Huawei CloudCampus WLAN Authentication and Encryption

Technology White Paper

HUAWEI

Executive Summary

802.11-based WLAN provides increasingly higher wireless access bandwidth, so more users start to use WLAN, which in turn have high requirements for WLAN security. Protecting the security of confidential data and user privacy is a top concern of many WLAN users.

This document describes Huawei WLAN authentication and encryption solutions in terms of general analysis, principles, and application scenarios.

Contents

1 Overview

1.1 Background

Radio signals are transmitted in a free space and can be received by any WLAN-capable devices. Security of radio signals has always been a concern since the inception of WLAN. As such, related authentication and encryption technologies keep evolving and improving for better WLAN security.

To date, the WLAN system has boasted a series of security mechanisms applying to various scenarios such as home WLANs, enterprise WLANs, campus WLANs, and large-scale carrier WLANs. In particular, a holistic set of authentication and encryption technologies are available to protect the security of users' wireless data.

1.2 Technical Implementation

WLAN access security includes the security attribute configuration, encryption and decryption of wireless packets, management of keys, and other functions.

WLAN security features primarily involve the following four aspects:

- STA identity authentication: Only authenticated STAs can be associated with the WLAN Access Points (APs).
- User identity authentication and encryption: Users are differentiated and their access rights are controlled before they connect to the network. They can access only limited network resources during link authentication, and are granted access to all network resources only after being authenticated.
- Authorization: Authentication is used to check whether the identity of a user who attempts to access the network is valid. In contrast, authorization is used to specify the network access rights that the identity-authenticated user has, that is, what resources the user can access.
- Packet encryption: Management packets and data packets are encrypted, and only specified devices can successfully decrypt the received packets. Other WLAN devices can receive data packets, but they fail to decrypt these packets because they do not have the required keys. This mechanism protects WLAN data.

1.3 Customer Benefits

WLAN access security features prevent wireless data from being intercepted by unauthorized users and ensure WLAN security. WLAN security is protected mainly in the following two ways:

- Prevents unauthorized users from accessing WLAN resources.
- Ensures data integrity and transmission confidentiality.

These protection measures make user and network data securer.

2 Implementation

A WLAN is built to provide network access services for wireless users, enabling them to access network resources, for example, accessing the Internet.

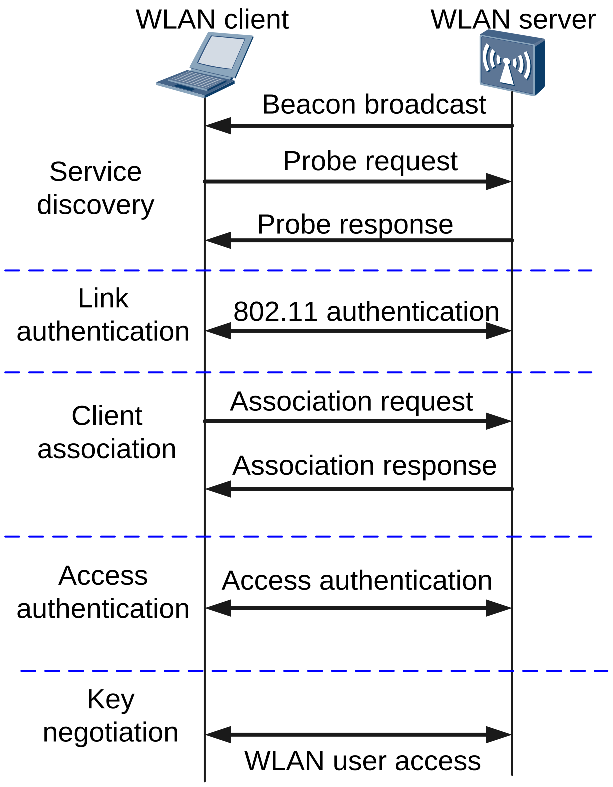
If access authentication is not required for the WLAN service, a STA can use the WLAN service directly. If access authentication is required, the WLAN server triggers access authentication, and a STA can access the WLAN service only after it is authenticated.

2.1 Introduction

A typical WLAN has two roles: STA and WLAN server. Of the two roles, a STA is a host with a wireless Network Interface Card (NIC), while a WLAN server is an access point (AP).

Figure 2-1 shows the WLAN access process.

Figure 2-1 WLAN access process



1. WLAN service discovery

   Before using any network, we must discover it first. Discovering a wired network is relatively easy, as long as we can find the network cable or the telecommunications outlet on the wall. However, to connect to a WLAN, a STA has to discover the WLAN service first. The WLAN service discovery stage is detailed as follows:

   - A WLAN server broadcasts a Beacon frame to advertise the WLAN service that it provides. A WLAN client locates the WLAN service based on the Beacon frame.
   - The client sends a probe request with the specified service set ID (SSID) or a broadcast probe request without an SSID to check whether the specified service exists. If yes, the WLAN server sends a probe response to the client.

   After the client discovers the WLAN service, the client and server enter the link authentication stage.

2. Link authentication

   Link authentication is the start point for a STA to connect to a wireless network, and also a way for a STA to inform the network of its own identity. A STA can connect to the network only after passing 802.11 link authentication.

   IEEE 802.11 defines two authentication modes: open system authentication and shared key authentication. Authentication packets are exchanged between the WLAN server and client during 802.11 link authentication.

3. Client association

   After being authenticated, a STA can connect to or reconnect to an AP to obtain the permission to access all network resources.

During the WLAN service discovery stage, the STA has already obtained the current service configurations and parameters. Typical parameters include as the access authentication algorithm and encryption key carried in the Beacon frame and probe response message sent by the WLAN server.

In the association stage, the association or re-association request sent by the STA carries not only the STA's own parameters, but also the parameters that the STA selects according to the service configurations (including the transmission rate, channel, QoS capabilities, access authentication algorithm, and encryption algorithm).

After link negotiation is complete, an 802.11 link is set up between the WLAN server and the STA. At this moment, if access authentication is not enabled, the STA already can access the WLAN. If access authentication is enabled, the WLAN server subsequently performs access authentication on the STA.

4. Access authentication

   Access authentication ensures network security. WLAN supports 802.1X authentication, pre-shared key (PSK) authentication, Portal authentication, and MAC address authentication.

   Of these, PSK authentication is dedicated to WLAN users only, while the other authentication modes can be used for both WLAN users and wired access users.

   If the Wi-Fi Protected Access (WPA) or WPA2 security protocol is used, the STA must negotiate the Extensible Authentication Protocol over LAN (EAPOL)-Key with the WLAN server. As defined in the WLAN protocol, WPA must be used together with 802.1X authentication and PSK authentication. Specifically, the access authentication algorithm is determined during 802.11 link negotiation; after link negotiation succeeds, the WLAN server triggers access authentication and negotiates a key with the STA; after the key is negotiated, the STA can access the WLAN.

5. Key negotiation

   Key negotiation strengthens data security. IEEE 802.11i and 802.1X define the EAPOL-Key mechanism, that is, a 4-way handshake mechanism, to ensure data security on the WLAN. This mechanism achieves key negotiation between the WLAN server and STAs. The negotiated key is used to encrypt and decrypt data transmitted on 802.11 links.

   If a WLAN provides the WPA and robust security network (RSN) service, EAPOL-Key negotiation is required. Key negotiation is a part of access authentication. The WLAN server accepts packets sent from the STA only after EAPOL-Key negotiation succeeds.

   WLAN key negotiation includes 4-way handshake and group key negotiation, during which APOL-Key packets are exchanged between a STA and a server. The 4-way handshake mechanism negotiates the key used by the STA for unicast data packets, while the group key handshake mechanism enables the server to notify all STAs of the keys used for broadcast and multicast packets.

6. Data encryption

   After a STA is authenticated and authorized to access a WLAN, the WLAN must use a mechanism to protect data of the STA from tampering and eavesdropping. Ensuring data privacy on WLANs is a challenge. Encryption protocols are often used to address this challenge. Only data of STAs that have keys and are authenticated is protected during data transmission.

Table 2-1 Authentication and encryption modes supported by Huawei WLAN solutions

Type	Feature
WEP	• Wired equivalent privacy (WEP) was included as a part of the IEEE 802.11 standard ratified in September 1999. WEP uses Rivest Cipher 4 (RC4) for confidentiality. • WEP uses the RC4 algorithm to encrypt packets exchanged between an AP and a STA. The encryption key cannot automatically change, and the stream cipher is easy to decipher. Therefore, WEP is seldom used.
WPA/WPA2-PSK	• Wi-Fi Protected Access (WPA) is a commercial standard promoted by the Wi-Fi Alliance to substitute for the insecure WEP standard before IEEE 802.11i was published. WPA uses the Temporal Key Integrity Protocol (TKIP) algorithm. • WPA2 is a common shorthand for the full IEEE 802.11i standard and uses the Counter Mode with CBC-MAC Protocol (CCMP) algorithm to encrypt data. • In WPA/WPA2-PSK authentication mode, a pre-shared key needs to be set on each WLAN node such as an AP, a wireless router, and a wireless network adapter. A STA can access the WLAN if its shared key is the same as that configured on the AP. The shared key is used only for authentication but not for encryption; therefore, it will not bring such security risks as the 802.11 pre-shared key authentication. Currently, AES CCMP is often used to encrypt the transmitted data. • No client needs to be installed. • WPA and WPA2-PSK are mainly used in home individuals or public places that do not have high requirements for security.
802.1X	• IEEE 802.1X defines only the identity authentication framework, but not a complete standard. IEEE 802.1X requires other protocols for authentication, and the supported authentication modes include EAP, LEAP, EAP-TLS, EAP-TTLS and PEAP. • 802.1X is a Layer 2 protocol and does not need to reach Layer 3. A STA and server mutually authenticate each other, which well supports multicast. • The commonly used iOS, Android, and Windows operating systems support 802.1X. No client needs to be installed. • 802.1X authentication has a high security level and is widely used on enterprise networks. Typically, an enterprise AD domain is used as the authentication database.
WAPI	• WLAN Authentication and Privacy Infrastructure (WAPI) is a Chinese National Standard for WLANs (GB15629.11). It includes a new WAPI security mechanism that consists of WLAN Authentication Infrastructure (WAI) and WLAN Privacy Infrastructure (WPI). • WAPI provides two identity authentication and key management modes: certificated-based mode (WAPI-CERT) and pre-shared key-based mode (WAPI-PSK).

Type	Feature
	• WAPI uses three-factor authentication, while WPA uses two-factor authentication. WAPI uses the CCMP algorithms, while WPA uses the SMS4 algorithms. • WAPI is a Chinese national standard, so it is widely used in China and seldom used outside of China.
Portal	• Portal authentication is also called web authentication or DHCP + web authentication. It uses standard web browsers such as Internet Explorer and does not require the installation of any special client software. • Before being authenticated, the user terminal has to obtain an IP address. Layer 3 devices such as routers can be deployed between the user terminal and access server. In this case, the access server cannot bind the MAC address and IP address of the terminal because the packet sent to the access server may not contain the MAC address of the user terminal. • The user names and passwords sent by user terminals are easy to be intercepted, resulting in a low security level. • Due to its convenience, Portal authentication is widely used on carrier networks. Enterprises often use it for guest logins.
MAC	• In MAC address authentication, a client sends its MAC address as the identity credentials to an access device for authentication. • Users do not need to enter their user names and passwords to access the network. As such, MAC address authentication is widely used in scenarios where high security is not required.

In terms of WLAN security, Huawei specializes in offering multiple authentication combinations tailored for customers in diverse scenarios. For example, on a carrier WLAN network, open system + Portal authentication is used. To connect to the carrier WLAN network, a user has to enter the correct user name and password on the authentication web page pushed to the user by the Portal server. If a user selects the MAC address binding function advertised on the authentication web page, MAC address authentication is used for the next connection and the user does not need to enter the user name and password.

2.2 STA Authentication

IEEE 802.11 requires that STAs pass link authentication before connecting to a WLAN. During link authentication, an AP and STA do not exchange or verify any encryption keys or authenticate the identity of each other. Therefore, link authentication is actual a process to initiate a handshake between an AP and STA.

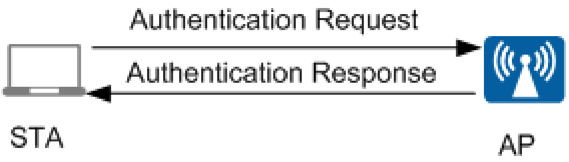
There are two STA authentication modes: open system authentication and shared key authentication. Some products support MAC address filtering that filters out STAs with unauthorized MAC addresses.

