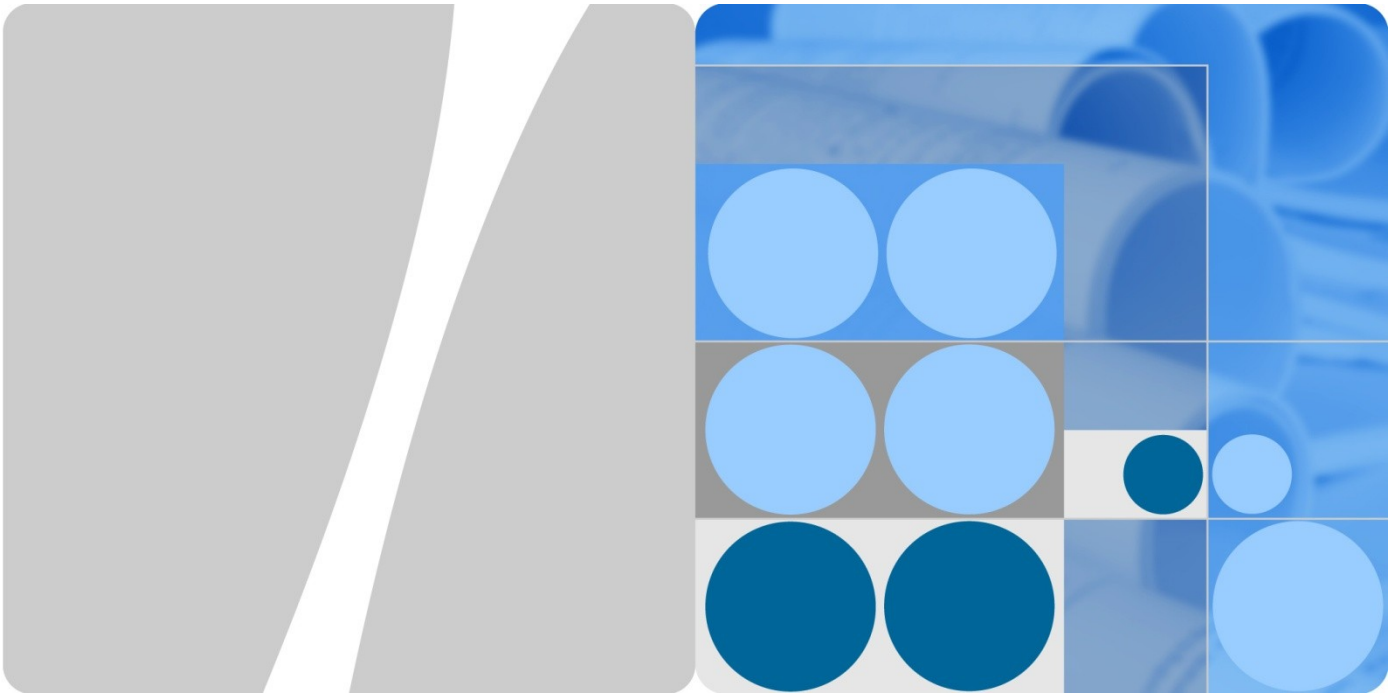


WLAN Access Security Technical White Paper

Issue 02

Date 2012-09-24

HUAWEI TECHNOLOGIES CO., LTD.

Trademarks and Permissions


and other Huawei trademarks are trademarks of Huawei Technologies Co., Ltd.

All other trademarks and trade names mentioned in this document are the property of their respective holders.

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 the 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://enterprise.huawei.com/
Email:	ChinaEnterprise_TAC@huawei.com
Address:	Huawei Industrial Base Bantian, Longgang Shenzhen 518129 People's Republic of China

1 WLAN Access Security

About This Chapter

1.1 Introduction to WLAN Access Security

Definition

802.11-based WLAN provides high wireless access bandwidth, so more users start to use the WLAN and have high requirements for security. How to protect the security of confidential data and user privacy is telecom operators' top concern.

Radio signals are transmitted in a free space and can be received by any device that supports 802.11. Security of radio signals has always been a concern. Related authentication and encryption technologies have been developed for WLAN security. The WLAN system has a series of security mechanisms applying to various scenarios such as home WLANs, enterprise WLANs, campus WLANs, and large-scale carrier WLANs.

WLAN access security includes the security attribute configuration, encryption and decryption of wireless frames, and key management.

WLAN security features involve the following aspects:

- STA authentication: Only authenticated STAs can be associated with the APs.
- Data encryption: Data packets are encrypted and only specified devices can successfully decrypt the data packets. Other WLAN devices can receive data packets but fail to decrypt these packets because they do not have the required key. This protects WLAN data.
- User authentication and encryption: Users are differentiated and their access authority is controlled. Users can access limited network resources during link authentication and can access all network resources only after being authenticated.

Purpose

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

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

Benefits

Benefits to users

WLAN security features ensure security for confidential data and user privacy on WLANs.

1.2 Principles

1.2.1 Introduction

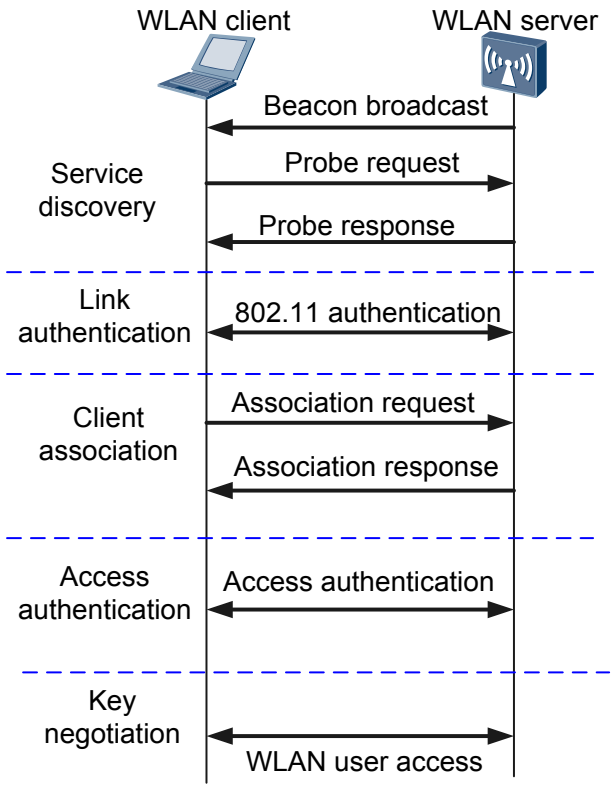
A WLAN enables STAs to access the Internet.

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

On a WLAN, there are STAs and WLAN servers. A STA is a host with a wireless network interface card (NIC), and a WLAN server is an access point (AP).

Figure 1-1 shows the WLAN access process.

Figure 1-1 WLAN access process



1. WLAN service discovery

   Before using any network, a network must be discovered. To use a wired network, the network cable must be inserted properly. However, to connect to a WLAN, a STA has to discover the WLAN service first.

   - The WLAN server sends a Beacon frame to advertise the WLAN service that it provides. The 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 network with the specified SSID exists. If the network exists, 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

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

   The STA has already obtained the service configuration parameters such as the access authentication algorithm and encryption key in the WLAN service discovery stage. These parameters are carried by the Beacon frame or Probe Response message sent by

the WLAN server. In the association stage, the association or re-association request sent by the STA carries the STA's parameters and the parameters that the STA selects according to the service configuration. The parameters include 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. If access authentication is not enabled, STAs can access the WLAN without authentication. If access authentication is enabled, the WLAN server performs access authentication on STAs.

4. Access authentication

   Access authentication ensures network security. WLAN supports 802.1x authentication, pre-shared key (PSK) authentication, portal authentication, and MAC address authentication. PSK authentication is dedicated to WLAN users, and 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 with 802.1x authentication and PSK authentication. The authentication algorithm is determined during 802.11 link negotiation. The WLAN server triggers access authentication after link negotiation succeeds 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 transmission security. IEEE 802.11i and 802.1x define the EAPOL-Key mechanism to ensure data security on WLANs. It is a 4-way handshake mechanism used for key negotiation between the WLAN server and STAs. The negotiated key is used to encrypt and decrypt data 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 stage in 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. EAPOL-Key packets are exchanged between the STA and server during key negotiation. A STA and a server use a 4-way handshake mechanism to negotiate the key used for unicast data packets, and the WLAN server uses the group key handshake mechanism to notify all STAs of the key 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 used to ensure data privacy. Only data of STAs that have keys and are authenticated are protected during data transmission.

Table 1-1 describes authentication and encryption modes supported by Huawei WLAN.

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

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 has two authentication modes: open system authentication and shared key authentication. • WEP uses the RC4 algorithm to encrypt packets exchanged between an AP

Type	Feature
	and a STA. The encryption key cannot automatically change, and the stream cipher is easy to decipher. Therefore, WEP is seldom used. • Open system authentication is the mainstream authentication mode used on carrier networks and usually used together with Portal authentication.
WPA/WPA2-PSK	• 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 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 security risks as the 802.11 pre-shared key authentication. • No client needs to be installed. • WPA and WPA2-PSK are seldom used because no one maintains the passwords.
802.1x	• IEEE 802.1x defines only the identity authentication framework, but not a complete standard. IEEE 802.1x requires other protocols for authentication. The protocols include Extensible Authentication Protocol (EAP), LEAP, EAP-TLS, EAP-TTLS and PEAP. • 802.1x is a Layer 2 protocol. A STA and AP mutually authenticate each other, and multicast is supported. • 802.1x requires specific client software. If 802.1x is used only for authentication, no client software is required and the ISO, Android, and Windows operating systems support 802.1x. • 802.1x authentication is widely used on enterprise networks and is seldom used on carrier networks.
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 authentication and key management modes: certificated-based mode (WAPI-CERT) and pre-shared key-based mode (WAPI-PSK). • 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 web browsers such as Internet Explorer and does not require 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

Type	Feature
	address and IP address of the terminal because the packet sent to the access server do not contain the MAC address of the user terminal. • Portal authentication is widely used on enterprise and carrier networks.
MAC	• In MAC address authentication, a user terminal sends its MAC address as the identity information to an access device. • Users do not need to enter the user name and password to access the network. MAC address authentication is widely used in scenarios where high security is not required.

