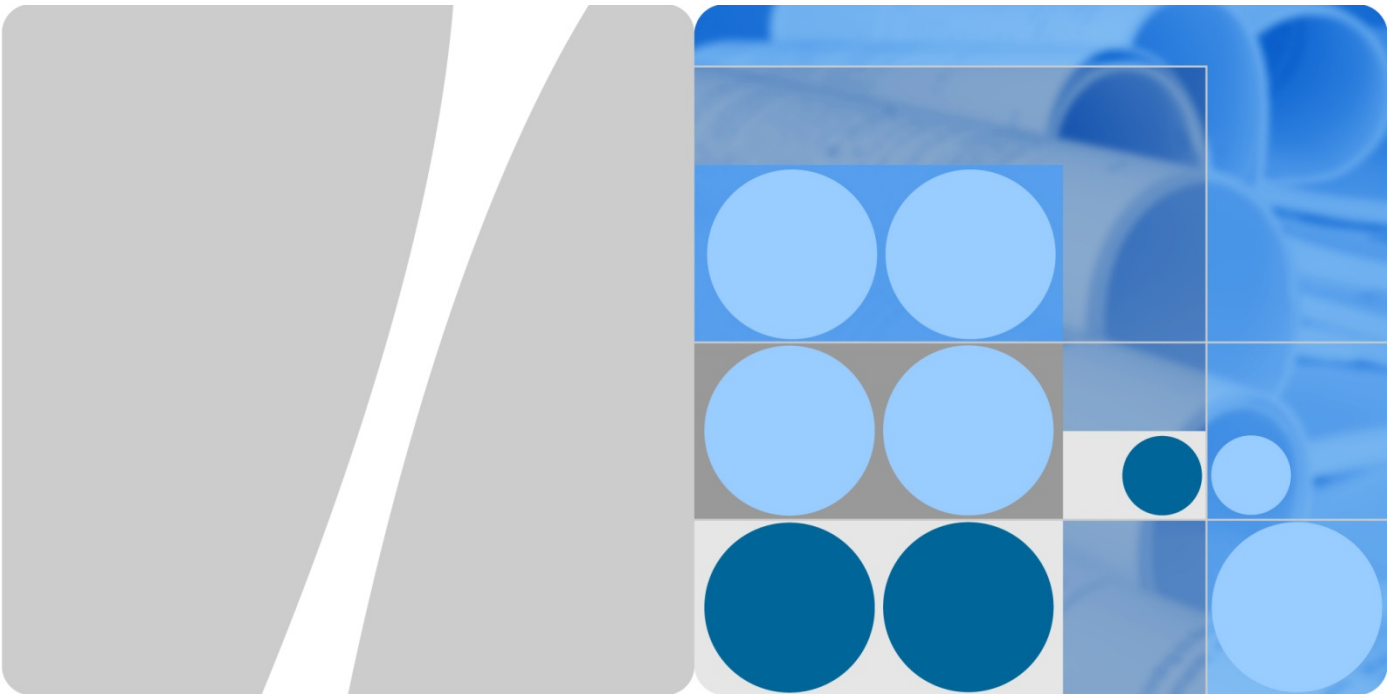


WLAN WIDS & WIPS Technology White Paper

Issue 02

Date 2017-07-05

HUAWEI TECHNOLOGIES CO., LTD.

HUAWEI

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 a warranty of any kind, express or implied.

Huawei Technologies Co., Ltd.

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

Website: http://enterprise.huawei.com

Change History

Changes between document issues are cumulative. The latest document issue contains all the changes made in earlier issues.

Issue 02 (2017-07-05)

This issue is the second official release to match WLAN products in V200R007C20, and has the following updates:

1. Updated the working modes of APs and the working mechanism of the modes.
2. Updated the concept of the long period for reporting device information.
3. Modified the rogue device identification error. Identification of rogue wireless bridges should be the same as that of rogue APs.
4. Updated the objects to which the containment function applies.

Issue 01 (2013-05-10)

This issue is the first official release.

WLAN WIDS & WIPS Technology White Paper

Keywords

WLAN, WIDS, WIPS

Abstract

This document describes WIDS &WIPS technologies used by Huawei WLAN products to ensure network border security. WIDS & WIPS technologies secure wireless networks, reduce interference from unauthorized devices, and protect STAs from malicious attacks, delivering better user experience.

Acronyms and Abbreviations

Acronym and Abbreviation	Full Name
Rogue AP	Rogue Access Point
SSID	Service Set Identifier
BSSID	Basic Service Set Identifier
CAPWAP	Control And Provisioning of Wireless Access Points
WIDS	Wireless Intrusion Detection System
WIPS	Wireless Intrusion Prevention System

Contents

List of Figures

1 Overview

802.11 networks are open wireless public networks, and vulnerable to various threats caused by unauthorized APs and STAs, ad hoc networks, bogus APs, and denial of service (DoS) attacks of malicious STAs. The Wireless Intrusion Detection System (WIDS) and Wireless Intrusion Prevention System (WIPS) functions monitor and prevent the preceding attacks on WLANs.

This document describes WIDS and WIPS technologies used by Huawei WLAN products. Enterprises can use the WIDS and WIPS functions to secure their wireless networks, reduce interference from unauthorized devices, protect STAs from malicious attacks, and deliver better user experience.

2 Implementation

2.1 Concepts

The WIDS detects rogue STAs, malicious user attacks, and wireless network intrusions. The WIPS is an extension to the WIDS, and further protects enterprise wireless networks and users from unauthorized access and provides defense against attacks to network systems. Some concepts related to the WIDS and WIPS are as follows:

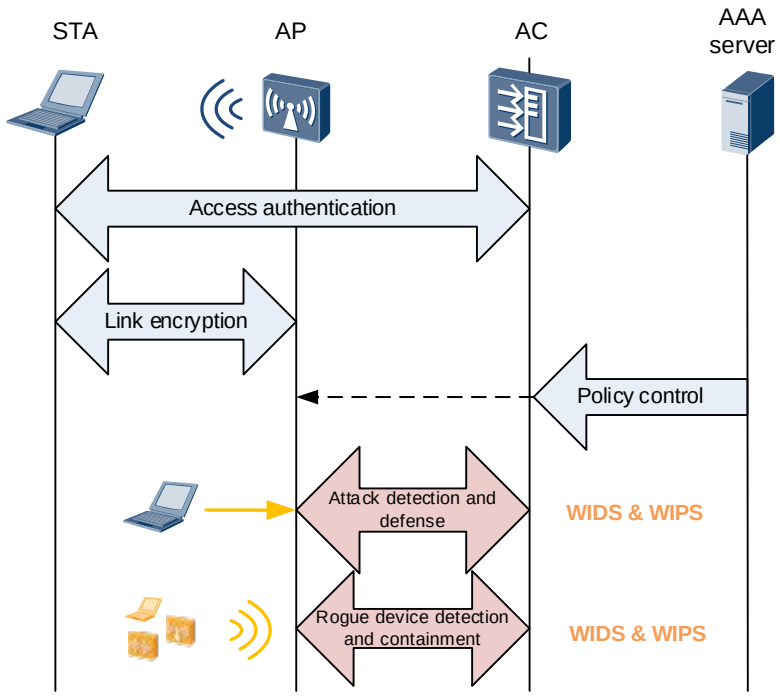
- Rogue AP: an unauthorized or malicious AP, which can be an AP that is connected to a network without permission, an unconfigured AP, a neighbor AP, or an AP manipulated by an attacker
- Rogue STA: an unauthorized or malicious STA, similar to a rogue AP
- Rogue wireless bridge: an unauthorized or malicious wireless bridge
- Monitor AP: an AP that scans or listens on wireless media and attempts to detect attacks to the wireless network
- Ad hoc mode: a working mode of STAs, in which the STAs can communicate with each other without using any other network device

The WIDS and WIPS provide different functions based on the network scale:

- On home networks or small-scale enterprise networks: Control access of APs and STAs using blacklists and whitelists. Access control is implemented on ACs and irrelevant to APs.
- On small- and medium-scale enterprise networks: Detect attacks from rogue devices.
- On medium- and large-scale enterprise networks: Detect, identify, defend against, and contain rogue devices to protect the networks.

