data traffic of carriers increase exponentially. To meet increasing requirements, carriers actively build WLANs. For carriers, WLANs have the following features:

1. High cost-effectiveness: WLANs can share traffic load of mobile cellular networks in hotspot areas, reducing carriers' cellular network construction costs.
2. Easy access to site resources: WLANs can reuse site resources of carriers, such as street cabinets of fixed network carriers and poles of mobile carriers.
3. Wi-Fi calling: that is voice over Wi-Fi (VoWiFi). The voice service is the most basic communication service for carriers. After deploying WLANs, carriers can build competitiveness of the VoWiFi service in the same way as the voice over Long Term Evolution (VoLTE) service. This enhances loyalty of cellular network users and improves the coverage rate of the voice service for carriers.

1.2 Standards Evolution

The Third Generation Partnership Project (3GPP) never stops focusing on Wi-Fi technologies.

In 2004, the Industrial Wireless LAN (IWLAN) mechanism was discussed in 3GPP TS23.234 Release 6, that is, untrusted WLAN access to 2G/3G networks.

In 2007, access to Evolved Packet Core (EPC) networks using non-3GPP access technologies was discussed in 3GPP TS23.402 Release 8. In the standard, WLAN access to EPC networks is still considered an untrusted access mode.

In 2011, the 3GPP established the S2a Mobility based On GTP (SaMOG) study item to discuss WLAN access to EPC networks through the GPRS Tunneling Protocol (GTP) as a trusted access mode, and wrote this access mode into the 3GPP TS23.402 Release 11.

In 2015, the 3GPP Release 13 started to discuss and define Licensed Assisted Access (LAA), LTE-WLAN Aggregation (LWA), and enhanced technologies. These technologies have the same purpose, that is, to allow carriers to use the unlicensed spectrum of WLANs more seamlessly to accelerate deployment of new services.

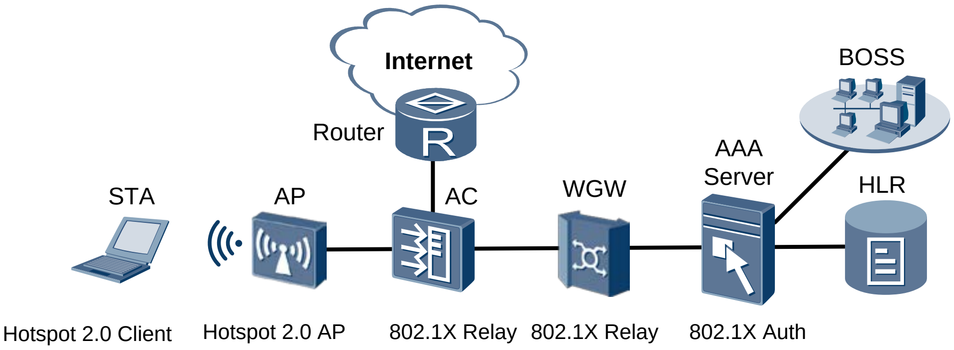
2 Network Architecture

The network architecture of WLANs consists of three planes: control, service, and management.

2.1 Control Plane

WLAN user authentication, authorization, and accounting are performed on the control plane.

