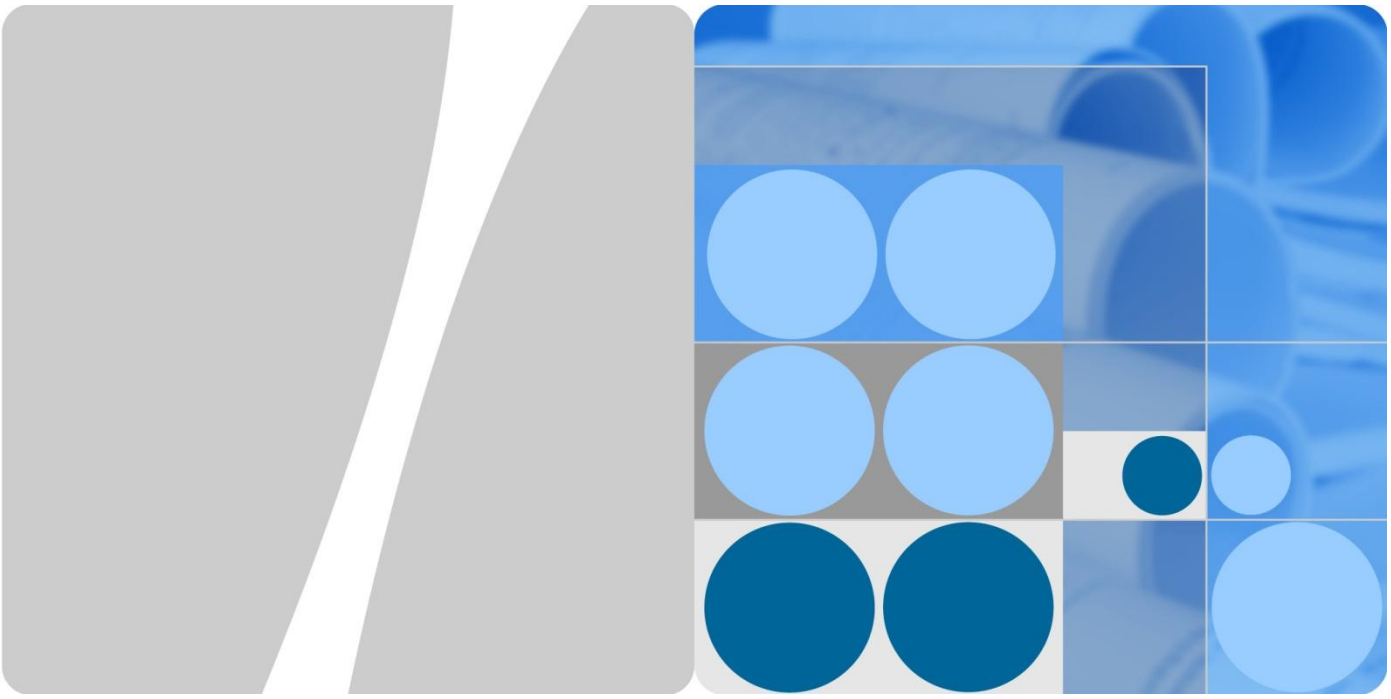


HUAWEI WIDS&WIPS Technology White Paper

Issue 01

Date 2013-05-10

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 a warranty of any kind, express or implied.

Huawei Technologies Co., Ltd.

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

Website: http://www.huawei.com

Email: support@huawei.com

About This Document

Purpose

This document describes WIDS and WIPS technologies provided in WLAN products of V200R003C00. These technologies secure a wireless network, reduce interference from unauthorized devices, and protect users from malicious attacks, delivering better user experience.

This document describes the working mechanisms and applications of WIDS and WIPS, and provides configuration examples.

Intended Audience

This document is intended for:

- Data configuration engineers
- Commissioning engineers
- Network monitoring engineering
- System maintenance engineers

Symbol Conventions

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

Symbol	Description
DANGER	Alerts you to a high risk hazard that could, if not avoided, result in serious injury or death.
WARNING	Alerts you to a medium or low risk hazard that could, if not avoided, result in moderate or minor injury.
CAUTION	Alerts you to a potentially hazardous situation that could, if not avoided, result in equipment damage, data loss, performance deterioration, or unanticipated results.
TIP	Provides a tip that may help you solve a problem or save time.

Symbol	Description
NOTE	Provides additional information to emphasize or supplement important points in the main text.

Change History

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

Issue 01 (2013-05-10)

This issue is the first official release.

Contents

1 WIDS and WIPS Overview

About This Chapter

1.1 Introduction to WIDS and WIPS

Definition

WIDS stands for Wireless Intrusion Detection System, and WIPS stands for Wireless Intrusion Prevention System.

An 802.11 network is vulnerable to threats from unauthorized AP users, Ad hoc networks, and denial of service (DoS) attacks. Rogue APs pose security threats on enterprise networks. WIDS can detect intrusions to a wireless network from malicious users. WIPS protects an enterprise network and users on the network against intrusions from unauthorized wireless devices.