In addition to secure WLAN access, a large-scale network requires a system that can detect rogue wireless devices and reject access from these devices to protect services of authorized users.

Figure 2-1 Overview of WLAN security technologies



In the preceding figure, the WIDS and WIPS are used to detect and contain rogue devices respectively. The WIDS can detect rogue APs, rogue wireless bridges, rogue STAs, ad hoc devices, and interference APs with duplicate channels. The WIPS can disassociate authorized STAs from rogue APs, and disconnect rogue STAs and ad hoc devices from the WLAN to contain rogue devices.

NOTE

APs in this document are Fit APs. Fat APs and cloud APs also provide the WIDS and WIPS functions. Different from Fat APs that provide the WIDS and WIPS functions themselves, Fit APs need to work with ACs to provide the functions.

2.2 Rogue Device Detection

Rogue device detection of WLANs is enabled to monitor the entire network. Monitor APs are deployed on a WLAN that needs protection to monitor the entire network. The monitor APs can periodically listen on wireless signals to detect rogue devices.

2.2.1 Working Modes of APs

Before enabling rogue device detection on a WLAN, configure APs' working modes.

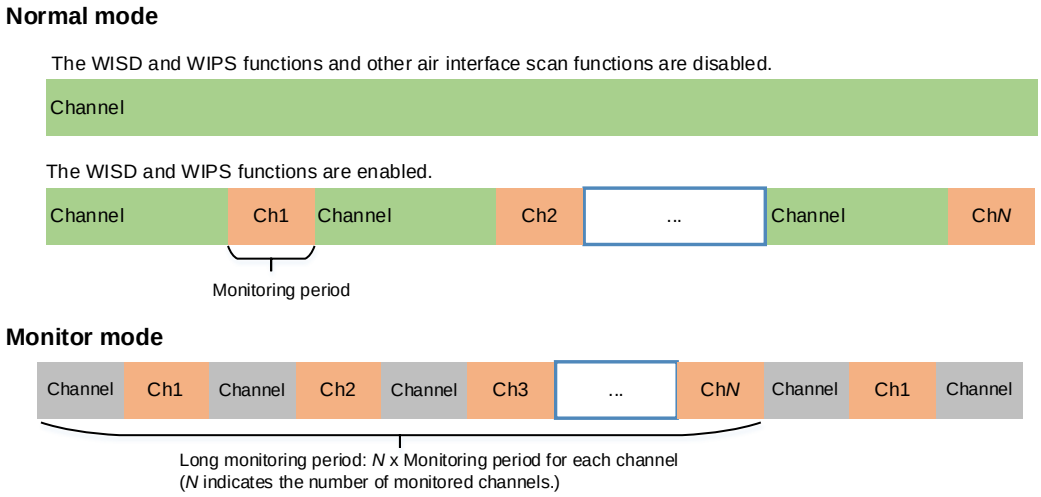
An AP works in normal or monitor mode.

- Normal mode: If the WIDS and WIPS functions and other air interface scan functions are disabled on a radio, such as spectrum analysis and STA location, this radio can be used only to transmit common WLAN service data. If the WIDS and WIPS functions are enabled, the working mode of the radio is automatically switched to hybrid. In addition to transmitting common WLAN service data, the radio can also provide the monitoring function. In this case, transmission of common WLAN service data is affected.

- Monitor mode: A monitor AP scans devices on the WLAN and listens on all 802.11 frames on wireless channels. In this case, the monitor AP provides only the monitoring function and cannot transmit WLAN service data.

The following figure shows the principles of the two working modes.

Figure 2-2 Principles of the two working modes



NOTE

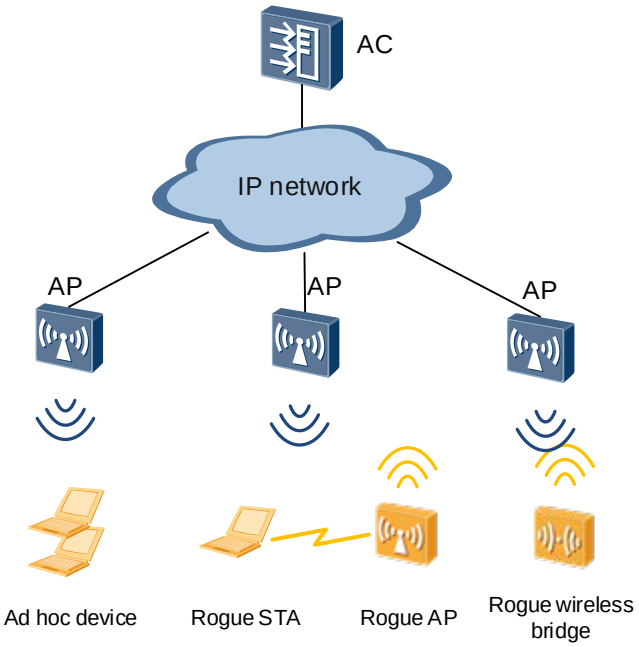
Rogue devices are detected in all the channels of the frequency band on which the current radio works, or channels allowed by a specified country code.

2.2.2 Wireless Device Identification

On WLANs, APs, STAs, ad hoc devices, and wireless bridges need to be monitored. When an AP working in normal mode with air interface scan functions enabled on radios or in monitor mode, it can identify the types of neighboring wireless devices based on detected 802.11 management and data frames. The wireless device identification process is as follows:

1. On the AC, the AP is configured to work in monitor mode or in normal mode with air interface scan functions enabled on radios.
2. The AC delivers the configuration to the AP.
3. The AP scans channels to collect information about neighboring wireless devices, and listens on frames sent by neighboring wireless devices to identify device types. The AP listens on the following types of frames:
   - Beacon
   - Association Request
   - Association Response
   - Reassociation Request
   - Reassociation Response
   - Probe Response
   - Data frame
4. The AP reports the identified device types to the AC. The AC then determines whether the identified devices are authorized and notifies the AP of rogue devices.

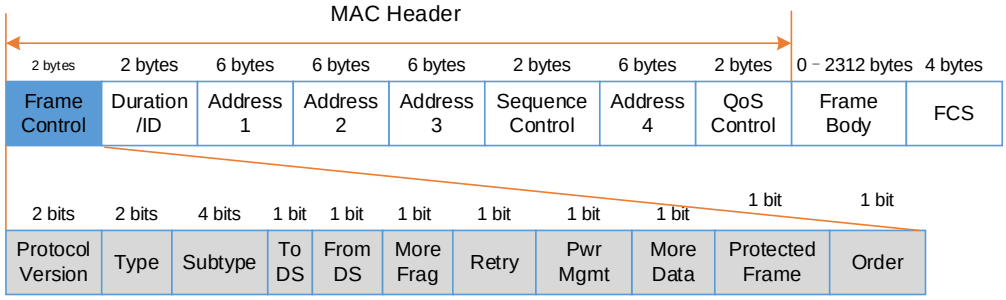
Figure 2-3 Rogue device detection and identification



The AP identifies the types of neighboring wireless devices based on detected 802.11 management and data frames.