Huawei WLAN security feature provides flexible solutions by combining multiple authentication and encryption modes for customers. 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.

1.2.2 STA Authentication

IEEE 802.11 requires that STAs pass link authentication before connecting to a WLAN. 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.

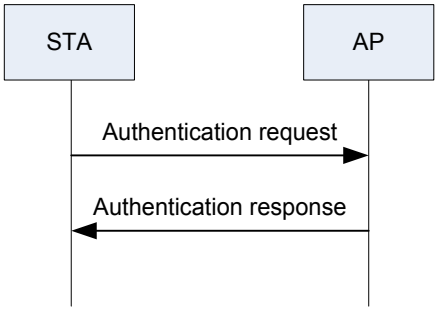
There are two STA authentication modes: open system authentication and shared key authentication. Some products support MAC address filtering that filters out STAs with unauthorized MAC addresses.

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 WLANs with a large number of users.

Open system authentication consists of only two steps, as shown in Figure 1-2. 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 1-2 Open system authentication



The open system authentication process is as follows:

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

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

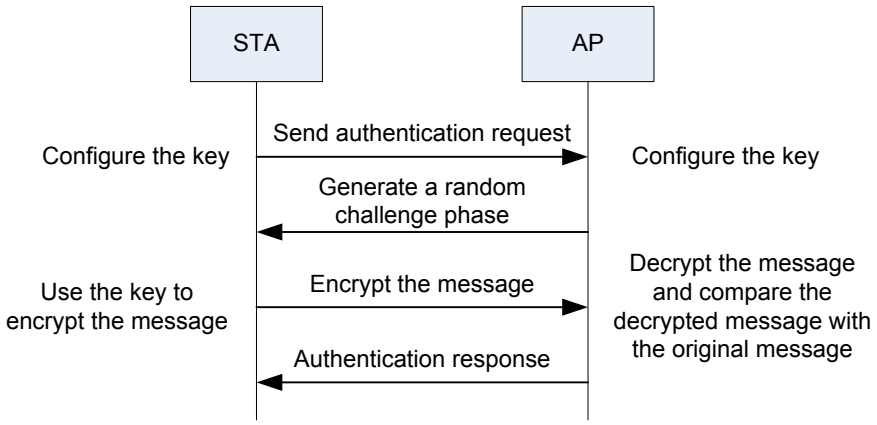
- Advantages: Open system authentication can be used on wireless devices that do not support complex authentication algorithms. This authentication mode allows STAs to connect to a WLAN quickly.
- Disadvantages: Open system authentication cannot distinguish hacker STAs from authorized STAs. When this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

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 1-3, 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).

Figure 1-3 Shared key authentication



The shared key authentication process is as follows:

1. The STA sends an authentication request to the AP.
2. The AP generates a random challenge phrase (character string) and sends it to the STA.
3. The STA copies the challenge phase 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 is not suitable for large-scale networks because a long key string must be configured on each device.
  - 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 by this key. This threatens WLAN security.

WEP authentication is widely used in the early stage of WLAN construction. When open system authentication is used, STAs do not need to be authenticated. When shared key authentication is used, STAs need to be authenticated. Encryption can be configured in both the two authentication modes. WEP supports the following authentication and encryption combinations:

- Open system authentication + plain text: The configuration details are as follows:

```
<Quidway> system-view
[Quidway] wlan
[Quidway-wlan-view] security-profile name huawei
[Quidway-wlan-sec-prof-huawei] security-policy wep
[Quidway-wlan-sec-prof-huawei] wep authentication-method open-system
```

- Open system authentication + cipher text: The configuration details are as follows:

```
<Quidway> system-view
[Quidway] wlan
[Quidway-wlan-view] security-profile name huawei
[Quidway-wlan-sec-prof-huawei] security-policy wep
[Quidway-wlan-sec-prof-huawei] wep authentication-method open-system data-
encrypt
```

- Shared key + plain text: The configuration details are as follows:

```
<Quidway> system-view
[Quidway] wlan
[Quidway-wlan-view] security-profile name huawei
[Quidway-wlan-sec-prof-huawei] security-policy wep
[Quidway-wlan-sec-prof-huawei] wep key wep-40 pass-phrase 0 simple 12345
[Quidway-wlan-sec-prof-huawei] wep default-key 0
```

- Shared key + cipher text: The configuration details are as follows:

```
<Quidway> system-view
[Quidway] wlan
[Quidway-wlan-view] security-profile name huawei
[Quidway-wlan-sec-prof-huawei] security-policy wep
[Quidway-wlan-sec-prof-huawei] wep key wep-40 pass-phrase 0 simple 12345
[Quidway-wlan-sec-prof-huawei] wep default-key 0
```

Configuring and managing static passwords are complex. Some products support dynamic WEP authentication. That is, 802.1x authentication is used to negotiate keys in open system authentication mode. The process of dynamic WEP authentication is similar to the process of WPA authentication. WEP authentication does not ensure high security, so WPA is used

instead of dynamic WEP. The combination mode of dynamic WEP is as follows: open system authentication + 802.1x + cipher text.

MAC Address Filtering

Each AP has a list of MAC addresses allowed to access the WLAN (whitelist) and a list of MAC addresses that are not allowed to access the WLAN (blacklist). The whitelist and blacklist can be configured.

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.

The STA blacklist configuration is as follows:

```
<Quidway> system-view
[Quidway] wlan
[Quidway-wlan-view] sta-access-mode ap 0 blacklist
[Quidway-wlan-view] sta-blacklist 286E-D488-B74F
```

The STA whitelist configuration is as follows:

```
<Quidway> system-view
[Quidway] wlan
[Quidway-wlan-view] sta-access-mode ap 0 whitelist
[Quidway-wlan-view] sta-whitelist 286E-D488-B74F
```

1.2.3 User Identity Authentication and Encryption

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

- Users can access limited network resources during link authentication and can access all network resources only after being authenticated.
- Access devices can differentiate users and control access authority of users.
- Link-layer authentication protocols apply to all network-layer protocols.

User identity authentication involves the following authentication modes:

- WPA/WPA2-PSK authentication
- 802.1x authentication
- WAPI authentication
- Portal authentication
- MAC address authentication

WPA-PSK Authentication

WPA-PSK uses the pre-shared key for authentication and the temporal key for pair main key (PMK) negotiation.

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

WPA-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, and the GTK is used to encrypt multicast and broadcast radio packets.

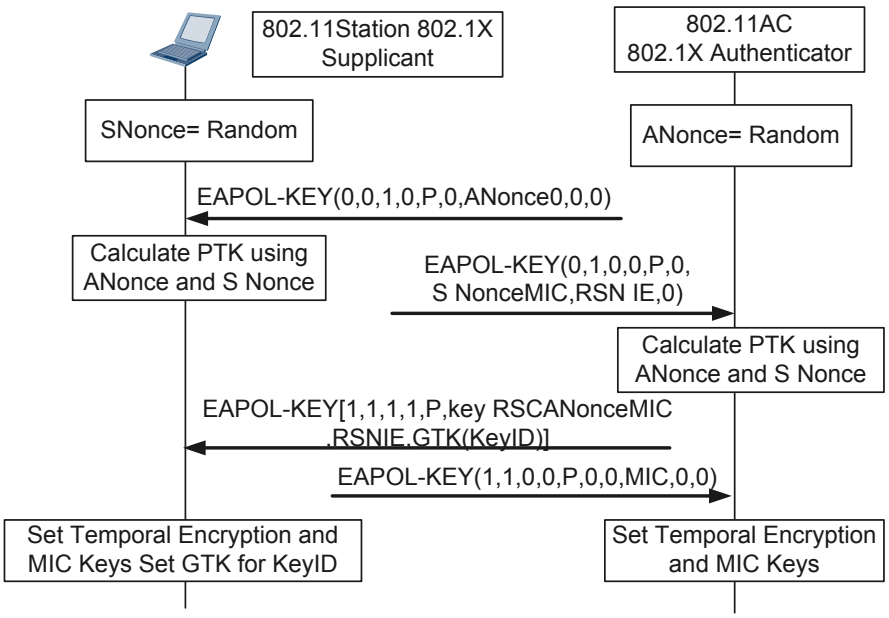
IEEE 802.l1i defines two key hierarchies: the pairwise key hierarchy that describes all keys used by a pair of devices, and the group key hierarchy that describes keys shared by all devices.

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 used 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 1-4 4-way unicast EAPOL-Key negotiation



As shown in Figure 1-4, 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 AC randomly generates the ANonce and sends it to the STA. 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 with the SNonce, robust security network (RSN) information element, and message integrity code (MIC) to the WLAN server.
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 temporal keys.
5. The WLAN client sends an EAPOL-Key frame to the WLAN server to confirm that the temporal keys are installed. The WLAN server starts to install the temporal keys after receiving the EAPOL-Key frame.