Figure 2-1 WLAN network architecture — control plane



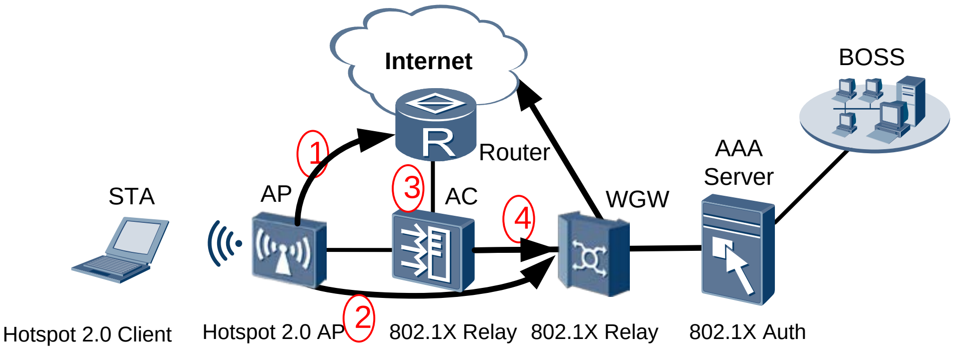
NE	Description
STA	Wireless terminal such as a smartphone, tablet, or laptop
AP	Wireless access point. Huawei Public Wi-Fi Solution supports only Fit APs, but no Fat APs or cloud APs.
AC	Wireless controller. It manages and configures APs in batches, and supports 802.1X authentication, and interworking with a Wi-Fi gateway (WGW) and an authentication, authorization, and accounting (AAA) server using the Remote Authenticated Dial-In User Service (RADIUS) protocol.
WGW	It functions as an AAA server to perform authentication, accounting, and authorization relay.

NE	Description
AAA server	It supports 802.1X, EAP subscriber identity module (EAP-SIM), EAP Authentication and Key Agreement (EAP-AKA), EAP Transport Layer Security (EAP-TLS), and EAP Tunneled Transport Layer Security (EAP-TTLS) authentication. EAP refers to the Extensible Authentication Protocol. An AAA server can obtain authentication vectors and WLAN account registration information from a home location register (HLR).
HLR/Home subscriber server (HSS)	It is a database used for saving user information on a mobile communication network. It also stores account registration information, mobile station location information, mobile station international ISDN numbers (MSISDNs) (ISDN refers to Integrated Services Digital Network), and international mobile subscriber identities (IMSIs).
Business and operation support system (BOSS)	It provides an end-to-end operation process for carriers to process daily tasks such as the customer service, rating, charging, settlement, and dunning.

2.2 Service Plane

Service traffic of WLAN users is aggregated and routed on the service plane.

Figure 2-2 WLAN network architecture — service plane



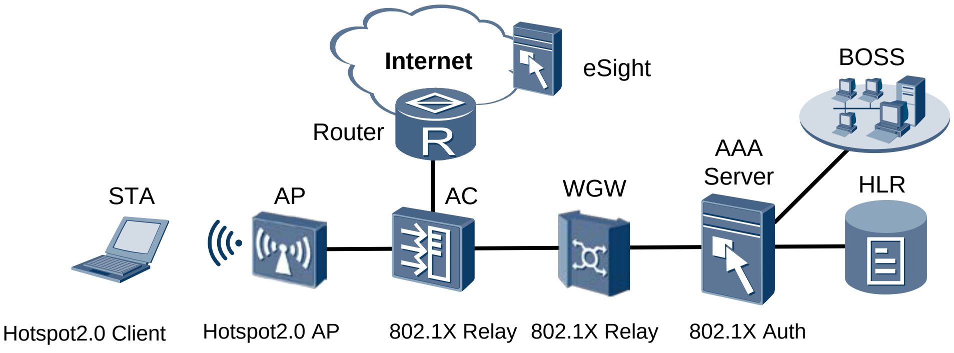
NE	Description
STA	Wireless terminal such as a smartphone, tablet, or laptop
AP	Wireless access point. It can directly forward service traffic of the STA to the Internet through a router, as shown by number 1 in Figure 2-2. It can also forward service traffic to the WGW through a soft Generic Routing Encapsulation (soft GRE) tunnel, as shown by number 2 in Figure 2-2.

NE	Description
AC	Wireless controller. It decapsulates CAPWAP packets that contain service traffic of the STA and are encapsulated by the AP. The AC then directly forwards the traffic to the Internet, as shown by number 3 in Figure 2-2. Alternatively, it encapsulates traffic again into an Ethernet over GRE (EoGRE) tunnel and then aggregates the traffic to the WGW as shown by number 4 in Figure 2-2. L2/L3 networking is supported between the AC and AP.
WGW	It is a core network device of a carrier, and supports EoGRE. It aggregates and centrally manages traffic of WLAN users through EoGRE, and forwards traffic to the Internet through the router.
AAA server	It supports 802.1X and EAP-SIM/AKA/TLS/TTLS authentication. It can obtain authentication vectors and WLAN account registration information from the HLR.
HLR/HSS	It is a database used for saving user information on a mobile communication network. It also stores account registration information, mobile station location information, MSISDNs, and IMSIs.
BOSS	It provides an end-to-end operation process for carriers to process daily tasks such as the customer service, rating, charging, settlement, and dunning.