The **Frame Control** field in the MAC header of a frame indicates the frame type. Figure 2-4 shows the subfields of the **Frame Control** field.

Figure 2-4 MAC header of an 802.11 frame

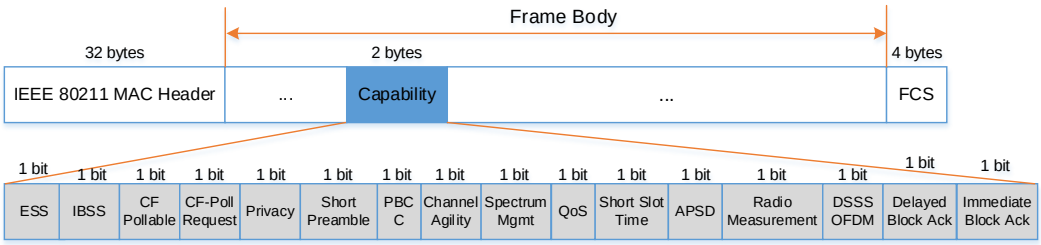


If the value of the **Type** subfield is 00, the frame is a management frame. The AP then checks the **Subtype** subfield. The mapping between **Subtype** subfield values and frame types is as follows:

- 1000: Beacon
- 0001: Association Response
- 0010: Reassociation Request
- 0011: Reassociation Response
- 0101: Probe Response

802.11 management frames carry the **Capability** subfield in the **Frame Body** field. The **Capability** subfield contains the Extend Service Set (ESS) and Independent BSS (IBSS) bits. The AP determines whether the sender is an ad hoc device or a wireless bridge according to the ESS and IBSS bits.

Figure 2-5 Capability field structure



If the IBSS bit is 1, the sender is an ad hoc device. If the IBSS bit and ESS bit are both 0, the sender is a wireless bridge. If the ESS bit is 1, the sender is an AP or a STA.

Table 2-1 Mapping between management frames and device types

ESS IBSS	Beacon, Association Response, and Reassociation Response	Association Request and Reassociation Request
10	AP	STA
01	Ad hoc device	Ad hoc device
00	Wireless bridge	Wireless bridge
11	Unused	

When the **Type** subfield is 10, the frame is a data frame. The **To DS** and **From DS** subfields indicate whether the data frame is sent to or from a distribution system (DS). The following table describes combinations of the two subfields.

Table 2-2 Meanings of the **To DS** and **From DS** subfields in a data frame

To DS	From DS	Meaning
0	0	Data frame in a non-basic service set (non-BSS)
0	1	Data frame sent from a wireless station in a BSS
1	0	Data frame sent to a wireless station in a BSS
1	1	Data frame sent between two wireless bridges

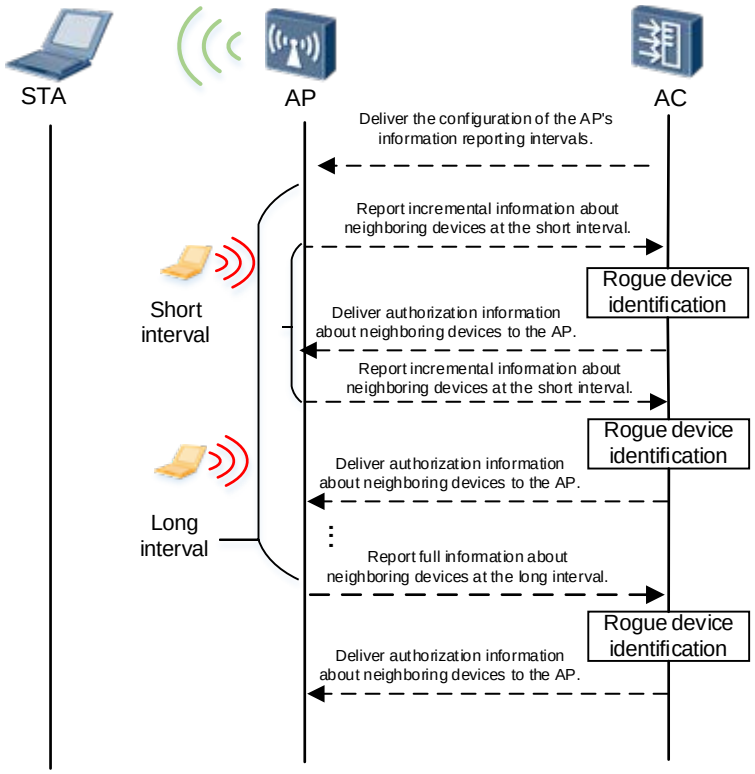
An AP identifies device types in the following ways based on 802.11 management and data frames:

- When receiving a Probe Request, an Association Request, or a Reassociation Request frame, the AP determines whether the sender is an ad hoc device or STA based on the network type specified by the **Capability** subfield in the **Frame Body** field of the 802.11 MAC frame.
  - Ad hoc device: The network type is IBSS. The ESS and IBSS bits are 0 and 1 (binary format) respectively in the **Capability** subfield.
  - STA: The network type is BSS. The ESS and IBSS bits are 1 and 0 (binary format) respectively in the **Capability** subfield.
- When receiving a Beacon, a Probe Response, an Association Response, or a Reassociation Response frame, the AP determines whether the sender is an ad hoc device or AP based on the network type specified by the **Capability** subfield in the **Frame Body** field of the 802.11 MAC frame.
  - Ad hoc device: The network type is IBSS. The ESS and IBSS bits are 0 and 1 (binary format) respectively in the **Capability** subfield.
  - AP: The network type is BSS. The ESS and IBSS bits are 1 and 0 (binary format) respectively in the **Capability** subfield.
- The AP listens on all 802.11 data frames and checks the DS subfields of the data frames to determine whether the sender is an ad hoc device, a wireless bridge, a STA, or an AP.
  - Ad hoc device: The **To DS** and **From DS** subfields are both 0.
  - Wireless bridge: The **To DS** and **From DS** subfields are both 1.
  - STA: The **To DS** subfield is 1 and the **From DS** subfield is 0.
  - AP: The **To DS** subfield is 0 and the **From DS** field is 1.

2.2.3 Device Information Reporting

A monitor AP scans channels to detect neighboring wireless devices. The monitor AP listens on packets sent by neighboring wireless devices to collect device information, and periodically reports collected information to the AC. The AC then determines whether the neighboring wireless devices are authorized based on the received information.

Figure 2-6 Device information reporting process



The device information reporting process is described as follows:

- On the AC, a short interval is configured for the AP to report information about neighboring wireless devices. (The long interval is provided by the system by default.)
- The AC delivers the configuration to the AP.
- The AP listens on frames to collect information about neighboring wireless devices, and reports the information to the AC at the specified short interval. The AC then determines whether the wireless devices are rogue devices and delivers the identification result to the AP. When the wireless devices are scanned again by the AP, the AP automatically checks whether they are rogue devices based on the identification result sent by the AC.
- The AP reports full information about all detected wireless devices to the AC at the long interval for information synchronization. The AC then determines whether the wireless devices are rogue devices and delivers the identification result to the AP. When the wireless devices are scanned again by the AP, the AP automatically checks whether they are rogue devices based on the identification result sent by the AC.

NOTE

The short interval is also called the instant report interval. An AP reports information about detected neighboring wireless devices to the AC at the short interval. This process is called incremental reporting. The value ranges from 10 to 3600, in seconds, and the default value is 300.

The long interval is also called the full report interval. The AP reports full information about detected neighboring wireless devices stored locally to the AC at the long interval. The default long interval is 60 minutes. The long interval is self-adapted based on the actual situation.