2.2.1 Open System Authentication

Open system authentication is the mandatory authentication mode defined by IEEE 802.11. In this mode, an AP identifies STAs by their MAC addresses, and it does not authenticate the STAs. Therefore, all the STAs that conform to IEEE 802.11 can access the WLAN. Open system authentication applies to carrier-deployed large-scale WLANs with a large number of users.

Open system authentication consists of only two steps, as shown in Figure 2-2. An AP only checks whether an STA uses the same authentication mode as itself and does not check the WEP encryption key of the STA.

Figure 2-2 Open system authentication



The open system authentication process is detailed as follows:

1. The STA sends an authentication request to the AP.
2. The AP responds with an authentication success packet. After receiving the authentication success packet, the STA registers with the AP.

The advantages and disadvantages of open system authentication are as follows:

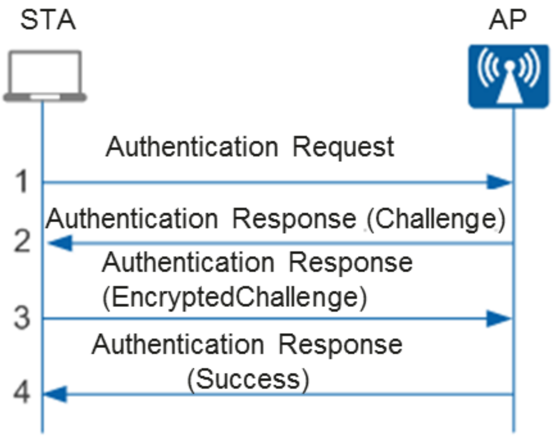
- Advantages: Open system authentication is a basic authentication mechanism. It can be used on wireless devices that do not support complex authentication algorithms. This authentication mode allows STAs to connect to a WLAN quickly.
- Disadvantages: Open system authentication cannot distinguish hacker STAs from authorized STAs. When this authentication mode is used, any users can connect to a WLAN if they know the SSID of the WLAN.

2.2.2 Shared Key Authentication

Shared key authentication is another link authentication mechanism.

Shared key authentication requires that an AP and a STA use the same key (static WEP key) and is implemented based on WEP encryption. As shown in Figure 2-3, shared key authentication consists of four steps. The last three steps complete a WEP encryption and decryption process, which is similar to the process of Challenge Handshake Authentication Protocol (CHAP). Verification of the WEP key ensures that a STA has the same encryption key as the AP it wants to associate with.

Figure 2-3 Shared key authentication



The shared key authentication process is detailed as follows:

1. The STA sends an authentication request to the AP.
2. The AP generates a random challenge and sends it to the STA.
3. The STA copies the received challenge to a new message, uses its key to encrypt the message, and sends the encrypted message to the AP.
4. After receiving the message from the STA, the AP decrypts it with its key and compares the decrypted character string with the original character string sent to the STA.
   - If the character strings are the same, the STA and AP have the same key and the STA is successfully authenticated.
   - If the character strings are different, the STA fails to be authenticated.

The advantages and disadvantages of shared key authentication are as follows:

- Advantages: Shared key authentication is more secure than open system authentication because data is encrypted.
- Disadvantages:
  - This authentication mode has a poor scalability because a long key string must be configured on each device.
  - This authentication mode is not secure enough. A static key is used until the next key is configured. If a key is used for a long time, malicious users can decipher the key by collecting data encrypted using this key. This threatens WLAN security. Static WEP keys are easy to decipher.

WEP authentication is widely used in the early stage of WLAN construction. It will be detailed in the subsequent sections in this document. When open system authentication is used, STAs do not need to be authenticated. When shared key authentication is used, STAs need to be authenticated. No matter which authentication mode is used, we can select whether to enable data encryption.

2.2.3 MAC Address Filtering

On a WLAN, blacklist or whitelist can be configured to filter access from STAs based on specified rules. The blacklist or whitelist allows authorized STAs to connect to the WLAN and rejects access from unauthorized STAs.

- Whitelist

A whitelist contains MAC addresses of STAs that are allowed to connect to a WLAN. After the whitelist function is enabled, only the STAs in the whitelist can connect to the WLAN, and access from other STAs is rejected.

- Blacklist

A blacklist contains MAC addresses of STAs that are not allowed to connect to a WLAN. After the blacklist function is enabled, STAs in the blacklist cannot connect to the WLAN, and other STAs can connect to the WLAN.

MAC address filtering is more an access control method than an authentication mode. It is not recommended that you use only the MAC authentication because MAC addresses are easy to be forged or copied. Some out-of-date devices still use only MAC authentication because they do not support better security mechanism.

2.3 User Identity Authentication and Encryption

Compared to simple STA identity authentication, user identity authentication has the following advantages:

- Only limited network resources are accessible to users during link authentication, and they are granted access to all network resources only after being authenticated.
- Users are differentiated and their access rights are controlled before they connect to the network.
- Link-layer authentication apply to all network-layer protocols.

User identity authentication involves the following authentication modes:

- WPA/WPA2-PSK authentication
- WPA/WAP2-PPSK authentication
- 802.1X authentication
- WAPI authentication
- Portal authentication
- MAC address authentication

2.3.1 WPA/WPA2-PSK Authentication

WPA/WPA2-PSK is an authentication and encryption mode that uses the pre-shared keys for authentication and regards the pre-shared keys as the temporal keys for pair main key (PMK) negotiation.

In WPA/WPA2-PSK authentication mode, a key needs to be pre-configured on a STA. The key validity is checked by a 4-way handshake between the STA and AP or between the STA and WLAN AC.

WPA/WPA2-PSK uses open system authentication in the authentication and association processes between the STA and AP. After the STA is associated with the AP, they perform a 4-way handshake to negotiate keys.

A 4-way handshake is performed to generate the pairwise transient key (PTK) and group temporal key (GTK). The PTK is used to encrypt unicast radio packets, while the GTK is used to encrypt multicast and broadcast radio packets.

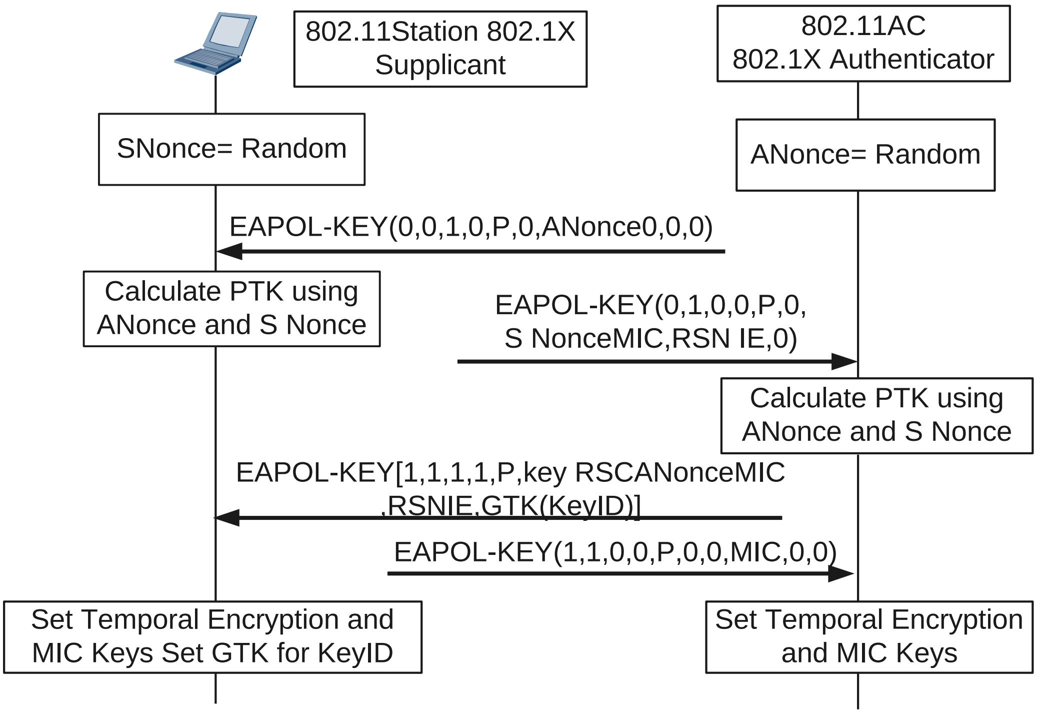
IEEE 802.l1i defines two key hierarchies: the pairwise key hierarchy that describes all keys used by a pair of devices, and the group key hierarchy that describes keys shared by all devices.

In the pairwise key hierarchy, the Temporal Key Integrity Protocol (TKIP) derives four 128-bit temporal keys from the master key: Extensible Authentication Protocol over LAN Key (EAPOL-Key) encryption key, EAPOL-Key integrity key, data encryption key, and data integrity key. The EAPOL-Key encryption key and EAPOL-Key integrity key are used to encrypt and check integrity of EAPOL-Key frames transmitted between a WLAN client and a WLAN server. The data encryption key and data integrity key are used to encrypt data transmitted between the client and server and prevent data from being modified. The CTR with CBC-MAC Protocol (CCMP) derives only three temporal keys from the master key because it integrates the data encryption key and data integrity key into one key.

In the group key hierarchy, TKIP derives an encryption key and an integrity key from the 128-bit group master key (GMK). The WLAN client and server use the two keys to encrypt and check integrity of multicast data. CCMP integrates the encryption key and integrity key into one key to protect multicast data.

4-way unicast EAPOL-Key negotiation

Figure 2-4 4-way unicast EAPOL-Key negotiation


802.11Station 802.1X Supplicant
802.11AC 802.1X Authenticator
SNonce= Random
ANonce= Random
EAPOL-KEY(0,0,1,0,P,0,ANonce0,0,0)
Calculate PTK using ANonce and S Nonce
EAPOL-KEY(0,1,0,0,P,0, S NonceMIC,RSN IE,0)
Calculate PTK using ANonce and S Nonce
EAPOL-KEY[1,1,1,1,P,key RSCANonceMIC ,RSNIE,GTK(KeyID)]
EAPOL-KEY(1,1,0,0,P,0,0,MIC,0,0)
Set Temporal Encryption and MIC Keys Set GTK for KeyID
Set Temporal Encryption and MIC Keys

As shown in Figure 2-4, the 4-way unicast EAPOL-Key negotiation process is as follows:

1. The WLAN server (authenticator) sends an EAPOL-Key frame containing an ANonce to the WLAN client (supplicant). Nonce is a random value used to prevent replay and includes ANonce and SNonce. The WLAN AC randomly generates the ANonce and sends it to the STA, while the SNonce is randomly generated after the STA receives the ANonce.
2. After receiving the EAPOL-Key frame, the WLAN client calculates a PTK using the PMK, ANonce, SNonce, its own MAC address, and the WLAN server's MAC address. The WLAN client then sends an EAPOL-Key frame to the WLAN server. The EAPOL-Key frame contains the SNonce, robust security network (RSN) information element, and message integrity code (MIC).
3. The WLAN server calculates a PTK using the PMK, ANonce, SNonce, its own MAC address, and the WLAN client's MAC address. It then validates the MIC to check whether the client's PMK is the same as its own PMK.
4. The WLAN server sends an EAPOL-Key frame containing the ANonce, RSN information element, MIC, and encrypted GTK to the WLAN client, instructing the WLAN client to install the encryption keys.
5. The WLAN client sends an EAPOL-Key frame to the WLAN server to confirm that the encryption keys are installed. The WLAN server starts to install the temporal keys after receiving the EAPOL-Key frame.

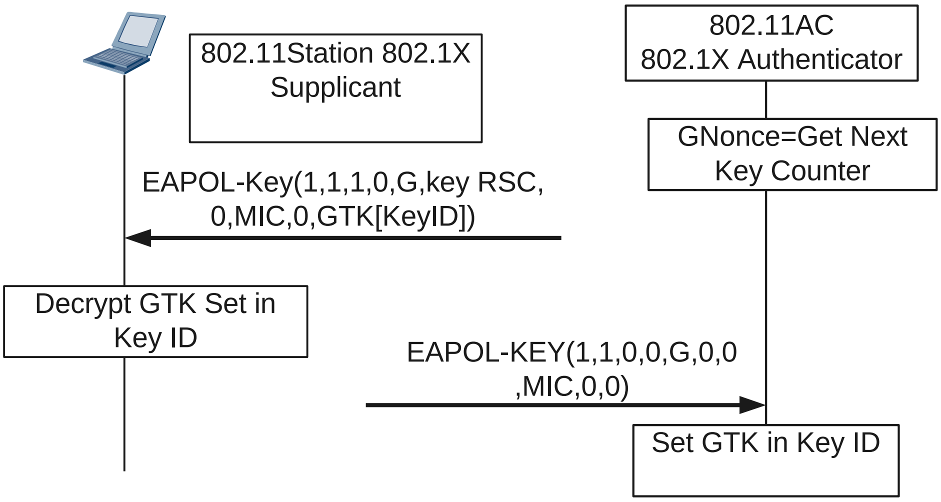
2-way multicast EAPOL-Key negotiation

During 2-way multicast EAPOL-Key negotiation, the WLAN server sends an EAPOL-Key frame to notify the WLAN client of the encryption key, and the WLAN client sends an EAPOL-Key frame to confirm that the encryption key is installed.