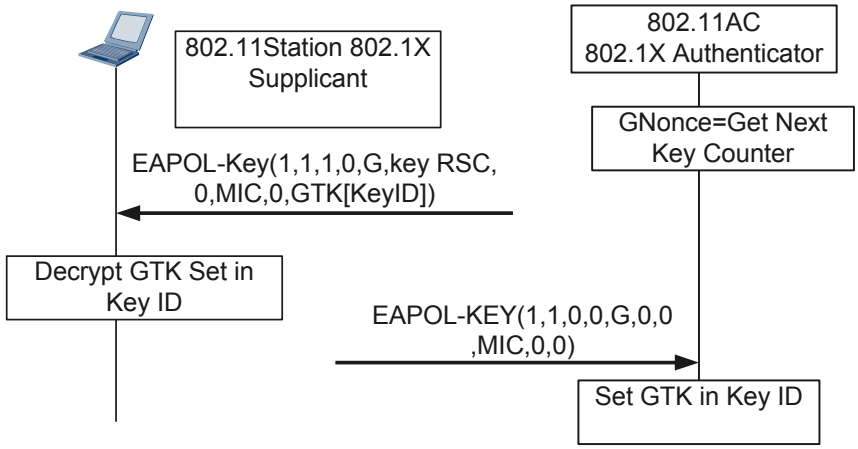
- 2-way multicast EAPOL-Key negotiation

  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 1-5 2-way multicast EAPOL-Key negotiation



As shown in Figure 1-5, the 4-way unicast 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.

802.1x

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 authentication users and control user access.

802.1x is a port-based network access control protocol that defines an authentication process and supports multiple authentication protocols. All authentication protocols used in 802.1x authentication use EAP to encapsulate protocol packets. 802.1x only controls the authentication process, and authentication protocols complete authentication.

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 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 used. 802.1x authentication can be used to authenticate a single user, user groups, or access devices.
- Industry standards: Both 802.1x and the Ethernet standard 802.3 are IEEE standards, so 802.1x can seamlessly integrate with the Ethernet technologies. Clients running the Windows, Linux, ISO, and Android operating systems support the 802.1x protocol.

802.1x authentication using EAP-TLS

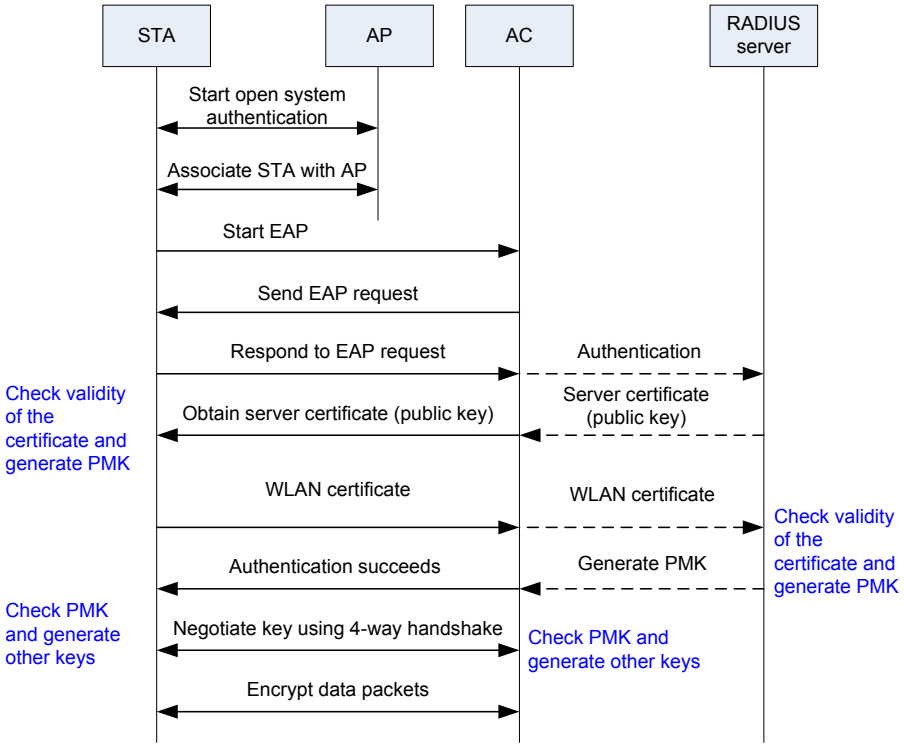
EAP-TLS uses Transport Layer Security (TLS) to ensure secure communication and data transfer. TLS is developed by the IETF to replace the Secure Socket Layer (SSL) protocol and can protect data from eavesdropping and tampering. EAP-TLS uses Public Key Infrastructure (PKI) to secure communication with 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 1-6 shows the EAP-TLS authentication process.

Figure 1-6 802.1x authentication using EAP-TLS



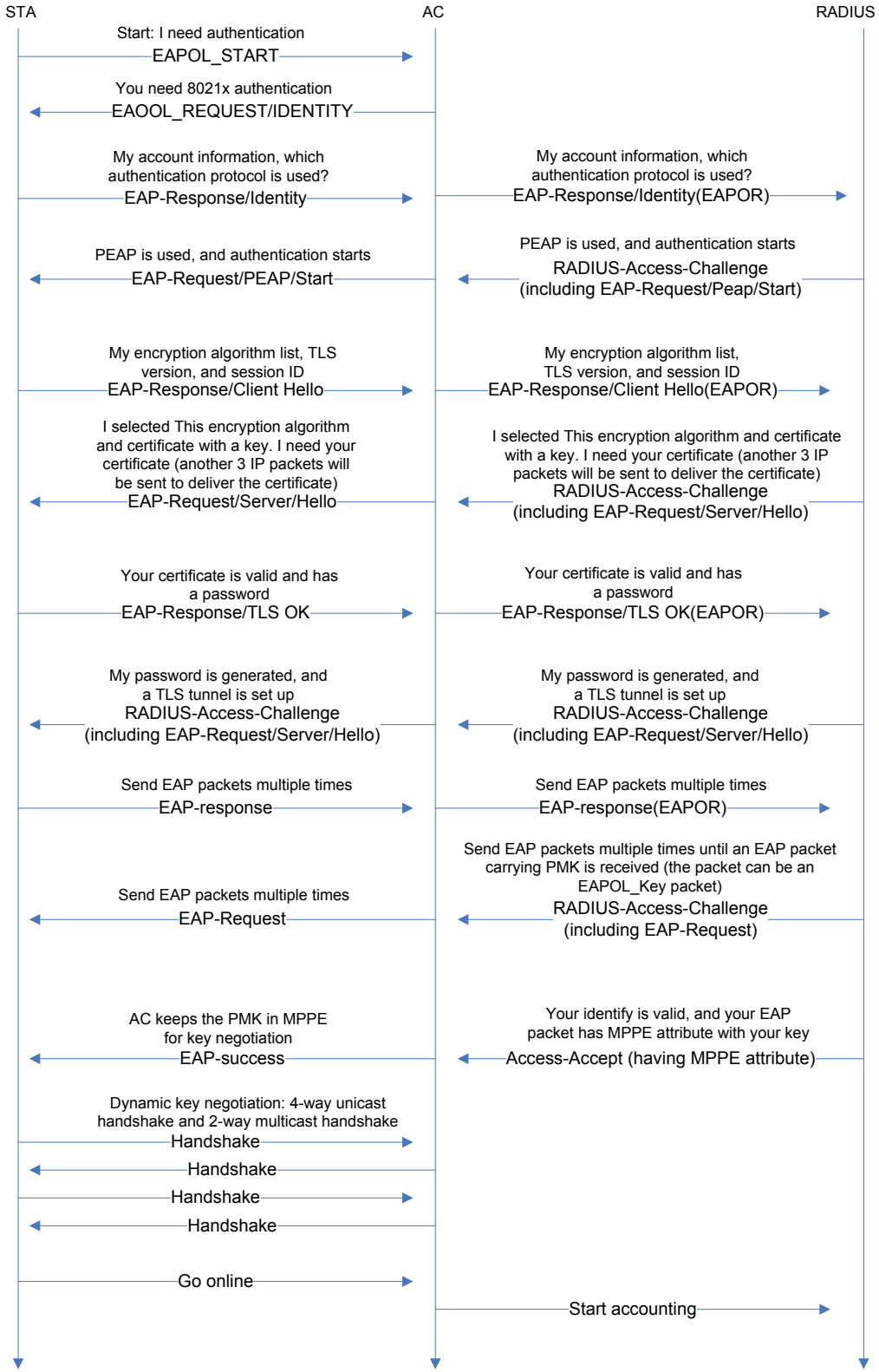
802.1x authentication using EAP-PEAP

When 802.1x authentication is used on WLANs, the message digest 5 (MD5) algorithm and EAP are not used, but 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 used. TLS negotiation in EAP-PEAP authentication is the same as TLS negotiation 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. PEAP-EAP can use only EAP for authentication, whereas EAP-TLS can use only EAP but also other authentication protocols such as PAP and CHAP.

Figure 1-7 shows the EAP-PEAP authentication process.

Figure 1-7 802.1x authentication using EAP-PEAP



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 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 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 be 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 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 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.

NOTE

The WAPI-PSK mode is applicable to individual users and small-scale enterprise networks, and the WAPI-CERT mode is applicable to large-scale enterprise networks and carrier networks. To use the WAPI-CERT mode, an enterprise or a carrier must deploy and maintain an expensive certificate system.

- WAPI certificate authentication

Figure 1-8 WAPI certificate authentication

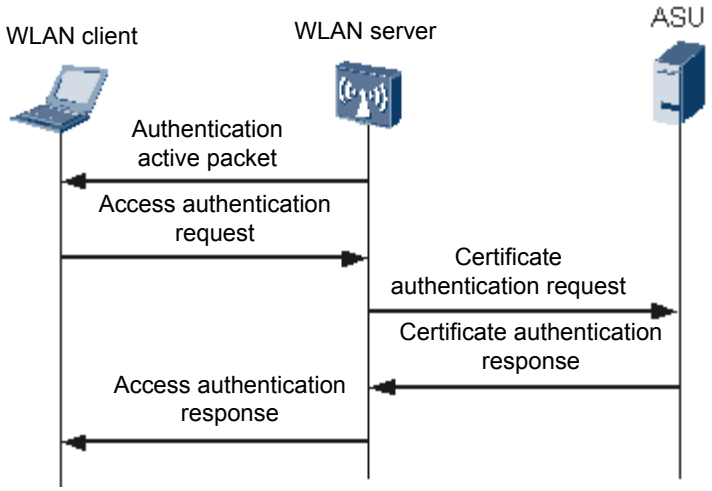


Figure 1-8 shows the WAPI certificate authentication process.