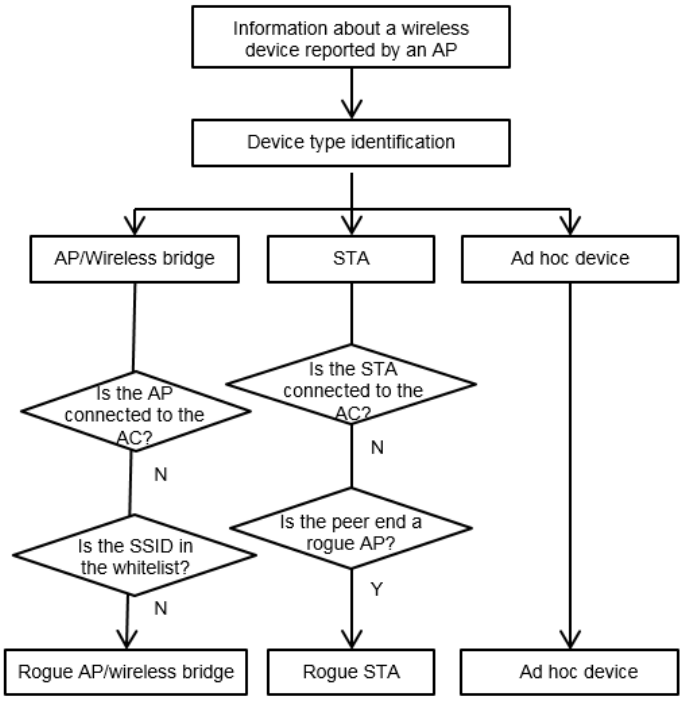
Table 2-3 Key information about a detected wireless device

Attribute	Description
MAC address	MAC address of the device
BSSID	BSSID of the device
Type	Ad hoc device, AP, STA, or wireless bridge
SSID	SSID of an ESS
Vendor	Vendor of the device
Channel	Channel in which the device is detected for the last time
RSSI	Maximum RSSI of the device
Beacon Interval	Interval at which an AP or ad hoc device sends Beacon frames
First Detected Time	First time at which the device is detected
Last Detected Time	Last time when the device is detected

2.2.4 Rogue Device Identification

When receiving information about neighboring devices reported by an AP, an AC starts rogue device identification. The following figure shows the rogue device identification process.

Figure 2-7 Rogue device identification process



The AC extracts neighbor information entries reported by the AP one by one and performs rogue device identification by device type as follows:

- If the device type is ad hoc, it is identified as a rogue device.

  If the device type is AP or wireless bridge, the AC first checks whether it is an authorized device. If the BSSID of the device is the same as that of another device currently managed by the AC, it is an authorized device. Otherwise, the identification continues. If the SSID of the device (such as CMCC) is in the SSID whitelist configured by the administrator, it is an authorized device. Otherwise, the device is identified as a rogue device.

- If the device type is STA, the AC first checks whether it is an authorized neighboring STA. If the MAC address of the STA is the same as that of another STA currently connected to the AC, it is an authorized STA. Otherwise, the identification continues. The STA may access an SSID in the whitelist, so the BSSID of the STA needs to be further checked. If the BSSID belongs to an AP in the list of unauthorized APs, the STA is identified as a rogue STA. Otherwise, the STA is an authorized STA

NOTE

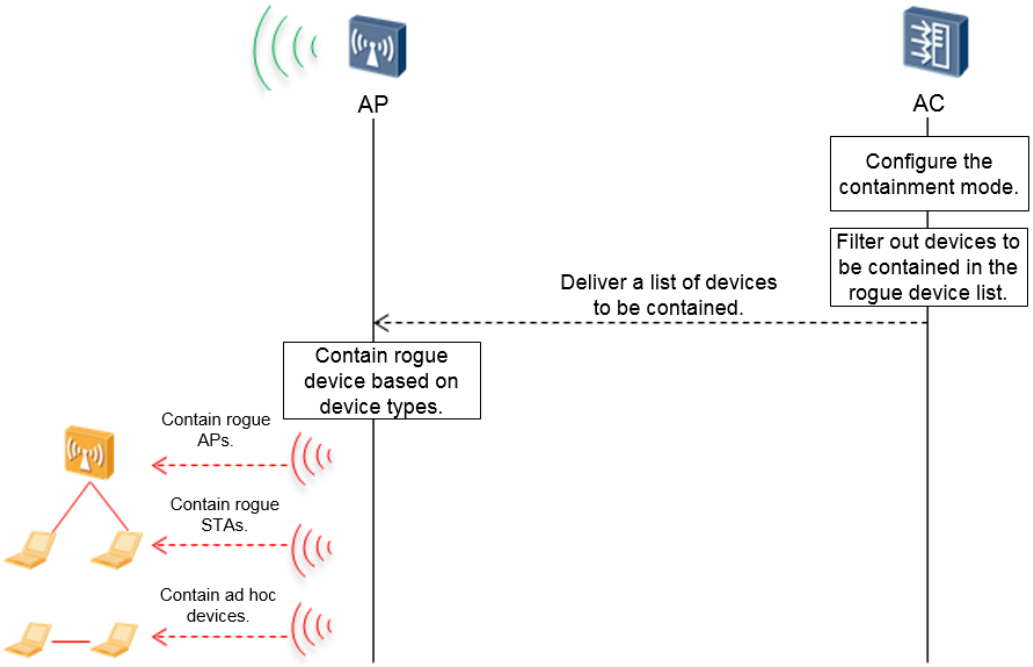
When the AC identifies an AP as a rogue AP, a rogue AP alarm is triggered and sent to the network management system (NMS) in an SNMP trap. When other types of rogue devices are identified, no rogue device alarm is triggered.

2.3 Rogue Device Defense and Containment

The defense and containment functions can be enabled to reject access of detected rogue devices. The attack defense function restricts access of rogue APs or STAs using blacklists. The containment function prevents a specified type of rogue devices from operating, depending on the configured containment mode. APs download the attacking device list from the AC and take measures to contain the rogue devices.

Figure 2-8 shows the rogue device containment process. Rogue device detection and identification must be configured before the containment function is enabled.

Figure 2-8 Rogue device containment process



After rogue device containment is enabled, rogue devices are filtered out from the list of rogue devices reported by an AP based on the type of devices to be contained specified by the administrator. A list of devices to be contained will then be delivered to the AP for containment. The rogue device containment process is described as follows:

1. The containment mode is configured on the AC and the containment function is enabled.
2. The AC selects rogue devices from the wireless device list reported by a monitor AP and sends the rogue device list to the monitor AP.
3. The monitor AP contains the rogue devices in the rogue device list sent by the AC.

Containment against different types of rogue devices is described as follows:

- Rogue APs: Currently, Huawei WLAN devices support containment against only two types of rogue APs: phishing APs that use open authentication and rogue APs with bogus SSIDs. When detecting a rogue AP, a monitor AP uses the rogue AP's IP address to send fake broadcast Deauthentication frames to prevent STAs from associating with the rogue AP. That is, the monitor AP forges the rogue AP to instruct all STAs to disassociate from the rogue AP.
- Rogue STAs: After detecting a rogue STA, a monitor AP uses the BSSID and MAC address of the rogue STA to send a fake unicast Deauthentication frame to contain it. A STA whitelist can also be configured to prevent STAs in the STA whitelist from associating with rogue APs.
- Ad hoc devices: After detecting an ad hoc device, a monitor AP uses the BSSID and MAC address of the ad hoc device to send a fake Beacon, Deasscociation, or Deauthentication frame to contain it.