After a PTK is generated and temporal keys are installed in the 4-way handshake process, the WLAN client and server start the 2-way handshake. The WLAN server calculates the GTK, encrypts the GTK with the unicast key of the client, and sends the encrypted GTK to the client. The WLAN client uses the temporal keys obtained in the 4-way handshake to decrypt the GTK.

The 2-way handshake may not be triggered after a new WLAN client goes online. The GTK can be obtained from the EAPOL-Key frame that the WLAN server sends in step 4 in the 4-way handshake. If the GTK is not obtained from the EAPOL-Key frame, a 2-way handshake is performed. A 2-way handshake is also performed when the GTK needs to be updated.

Figure 2-5 2-way multicast EAPOL-Key negotiation


802.11Station 802.1X Supplicant
802.11AC 802.1X Authenticator
GNonce=Get Next Key Counter
EAPOL-Key(1,1,1,0,G,key RSC, 0,MIC,0,GTK[KeyID])
Decrypt GTK Set in Key ID
EAPOL-KEY(1,1,0,0,G,0,0 ,MIC,0,0)
Set GTK in Key ID

As shown in Figure 2-5, the 2-way multicast EAPOL-Key negotiation process is as follows:

1. The WLAN server calculates the GTK, encrypts it with the unicast key, and sends an EAPOL-Key frame with the encrypted GTK to the WLAN client.
2. After the WLAN client receives the EAPOL-Key frame, it validates the MIC, decrypts the GTK, installs the GTK, and sends an EAPOL-Key frame to the WLAN server.
3. After the WLAN server receives the EAPOL-Key frame, it validates the MIC and installs the GTK.

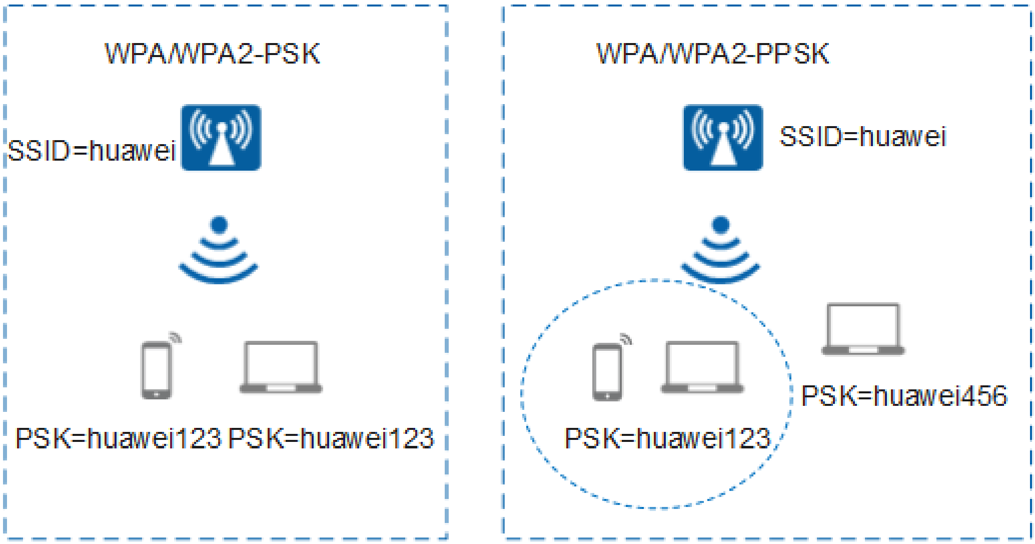
2.3.2 WPA/WAP2-PPSK Authentication

WPA/WPA2-PPSK has the same authentication and association processes between the STA and AP as well as the 4-way key negotiation process as WPA/WPA2-PSK.

WPA/WPA2-PPSK inherits the advantages of WPA/WPA2-PSK, such as easy deployment, and adds the flexibility of providing the pre-shared keys for different WLAN clients, effectively enhancing network security.

WPA/WPA2-PSK requires that all WLAN clients connecting to a single SSID have the same key, which may result in security vulnerabilities. WPA/WPA2-PPSK, however, allows each WLAN client connecting to a single SSID to have a different key, and different users are granted different authorizations. Additionally, in WPA/WPA2-PPSK mode, a user who owns multiple WLAN clients can use the same PPSK account to connect to the network.

Figure 2-6 Comparison between WPA/WPA2-PSK and WPA/WPA2-PPSK



WPA/WPA2-PPSK has the following characteristics:

- Each WLAN client connecting to a single SSID has a different key.
- Configuration and deployment are simple.
- A user who owns multiple WLAN clients can use the same PPSK account to connect to the network.
- PPSK users are bound to user groups or authorization VLANs, and different PPSK users are granted different authorizations.

2.3.3 802.1X Authentication

The 802.1X protocol derived from the development and application of WLAN. Users need to be authenticated and user access needs to be controlled because of the mobility and openness of WLANs. In this way, spectrum and bandwidth resources are efficiently used and network security is ensured. The 802.1X protocol can also be used on wired LANs to authenticate users and control user access.

802.1X is a port-based network access control protocol which defines an authentication process framework that supports multiple authentication protocols. All authentication protocols used in 802.1X authentication use EAP to encapsulate protocol packets. That is, 802.1X only controls the authentication process and is an access authentication means, but specific authentication requires the use of other authentication protocols.

802.1X controls user access based on access ports of a LAN access device. User devices connected to a port can access resources on the LAN only after being authenticated.

802.1X authentication is widely used on enterprise networks and carrier networks such as 3G networks and WLANs because of the following advantages:

- Secure and reliable: EAP-TLS, EAP-PEAP, or others can be used with 802.1X on a WLAN to implement dynamic distribution of certificate keys, preventing security loopholes on the WLAN.
- Easy to implement and flexible application: 802.1X authentication can be implemented in the existing AAA authentication network architecture and existing RADUIS devices can be reused. This is easy to implement and flexible to control authentication granularity. 802.1X authentication can be used flexibly to authenticate a single user, user groups, or access devices.
- Industry standards: Both 802.1X and the Ethernet standard are IEEE standards, so 802.1X can seamlessly integrate with the Ethernet technologies. Clients running the Windows, Linux, iOS, and Android operating systems support the 802.1X protocol.

802.1X authentication using EAP-TLS

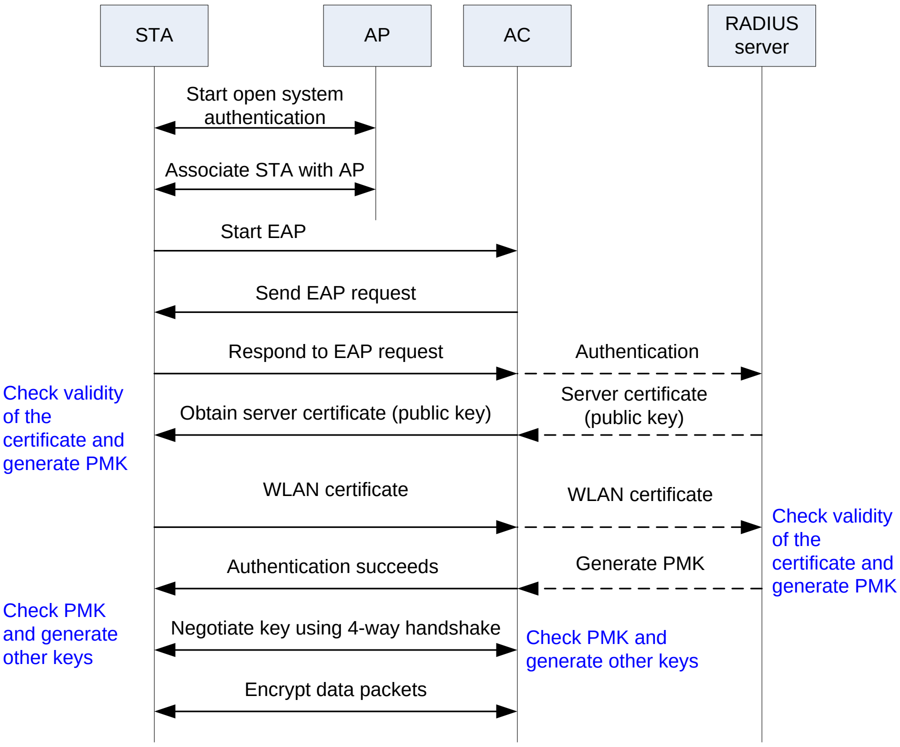
EAP-TLS uses Transport Layer Security (TLS) to ensure secure communication and data transfer. TLS is developed by the IETF to replace the Secure Socket Layer (SSL) protocol and can protect data from eavesdropping and tampering. EAP-TLS uses Public Key Infrastructure (PKI) to secure communication with an authentication server. PKI has the following requirements:

- A STA must obtain a certificate so that it can be authenticated by an AAA server.
- The AAA server must have a certificate so that STAs can verify the identity of the server.
- A certificate authority (CA) server must issue certificates to the AAA server and STAs.

During EAP-TLS authentication, a STA associates with an AP through open system authentication. Before the STA is authenticated by the RADIUS server, the AP restricts or rejects all traffic from the STA except EAP traffic.

Figure 2-7 shows the process for 802.1X authentication using EAP-TLS.

Figure 2-7 802.1X authentication using EAP-TLS


STA
AP
AC
RADIUS server
Start open system authentication
Associate STA with AP
Start EAP
Send EAP request
Respond to EAP request
Authentication
Check validity of the certificate and generate PMK
Obtain server certificate (public key)
Server certificate (public key)
WLAN certificate
WLAN certificate
Check validity of the certificate and generate PMK
Authentication succeeds
Generate PMK
Check PMK and generate other keys
Negotiate key using 4-way handshake
Check PMK and generate other keys
Encrypt data packets

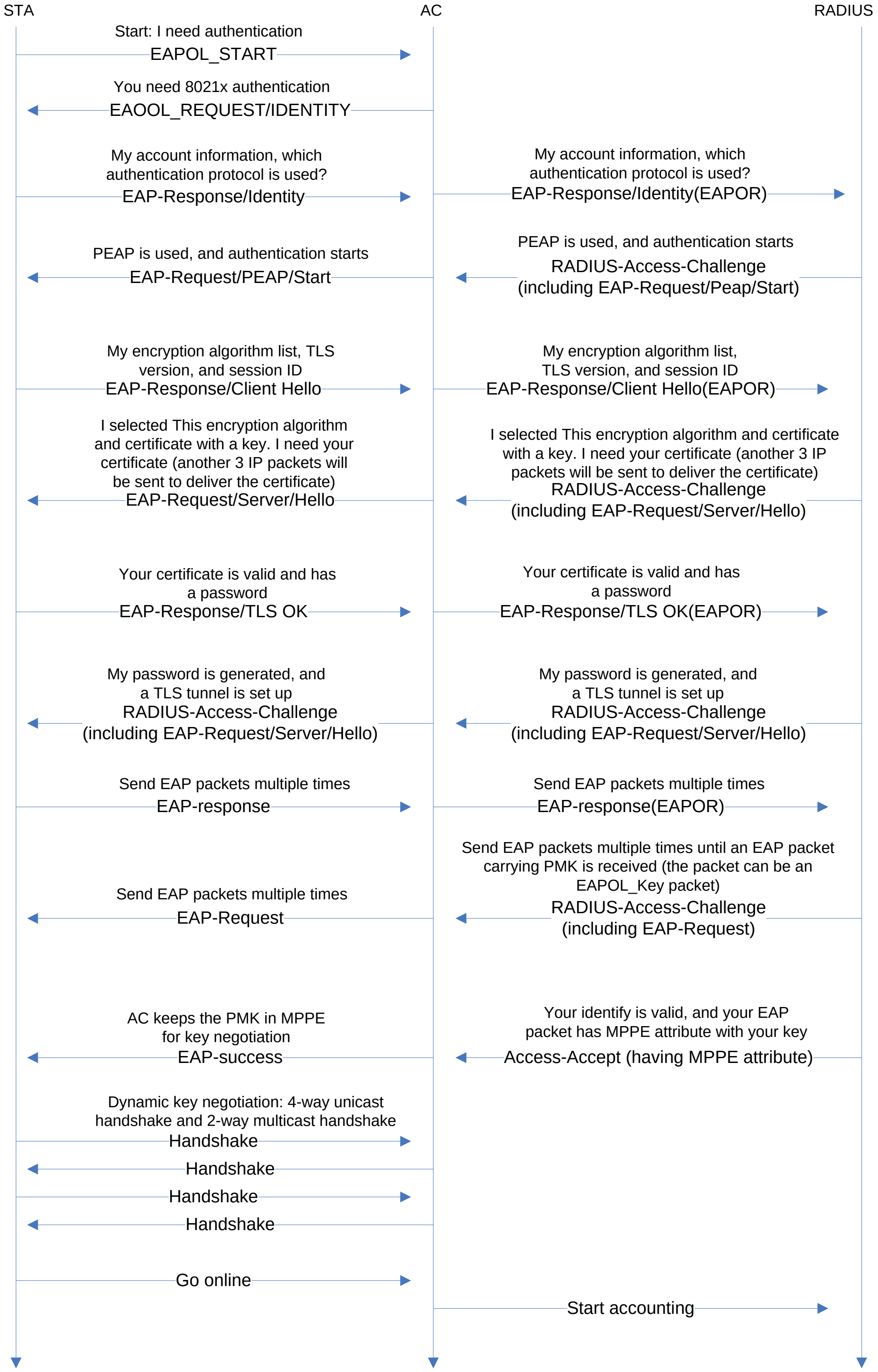
802.1X authentication using EAP-PEAP

When 802.1X authentication is used on WLANs, EAPs in message digest 5 (MD5) are not used; instead, protected EAPs such as EAP-PEAP, EAP-TLS, and EAP-SIM are used. EAP-PEAP is the most commonly used one. EAP-PEAP was jointly developed by Microsoft, Cisco, and RAS Security, and is supported by Windows operating systems by default.