2.3 Management Plane

WLAN APs and ACs are managed on the management plane.

Figure 2-3 WLAN network architecture — management plane



NE	Description
STA	Wireless terminal such as a smartphone, tablet, or laptop
AP	Wireless access point. Huawei Public Wi-Fi Solution supports only

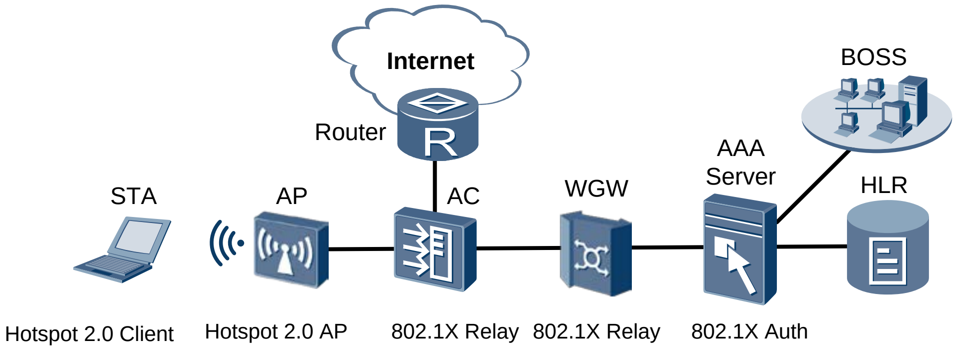
NE	Description
	Fit APs, but no Fat APs or cloud APs.
AC	Wireless controller. It manages and configures APs in batches, and supports 802.1X authentication, and interworking with a WGW and an AAA server using RADIUS. A WLAN AC supports local network management capabilities of a web server.
eSight	As the network management system (NMS) for the AP and AC, eSight provides basic network management, NE, service, and system management functions.

3 Service Process

3.1 Network Discovery and Selection

Hotspot 2.0 is a technical specification designed by the Wi-Fi Alliance (WFA). Building in compliance with 802.11u, Hotspot 2.0 achieves automatic identity identification and seamless switchovers on WLANs without additional identity authentication. Hotspot 2.0 enables wireless terminals to roam on Wi-Fi networks, delivering cellular network–like user experience.

Figure 3-1 Hotspot 2.0 network structure



NE	Description
STA	Wireless terminal. It supports Hotspot 2.0 and can work as a WPA2-802.1X client. A STA queries Hotspot 2.0 network information by sending Access Network Query Protocol (ANQP) packets. Therefore, A STA is called an ANQP client.
AP	Wireless access point. It supports Hotspot 2 and WAP2-802.1X access. An AP can send Hotspot 2 network information to STAs through ANQP. Therefore, an AP can serve as an ANQP server.
AC	Wireless controller. It manages and configures APs in batches, and support 802.1X authentication.