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 packet time.
3. Certificate authentication request: after the WLAN server receives the access authentication request, it constructs a certificate authentication request 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 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 client.
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 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 certain amount of data.

Figure 1-9 WAPI key negotiation

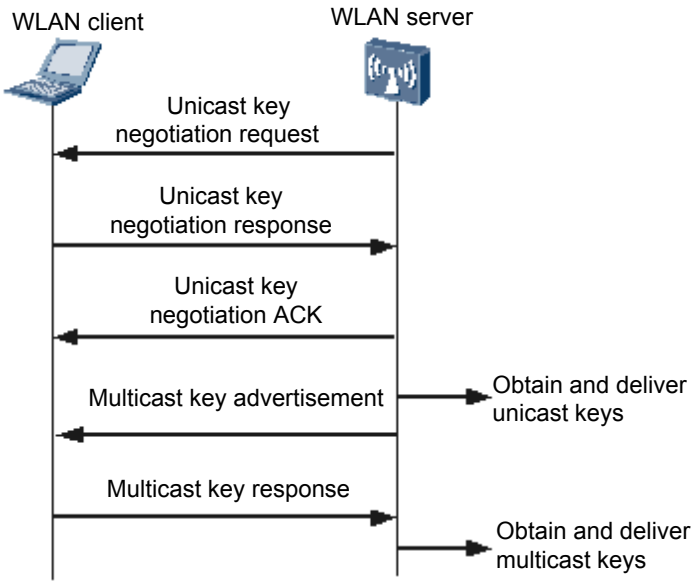


Figure 1-9 shows the process of WAPI key negotiation.

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 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 packet 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:

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

  b 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 the 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 packet.

  c 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.

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

2. Multicast key advertisement

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

   - Multicast key advertisement

     The WLAN client 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:

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 server discards the response packet.

b. 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 controller port status to On.

NOTE

WAPI differs from WEP/WPA/WPA2 in the following aspects:

- WAPI allows a WLAN client and a WLAN server to authenticate each other.
- The WAPI-CERT mode uses a public key to authenticate certificates of the WLAN server and client.
- Although WAPI uses an asymmetric encryption algorithm in authentication, it uses a symmetric encryption algorithm in data transmission. This improves the encryption and decryption efficiency and facilitates software and hardware implementation.

Combination of WAPI authentication and encryption

- WAPI certificate authentication

```
<Quidway> system-view
[Quidway] wlan
[Quidway-wlan-view] security-profile name huawei
[Quidway-wlan-sec-prof-huawei] security-policy wapi
[Quidway-wlan-sec-prof-huawei] wapi authentication-method certificate
[Quidway-wlan-sec-prof-huawei] wapi asu ip 10.10.10.1
[Quidway-wlan-sec-prof-huawei] wapi import certificate ac file-name
flash:/huawei-ac.cer
[Quidway-wlan-sec-prof-huawei] wapi import certificate asu file-name
flash:/huawei-asu.cer
[Quidway-wlan-sec-prof-huawei] wapi import certificate issuer file-name
flash:/huawei-asu.cer
[Quidway-wlan-sec-prof-huawei] wapi import private-key file-name flash:/huawei-
ac.cer
```

- WAPI pre-shared key authentication

```
<Quidway> system-view
[Quidway] wlan
[Quidway-wlan-view] security-profile name huawei
[Quidway-wlan-sec-prof-huawei] security-policy wapi
[Quidway-wlan-sec-prof-huawei] wapi authentication-method psk pass-phrase
simple 01234567
```

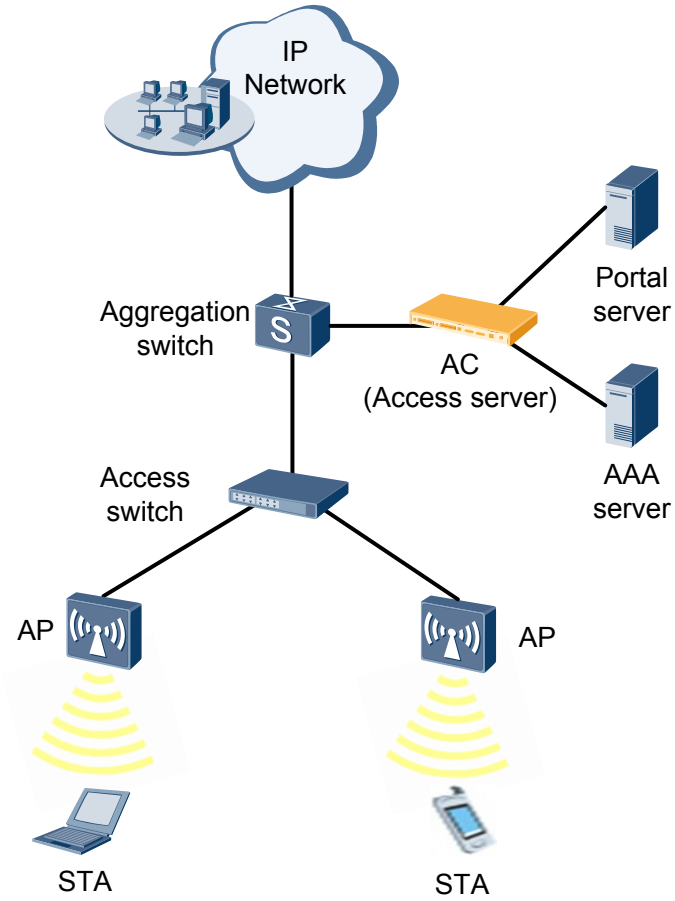
Portal Authentication

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.

The 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 Internet content union. The Portal authentication is frequently used on carrier or enterprise WLANs.

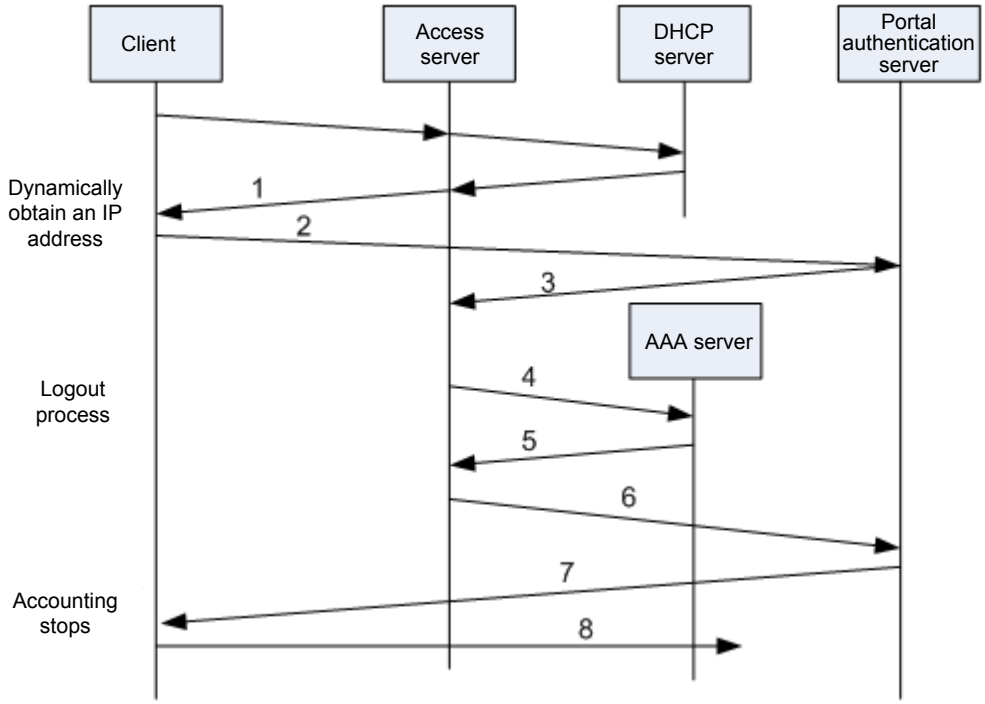
The Portal authentication system consists of four basic elements: client, access server, Portal server, and AAA server. Figure 1-10 shows the networking diagram. The AC functions as an access server.

Figure 1-10 Portal authentication system



The Portal authentication includes the Layer 2 authentication and Layer 3 authentication. Layer 2 authentication differs from Layer 3 authentication. In the Layer 2 authentication, the MAC address of the server to which a user is to visit cannot be obtained. Therefore, binding information check between MAC and IP addresses cannot be performed. The Layer 2 authentication has low security. In the Layer 3 authentication, ARP request packets cannot be routed, and ARP detection cannot be performed to check whether a user is online. The Layer 2 authentication and Layer 3 authentication processes are the same, as shown in Figure 1-11.

Figure 1-11 Portal authentication system



1. A dynamic user obtains the IP address through DHCP (a static user can manually configure the address).
2. The user visits the authentication page of the Portal authentication server, and enters the user name and password to log in.
3. The Portal authentication server notifies the access server of the user information through internal protocols.
4. The AAA server authenticates the user.
5. The AAA server sends the authentication result to the access server.
6. The access server notifies the Portal authentication server of the authentication result.
7. The Portal authentication server displays the authentication result on the HTTP page to notify the user.
8. If the authentication succeeds, the user can access network resources.