On large-scale enterprise networks, EAP-PEAP is typically used. TLS negotiation in EAP-PEAP authentication is the same as that in EAP-TLS authentication. During TLS negotiation, a client and a server authenticate each other or the client authenticates the server. After a successful authentication, the client and server establish a TLS tunnel. Then the client and server complete user authentication by exchanging authentication data over the TLS tunnel. Currently, PEAP can use only EAP for authentication, whereas EAP-TLS can use not only EAP, but also other user authentication modes such as PAP and CHAP.

Figure 2-8 shows the process for 802.1X authentication using EAP-PEAP.

Figure 2-8 802.1X authentication using EAP-PEAP


STA
AC
RADIUS
Start: I need authentication
EAPOL_START
You need 8021x authentication
EAOOL_REQUEST/IDENTITY
My account information, which authentication protocol is used?
EAP-Response/Identity
My account information, which authentication protocol is used?
EAP-Response/Identity(EAPOR)
PEAP is used, and authentication starts
EAP-Request/PEAP/Start
PEAP is used, and authentication starts
RADIUS-Access-Challenge (including EAP-Request/Peap/Start)
My encryption algorithm list, TLS version, and session ID
EAP-Response/Client Hello
My encryption algorithm list, TLS version, and session ID
EAP-Response/Client Hello(EAPOR)
I selected This encryption algorithm and certificate with a key. I need your certificate (another 3 IP packets will be sent to deliver the certificate)
EAP-Request/Server/Hello
I selected This encryption algorithm and certificate with a key. I need your certificate (another 3 IP packets will be sent to deliver the certificate)
RADIUS-Access-Challenge (including EAP-Request/Server/Hello)
Your certificate is valid and has a password
EAP-Response/TLS OK
Your certificate is valid and has a password
EAP-Response/TLS OK(EAPOR)
My password is generated, and a TLS tunnel is set up
RADIUS-Access-Challenge (including EAP-Request/Server/Hello)
My password is generated, and a TLS tunnel is set up
RADIUS-Access-Challenge (including EAP-Request/Server/Hello)
Send EAP packets multiple times
EAP-response
Send EAP packets multiple times
EAP-response(EAPOR)
Send EAP packets multiple times
EAP-Request
Send EAP packets multiple times until an EAP packet carrying PMK is received (the packet can be an EAPOL_Key packet)
RADIUS-Access-Challenge (including EAP-Request)
AC keeps the PMK in MPPE for key negotiation
EAP-success
Your identify is valid, and your EAP packet has MPPE attribute with your key
Access-Accept (having MPPE attribute)
Dynamic key negotiation: 4-way unicast handshake and 2-way multicast handshake
Handshake
Handshake
Handshake
Handshake
Go online
Start accounting

2.3.4 WAPI Authentication

WLAN Authentication and Privacy Infrastructure (WAPI) is a Chinese national standard developed based on IEEE 802.11. WAPI is identified by the Ethernet Type value 0x88B4 in an Ethernet frame. The WAPI protocol defines the following security schemes:

- WLAN Authentication Infrastructure (WAI): authenticates user identities and manages keys.
- WLAN Privacy Infrastructure (WPI): protects data transmitted on WLANs and provides the data encryption, data verification, and anti-replay functions.

WAPI allows only robust security network association (RSNA), providing higher security than Wired Equivalent Privacy (WEP) and Wi-Fi Protected Access (WPA). WAPI can be identified by the Information Element field in a Beacon frame.

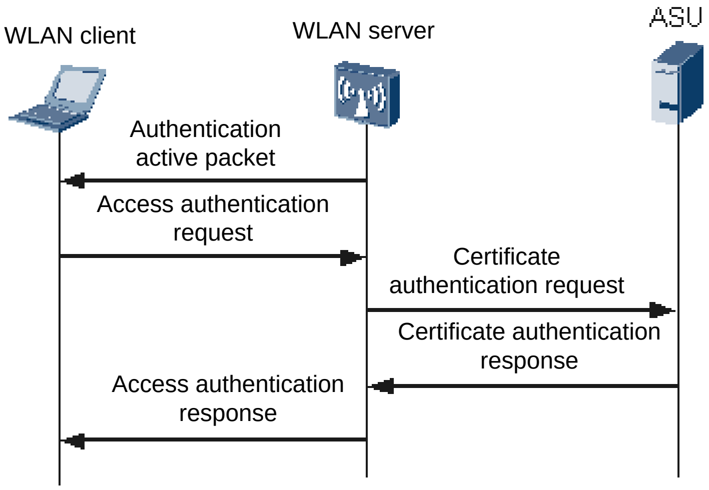
WAPI is an application of Triple-Element Peer Authentication (TePA) on WLANs.

If WAPI is used to associate a WLAN client with a WLAN server, the client and server must authenticate each other and negotiate a key. WAPI provides two identity authentication and key management modes: certificated-based mode (WAPI-CERT) and pre-shared key-based mode (WAPI-PSK).

- WAPI-CERT: involves certificate authentication, unicast key negotiation, and multicast key advertisement. The WLAN client and server verify the certificate of each other. The certificates must have been loaded on the WLAN client and server and verified by the authentication server unit (ASU). After certificate authentication is complete, the client and server use the temporal public key and private key to generate a base key (BK). The BK is used for subsequent unicast key negotiation and multicast key advertisement.
- WAPI-PSK: involves unicast key negotiation and multicast key advertisement. The WLAN client and server verify the pre-shared key of each other. The WLAN client and server must be configured with the same pre-shared key. The pre-shared key is then converted into a BK and the BK is used for subsequent unicast key negotiation and multicast key advertisement. After completing unicast key negotiation and multicast key advertisement, the WLAN client and server use the negotiated key and WPISMS4 algorithm to encrypt data and transmit data to each other.

WAPI certificate authentication

Figure 2-9 WAPI certificate authentication


WLAN client
WLAN server
ASU
Authentication active packet
Access authentication request
Certificate authentication request
Certificate authentication response
Access authentication response

The WAPI certificate authentication process is detailed as follows:

1. Authentication activation: When a WLAN client requests to associate or re-associate with a WLAN server, the server sends an authentication active packet to the client to trigger certificate authentication.
2. Access authentication request: The WLAN client sends an access authentication request packet with its certificate and the current system time to the WLAN server. The current system time is called the access authentication request time.
3. Certificate authentication request: After the WLAN server receives the access authentication request packet, it constructs a certificate authentication request packet with the WLAN client's certificate, access authentication request time, its own certificate, and the signature generated by using the private key, and sends the certificate authentication request packet to the ASU.
4. Certificate authentication response: When the ASU receives the certificate authentication request packet, it checks whether the server's signature and certificate are valid. If they are invalid, the server fails to be authenticated. If they are valid, the ASU starts to check the client's certificate. The ASU constructs a certificate authentication response packet with the certificate authentication results and the signature generated according to the results, and sends the certificate authentication response packet to the WLAN server.
5. Access authentication response: After the WLAN server receives the certificate authentication response packet, it checks the signature to obtain the certification authentication result of the client so that it can control access of the WLAN client based on the certification authentication result. The WLAN server forwards the certification authentication response packet to the WLAN client. The WLAN client then checks the signature to obtain the certification authentication result of the server and determines whether to associate with the WLAN server based on the result.

   Till now, the certificate authentication process is complete. If certificate authentication is successful, the WLAN server allows the client to use the WLAN service; otherwise, the client is dissociated from the server.

WAPI key negotiation

The WLAN client and server negotiate a unicast encryption key and a unicast integrity key to protect unicast data. The WLAN server generates a multicast encryption key and a multicast integrity key using a multicast master key to encrypt multicast and broadcast data. The WLAN client uses the multicast encryption key and multicast integrity key advertised by the WLAN server to decrypt received multicast and broadcast data.

To enhance data confidentiality, the WLAN server and client start to negotiate a new key after communicating for a certain period of time or transmitting a certain amount of data.

Figure 2-10 WAPI key negotiation

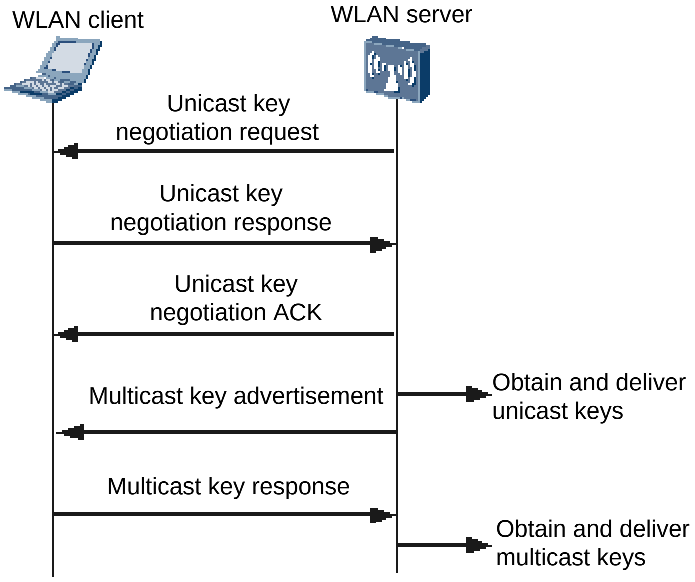

WLAN client
WLAN server
Unicast key negotiation request
Unicast key negotiation response
Unicast key negotiation ACK
Multicast key advertisement
Obtain and deliver unicast keys
Multicast key response
Obtain and deliver multicast keys

Figure 2-10 shows the process of WAPI key negotiation.

1. Unicast key negotiation

   After certificate authentication is complete, the WLAN client and server use the KD-HMAC-SHA256 algorithm to generate a unicast session key (USK) based on the BK, client challenge word, and server challenge word. In addition to the USK, the encryption key and identity key used to generate the multicast key are also negotiated in this process.

   – Unicast key negotiation request

     After a BK is generated, the WLAN server sends a unicast key negotiation request packet to the WLAN client.

   – Unicast key negotiation response

     After the WLAN client receives the unicast key negotiation request packet, it performs the following steps:

     a. Checks whether the negotiation is triggered to update the unicast key. If yes, it performs step b; if no, it performs step c.

     b. Checks whether the server challenge word in the unicast key negotiation request packet is the same as the challenge word used in the last unicast key negotiation. If they are different, the client discards the unicast key negotiation request packet.

c. Generates a random challenge word, and then uses the BK, server challenge word, client challenge word, and the KD-HMAC-SHA256 algorithm to calculate a USK and the server challenge word used for the next unicast key negotiation.

d. Uses the message authentication key and HMAC-SHA256 algorithm to calculate a local message authentication code, and sends it to the WLAN server with a unicast key negotiation response packet.

WAI allows the WLAN client to send a unicast key negotiation response to initiate unicast key update without receiving a request packet from the WLAN server.