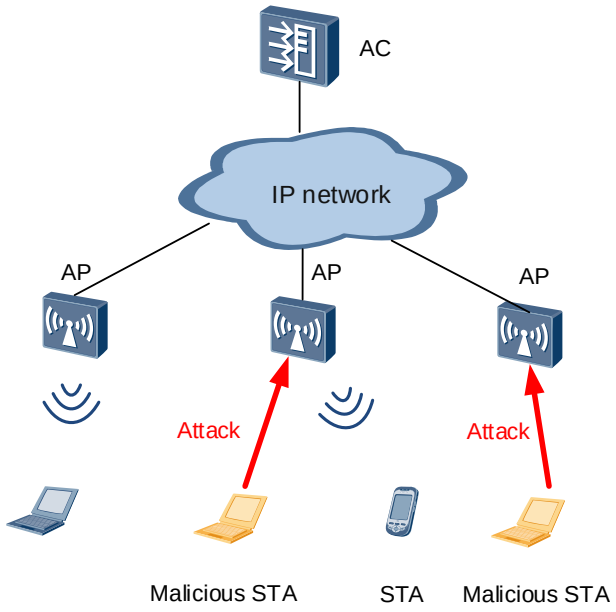
NOTE

Monitor APs contain rogue devices periodically based on the configured detection mode. Currently, only rogue APs, rogue STAs, and ad hoc devices can be contained, and wireless bridges cannot be contained. When a rogue device is moved to the historical list, the AC sends an instruction to the monitor AP to request the AP to stop containment against the rogue device.

2.4 WIDS Attack Detection

To protect a WLAN against attacks, you can configure real-time attack detection on APs. When detecting abnormal behavior or packets, the system considers that it is attacked and performs automatic security protection.

Figure 2-9 WIDS attack detection scenario



On the WLAN shown in the preceding figure, WIDS attack detection can be enabled on the AC when the WLAN access service is provided. The WIDS can detect 802.11 flood attacks, spoofing attacks, and weak initialization vector (IV) attacks, and can also defend the WLAN against brute force cracking.

2.4.1 Flood Attack Detection

A flood attack occurs when an AP receives a large number of management packets of the same type from a source MAC address within a short time period. These attack packets consume many system resources of the AP, and therefore the AP cannot process packets from authorized STAs.

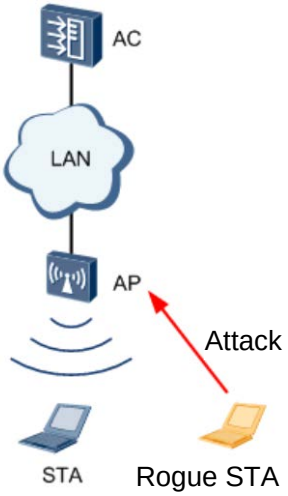
Flood attack detection allows an AP to keep monitoring the traffic rate of each STA to defend against flood attacks. When the rate of traffic received from a STA exceeds the allowed threshold (for example, more than 100 packets per second), the AP considers that the STA will flood packets and reports an alarm to the AC. If the dynamic blacklist function is enabled, the detected attack STA will be added to the dynamic blacklist. Before the dynamic blacklist entry

ages out, the AP discards all the packets sent by this STA to protect the network against a flooding attack.

An AP can detect flood attacks of the following types of frames:

- Authentication Request
- Deauthentication frame
- Association Request
- Disassociation frame
- Probe Request
- Action frame (extended management frame, which is used for spectrum management, QoS, and HT mode setting)
- EAPOL Start frame
- EAPOL-Logoff frame
- PS-Poll frame (management frame sent by a STA when it recovers from the power-saving mode)

Figure 2-10 Flood attack



NOTE

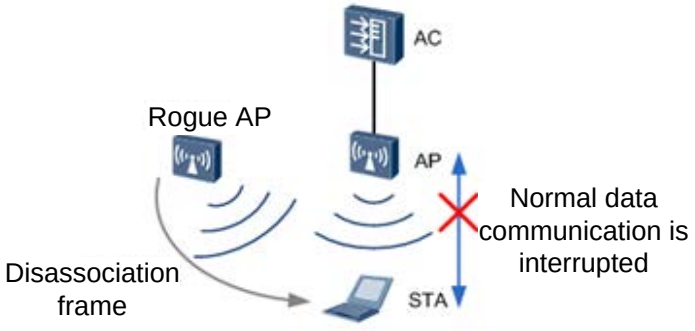
By default, when the system receives 300 (x) packets of the same type within 60 (y) seconds (x and y are configurable), it considers that the packet sender initiates a flood attack.

2.4.2 Spoofing Attack Detection

A spoofing attack is also called a man-in-the-middle (MITM) attack. An attacker (a rogue AP or malicious user) uses an authorized user's identity to send spoofing packets to STAs. As a result, the STAs cannot go online. Spoofing attack packets include broadcast Disassociation frames and Deauthentication frames.

After the spoofing attack detection function is enabled, an AP checks whether the source MAC address of received Disassociation frames or Deauthentication frames is its own MAC address. If so, the WLAN is undergoing a spoofing attack of Disassociation or Deauthentication packets. The AP then sends an alarm to the AC. The AC then records a log and sends an alarm to notify the administrator.

Figure 2-11 Spoofing attack



NOTE

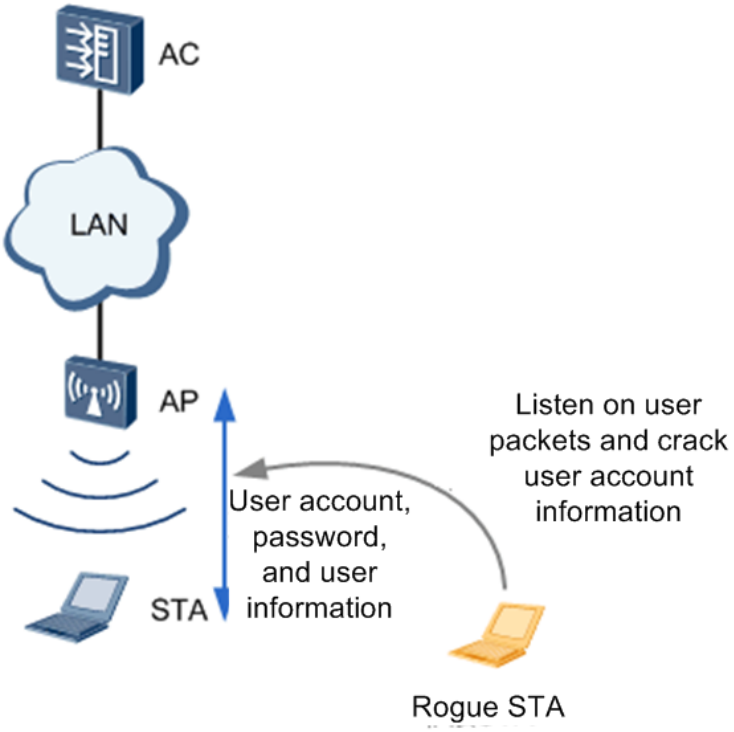
In a spoofing attack, a rogue AP does not use its own MAC address. Therefore, even if the system detects the spoofing attack, it cannot obtain the real MAC address of the rogue AP. The dynamic blacklist function cannot be used to defend against spoofing attacks.

2.4.3 Weak IV Detection

When wired equivalent privacy (WEP) encryption is used on a WLAN, a 3-byte IV is generated for each WEP packet. The IV and a fixed shared key are used to generate a key string for a WEP packet to be sent. The key string and plaintext are encrypted to generate the cipher text. A weak IV refers to that generated using an insecure method, for example, a duplicate IV or the same IV generated frequently. If a STA uses a weak IV, attackers can easily crack the shared key because the STA sends the IV in plain text in the packet header. The attackers can then access the WLAN.