A Portal authentication user may request the termination of service or be disconnected unexpectedly.

Figure 1-12 Request termination of service

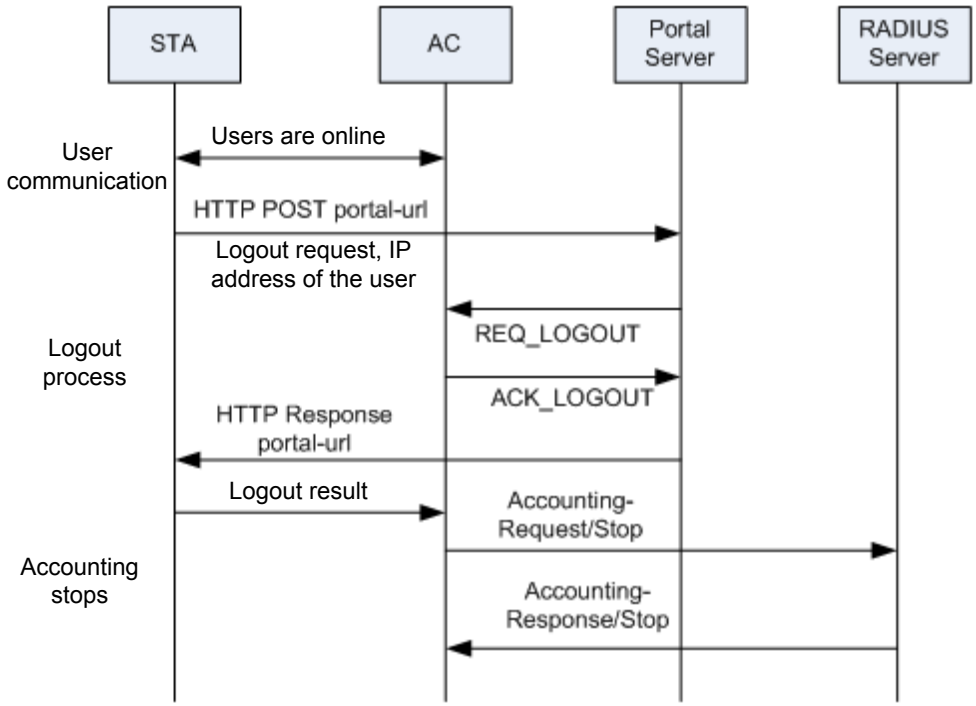


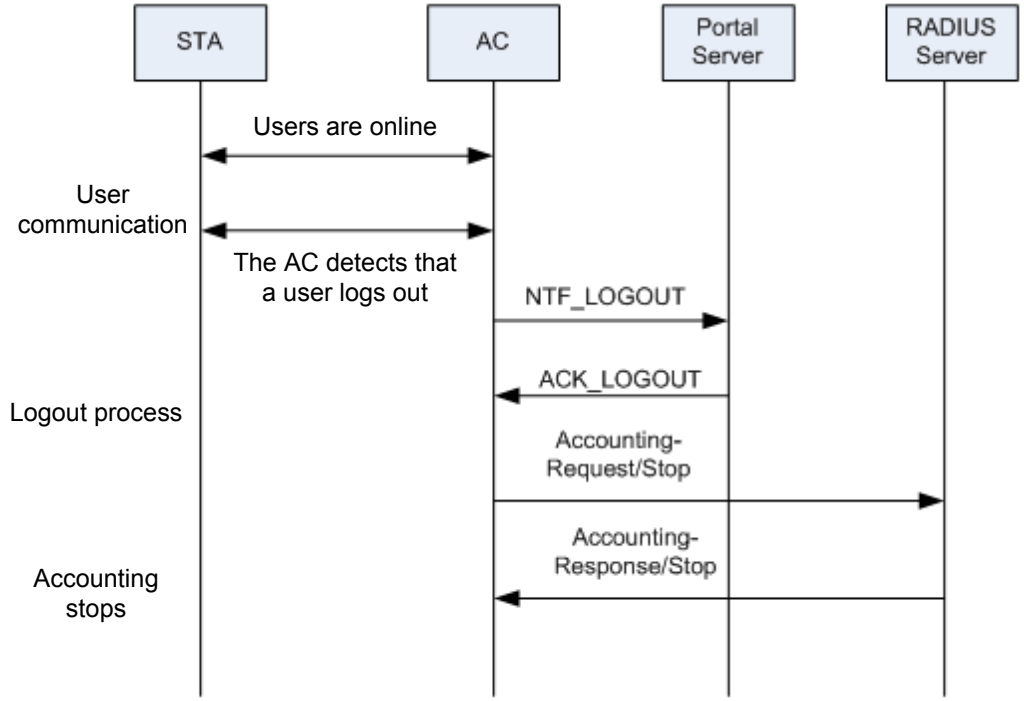
Figure 1-12 shows the process for a user to request termination of services.

1. To go offline, a user clicks **Logout** on the authentication page and sends a logout request to the Portal server.
2. The Portal server sends a logout request to the AC.
3. The AC returns a logout ACK packet to the Portal server.
4. The Portal server returns the HTTP response and directs the user to the HTTP page that contains corresponding information based on the logout ACK packet.
5. When the AC receives a logout request, it sends an accounting-stop packet to the RADIUS server.
6. The RADIUS server sends a response packet to the AC.

A user is disconnected unexpectedly.

The AC detects that a user logs out. Figure 1-13 shows the process:

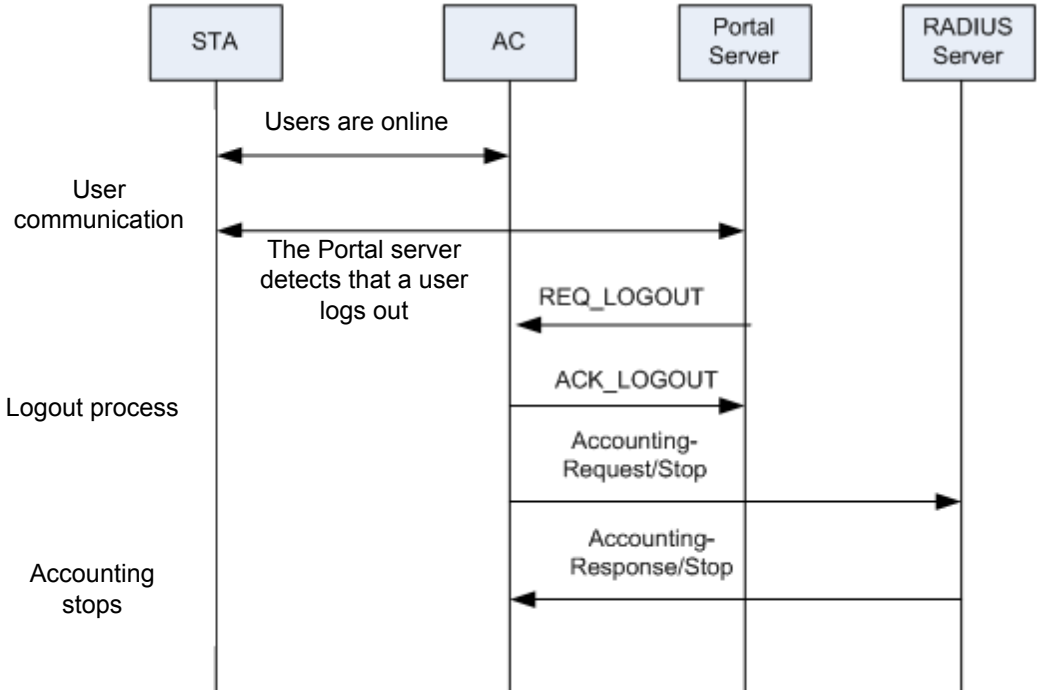
Figure 1-13 Unexpected user logout detected by the AC



1. The AC detects that a user logs out and sends a logout request to the Portal server.
2. The Portal server returns a logout ACK packet.
3. After receiving the logout ACK packet, the AC sends an accounting-stop packet to the RADIUS server.
4. The RADIUS server sends a response packet to the AC.

The Portal server detects that a user logs out. Figure 1-14 shows the process:

Figure 1-14 Unexpected logout detected by the Portal server



1. The Portal server detects that a user logs out and sends a logout request to the AC.
2. The AC returns a logout ACK packet.
3. When the AC receives a logout request, it sends an accounting-stop packet to the RADIUS server.
4. The RADIUS server sends a response packet to the AC.

MAC Address Authentication

MAC address authentication controls the network access authority of a user based on the access interface and MAC address of the user. The user does not need to install any client software. After detecting the MAC address of a user for the first time, the device starts authenticating the user. The RADIUS server is used to authenticate WLAN terminals in MAC address authentication. After the access device obtains the MAC address of a client, it sends an authentication request to the RADIUS server. The RADIUS server authenticates the user MAC address and notifies the access device of the authentication result and authorization information. Accounting and authorization can also be implemented based on MAC addresses.

1.2.4 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
- Network layer encryption protocol

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.

For details about the WEP authentication process, see shared key authentication in 1.2.2 STA Authentication.