- Unicast key negotiation ACK

  After the WLAN server receives the unicast key negotiation response packet, it performs the following steps:

  e. Checks whether the server challenge word is correct. If not, it discards the unicast key negotiation response packet.

  f. Uses the BK, server challenge word, client challenge word, and KD-HMAC-SHA256 algorithm to calculate a USK and the server challenge word used for the next unicast key negotiation. The server then calculates a local message authentication code using the message authentication key and HMAC-SHA256 algorithm, and compares the local message authentication code with that in the received unicast key negotiation response packet. If they are different, the server discards the unicast key negotiation response.

  g. If this is the first unicast key negotiation after the BK is generated, the server acts differently based on the service set type. If the network is a basic service set, the server checks whether the WAPI information element in the response packet is the same as that in the association request packet it received before. If they are different, the client is dissociated from the server. If the network is an independent basic service set (IBSS), the server checks whether the unicast key algorithm supports the information element in the response packet. If not, the client is dissociated from the server.

  h. Uses the message authentication key and HMAC-SHA256 algorithm to calculate a local message authentication code, and sends it to the WLAN client with a unicast key negotiation ACK.

2. Multicast key advertisement

   Multicast key advertisement is performed after unicast key negotiation is complete.

   - Multicast key advertisement

     The WLAN server uses the random number algorithm to calculate a multicast master key, encrypts the multicast master key using the negotiated unicast key, and sends an advertisement packet to notify the client of the multicast key.

   - Multicast key response

     After the WLAN client receives the multicast key advertisement packet, it performs the following steps:

     a. Calculates the checksum using the message authentication key identified by the unicast key identifier, and compares the checksum with the message authentication code. If they are different, the client discards the advertisement packet.

b. Checks whether the identifier of the advertisement packet is larger than that of the last advertisement packet. If not, the client discards the advertisement packet. Identifiers of advertisement packets must be monotonic increasing.

c. Decrypts the multicast key to obtain the 16-byte master key and uses the KD-HMAC-SHA256 algorithm to extend it to 32 bytes. The first 16 bytes indicate the encryption key, and the last 16 bytes indicate the integrity key.

d. Saves the identifier of the multicast key advertisement packet and sends a multicast key response packet to the server.

After the WLAN server receives the multicast key response packet, it performs the following steps:

e. Calculates the checksum using the message authentication key identified by the unicast key identifier, and compares the checksum with the message authentication code. If they are different, the server discards the response packet.

f. Compares the key advertisement identifier in the multicast key response packet with that in the multicast key advertisement packet it sends to the client. If they are the same, the multicast key advertisement is successful; otherwise, the server discards the multicast key response packet.

If this is the first multicast key advertisement after the BK is generated, the server sets the controlled port status to On.

2.3.5 Portal Authentication

Portal authentication is also called web authentication.
When a user accesses the authentication page on the Portal server or when a user attempts to access other websites using HTTP, the user is redirected to the web authentication page. After the user enters the account information and submits the web page, the Portal server obtains the account information. The Portal server sends the user account information to the WLAN server using the Portal protocol. The WLAN server and authentication server exchange messages to complete user authentication.

Portal authentication can provide convenient management functions. Portal websites can develop advertisement and community services and personalized businesses. In this manner, carriers, device providers, and content and service providers can form an industry ecosystem. The Portal authentication is frequently used on carrier or enterprise WLANs.

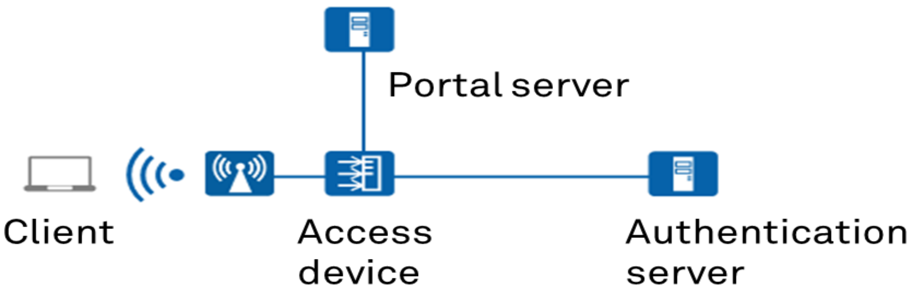
Portal authentication has the following advantages:

- Ease of use: In most cases, Portal authentication does not require the client to have additional software installed and allows the client to be directly authenticated on a web page.
- Convenient operations: Portal authentication achieves service expansion on the Portal page, including advertisement push, responsibility announcement, and enterprise publicity.
- Mature technology: Portal authentication has been widely used in networks of carriers, fast food chains, hotels, and schools.
- Flexible deployment: Portal authentication implements access control at the access layer or at the ingress of key data.

- Flexible user management: Portal authentication can be performed on users based on the combination of user names and any one of VLANs, IP addresses, and MAC addresses.

The Portal authentication system consists of four basic elements: client, access server, Portal server, and AAA server. Figure 2-11 shows the networking diagram. The WLAN AC functions as an access device.

Figure 2-11 Portal authentication system



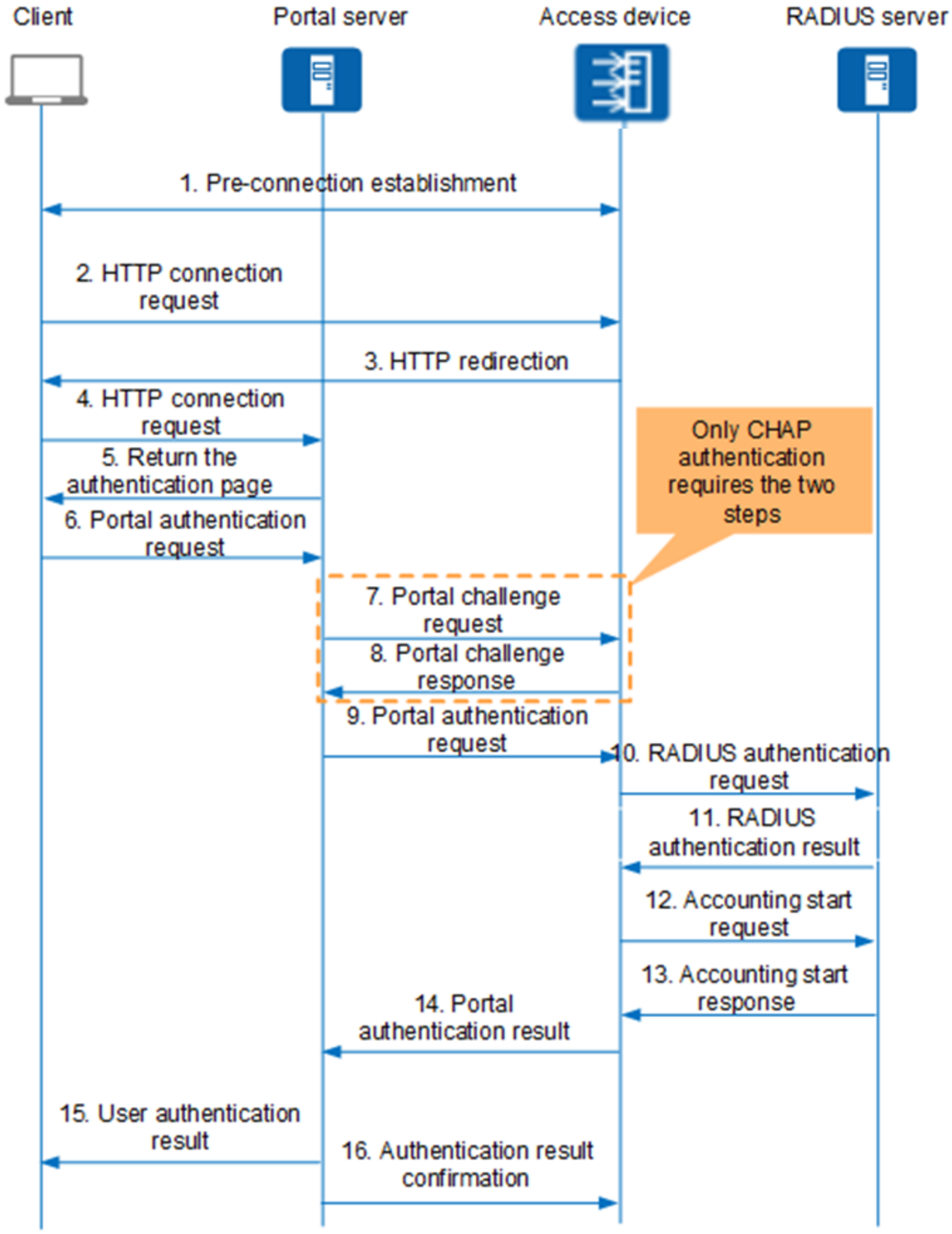
Huawei WLAN Portal authentication is based on two types of protocols: Portal and HTTP/HTTPS. These will be described in subsequent sections.

Portal-based Portal authentication process

The following describes the Layer 2 authentication process of an external Portal server. The authentication process of a built-in Portal server is similar to that of an external Portal server, which is not described in this document.

Figure 2-12 illustrates the packet interaction process when the user goes online and Layer 2 authentication is used.

Figure 2-12 Portal-based Portal authentication process


Client
Portal server
Access device
RADIUS server
1. Pre-connection establishment
2. HTTP connection request
3. HTTP redirection
4. HTTP connection request
5. Return the authentication page
6. Portal authentication request
Only CHAP authentication requires the two steps
7. Portal challenge request
8. Portal challenge response
9. Portal authentication request
10. RADIUS authentication request
11. RADIUS authentication result
12. Accounting start request
13. Accounting start response
14. Portal authentication result
15. User authentication result
16. Authentication result confirmation

1. Before the authentication, the client establishes a pre-connection with the access device. That is, the access device has established a user online entry for the client before the authentication succeeds and the client is granted access to some network resources.

2. The client initiates an HTTP connection request.

3. The access device receives the HTTP connection request packet and determines whether to permit the packet. It permits an HTTP packet destined for either the Portal server or configured non-authentication network resources and redirects an HTTP packet destined for other addresses to the Portal authentication page.

4. The client initiates an HTTP connection request to the Portal server based on the obtained URL.

5. The Portal server returns the Portal authentication page to the client.

6. The user enters the user name and password on the Portal authentication page to initiate a Portal authentication request to the Portal server.

7. The Portal server receives the Portal authentication request. If CHAP authentication is used between the Portal server and access device, the Portal server sends a Portal challenge request packet (REQ_CHALLENGE) to the access device. If PAP authentication is used between the Portal server and access device, the access device goes to step 9.

8. The access device sends a Portal challenge response packet (ACK_CHALLENGE) to the Portal server.

9. The Portal server encapsulates the entered user name and password into a Portal authentication request packet (REQ_AUTH) and sends the packet to the access device.

10. The access device sends a RADIUS authentication request packet (ACCESS-REQUEST) to the RADIUS server based on the obtained user name and password.

11. The RADIUS server authenticates the user name and password. If authentication succeeds, the RADIUS server sends an authentication accept packet (ACCESS-ACCEPT) to the access device. If authentication fails, the RADIUS server sends an authentication reject packet (ACCESS-REJECT) to the access device.

    The ACCESS-ACCEPT packet contains user authorization information because RADIUS provides both authentication and authorization functions.

12. The access device permits or denies the user access according to the authentication result. If the user access is permitted, the access device sends an accounting start request packet (ACCOUNTING-REQUEST) to the RADIUS server.

13. The RADIUS server replies with an accounting start response packet (ACCOUNTING-RESPONSE), starts accounting, and adds the user to the local online user list.

14. The access device sends the Portal authentication result (ACK_AUTH) to the Portal server and adds the user to the local online user list.