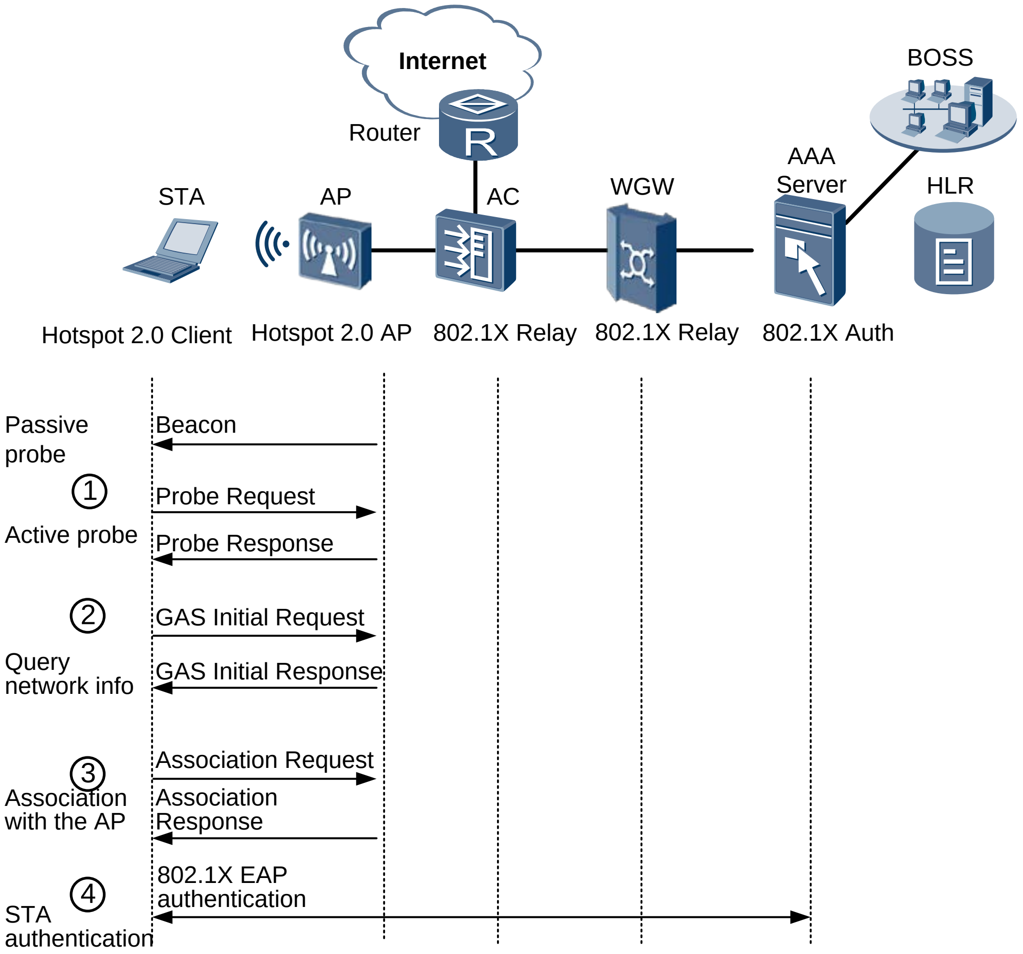
NE	Description
WGW	It functions as an AAA server to perform authentication, accounting, and authorization relay.
AAA server	It supports 802.1X and EAP-SIM/AKA/TLS/TTLS authentication. It can obtain authentication vectors and WLAN account registration information from the HLR.
HLR	It is a database used for saving user information on a mobile communication network. It also stores account registration information, mobile station location information, MSISDNs, and IMSIs.
BOSS	It provides an end-to-end operation process for carriers to process daily tasks such as the customer service, rating, charging, settlement, and dunning.

Hotspot 2.0 implements WLAN discovery and selection through 802.11u. 802.11u defines a mechanism for wireless terminals to obtain WLAN information. In local or roaming scenarios, wireless terminals can obtain WLAN information by querying Beacon frames, Probe frames, and generic advertisement service (GAS) frames. In this way, they can automatically select the optimal network to access and automatically complete access authentication.

WLAN information is transferred through GAS and ANQP.

- GAS: 802.11u defines a general mechanism for STAs and network devices to obtain network information by exchanging Request and Response messages.
- ANQP: is a network information query protocol carried on the GAS.

Figure 3-2 Hotspot 2.0 network discovery and selection



Prerequisites:

- A STA has been registered with the home service provider. The identity credential (such as the USIM/SIM card, certificate, and user name/password) and home carrier OI have been configured on the STA.
- In STA roaming scenarios, the roaming network must have been connected to the home network. Information about the home network information has been configured on the roaming network, and the home network has been configured as a roaming consortium.