Static WEP Encryption

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 1-15 WEP encryption process

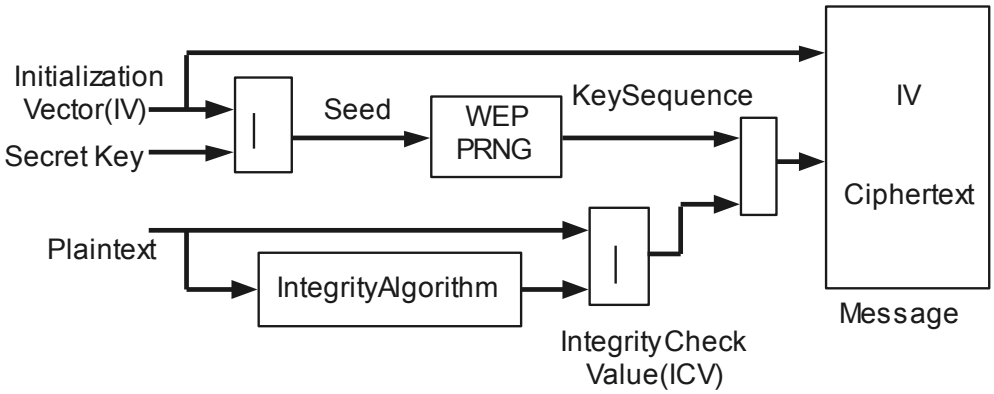


Figure 1-15 shows the WEP encryption process.

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.

Figure 1-16 WEP decryption process

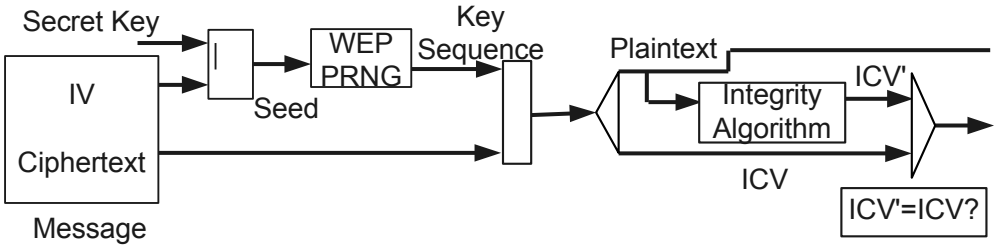


Figure 1-16 shows the WEP decryption process.

1. WEP finds the decryption key according to the Key ID field value in the received MPDU.
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 1-19, 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.

802.1x Dynamic WEP Encryption

Dynamic WEP encryption is more secure than static WEP encryption**.** In dynamic WEP encryption, each client has a private key and a shared key. The private key protects unicast frames, and the shared key protects broadcast and multicast frames. The dynamic WEP keys change periodically to enhance data protection.

802.1x is designed to authenticate the user identity and also plays an important role in WEP encryption improvement. 802.1x allows the keys to be transmitted from the Fat AP or AC to the STA.

Dynamic WEP encryption is only a transition solution and is not used unless the device does not support TKIP. The time for using the WEP key should be short. It is recommended that the time is set to less than 15 minutes to prevent attacks on authorized user data and WLNs.

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 security risks as the 802.11 pre-shared key authentication.

NOTE

Large-scale enterprise networks usually use the WPA enterprise edition.

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.

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 to combine a temporal key, the sender MAC address, and the TKIP sequence counter (TSC) into the WEP seed. Each frame is encrypted using a specific RC4 key, improving security of the IV.

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:

1. 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.
2. TKIP adds a TSC in the IV of each MAC service data unit (MSDU) to prevent replay attacks.
3. TKIP uses the Fast Packet Keying algorithm to generate an encryption key by combining the temporal key with the TSC.
4. TKIP uses the 802.1x EAPoL Key protocol to update temporal keys and MIC keys.

TKIP has the following advantages:

1. 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.
2. Protects SAs and DAs. TKIP can detect SAs and DAs that have been tampered. A MIC is calculated using an SA, DA, and MIC key. Therefore, if the DA or SA is tampered, the

MIC calculated by the receiver is different from the MIC in the received MAC service data unit (MSDU).

3. 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.
4. 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.

CCMP Encryption

Although TKIP improves 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 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:

1. Uses the AES algorithm at the physical layer so that encryption and decryption are performed by hardware. The defects of WEP 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.
2. 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.
   - 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.

WPA supports the following combination of authentication and encryption:WPA-PSK+TKIP

```
<Quidway> system-view
[Quidway] wlan
[Quidway-wlan-view] security-profile name huawei
[Quidway-wlan-sec-prof-huawei] security-policy wpa
[Quidway-wlan-sec-prof-huawei] wpa authentication-method psk pass-phrase simple
01234567 encryption-method tkip
```

- WPA-PSK+CCMP

```
<Quidway> system-view
[Quidway] wlan
[Quidway-wlan-view] security-profile name huawei
[Quidway-wlan-sec-prof-huawei] security-policy wpa
[Quidway-wlan-sec-prof-huawei] wpa authentication-method psk pass-phrase simple
01234567 encryption-method ccmp
```

- WPA2-PSK+TKIP

```
<Quidway> system-view
[Quidway] wlan
[Quidway-wlan-view] security-profile name huawei
[Quidway-wlan-sec-prof-huawei] security-policy wpa2
[Quidway-wlan-sec-prof-huawei] wpa2 authentication-method psk pass-phrase
simple 01234567 encryption-method tkip
```

- WPA2-PSK+CCMP

```
<Quidway> system-view
[Quidway] wlan
[Quidway-wlan-view] security-profile name huawei
[Quidway-wlan-sec-prof-huawei] security-policy wpa2
[Quidway-wlan-sec-prof-huawei] wpa2 authentication-method psk pass-phrase
simple 01234567 encryption-method ccmp
```

- WPA-802.1X+PEAP+TKIP

```
<Quidway> system-view
[Quidway] radius-server template radius_huawei
[Quidway-radius-radius_huawei] radius-server authentication 10.138.18.152 1812
[Quidway-radius-radius_huawei] radius-server accounting 10.138.18.152 1813
[Quidway-radius-radius_huawei] radius-server shared-key simple huawei
[Quidway-radius-radius_huawei] quit
[Quidway] aaa
[Quidway-aaa] authentication-scheme radius_huawei
[Quidway-aaa-authen-radius_huawei] authentication-mode radius
[Quidway-aaa-authen-radius_huawei] quit
[Quidway-aaa] accounting-scheme radius_huawei
[Quidway-aaa-accounting-radius_huawei] accounting-mode radius
[Quidway-aaa-accounting-radius_huawei] quit
[Quidway-aaa] domain peap.radius.com
[Quidway-aaa-domain-peap.radius.com] authentication-scheme radius_huawei
[Quidway-aaa-domain-peap.radius.com] accounting-scheme radius_huawei
[Quidway-aaa-domain-peap.radius.com] radius-server radius_huawei
[Quidway-aaa-domain-peap.radius.com] quit
[Quidway-aaa] quit
[Quidway] interface wlan-ess 0
[Quidway-Wlan-Ess0] dot1x-authentication enable
[Quidway-Wlan-Ess0] dot1x authentication-method eap
[Quidway-Wlan-Ess0] force-domain huawei
[Quidway-Wlan-Ess0] peimit-domain huawei
[Quidway-Wlan-Ess0] quit
[Quidway] wlan
[Quidway-wlan-view] security-profile name huawei
[Quidway-wlan-sec-prof-huawei] security-policy wpa
[Quidway-wlan-sec-prof-huawei] wpa authentication-method dot1x peap encryption-
```

```
method tkip
```

- WPA-802.1x+PEAP+CCMP

```
<Quidway> system-view
[Quidway] radius-server template radius_huawei
[Quidway-radius-radius_huawei] radius-server authentication 10.138.18.152 1812
[Quidway-radius-radius_huawei] radius-server accounting 10.138.18.152 1813
[Quidway-radius-radius_huawei] radius-server shared-key simple huawei
[Quidway-radius-radius_huawei] quit
[Quidway] aaa
[Quidway-aaa] authentication-scheme radius_huawei
[Quidway-aaa-authen-radius_huawei] authentication-mode radius
[Quidway-aaa-authen-radius_huawei] quit
[Quidway-aaa] accounting-scheme radius_huawei
[Quidway-aaa-accounting-radius_huawei] accounting-mode radius
[Quidway-aaa-accounting-radius_huawei] quit
[Quidway-aaa] domain peap.radius.com
[Quidway-aaa-domain-peap.radius.com] authentication-scheme radius_huawei
[Quidway-aaa-domain-peap.radius.com] accounting-scheme radius_huawei
[Quidway-aaa-domain-peap.radius.com] radius-server radius_huawei
[Quidway-aaa-domain-peap.radius.com] quit
[Quidway-aaa] quit
[Quidway] interface wlan-ess 0
[Quidway-Wlan-Ess0] dot1x-authentication enable
[Quidway-Wlan-Ess0] dot1x authentication-method eap
[Quidway-Wlan-Ess0] force-domain huawei
[Quidway-Wlan-Ess0] peimit-domain huawei
[Quidway-Wlan-Ess0] quit
[Quidway] wlan
[Quidway-wlan-view] security-profile name huawei
[Quidway-wlan-sec-prof-huawei] security-policy wpa
[Quidway-wlan-sec-prof-huawei] wpa authentication-method dot1x peap encryption-
method ccmp
```