Weak IV detection identifies the IV of each WEP packet to prevent attackers from cracking the shared key. When an AP detects a packet carrying a weak IV, it sends an alarm to the AC so that users can use other security policies to prevent STAs from using the weak IV for encryption.

Figure 2-12 User account cracking through weak IVs



NOTE

- Weak IV detection does not require the dynamic blacklist function.
- Currently, WEP authentication is seldom used due to high security risks.

2.4.4 Defense Against Brute Force Cracking

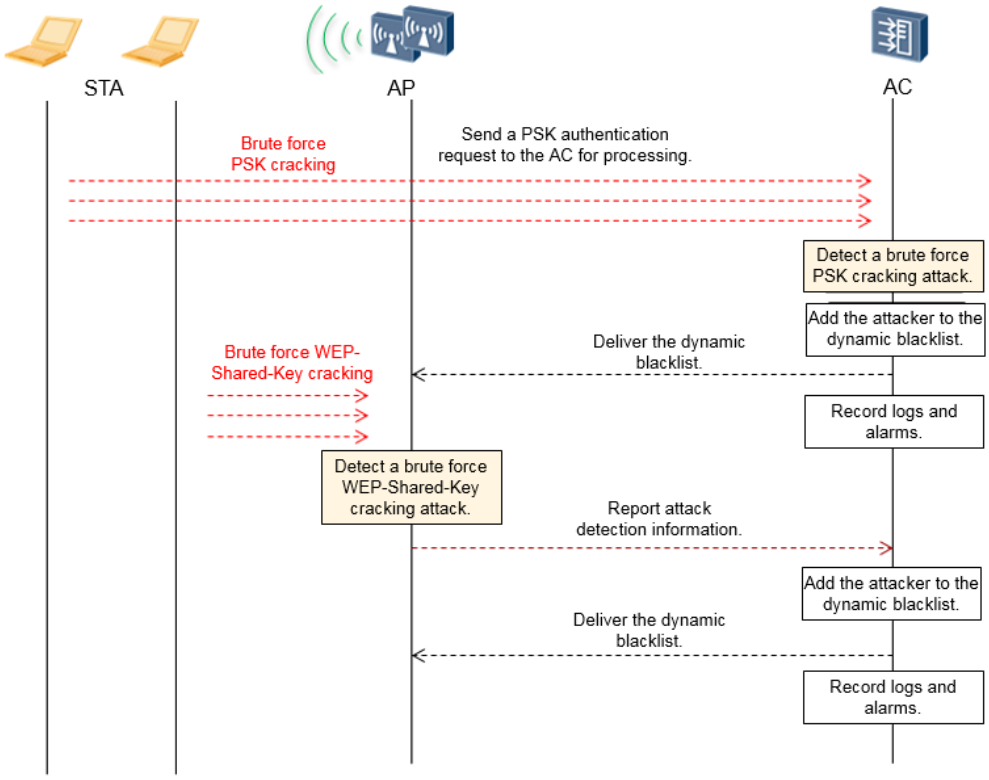
A brute force attack, or exhaustive key search, is a cryptanalytic attack that tries every possible password combination to find the real password. For example, a password that contains only four digits may have a maximum of 10,000 combinations. The password can be cracked after a maximum of 10,000 attempts. Theoretically, an attacker can use the brute force method to crack any password. The cracking duration varies depending on the security mechanism and password length. Therefore, brute force cracking threats exist when any authentication mode is used.

- When a WLAN uses the WPA/WPA2-PSK, WAPI-PSK, or WEP-Shared-Key security policy (link authentication), attackers may use the brute force method to crack passwords.
- When a user authentication mode is used, such as MAC address, Portal, or 802.1X authentication, brute force cracking threats also exist.

To improve password security, enable defense against brute force cracking to prolong the time used to crack passwords. An AP checks whether the number of key negotiation attempts within a specified time period during WPA/WPA2-PSK, WAPI-PSK, or WEP-Shared-Key authentication exceeds the specified threshold (configurable). If so, the AP considers that the STA is using the brute force method to crack the password and reports an alarm to the AC. If the dynamic blacklist function is enabled, the AP adds the STA to the dynamic blacklist, discards all the packets from the STA until the dynamic blacklist entry ages out.

PSK authentication and WEP-Shared-Key authentication are implemented on ACs and APs, respectively. Therefore, the corresponding brute force cracking detection methods are different.

Figure 2-13 Brute force PSK cracking and WEP-Shared-Key cracking



When different user access authentication modes are used, such as MAC address, Portal, and 802.1X authentication, defense against brute force cracking is also needed. The basic principle is similar, which is described as follows:

- MAC address authentication: The MAC address of a STA is used as an account and sent to the RADIUS server for authentication. If authentication fails, the STA is added to the STA blacklist and prohibited from accessing the network within a short time period (configurable and 60s by default).
- Portal and 802.1X authentication: If a STA fails authentication for three consecutive times (configurable) within 60 seconds, the STA is considered as an attacker that initiates brute force cracking attacks and added to the STA blacklist. The STA will be prohibited from accessing the network within a short time period (configurable and 60s by default).

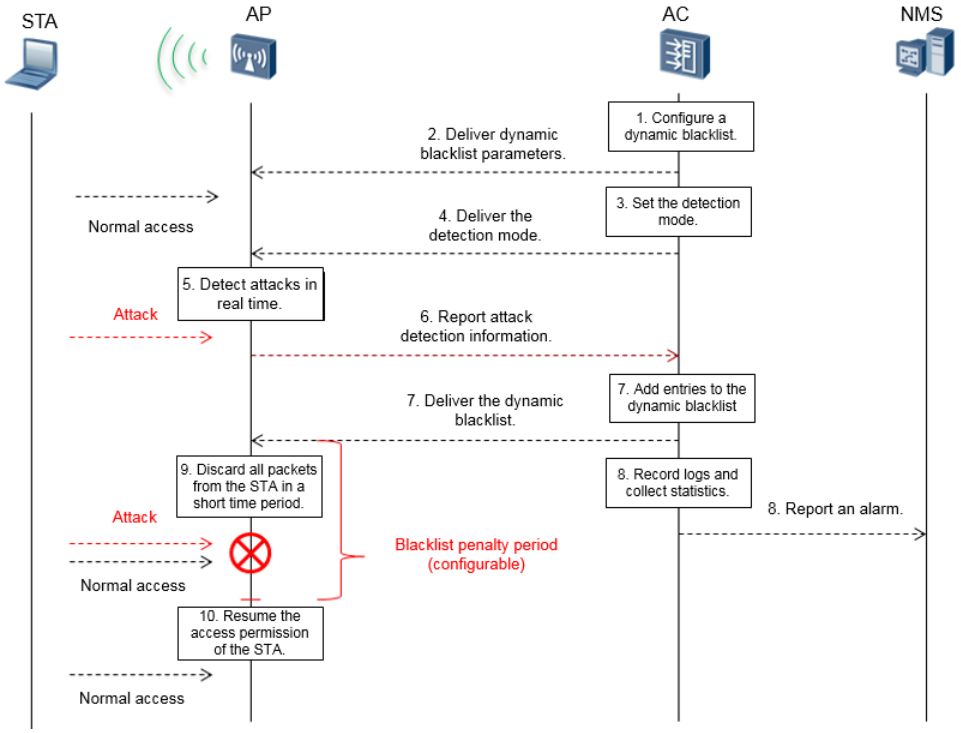
2.5 WIDS Attack Defense

To detect attacks on a WLAN in a timely manner, you can enable the WIDS attack defense function. This function enables WLAN devices to detect flood, weak IV, and spoofing attacks to discover network security threats. After this function is enabled, attackers can be added to the dynamic blacklist, and alarms are sent to ACs, notifying administrators of attacks in a timely manner.