1. Passive or active STA probing
   - Passive STA probing

     An AP sends a Beacon frame containing information such as the Hotspot 2.0 indication, BSS load, Internet reachability, network type, and service provider.

     When the STA receives the Beacon frame and finds that it contains the Hotspot 2.0 indication, the STA considers that the AP supports Hotspot 2.0. The STA then parses the roaming consortium field to obtain the service provider OI, and checks whether it can access the WLAN. Before accessing the WLAN, the STA can select an AP with a lighter load to access based on the BSS load.
   - Active STA probing

The STA sends a Probe Request frame containing information about the network type. The AP checks whether the network type matches the network type provided by itself. If so, the AP sends a Probe Response frame to the STA, which contains the Hotspot 2.0 indication, BSS load, Internet reachability, network type, and information about one to three service providers.

When the STA receives the Probe Response frame and finds that it contains the Hotspot 2.0 indication, the STA considers that the AP supports Hotspot 2.0. The STA then parses the roaming consortium field to obtain the service provider OI, and checks whether it can access the WLAN. Before accessing the WLAN, the STA can select an AP with a lighter load to access based on the BSS load.

2. Network information query and obtaining in STA roaming scenarios

   The STA can obtain more WLAN information by sending a GAS Initial Request message that contains information such as the list of all service providers, supported authentication modes, hotspot carriers, IP addresses, port numbers, and traffic on wired interfaces. The AP sends a GAS Initial Response message to the STA and returns the ANQP network parameters requested by the STA.

3. STA association with the AP

   The STA automatically selects a WLAN to access according to the obtained network information (such as the domain name and authentication mode), and the home network access identifier (NAI) and corresponding access credential preconfigured on the STA. The STA sends an Association Request message carrying the Hotspot 2.0 indication, and uses AES encryption and 802.1X authentication. The AP sends an Association Response message to the STA.

4. STA identity authentication

   The STA sends an 802.1X authentication request to the AC. The AC then transfers the authentication request to the AAA server/WGW for authentication. The STA also reports the NAI. The AAA server forwards the authentication request to the authentication server of the service provider in the home area based on the NAI field. After authentication succeeds, the STA accesses the WLAN.

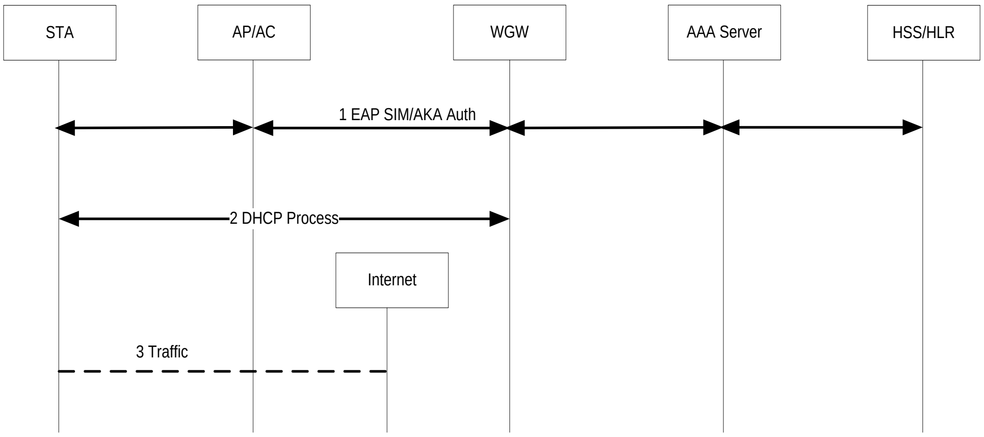
   Currently, WLANs support four authentication modes: EAP-SIM, EAP-AKA, EAP-TLS, and EAP-TTLS.

3.2 User Registration

In different WLAN planning and business models, carriers select different traffic distribution modes. For example, WLAN users can directly register or register through a WGW. This section describes the detailed service processes.