- WPA-802.1x+TLS+TKIP

```
<Quidway> system-view
[Quidway] radius-server template radius_huawei
[Quidway-radius-radius_huawei] radius-server authentication 10.138.18.152 1812
[Quidway-radius-radius_huawei] radius-server accounting 10.138.18.152 1813
[Quidway-radius-radius_huawei] radius-server shared-key simple huawei
[Quidway-radius-radius_huawei] quit
[Quidway] aaa
[Quidway-aaa] authentication-scheme radius_huawei
[Quidway-aaa-authen-radius_huawei] authentication-mode radius
[Quidway-aaa-authen-radius_huawei] quit
[Quidway-aaa] accounting-scheme radius_huawei
[Quidway-aaa-accounting-radius_huawei] accounting-mode radius
[Quidway-aaa-accounting-radius_huawei] quit
[Quidway-aaa] domain peap.radius.com
[Quidway-aaa-domain-peap.radius.com] authentication-scheme radius_huawei
[Quidway-aaa-domain-peap.radius.com] accounting-scheme radius_huawei
[Quidway-aaa-domain-peap.radius.com] radius-server radius_huawei
[Quidway-aaa-domain-peap.radius.com] quit
[Quidway-aaa] quit
```

```
[Quidway] interface wlan-ess 0
[Quidway-Wlan-Ess0] dot1x-authentication enable
[Quidway-Wlan-Ess0] dot1x authentication-method eap
[Quidway-Wlan-Ess0] force-domain huawei
[Quidway-Wlan-Ess0] peimit-domain huawei
[Quidway-Wlan-Ess0] quit
[Quidway] wlan
[Quidway-wlan-view] security-profile name huawei
[Quidway-wlan-sec-prof-huawei] security-policy wpa
[Quidway-wlan-sec-prof-huawei] wpa authentication-method dot1x tls encryption-
method tkip
```

- WPA-802.1x+TLS+CCMP

```
<Quidway> system-view
[Quidway] radius-server template radius_huawei
[Quidway-radius-radius_huawei] radius-server authentication 10.138.18.152 1812
[Quidway-radius-radius_huawei] radius-server accounting 10.138.18.152 1813
[Quidway-radius-radius_huawei] radius-server shared-key simple huawei
[Quidway-radius-radius_huawei] quit
[Quidway] aaa
[Quidway-aaa] authentication-scheme radius_huawei
[Quidway-aaa-authen-radius_huawei] authentication-mode radius
[Quidway-aaa-authen-radius_huawei] quit
[Quidway-aaa] accounting-scheme radius_huawei
[Quidway-aaa-accounting-radius_huawei] accounting-mode radius
[Quidway-aaa-accounting-radius_huawei] quit
[Quidway-aaa] domain peap.radius.com
[Quidway-aaa-domain-peap.radius.com] authentication-scheme radius_huawei
[Quidway-aaa-domain-peap.radius.com] accounting-scheme radius_huawei
[Quidway-aaa-domain-peap.radius.com] radius-server radius_huawei
[Quidway-aaa-domain-peap.radius.com] quit
[Quidway-aaa] quit
[Quidway] interface wlan-ess 0
[Quidway-Wlan-Ess0] dot1x-authentication enable
[Quidway-Wlan-Ess0] dot1x authentication-method eap
[Quidway-Wlan-Ess0] force-domain huawei
[Quidway-Wlan-Ess0] peimit-domain huawei
[Quidway-Wlan-Ess0] quit
[Quidway] wlan
[Quidway-wlan-view] security-profile name huawei
[Quidway-wlan-sec-prof-huawei] security-policy wpa
[Quidway-wlan-sec-prof-huawei] wpa authentication-method dot1x tls encryption-
method ccmp
```

- WPA2-802.1X+PEAP+TKIP

```
<Quidway> system-view
[Quidway] radius-server template radius_huawei
[Quidway-radius-radius_huawei] radius-server authentication 10.138.18.152 1812
[Quidway-radius-radius_huawei] radius-server accounting 10.138.18.152 1813
[Quidway-radius-radius_huawei] radius-server shared-key simple huawei
[Quidway-radius-radius_huawei] quit
[Quidway] aaa
[Quidway-aaa] authentication-scheme radius_huawei
[Quidway-aaa-authen-radius_huawei] authentication-mode radius
```

```
[Quidway-aaa-authen-radius_huawei] quit
[Quidway-aaa] accounting-scheme radius_huawei
[Quidway-aaa-accounting-radius_huawei] accounting-mode radius
[Quidway-aaa-accounting-radius_huawei] quit
[Quidway-aaa] domain peap.radius.com
[Quidway-aaa-domain-peap.radius.com] authentication-scheme radius_huawei
[Quidway-aaa-domain-peap.radius.com] accounting-scheme radius_huawei
[Quidway-aaa-domain-peap.radius.com] radius-server radius_huawei
[Quidway-aaa-domain-peap.radius.com] quit
[Quidway-aaa] quit
[Quidway] interface wlan-ess 0
[Quidway-Wlan-Ess0] dot1x-authentication enable
[Quidway-Wlan-Ess0] dot1x authentication-method eap
[Quidway-Wlan-Ess0] force-domain huawei
[Quidway-Wlan-Ess0] peimit-domain huawei
[Quidway-Wlan-Ess0] quit
[Quidway] wlan
[Quidway-wlan-view] security-profile name huawei
[Quidway-wlan-sec-prof-huawei] security-policy wpa2
[Quidway-wlan-sec-prof-huawei] wpa2 authentication-method dot1x peap
encryption-method tkip
```

- WPA2-802.1x+PEAP+CCMP

```
<Quidway> system-view
[Quidway] radius-server template radius_huawei
[Quidway-radius-radius_huawei] radius-server authentication 10.138.18.152 1812
[Quidway-radius-radius_huawei] radius-server accounting 10.138.18.152 1813
[Quidway-radius-radius_huawei] radius-server shared-key simple huawei
[Quidway-radius-radius_huawei] quit
[Quidway] aaa
[Quidway-aaa] authentication-scheme radius_huawei
[Quidway-aaa-authen-radius_huawei] authentication-mode radius
[Quidway-aaa-authen-radius_huawei] quit
[Quidway-aaa] accounting-scheme radius_huawei
[Quidway-aaa-accounting-radius_huawei] accounting-mode radius
[Quidway-aaa-accounting-radius_huawei] quit
[Quidway-aaa] domain peap.radius.com
[Quidway-aaa-domain-peap.radius.com] authentication-scheme radius_huawei
[Quidway-aaa-domain-peap.radius.com] accounting-scheme radius_huawei
[Quidway-aaa-domain-peap.radius.com] radius-server radius_huawei
[Quidway-aaa-domain-peap.radius.com] quit
[Quidway-aaa] quit
[Quidway] interface wlan-ess 0
[Quidway-Wlan-Ess0] dot1x-authentication enable
[Quidway-Wlan-Ess0] dot1x authentication-method eap
[Quidway-Wlan-Ess0] force-domain huawei
[Quidway-Wlan-Ess0] peimit-domain huawei
[Quidway-Wlan-Ess0] quit
[Quidway] wlan
[Quidway-wlan-view] security-profile name huawei
[Quidway-wlan-sec-prof-huawei] security-policy wpa2
[Quidway-wlan-sec-prof-huawei] wpa2 authentication-method dot1x peap
encryption-method ccmp
```

- WPA2-802.1x+TLS+TKIP

```
<Quidway> system-view
[Quidway] radius-server template radius_huawei
[Quidway-radius-radius_huawei] radius-server authentication 10.138.18.152 1812
[Quidway-radius-radius_huawei] radius-server accounting 10.138.18.152 1813
[Quidway-radius-radius_huawei] radius-server shared-key simple huawei
[Quidway-radius-radius_huawei] quit
[Quidway] aaa
[Quidway-aaa] authentication-scheme radius_huawei
[Quidway-aaa-authen-radius_huawei] authentication-mode radius
[Quidway-aaa-authen-radius_huawei] quit
[Quidway-aaa] accounting-scheme radius_huawei
[Quidway-aaa-accounting-radius_huawei] accounting-mode radius
[Quidway-aaa-accounting-radius_huawei] quit
[Quidway-aaa] domain peap.radius.com
[Quidway-aaa-domain-peap.radius.com] authentication-scheme radius_huawei
[Quidway-aaa-domain-peap.radius.com] accounting-scheme radius_huawei
[Quidway-aaa-domain-peap.radius.com] radius-server radius_huawei
[Quidway-aaa-domain-peap.radius.com] quit
[Quidway-aaa] quit
[Quidway] interface wlan-ess 0
[Quidway-Wlan-Ess0] dot1x-authentication enable
[Quidway-Wlan-Ess0] dot1x authentication-method eap
[Quidway-Wlan-Ess0] force-domain huawei
[Quidway-Wlan-Ess0] peimit-domain huawei
[Quidway-Wlan-Ess0] quit
[Quidway] wlan
[Quidway-wlan-view] security-profile name huawei
[Quidway-wlan-sec-prof-huawei] security-policy wpa2
[Quidway-wlan-sec-prof-huawei] wpa2 authentication-method dot1x tls encryption-
method tkip
```

- WPA2-802.1x+TLS+CCMP

```
<Quidway> system-view
[Quidway] radius-server template radius_huawei
[Quidway-radius-radius_huawei] radius-server authentication 10.138.18.152 1812
[Quidway-radius-radius_huawei] radius-server accounting 10.138.18.152 1813
[Quidway-radius-radius_huawei] radius-server shared-key simple huawei
[Quidway-radius-radius_huawei] quit
[Quidway] aaa
[Quidway-aaa] authentication-scheme radius_huawei
[Quidway-aaa-authen-radius_huawei] authentication-mode radius
[Quidway-aaa-authen-radius_huawei] quit
[Quidway-aaa] accounting-scheme radius_huawei
[Quidway-aaa-accounting-radius_huawei] accounting-mode radius
[Quidway-aaa-accounting-radius_huawei] quit
[Quidway-aaa] domain peap.radius.com
[Quidway-aaa-domain-peap.radius.com] authentication-scheme radius_huawei
[Quidway-aaa-domain-peap.radius.com] accounting-scheme radius_huawei
[Quidway-aaa-domain-peap.radius.com] radius-server radius_huawei
[Quidway-aaa-domain-peap.radius.com] quit
[Quidway-aaa] quit
[Quidway] interface wlan-ess 0
[Quidway-Wlan-Ess0] dot1x-authentication enable
```

```
[Quidway-Wlan-Ess0] dot1x authentication-method eap
[Quidway-Wlan-Ess0] force-domain huawei
[Quidway-Wlan-Ess0] peimit-domain huawei
[Quidway-Wlan-Ess0] quit
[Quidway] wlan
[Quidway-wlan-view] security-profile name huawei
[Quidway-wlan-sec-prof-huawei] security-policy wpa2
[Quidway-wlan-sec-prof-huawei] wpa2 authentication-method dot1x tls encryption-
method ccmp
```

WAPI: SMS4 Algorithm

Chinese National Standard for WLANs 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 Korea.