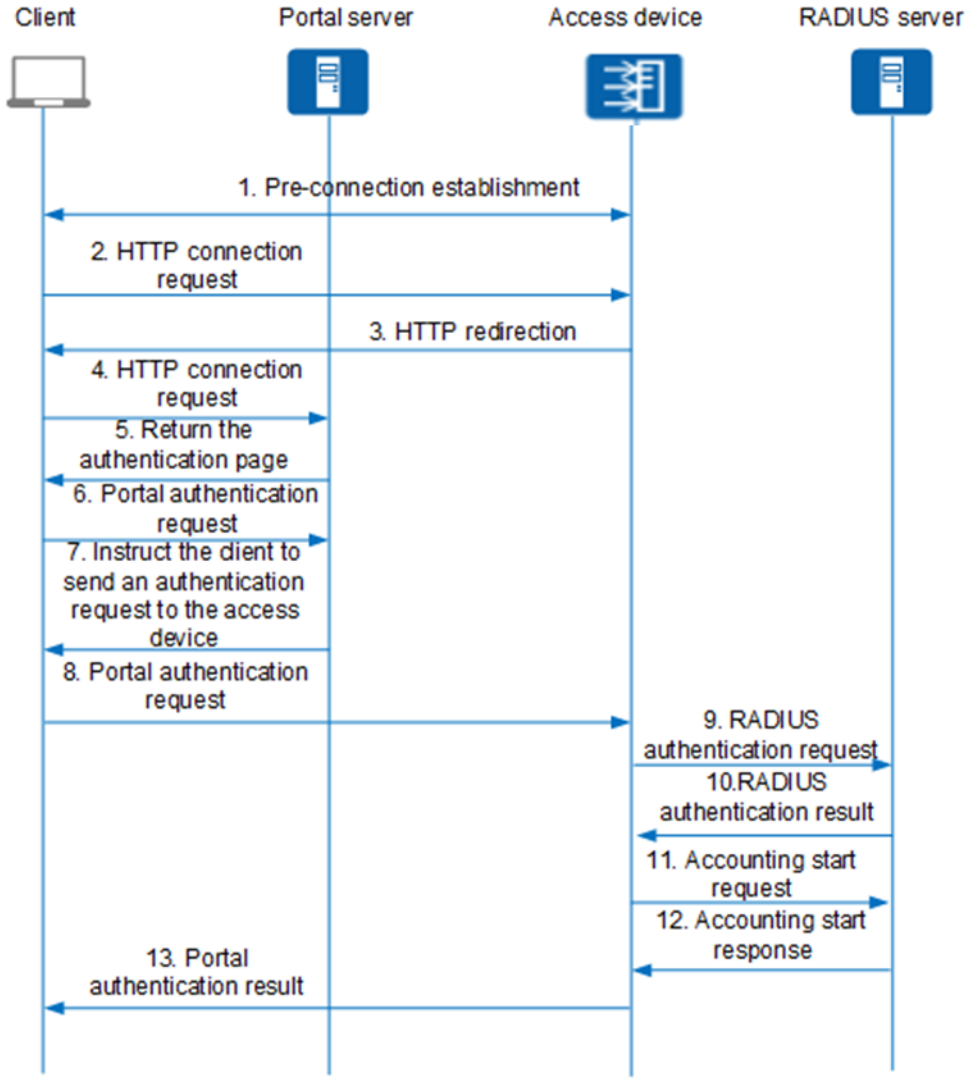
15. The Portal server sends the authentication result to the client to inform the client that authentication succeeds and adds the user to the local online user list.

16. The Portal server sends an authentication acknowledgment packet (AFF_ACK_AUTH) to the access device.

HTTP-based or HTTPS-based Portal authentication process

The exchange process of HTTPS packets is similar to that of HTTP packets except that HTTPS packets need to be encrypted and decrypted.

Figure 2-13 HTTP-based Portal authentication process


Client
Portal server
Access device
RADIUS server
1. Pre-connection establishment
2. HTTP connection request
3. HTTP redirection
4. HTTP connection request
5. Return the authentication page
6. Portal authentication request
7. Instruct the client to send an authentication request to the access device
8. Portal authentication request
9. RADIUS authentication request
10.RADIUS authentication result
11. Accounting start request
12. Accounting start response
13. Portal authentication result

1. Before the authentication, the client establishes a pre-connection with the access device. That is, the access device has established a user online entry for the client before the authentication succeeds and the client is granted access to some network resources.
2. The client initiates an HTTP connection request.
3. The access device receives the HTTP connection request packet and determines whether to permit the packet. It permits an HTTP packet destined for either the Portal server or configured non-authentication network resources and redirects an HTTP packet destined for other addresses to the Portal authentication page.
4. The client initiates an HTTP connection request to the Portal server based on the obtained URL.
5. The Portal server returns the Portal authentication page to the client.

6. The user enters the user name and password on the Portal authentication page to initiate a Portal authentication request to the Portal server.
7. The Portal server instructs the client to send a Portal authentication request to the access device.
8. The client sends a Portal authentication request (HTTP POST/GET) to the access device.
9. The access device sends a RADIUS authentication request packet (ACCESS-REQUEST) to the RADIUS server based on the obtained user name and password.
10. The RADIUS server authenticates the user name and password. If authentication succeeds, the RADIUS server sends an authentication accept packet (ACCESS-ACCEPT) to the access device. If authentication fails, the RADIUS server sends an authentication reject packet (ACCESS-REJECT) to the access device.

    The ACCESS-ACCEPT packet contains user authorization information because RADIUS provides both authentication and authorization functions.
11. The access device permits or denies the user access according to the authentication result. If the user access is permitted, the access device sends an accounting start request packet (ACCOUNTING-REQUEST) to the RADIUS server.
12. The RADIUS server replies with an accounting start response packet (ACCOUNTING-RESPONSE), starts accounting, and adds the user to the local online user list.
13. The access device returns the Portal authentication result to the client and adds the user to the local online user list.

2.3.6 MAC Address Authentication

In MAC address authentication, a user terminal sends its MAC address as the identity information to an access device.

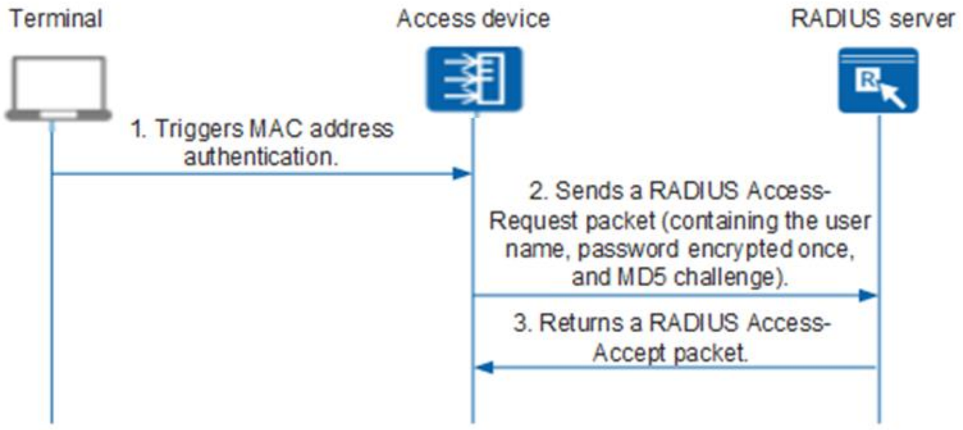
A RADIUS server is used to authenticate user terminals in MAC address authentication. After the access device obtains the user terminal's MAC address, it sends an authentication request to the RADIUS server. The RADIUS server authenticates the user terminal's MAC address and notifies the access device of the authentication result and authorization information. User terminals do not need the client software in MAC address authentication.

The access device exchanges RADIUS packets with the RADIUS server and encrypts passwords of MAC address authentication users in Password Authentication Protocol (PAP) or Challenge Handshake Authentication Protocol (CHAP) mode.

- PAP: The access device uses the randomly-generated MD5 challenge to encrypt passwords of MAC address authentication users once.
- CHAP: The access device uses the randomly-generated MD5 challenge to encrypt passwords of MAC address authentication users twice.

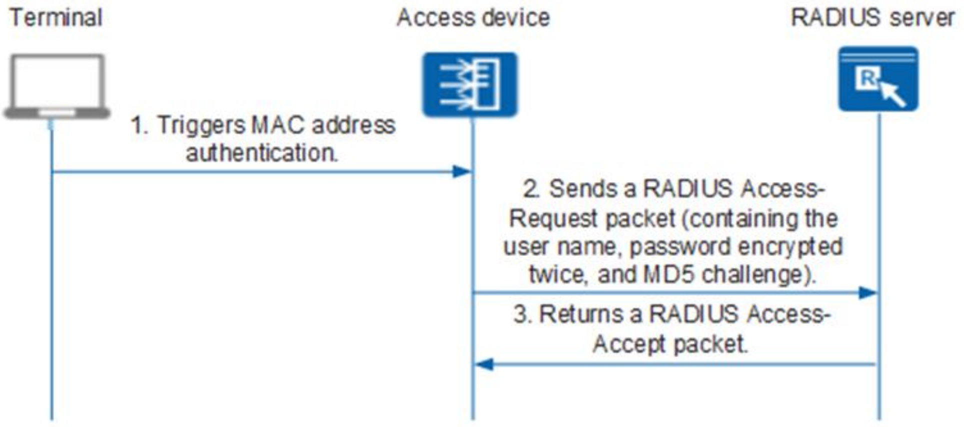
Figure 2-14 and Figure 2-15 show MAC address authentication processes in PAP and CHAP modes, separately.

Figure 2-14 MAC address authentication process (PAP mode)


Terminal
Access device
RADIUS server
1. Triggers MAC address authentication.
2. Sends a RADIUS Access-Request packet (containing the user name, password encrypted once, and MD5 challenge).
3. Returns a RADIUS Access-Accept packet.

1. After detecting the MAC address of a terminal for the first time, the access device learns the MAC address and triggers MAC address authentication.
2. The access device generates a random MD5 challenge and uses the challenge to encrypt the password of the MAC address authentication user once. The access device then encapsulates the user name, encrypted password, and MD5 challenge into a RADIUS Access-Request packet, and sends this packet to the RADIUS server, requesting the RADIUS server to perform MAC address authentication on the user.
3. The RADIUS server uses the received MD5 challenge to encrypt the password of the MAC address authentication user stored in the local database once. If the password is the same as the password sent by the access device, the RADIUS server sends an Access-Accept packet to the access device, indicating that the MAC address authentication succeeds and the terminal is allowed to access the network.

Figure 2-15 MAC address authentication process (CHAP mode)


Terminal
Access device
RADIUS server
1. Triggers MAC address authentication.
2. Sends a RADIUS Access-Request packet (containing the user name, password encrypted twice, and MD5 challenge).
3. Returns a RADIUS Access-Accept packet.

1. After detecting the MAC address of a terminal for the first time, the access device learns the MAC address and triggers MAC address authentication.

2. The access device generates a random MD5 challenge and uses the challenge to encrypt the password of the MAC address authentication user twice. The access device then encapsulates the user name, encrypted password, and MD5 challenge into a RADIUS Access-Request packet, and sends this packet to the RADIUS server, requesting the RADIUS server to perform MAC address authentication on the user.
3. The RADIUS server uses the received MD5 challenge to encrypt the password of the MAC address authentication user stored in the local database twice. If the password is the same as the password sent by the access device, the RADIUS server sends an Access-Accept packet to the access device, indicating that the MAC address authentication succeeds and the terminal is allowed to access the network.

Accounting and authorization can also be implemented based on MAC addresses.

2.4 Authorization

Authorization is used to differentiate user rights based on factors like user identities, types of terminals in use, locations (or connected APs), and access time.

ACLs and UCL groups are often used. RADIUS authorization is used as an example.

ACL

An Access Control List (ACL) is a collection of one or more rules. Rules describe the packet matching conditions, such as the source address, destination address, and port number of packets. An ACL is a packet filter that filters packets based on rules. After a user is authenticated, the authentication server authorizes the specified ACL to the user. Then, the access device controls the user packets according to the ACL.

- If the user packets match the permit rule in the ACL, the packets are allowed to pass through.
- If the user packets match the deny rule in the ACL, the packets are discarded.

The RADIUS server can use the following methods to authorize an ACL:

- Authorize a static ACL: The RADIUS server authorizes the ACL ID to the user through the standard RADIUS attribute **Filter-Id**. To make the authorized ACL take effect, you need to configure the ACL and corresponding rules on the access device in advance.
- Authorize a dynamic ACL: The RADIUS server uses the RADIUS attribute **HW-Data-Filter** extended by Huawei to authorize the ACL ID and corresponding ACL rules to the user. The ACL ID and ACL rules need to be configured only on the RADIUS server instead of the access device.

User Group

A user group consists of users (terminals) with the same attributes such as the role and rights, which is similar to the user group in the Windows system.

Each user group can be associated with different ACLs, CAR, user VLANs, and packet priorities, so user group-based authorization can implement ACL-based access control, VLAN-based access control, traffic control, and priority control for each type of users. This implements flexible management.

For example, each user requires a large number of ACLs for authorization and the number of online users cannot reach the upper limit, but there are many access users and user categories are limited. In this case, the user group can be used because ACL resources are limited. Each user group multiplexes ACLs. User groups can be configured on the RADIUS server or device (the user groups must be applied to the AAA domain).

The mode for the RADIUS server to deliver user group authorization is the same as that for delivering the ACL ID. Standard attribute 11 (Filter-Id) is used and the value is the user group name. Standard attribute 11 is preferentially parsed as the ACL ID. If this ACL ID does not exist on the device, the device considers the parsing result to be a user group. If the user group also does not exist on the device, authorization fails.

User group-based authorization delivered by the RADIUS server takes precedence over that configured on the device. If user group-based authorization delivered by the RADIUS server fails, user group-based authorization configured on the device is used. For example, if only user group B is configured on the device and applied to the AAA domain, when the RADIUS server delivers user group A, authorization of user group A fails and authorization of user group B is used.