2.5.1 Dynamic Blacklist

The following figure shows the WIDS attack defense process.

Figure 2-14 WIDS attack defense

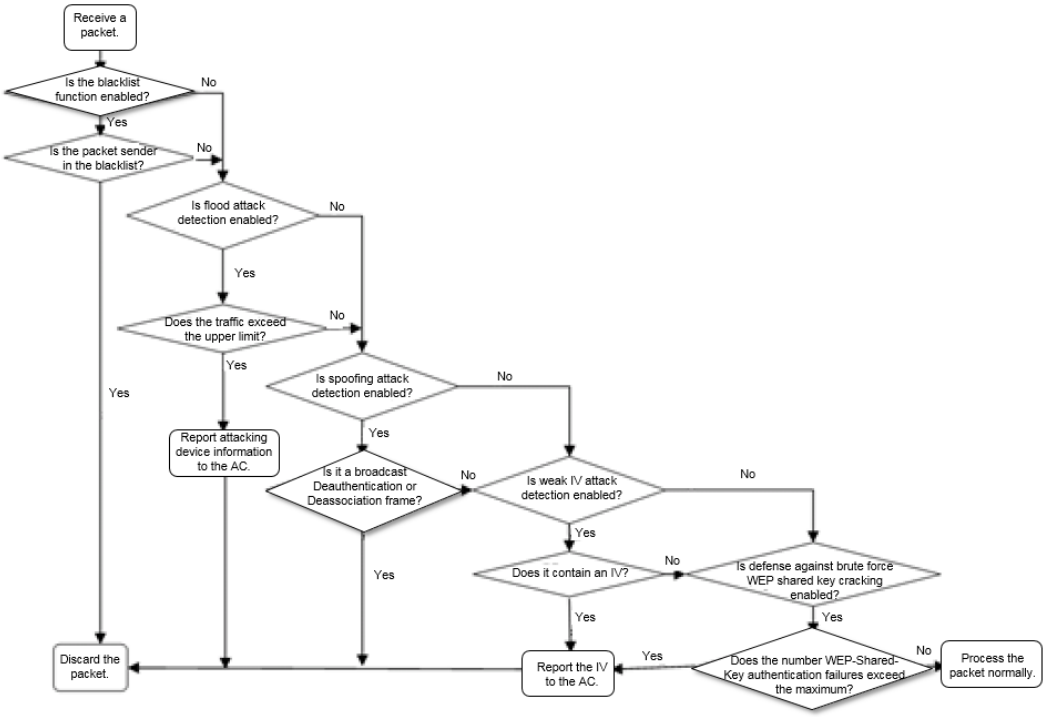


1. The dynamic blacklist function is configured on the AC and the blacklist entry aging time is specified.
2. The AC sends the dynamic blacklist enabled flag and blacklist entry aging time to the AP.
3. The WIDS attack detection mode is configured on the AC. The detection period and detection threshold (number of packets detected within the specified time period to identify an attack) are set.
4. The AC delivers the detection mode, detection period, and detection threshold to the AP.
5. The AP detects attacks in attack detection mode delivered by the AC.
6. When the AP detects an attack, it reports attack information to the AC, such as the MAC address of the attacking device and the attack type. After receiving the attack information, the AC adds the attacking device to the attacking device list. If the AP detects no attack from this attacking device in the next three attack detection periods, it requests the AC to delete the attacking device from the list.
7. The AC determines whether to add the attacking device to the dynamic blacklist. It records detected brute force PSK crackers to the dynamic blacklist cache table, and delivers the table to the AP.
8. The AC collects statistics on attack types and sends trap messages to report the attack types to the NMS.
9. After receiving the dynamic blacklist, the AP discards the packets from the attacking devices in the dynamic blacklist.

10. The dynamic blacklist entries are automatically aged according to the specified aging time (penalty period in the preceding figure). When the aging period expires, the entries are automatically deleted and the attackers can access the network properly.

The following figure shows the WIDS attack detection process on an AP.

Figure 2-15 WIDS attack detection



After receiving information about an attacking device reported by the AP, the AC adds the device to the attacking device list, collects statistics on attack types, and sends trap messages based on the attack type. Attacking devices are sorted by time in the attacking device list. After the number of attacking devices reaches the upper limit, new attacking devices override earlier ones.

- Statistics information: After receiving a WIDS attack detection packet reported by an AP, the AC collects statistics on the types and number of attacks.
- Trap messages: Trap messages are sent only when flood attacks and spoofing attacks are detected. A trap message contains the MAC address of the attacked AP, MAC address of the attacking device, channel, and attack type. Alarm suppression and alarm matching are required.

If the AC detects a flood attacking device or brute force PSK cracking device and the dynamic blacklist function is enabled, the AC adds the attacking device to the dynamic blacklist and delivers the device information to the corresponding AP. The AP then discards packets from the attacking device. If the attacking device is associated with the AP, the AP needs to disassociate from it. The AC needs to maintain the dynamic blacklist entries and the aging mechanism of these entries. After the dynamic blacklist is aged, the AC needs to instruct the AP to delete the blacklist. One attacking device may be detected by different APs. Therefore, the dynamic blacklist needs to be associated with a list of monitor APs. The aging mechanism takes effect for each specific AP. If the AC fails to deliver a dynamic blacklist deletion

message to an AP, the dynamic blacklist will not be deleted. To prevent this problem, the AC and AP must use the same dynamic blacklist aging mechanism.

2.5.2 Static Blacklist

The system administrator can configure static blacklists, and manually add MAC addresses of detected rogue STAs or APs to the static STA or AP blacklist. In this way, the system will reject unauthorized access of these rogue devices. A WLAN system provides two types of static blacklists as follows:

- Static STA blacklist

  When a STA in the static STA blacklist (based on MAC addresses) accesses the network, the AP discards the access request and rejects access of the STA.

- Static AP blacklist

  When an AP in the static AP blacklist (based on MAC addresses) accesses an AC through a CAPWAP tunnel, the AC discards the access request and rejects access of the AP.

The WLAN system can also use a whitelist to access only from specified authorized devices in the whitelist. Huawei also provides the STA- and AP-based whitelist functions.

NOTE

Huawei's static STA blacklist function also supports static containment of rogue devices. The administrator can add devices to be contained on air interfaces to the static STA blacklist. When the system detects a rogue STA in the blacklist, it performs the containment action on the air interface.

3 Customer Benefits

The WIDS and WIPS functions of Huawei WLAN products ensure security of customers' wireless networks, reduce interference from rogue devices, and protect STAs from malicious attacks, delivering better user experience.

- Selection of different protection measures based on their network scale

  The WIDS and WIPS functions provide different protection measures based on the scale of customer networks.

  - For home networks or small enterprise networks, protection measures are provided to control access of APs and STAs using blacklists and whitelists.
  - For small- and medium-scale enterprise networks, WIDS attack detection and defense are provided.
  - For medium- and large-scale enterprise networks, rogue device detection, identification, defense, and containment are provided.