For details about the SMS4 algorithm, see related technical documents.

Encryption Protocols Used on the Network Layer

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

1.3 Applications

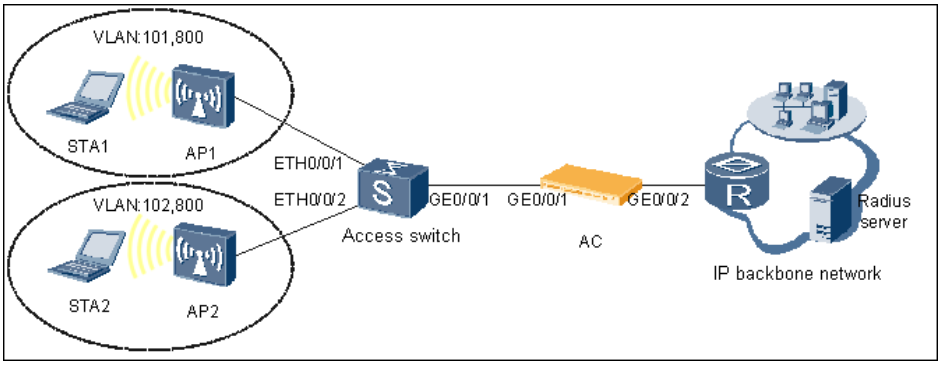
1.3.1 Example for Configuring WPA and 802.1x Authentication

Networking Requirements

As shown in Figure 1-17, the AC connects to the RADIUS server on the upper-layer network, and APs connect to the AC through an access switch.

A simple security policy on a WLAN cannot ensure the network security. The encrypted data on the WLAN may still be deciphered. To ensure network security, RADIUS servers are used to configure 802.1x authentication on a WLAN.

Figure 1-17 Networking diagram of WPA and 802.1x authentication



Configuration Roadmap

The configuration roadmap is as follows:

Configure 802.1x authentication.

1. Enable 802.1x authentication in the system view.
2. Configure a RADIUS authentication scheme used for 802.1x authentication.
3. Create a domain for 802.1x authentication and reference the RADIUS authentication scheme in the AAA domain.

Configure the AC.

1. Configure the switch and the AC to enable APs to communicate with the AC.
2. Configure basic AC attributes, including the AC ID, carrier ID, and source interface that the AC uses to communicate with APs. Configure the AC as a DHCP server.
3. Set the AP authentication mode and add APs to an AP region.
4. Configure virtual APs (VAPs) and deliver VAP parameters so that STAs can access the WLAN.

   Pay attention to the following items when configuring VAPs:

   a Configure a WLAN-ESS interface and bind it to a service set so that radio packets can be sent to the WLAN service module after reaching the AC.

   b Configure a radio profile on the AP and bind it to a radio to enable STAs to communicate with the AP.

   c Configure a security profile on the AP, and configure the security policy as WPA+802.1X+PEAP+CCMP.

   d Configure a service set, set the direct forwarding mode in the service set, and bind the security profile and a traffic profile to it to ensure security and QoS for STAs.

   e Configure a VAP and deliver VAP parameters so that STAs can access the WLAN.

Configuration Files

- Configuration file of the AC

```
#
 sysname AC
#
 vlan batch 101 800
#
 dhcp enable
#
 wlan ac-global carrier id other ac id 1
#
radius-server template radius_huawei
 radius-server authentication 10.1.1.5 1812
 radius-server accounting 10.1.1.5 1813
#
aaa
 authentication-scheme radius_huawei
  authentication-mode radius
 accounting-scheme radius_huawei
  accounting-mode radius
```

```
domain peap.radius.com
  authentication-scheme radius_huawei
  accounting-scheme radius_huawei
  radius-server radius_huawei
#
interface Vlanif101
 ip address 128.1.1.1 255.255.255.0
 dhcp select interface
#
interface Vlanif800
 ip address 172.1.1.1 255.255.255.0
 dhcp select interface
#
interface WLAN-ESS0
 port hybrid pvid vlan 101
 port hybrid untagged vlan 101
 dot1x-authentication enable
 dot1x authentication-method eap
 permit-domain peap.domain.com
 force-domain peap.domain.com
 dhcp enable
#
interface XGigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 101 800
#
wlan
 wlan ac source interface vlanif800
 ap-region id 101
 ap-auth-mode mac-auth
 ap id 1 type-id 6 mac 286E-D42B-0CE5 sn AB34002078
  region-id 101
 wmm-profile name huawei-ap id 0
 traffic-profile name huawei-ap id 0
 security-profile name huawei-ap id 0
  security-policy wpa
  wpa authentication-method dot1x peap encryption-method ccmp
 service-set name huawei id 0
  wlan-ess 0
  ssid huawei
  traffic-profile id 0
  security-profile id 0
  service-vlan 101
 radio-profile name huawei-ap id 0
  wmm-profile id 0
 ap 1 radio 0
  radio-profile id 0
  service-set id 0 wlan 1
#
return
```

1.3.2 Example for Configuring Portal Authentication

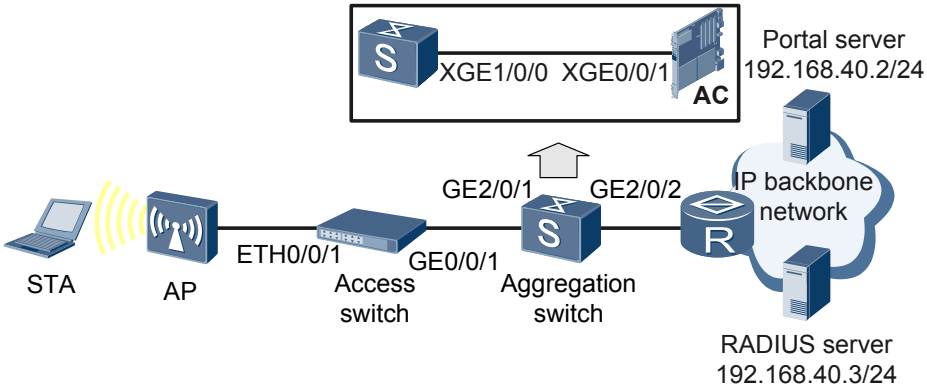
Networking Requirements

As shown in Figure 1-18, the AC connects to a Portal server and a RADIUS server. APs connect to the AC through an access switches.

Due to the openness feature of WLAN, user data on the WLAN faces security risks if no security policy is used on the WLAN. The requirements are as follows:

- The AC performs Portal authentication.
- The RADIUS server performs authentication and accounting.
- Users can access only the Portal authentication server before Portal authentication.
- Users can access the external network after they are authenticated successfully.

Figure 1-18 Portal authentication configuration



The configuration roadmap is as follows:

1. Configure the access switch, wired-side and wireless-side interfaces of the AC to ensure connectivity of the devices.
2. Configure a RADIUS authentication scheme used for Portal authentication.
3. Create a domain for Portal authentication and reference the RADIUS authentication scheme in the AAA domain.
4. Configure a Portal server and bind the Portal server to a VLAN.
5. Configure the WLAN service on the AC.
6. Deliver the WLAN service to APs and verify the configuration.

Configuration Files

- Configuration file of the AC

```
#
 sysname AC
#
 vlan batch 101 800
#
 dhcp enable
#
radius-server template radius_huawei
 radius-server authentication 192.168.40.2 1812
```

```
 radius-server accounting 192.168.40.2 1813
#
web-auth-server test
 server-ip 192.168.40.3
 port 50100
 shared-key simple huawei
 url http://192.168.40.3
#
aaa
 authentication-scheme radius_huawei
  authentication-mode radius
 accounting-scheme radius_huawei
  accounting-mode radius
 domain peap.radius.com
  authentication-scheme radius_huawei
  accounting-scheme radius_huawei
  radius-server radius_huawei
#
 wlan ac-global carrier id other ac id 1
#
interface Vlanif101
 ip address 192.168.20.1 255.255.255.0
 dhcp select interface
 web-auth-server test direct
#
interface Vlanif200
 ip address 192.168.40.1 255.255.255.0
 web-auth-server test direct
#
interface Vlanif800
 ip address 192.168.10.1 255.255.255.0
 dhcp select interface
#
interface WLAN-ESS0
 port hybrid tagged vlan 101
 mac-authentication enable
 dot1x authentication domain peap.huawei.com
#
interface Ethernet2/0/0
 port link-type trunk
 port trunk allow-pass vlan 101 800
#
interface Ethernet2/0/1
 port link-type access
 port default vlan 200
#
wlan
 wlan ac source interface vlanif800
 ap-region id 5
 ap-auth-mode no-auth
 ap id 1 type-id 6 mac 286E-D42B-0CE5 sn AB34002078
  region-id 5
 wmm-profile name huawei id 0
 traffic-profile name huawei id 0
 security-profile name huawei id 0
```

```
 wep authentication-method share-key
 wep key wep-40 pass-phrase 0 simple 12345
service-set name huawei id 0
 wlan-ess 0
 ssid huawei-portal-test
 traffic-profile id 0
 security-profile id 0
 service-vlan 101
radio-profile name huawei-ap id 0
 wmm-profile id 0
ap 1 radio 0
 radio-profile id 0
 service-set id 0 wlan 1
#
return
```