To use user group-based authorization delivered by the RADIUS server, ensure that the user group has been configured on the device (the user group does not need to be applied to the AAA domain).

2.5 Data Encryption

WLANs are challenged with data confidentiality. Different than the wired network, data frames on the WLAN can be intercepted and analyzed by anyone using proper receiving devices.

To ensure data security, data must be encrypted to prevent attackers from intercepting data. WLAN provides a series of encryption protocols. These protocols allow only authorized users with keys to access data and prevent data from being modified during transmission.

WLAN supports the following encryption protocols.

- Wired Equivalent Privacy (WEP)
- Temporal Key Integrity Protocol (TKIP)
- Counter Mode with CBC-MAC Protocol (CCMP)
- SMS4 encryption algorithm
- Protected Management Frame (PMF)
- Network layer encryption protocol

2.5.1 WEP Encryption

WEP is the earliest security standard defined in IEEE 802.11. WEP involves authentication and encryption. A station (STA) can join an access point (AP) only after it is authenticated by the AP. After authentication is complete, the STA and AP use the RC4 algorithm to encrypt and decrypt data.

As defined in IEEE 802.11, WEP uses the RC4 stream cipher to encrypt wireless data. WEP uses a 64-bit or 128-bit encryption key that contains a 24-bit initialization vector (IV) generated by the WLAN server. The other 40 bits or 104 bits of the key must be configured on the WLAN server and client.

IEEE 802.11 does not define a specific key assignment mechanism for WEP encryption. Earlier WEP encryption uses manually configured keys. This encryption mode increases workload of administrators. Therefore, the same key is used for a long time on most networks. WEP without a key assignment mechanism is called manual WEP or static WEP.

Static WEP is only used for some old low power terminals such as handheld code scanner, PDA, and Wi-Fi phone. These terminals do not support advanced encryption protocols.

Figure 2-16 WEP encryption process

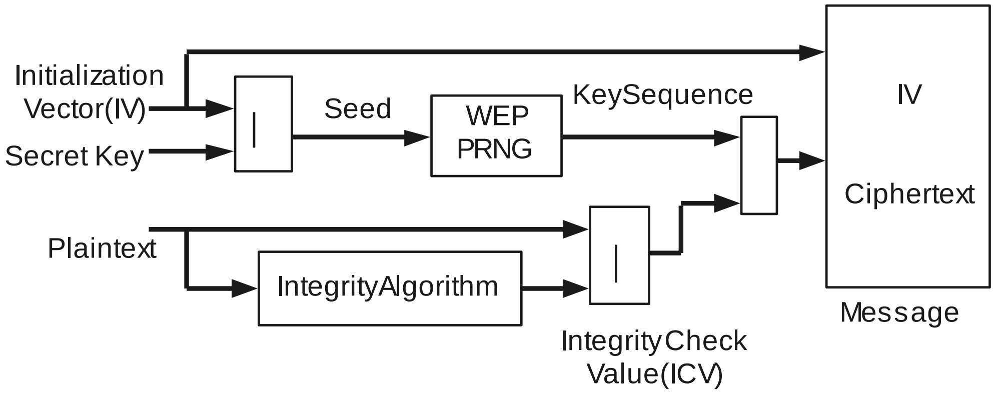


Figure 2-16 shows the WEP encryption process.

1. A WLAN device generates an IV and concatenates an encryption key to the IV to construct a WEP seed. WEP uses the RC4 algorithm to generate a key stream of the same length as the plain text data stream. The key stream length equals the total length of the MAC protocol data unit (MPDU) and the integrity check value (ICV).

2. WEP computes the ICV over the plain text data and appends it to the MPDU.

3. WEP exclusive-ORs the key stream with the plain text data stream to produce a cipher text.

4. A 4-byte field is prefixed to the cipher text to store the IV and key ID. This field contains three subfields: a 3-byte subfield that contains the IV, a 2-bit Key ID subfield, and a 6-bit Pad subfield (all 0s). When a key-mapping key is used, the Key ID field value is 0. When a default key is used, the Key ID field value is the key identifier that ranges from 0 to 3.

Figure 2-17 WEP decryption process

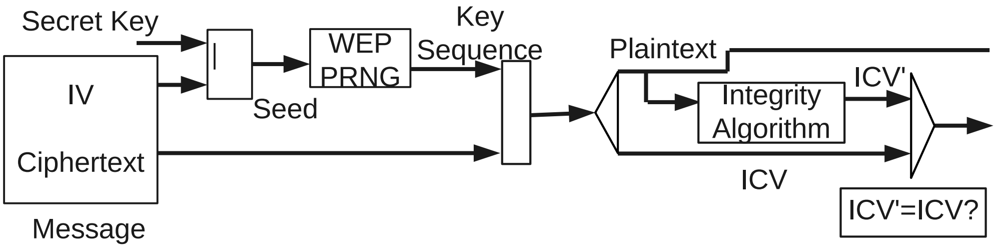


Figure 2-17 shows the WEP decryption process.

1. WEP finds the decryption key.
2. WEP concatenates the key to the IV and uses them as the input to the RC4 algorithm to generate the key stream of the same length as the cipher text data.
3. WEP exclusive-ORs the key stream with the cipher text data bit by bit to obtain the ICV and plain text data. The ICV follows the plain text data and is the last 4 bytes in the MPDU.
4. WEP computes an ICV' value over the plain text data and compares it with the ICV value. If they are the same, the data is decrypted successfully; otherwise, the data is discarded.

WEP weakness

- WEP uses the RC4 algorithm to encrypt packets exchanged between an AP and a STA. After the key is configured, the key cannot be automatically updated. The password is easy to decipher. Lots of WEP decryption methods exist.

  WEP uses two types of encryption keys: 40- or 104-bit keys pre-shared by the receiver and sender and a 24-bit initialization vector (IV) inserted in the packet by the sender. As shown in Figure 2-16, to notify the receiver of the IV key, the sender inserts the IV key into the packet without encrypting it. In this situation, if packets that contain IV keys are intercepted and analyzed, the secret keys may also be disclosed.
- Message integrity check (MIC) is not performed. Messages can be easily modified by attackers.
  - The Integrity Check Value (ICV) field in the message uses the simple and effective CRC algorithm to prevent data transmission errors caused by physical factors such as signal noises. Hackers can change the ICV in messages to make it consistent with the modified packets.
  - In addition, WEP lacks an effective mechanism to authenticate users that access the network.

2.5.2 WPA/WPA2: TKIP and CCMP Encryption

Wi-Fi Protected Access (WPA) is a commercial standard drafted by the Wi-Fi Alliance to substitute for the insecure WEP standard before IEEE 802.11i was published. WPA uses the RC4 algorithm, which is called the Temporal Key Integrity Protocol (TKIP) algorithm.

After IEEE 802.11i was published, the WPA2 Wi-Fi Alliance developed WPA2. Different from WPA, WPA2 uses an 802.1X authentication framework that supports various authentication standards such as the Extensible Authentication Protocol-Protected Extensible Authentication Protocol (EAP-PEAP) and EAP-Transport Layer Security (EAP-TLS). The pairwise master key (PMK) is used as a seed to produce an encryption key. A different PMK is generated every time a user goes online, which ensures security of the encryption key. WPA2 encrypts data by using the CTR with CBC-MAC Protocol (CCMP).

In the latest WAP implementation, both WPA1 and WPA2 can use the 802.1X, TKIP, or CCMP protocol to encrypt data. They provide the same security feature but use different protocol packet formats.

WAP is the wireless security standard replacing WEP and providing more powerful security performance for IEEE 802.11 WLANs before IEEE 802.11i was issued. WPA is a subset of IEEE 802.11i and uses IEEE 802.1X authentication and TKIP encryption.

WPA and WPA2 provide higher security than WEP in terms of user authentication, data encryption, and integrity check, and improve WLAN management capabilities.

- User authentication

  WPA and WPA2 require users to provide identity information and determine whether a user is authorized to use network resources according to the identity information.

  WPA enterprise edition and personal edition are provided to meet different user requirements:

  - WPA enterprise edition: uses the WPA-802.1X authentication mode. Users provide identity information such as the user name and password and are authenticated by an authentication server (usually a RADIUS server).
  - WPA personal edition: A dedicated authentication server is expensive and difficult to maintain for small- and medium-scale enterprises and individual users. The WPA personal edition provides a simplified authentication mode WPA-pre-shared key (WPA-PSK). This mode does not require a dedicated authentication server. Users only need to set a pre-shared key on each WLAN node, such as an AP, AC, and a wireless network adapter. A WLAN client can access the WLAN if its shared key is the same as that configured on the WLAN server. The shared key is used only for authentication but not for encryption; therefore, it will not bring such security risks as the 802.11 pre-shared key authentication.

IEEE 802.11i defines the robust security network (RSN) to enhance WLAN performance on data encryption and authentication. IEEE 802.11i has improved WEP encryption in the following aspects.

- Enhances the mechanism to authenticate STAs and APs.
  - Supports 802.1X authentication.
  - Supports pre-shared key authentication.
- Adds the mechanism for key generation, management, and transmission.
  - Each user uses a separate key.
  - The key for data encryption is transmitted in a more secure way.
- Adds two types of symmetric encryption algorithms to provide stronger encryption.
  - TKIP: uses the same RC4 algorithms as WEP. TKIP can provide high WLAN security by upgrading firmware and drive programs on the device.
  - CCMP: uses the advanced encryption standard (AES) encryption algorithms. AES has high requirements on the hardware. Therefore, CCMP cannot be implemented by upgrading the existing device.

- WRAP: uses AES encryption algorithms and Offset Codebook (OCB) mode. WRAP is an optional encryption mechanism.

2.5.3 TKIP

To remove major defects in the WEP design, the IEEE 802.11i working group developed Temporal Key Integrity Protocol (TKIP) and Counter Mode with CBC-MAC Protocol (CCMP) to modify the encryption protocol at the link layer. TKIP improves network security without requiring the replacement of legacy hardware. CCMP, as a new encapsulation protocol, ensures a higher level of security.

The name of the first technology was WEP2 at the beginning and later changed to TKIP to differ from WEP.

WEP is vulnerable to attacks because it generates a random seed using the IV and key but the IV is not long enough. TKIP increases the IV length from 24 bits to 48 bits so that more IV values are supported. In addition, TKIP uses a cryptographic mixing function defend against attacks to WEP. TKIP encrypts each frame using a specific RC4 key and expands the IV space.

In fact, TKIP is an improvement to WEP and uses RC4 as its core algorithm. TKIP also provides extended IV (EIV) and message integrity code (MIC) to prevent replay attacks and information tampering.

TKIP has the following improvements compared with WEP:

- A sender calculates MIC to protect data integrity. The MIC contains plain text data, source address (SA), and destination address (DA), and is encrypted using a MIC key.
- TKIP adds a TSC in the IV of each MAC service data unit (MSDU) to prevent replay attacks.
- TKIP uses the Fast Packet Keying algorithm to generate an encryption key by combining the temporal key with the TSC.
- TKIP uses the 802.1X EAPoL Key protocol to update temporal keys and MIC keys.

TKIP has the following advantages:

- Protects MAC addresses of authorized users from theft. Because MAC addresses are not encrypted, attackers can still obtain MAC addresses of authorized users. However, attackers cannot use the obtained MAC addresses to decipher TKIP-encrypted data because they do not have MIC keys to calculate the correct MICs.
- Protects SAs and DAs. TKIP can detect SAs and DAs that have been tampered with. A MIC is calculated using an SA, DA, and MIC key. Therefore, if the DA or SA is tampered with, the MIC calculated by the receiver is different from the MIC in the received MAC service data unit (MSDU).
- Provides the anti-replay function using TSC. Each MSDU has a unique TSC. The TSC increases every time an MSDU is sent. This prevents attackers from sending messages to a receiver based on intercepted MSDUs.
- Prevents attackers from guessing keys of authorized users. TKIP uses a cryptographic mixing function to combine a temporal key with the IV, whereas WEP merely concatenates the IV to the key. Using TSC in the cryptographic mixing function enhances key security.

2.5.4 CCMP Encryption

Although TKIP outperforms WEP, it still faces security risks because it is a stream cipher algorithm.

Then the IEEE 802.11i working group developed a link-layer security protocol based on cipher block defined in Advanced Encryption Standard (AES). AES uses a 128-bit key and a 128-bit block size.

This security protocol is called the Counter Mode with CBC-MAC Protocol (CCMP).

CCMP provides the encryption, authentication, integrity check, and anti-replay functions. It is based on the CCM that uses the AES algorithm. CCM combines the Counter Mode (CTR) with Cipher Block Chaining Message Authentication Code (CBC-MAC) to ensure integrity of MPDU data and MPDU header.