  Customers can also perform other protection configurations.
- Rogue device identification and defense

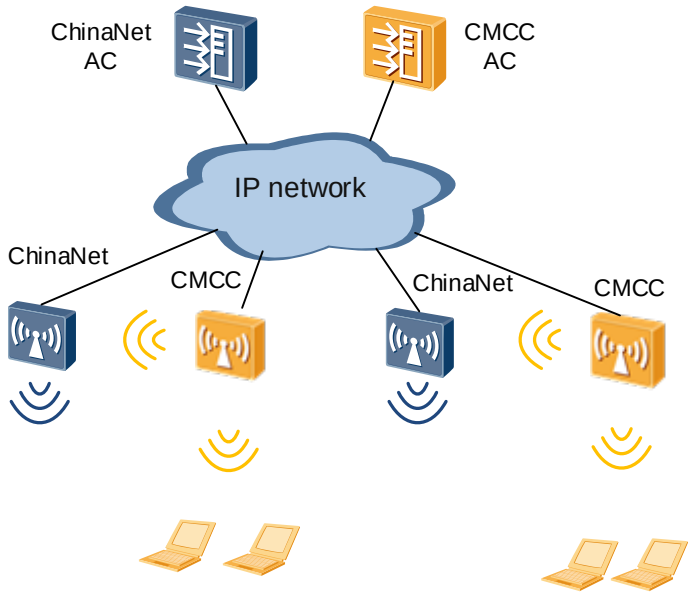
  The WIDS and WIPS functions can identify rogue devices on the WLAN and take preventive measures to protect customer networks against intrusions or interference of rogue devices.
- Customer network protection against attacks

  The WIDS and WIPS functions can detect multiple types of attacks such as flood attacks, weak IV attacks, spoofing attacks, brute force WPA/WPA2/WAPI PSK cracking, and WEP shared key cracking. The functions protect customer networks from being attacked by rogue devices.

4 Application Scenarios

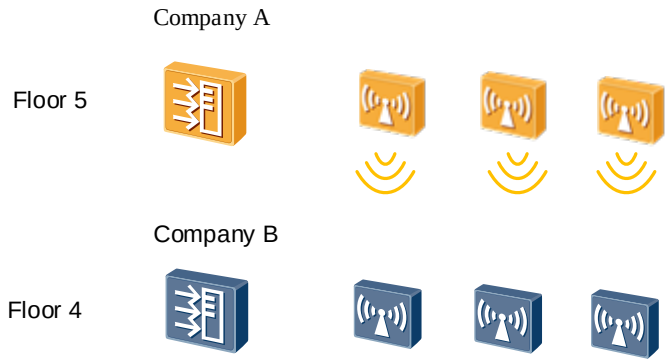
4.1 WLANs in Public Places or Adjacent Companies

Figure 4-1 Airport with multiple carrier networks



In public places such as airports and bus stations, multiple carriers deploy WLAN systems to provide wireless coverage. APs in each WLAN system can detect Wi-Fi signals of other WLAN systems, causing signal interference to each other. In this case, an SSID whitelist can be configured in a WLAN system to prevent detection of APs/STAs in other WLAN systems as rogue devices.

Figure 4-2 Building with multiple companies

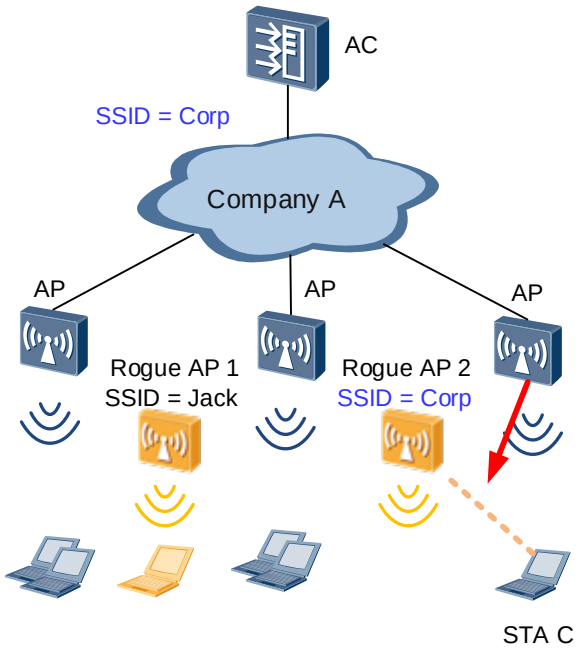


As shown in the preceding figure, employees of company A work on floor 5 and employees of company B work on floor 4, and employees in company B can receive Wi-Fi signals of company A. In this case, company B can add the SSID of company A's WLAN to the SSID whitelist so that APs in company A will not be detected as rogue devices by the WLAN of company B.

4.2 Unauthorized AP Deployment in a Company

To ensure data security or prevent interference to a WLAN, a company generally forbids deployment of unauthorized APs. In this case, the company can enable the WIDS function to detect other WLAN devices that do not belong to its own WLAN.

Figure 4-3 Unauthorized AP deployment in a company

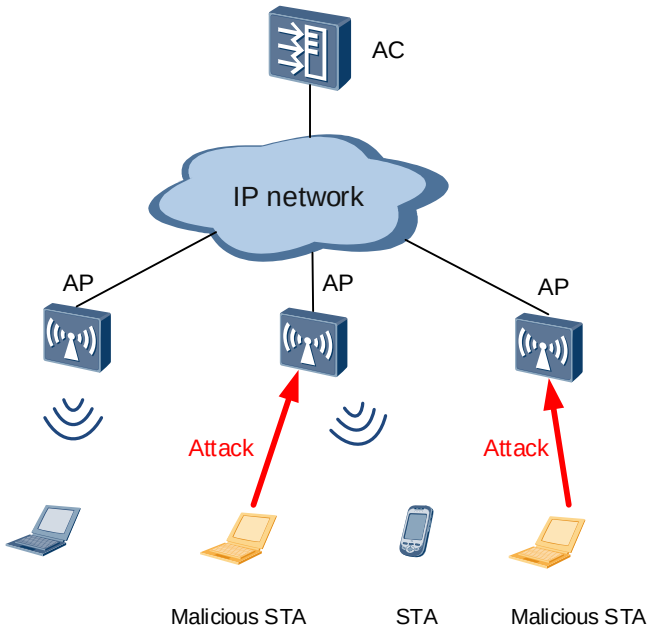


As shown in the preceding figure, employees deploy unauthorized APs (rogue APs 1 and 2, which are Fat APs or smart terminals with the AP function enabled) to the WLAN of a company. Rogue AP 1 uses the SSID **Jack** and provides wireless services for an employee's own STA (such as a tablet). The company's WLAN may be interfered, causing leakage of the company's information assets. Rogue AP 2 uses the same SSID as the WLAN system of the company, and attempts to steal company information assets by forging an authorized AP and establishing connections with devices in the company.

In this case, the WIDS and WIPS functions can be enabled on the company's WLAN to contain rogue APs using the same SSID. After the WIDS and WIPS functions are configured on the AC, the monitor AP collects information about neighboring device and reports the information to the AC. When the AC identifies a rogue AP, it notifies the monitor AP of the rogue AP's identity information. The monitor AP then uses the rogue AP's identity information to broadcast a Deauthentication frame. After STAs associating with the rogue AP receive the Deauthentication frame, they disassociate from the rogue AP. This containment mechanism prevents STAs from associating with the rogue AP.

4.3 WLAN Attack Scenario

Figure 4-4 WLAN attack scenario



Malicious or virus-infected STAs may attack a WLAN. The WIDS and WIPS functions can be enabled on the WLAN of a company to detect flood, spoofing, and brute force cracking attacks. After an attack is detected, the attacking STA will be added to a dynamic blacklist. APs discard all packets from the STA within a specified time period to protect the WLAN against attacks.