3.2.1 Direct Registration

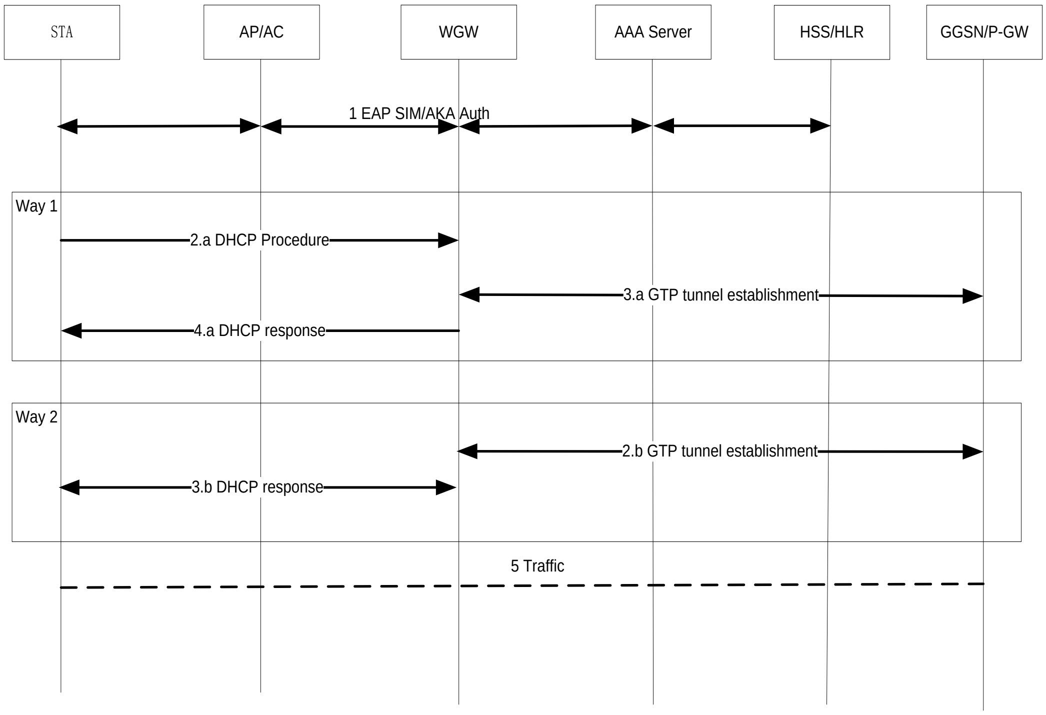
Figure 3-3 Direct registration



1. A STA accesses a WLAN through SSID authentication in 802.1X or EAP-SIM/AKA mode. EAP-SIM/AKA authentication is performed among the STA, AC, and AAA server. In the preceding figure, the WGW functions as an AAA proxy to forward RADIUS packets between the AC and AAA server.
2. After the STA authentication succeeds, the STA triggers the Dynamic Host Configuration Protocol (DHCP) process. The WGW functions as a DHCP server to assign an IP address to the STA and informs the STA of the default gateway IP address (the DHCP server capability can also be provided by other devices).
3. After the STA authentication succeeds, service packets of the STA are locally forwarded by the AP or centrally by the AC to the Internet.

3.2.2 Proxy Registration Through a WGW

Figure 3-4 STA access to the Internet through a WGW



A STA accesses a WLAN through SSID authentication in 802.1X or EAP-SIM/AKA mode. EAP-SIM/AKA authentication is performed among the STA, AC, AAA server, HLR, and HSS. The WGW serves as an AAA proxy to forward RADIUS packets between the AC and AAA server. During the forwarding process, the WGW obtains the STA's mobile network identifier (such as the IMSI and MSISDN). The WGW establishes a GTP tunnel with the Gateway GPRS support node (GGSN)/Packet Data Network gateway (P-GW) in two ways.