CCMP defines a series of dynamic key negotiation and management mechanisms. Each WLAN client negotiates with a server to obtain a dynamic key. The dynamic key is updated periodically to enhance key security. CCMP allocates a unique 48-bit packet number (PN) to each encrypted packet, improving packet transmission security.

CCMP has the following advantages:

- Uses the AES algorithm at the physical layer so that encryption and decryption are performed by hardware. This overcomes WEP defects that hinder the popularization of WLANs on enterprises. To improve network security, WLAN must be treated like an access network but not a core network. If two enterprise employees communicate with each other through the switching center of a LAN, they are considered as trusted users.
- Overcomes defects of the RC4 algorithm.
  - The RC4 algorithm uses a stream cipher to encrypt packets exchanged between an AP and a STA. The stream cipher is easy to decipher.

    Both WEP encryption and TKIP encryption use the RC4 algorithm as the core. Due to the inherent shortcomings of the RC4 algorithm, a stream cipher used to encrypt packets between an AP and a STA is easy to decipher.

    AES is a symmetric block cipher technology that provides higher encryption performance than the RC4 algorithm used in WEP/TKIP encryption.

    A symmetric key system requires both the sender and the receiver to know the key. The biggest difficulty of this system is how to securely assign the key to both parties. Especially in the network environment, the 802.11i system uses 802.1X authentication and key negotiation mechanism to manage keys.

    The AES encryption algorithm uses 128-bit encryption, and its output is more random. To attack 128-bit 7-round ciphertexts, almost the entire codebook is required. To attack 192- and 256-bit encrypted ciphertexts both a codebook and related but key-unknown ciphertexts are required, which is more secure than WEP.

    The attacker needs to obtain a large number of ciphertexts, consumes a lot of resources, and takes longer to decipher. The decrypted password table and the encrypted password table are separate. Subkey encryption is also supported. This method is better than the original decryption that used a special key. It is easy to fend off attacks such as synchronization attacks. The encryption and decryption speeds are fast. Therefore, security is better than that of WEP.

- AES is a symmetric block cipher algorithm that uses a 128-bit key and a 128-bit block size. Deciphering an AES key requires more cipher text data, resources, and time than other types of keys.

The AES algorithm supports any packet size, and has three different key lengths: 128, 192 and 256 bits, for flexible combinations. In addition, AES has the advantages of wide usage, short waiting time, relatively easy to hide, and high throughput. After comparative analysis, it can be seen that the AES algorithm is superior to WEP and TKIP in performance and other aspects. With the AES algorithm in use, WLAN will greatly improve security, effectively defending against external attacks.

The WPA2-PSK algorithm is at risk of being cracked. The Wi-Fi Alliance released the WPA3 standard in 2018 that provides a more secure encryption method. The WPA3 standard encrypts all data on the public Wi-Fi network and therefore can further protect unsecured Wi-Fi networks. Especially when users use public networks such as Wi-Fi hotspots in hotels and tourist sites, WPA3 creates more secure connections, so that hackers cannot snoop on users' traffic and steal private information. However, it is expected to take 1-2 years for the popularity of WPA3.

2.5.5 WAPI: SMS4 Algorithm

China defines a new security mechanism WAPI. WAPI allows an AP and a STA to check their certificates to authenticate each other.

WAPI can be used with various cryptographic algorithms, such as SMS4 in China, AES in USA, and SEED in South Korea.

2.5.6 PMF

PMF is a specification released by Wi-Fi Alliance (WFA) based on IEEE 802.11w standards. It aims to apply security measures defined in WPA2 to unicast and multicast management action frames to improve network credibility.

If management frames transmitted on WLANs are not encrypted, security problems may occur. PMF can address the problems including the following:

- Hackers intercept management frames exchanged between the APs and users.
- Hackers pretend to be APs and send dissociation and deauthentication frames to disconnect users.
- Hackers pretend to be users and send dissociation frames to APs to disconnect the users.

2.5.7 Encryption Protocols Used on the Network Layer

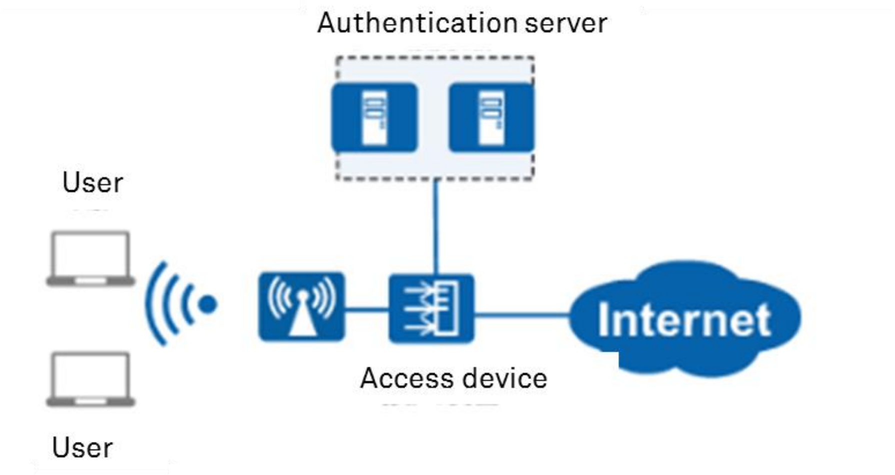
Apart from the preceding encryption methods, WLAN also supports some field-proven network-layer encryption protocols, such as IP Security (IPSec), SSL, and Secure Shell (SSH).

3 Application Scenario

3.1 Typical 802.1X Authentication Scenario

To ensure network security, user access to the network needs to be controlled. Only the users who are successfully authenticated can access network resources authorized by administrators.

Figure 3-1 Typical 802.1X authentication scenario



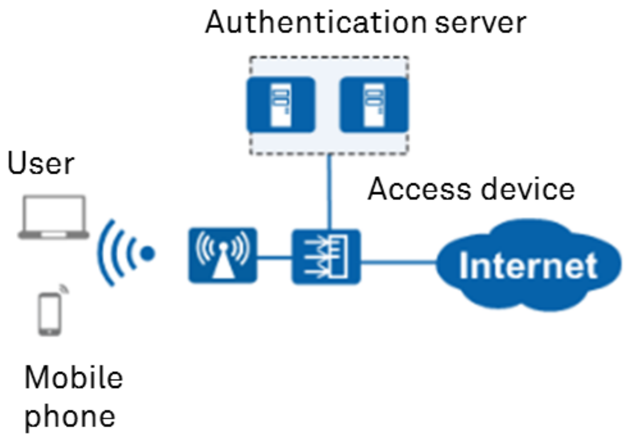
After 802.1X client software is installed on a user's terminal (note that a smartphone comes with an 802.1X client), the user can initiate an authentication request to the access device. Then, the access device exchanges information with the user's terminal and sends user information to the authentication server for authentication.

If authentication is successful, the access device enables the interface connected to the user's terminal and allows the user to access the network. If authentication fails, the access device forbids the user to access the network.

3.2 Typical MAC Address Authentication Scenario

To ensure network security, user access to the network needs to be controlled. Only the users who are successfully authenticated can access network resources authorized by administrators.

Figure 3-2 Typical MAC address authentication scenario



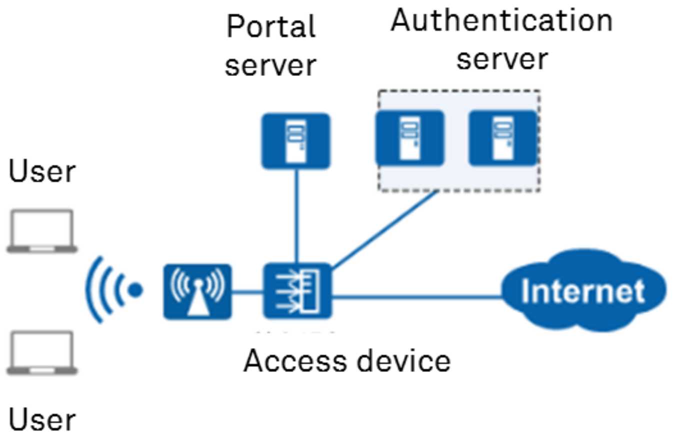
In some cases, user terminals cannot be installed with the 802.1x client software; and mobile phones directly implement 802.1x dial-up, without the need to install the 802.1x client software. For such user terminals and mobile phones, MAC address authentication can be enabled on the access device connected to them. After that, the access device uses the terminal's or mobile phone's MAC address as the user name and password, and sends it to the authentication server for authentication.

If authentication is successful, the access device enables the interface connected to the user's terminal and allows the user to access the network. If authentication fails, the access device forbids the user to access the network.

3.3 Typical Portal Authentication Scenario

To ensure network security, user access to the network needs to be controlled. Only the users who are successfully authenticated can access network resources authorized by administrators.

Figure 3-3 Typical Portal authentication scenario



If a user wants only to perform Portal authentication through web access, Portal authentication can be enabled on the access device connected to the user.

After that, when the user attempts to access the Internet, the access device will forcibly redirect the user to the Portal authentication website to start Portal authentication.

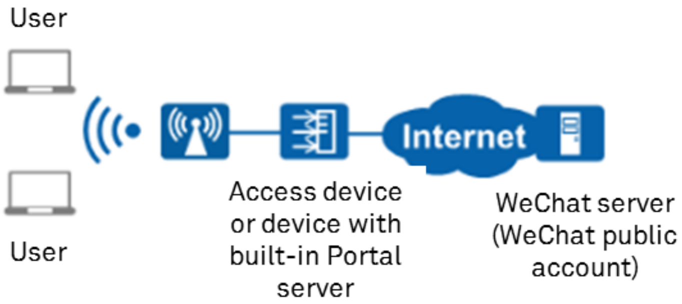
If authentication is successful, the access device enables the interface connected to the user and allows the user to access the network. If authentication fails, the access device forbids the user to access the network.

3.4 Typical WeChat Authentication Scenario

In order to attract more customers, merchants prefer to provide free Wi-Fi services and push advertisements to them through their WeChat public accounts.

To ensure network security, user access to the network needs to be controlled. Only the users whose WeChat accounts are successfully authenticated can access network resources authorized by administrators.

Figure 3-4 Typical WeChat authentication scenario


User
Internet
User
Access device or device with built-in Portal server
WeChat server (WeChat public account)

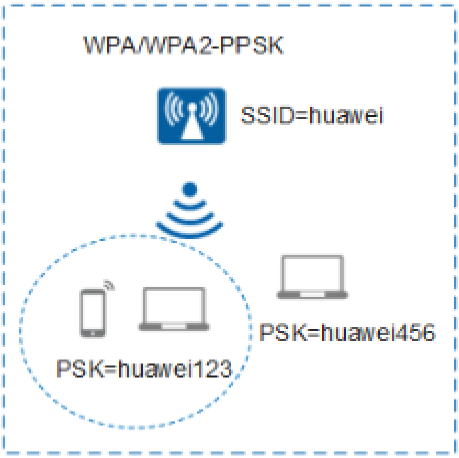
The WeChat authentication function is configured on the access device. After that, when a user attempts to access the network, the user is forcibly redirected to the WeChat authentication page to start WeChat authentication. The authentication process starts with a period of pre-authentication time, during which the user can temporarily access the network.

If authentication is successful, the access device allows the user to continue to access the network. If authentication fails, the access device forbids the user to access the network after the period of pre-authentication time expires.

3.5 Typical WPA/WPA2-PPSK Authentication Scenario

A hotel wants to deploy a simple and secure network for wireless Internet access. With WPA/WPA2–PPSK authentication enabled, different STAs can use different passwords.

Figure 3-5 Typical WPA/WPA2-PPSK authentication scenario



WPA/WPA2-PSK requires that all WLAN clients connecting to a single SSID have the same key, which may result in security vulnerabilities. WPA/WPA2-PPSK, however, allows each WLAN client connecting to a single SSID to have a different key, and different users are granted different authorizations. Additionally, in WPA/WPA2-PPSK mode, a user who owns multiple WLAN clients can use the same PPSK account to connect to the network.

A Acronyms and Abbreviations

A	
AP	Access Point
AC	Access Controller
AES	Advanced Encryption Standard
ACL	Access Control List
C	
CCMP	Counter CBC-MAC Protocol
P	
PSK	Pre-Shared Key
PPSK	Private Pre-Shared Key
S	
STA	Station
SSID	Service Set Identifier
T	
TKIP	Temporal Key Integrity Protocol
W	
WLAN	Wireless Local Area Network
WPA	Wi-Fi Protected Access

WAPI	Wireless LAN Authentication and Privacy Infrastructure
WEP	Wired Equivalent Privacy

Huawei Technologies Co., Ltd.
Address: Huawei Industrial Base Bantian,
Longgang Shenzhen 518129 People's Republic of China
Website: e.huawei.com