GTP tunnel establishment way 1:

1. The STA triggers the DHCP process. The WGW functions as a DHCP server to process DHCP packets.
2. The WGW selects a GGSN/P-GW based on the STA's subscription data or default APN information, and establishes a GTP tunnel with the GGSN/P-GW. The GGSN/P-GW records the Packet Data Protocol (PDP) context of the STA, assigns an IP address to the STA, and returns a Response message.
3. The WGW, functioning as a DHCP server, returns the STA's IP address assigned by the GGSN/P-GW and the default gateway address.

GTP tunnel establishment way 2:

1. After the STA authentication succeeds, the WGW selects a GGSN/P-GW based on the STA's subscription data or default APN information, and establishes a GTP tunnel with the GGSN/P-GW. The GGSN/P-GW records the PDP context of the STA, assigns an IP address to the STA, and returns a Response message.
2. The STA triggers the DHCP process. The WGW, functioning as a DHCP server, returns the STA's IP address assigned by the GGSN/P-GW and the default gateway address.

3. Service packets of the STA are sent through packets switching (PS), and data packets between the AP/AC and WGW are sent through the following tunnels:
   - EoGRE tunnel: established between the AC and WGW
   - Soft GRE tunnel: established between the AP and WGW

3.3 Charging Process

WLANs can interwork with carriers' AAA servers through the RADIUS protocol or WGW proxy (RADIUS proxy) to implement charging.

Specific charging capabilities are provided by the online charging system (OCS) and charging gateway functionality (CGF) interworked with AAA servers.

3.4 Roaming Switchover

User experience varies when different services switch on air interfaces between WLANs and 3GPP networks.

- HTTP browsing

  In request/response mode, users need to request data from servers again to refresh web pages. Therefore, roaming switchover does not affect service experience.
- Video services

  Generally, cache and resumable download mechanisms are provided. After a STA switches between a WLAN and a 3GPP network, currently cached videos can be continuously played and a new wireless service connection is established. Therefore, user experience is not affected.
- Interactive services such as online game, voice, and online video services

  Most interactive services are TCP connection services. When a STA performs a switchover, the STA proactively initiates a TCP disconnection and reconnection due to a long switchover delay. As a result, services are interrupted, leading to poor user experience.

Ensuring service continuity during network switchovers is significant for real-time interactive services.

The following factors are critical for implementing network switchovers:

- STAs establish connections on the target side and then delete original wireless connections during the switchover process. This avoids TCP disconnections.

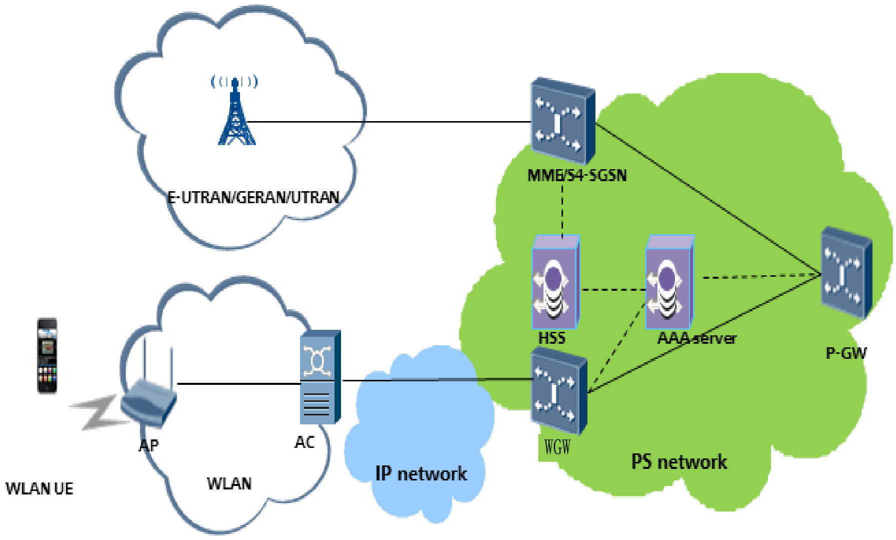
NOTE

Currently, commercial terminals including smartphones, tablets, and laptops do not support this feature.

- On the network side, the same IP address must be assigned to a STA before and after switchover.

  The specific mechanism is as follows: A STA sets up an IP connection before switchover, and the PGW IP address is registered with the HSS on the network side. When the STA switches to the target side, the P-GW IP address is delivered to the access gateway on the target side with the subscription data. The access gateway then establishes a connection with the P-GW. The P-GW assigns the same IP address to the STA. To implement this mechanism, the network side must be upgraded to an EPC network.

Figure 3-5 Network structure for switchovers



4 Features of Huawei WLAN Solution

Huawei WLAN Solution has the following features:

- Interworking and networking with cellular network devices of multiple vendors

  Huawei WLAN products have been successfully interworked with Huawei cellular network devices (such as the UGW9811 and vUGWs).

  Huawei WLAN products can also interwork with WGWs such as Huawei's virtual evolved packet data gateways (vePDGs) (providing non-3GPP EPC network access) and Cisco's intelligent wireless access gateways (IWAGs) (integrated WGWs used on cellular networks).

- Flexible user service routing

  Huawei WLANs provide four solutions for traffic routing to the Internet.

- Support for four EAP user authentication modes

  For users' Wi-Fi services, Huawei WLANs support four authentication modes: EAP-SIM, EAP-AKA, EAP-TLS, and EAP-TTLS.

  In addition, Huawei WLANs support Portal, MAC address, and wired equivalent privacy (WEP) authentication.

NOTE

EAP-AKA/SIM authentication: It is based on 802.1X. SIM cards of STAs are used as credentials for authentication. This authentication mode does not require user participation. Therefore, user experience is good.

Protected EAP (PEAP) authentication: A tunnel is established between a PEAP client and the authentication server to perform EAP security authentication. The authentication process can be divided into two phases:

1. The PEAP client and authentication server use certificates to authenticate each other, and establish a TLS tunnel.
2. EAP communication is implemented through TLS. User names and passwords are used as credentials for authentication. (Users need to complete configuration on STAs.)
   This authentication mode requires user participation in configuration on PEAP client. Users do not need to participate in the subsequent WLAN access process. Therefore, user experience is good.

Portal authentication: It is an HTTP-based authentication mode. User names and passwords are used as credentials for authentication. Users need to enter their user names or passwords for authentication.

MAC address authentication: It is essentially Portal authentication. The difference is that users need to manually enter the user name and password to connect to a WLAN for the first time. Subsequent Internet access authentication is automatically performed. Users do not need to enter any information. Therefore, user experience is good.

- Service innovation

For service innovation of carriers, a WLAN is the best wireless access pipe with the highest deployment efficiency and best compatibility. WLANs support multi-network convergence, IoT, and customer flow analysis (location service, content push, and advertisements).

Huawei WLAN Solution has the following scenario constraints:

- Huawei WLAN devices cannot use the same unified NMS as Huawei cellular network devices.

  The unified NMS for Huawei cellular network devices is the U2000, while the NMS for Huawei WLAN devices is eSight.
- It does not support Lightweight Extensible Authentication Protocol (LEAP), EAP-fast, or EAP-AKA authentication.
- It does not support WISPr 2.0.

  Currently, a Huawei WLAN AC can manage a maximum of 2048 APs.

5 Acronyms and Abbreviations

Acronym or Abbreviation	Full Name
AAA	Authentication, Authorization, and Accounting
AC	Access controller
AP	Access point
APN	Access point name
BG	Border gateway
DHCP	Dynamic Host Configuration Protocol
EAP	Extensible Authentication Protocol
GGSN	Gateway GPRS support node
GRE	Generic Routing Encapsulation
GTP	GPRS Tunneling Protocol
HEIW	Huawei EPC Integrated WLAN Solution
HLR	Home location register
HSS	Home subscriber server
IMSI	International mobile subscriber identity
IPSec	Internet protocol security
MAC	Media Access Control
NAI	Network access identifier
OMA DM	Open Mobile Alliance Device Management
WGW	Wi-Fi gateway
P-GW	PDN gateway
PS	Packet switching

Acronym or Abbreviation	Full Name
RADIUS	Remote Authentication Dial-In User Service