WIDS and WIPS provide different functions on enterprise networks of different scales:

- On family networks or small enterprise networks: control access from APs and clients using blacklist and whitelist. Access control is implemented on ACs and irrelevant to APs.
- On small and medium enterprise networks: WIDS detects attacks from unauthorized devices.
- On medium and large enterprise networks: detect and identify rogue devices, and take countermeasures to protect the networks.

Purpose

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

Benefits to Users

WIDS and WIPS technologies secure a wireless network, reduce interference from unauthorized devices, and protect users from malicious attacks, delivering better user experience.

1.2 Availability

Product Support

Table 1-1 Products and versions that support WIDS and WIPS

Device Type	Product
AC	ACU2
	X1E(native AC)
	AC6605
	AC6005
AP	AP8030DN/AP8130DN AP7050DE/AP7030DE AP6050DN/AP6150DN AP5030DN/AP5130DN AP4050DN-E/AP4050DN-HD AP4030DN/AP4130DN AP6010SN/DN / WA615DN AP6310SN / WA635SN AP6510DN / WA655DN AP6610DN AP3010DN / AP5010SN/DN AP7110SN/DN

1.3 Principles

1.3.1 Concepts

- Rogue AP: an authorized or malicious AP. A rogue AP can be an AP that is connected to a network without permission, unconfigured AP, neighbor AP, or an AP manipulated by an attacker. Hackers may use vulnerabilities of such APs to attack your network.
- Rogue client: an unauthorized or malicious client, similar to a rogue AP.
- Rogue wireless bridge: an unauthorized or malicious wireless bridge.

- Monitor AP: an AP that scans or listens on wireless channels and attempts to detect attacks to the wireless network.
- Ad hoc mode: a client working mode, in which clients can communicate with each other without using any other network device.

1.3.2 Rogue Device Identification (WIDS)

Monitor APs can be deployed on a network that needs protection to monitor the entire network. The monitor APs can periodically listen on wireless frames to detect rogue devices.

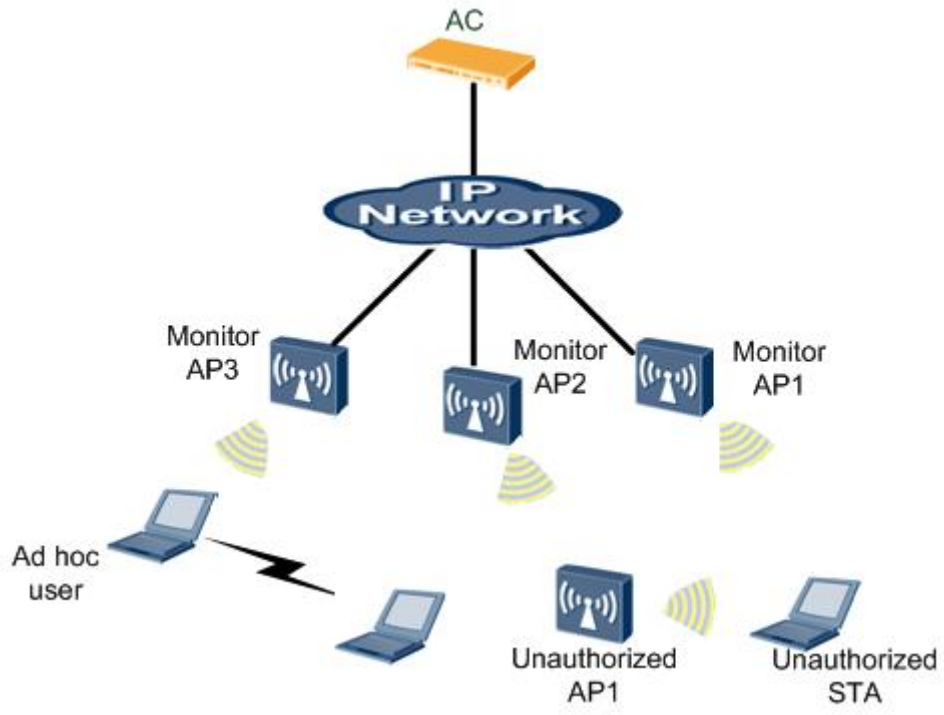
Before configuring rogue device identification on an AP, configure the AP working mode.

An AP supports three working modes: access, monitoring, and hybrid:

- Access mode: If background neighbor probing is not enabled on an AP, the AP only transmits data of wireless users and does not monitor wireless devices on the network. If background neighbor probing is enabled, the AP can not only transmit data of wireless users but also scan wireless devices and listen on all 802.11 frames on wireless channels.
- Monitoring mode: An AP scans wireless devices on the network and listens on all 802.11 frames on wireless channels. In this mode, all WLAN services on the AP are disabled and the AP cannot transmit data of wireless users.
- Hybrid mode: An AP can monitor wireless devices while transmitting data of wireless users.

An AP can implement the WIDS or WIPS function only when it works in monitor or hybrid mode.

Figure 1-1 Rogue device identification



On a WLAN network, APs, clients, Ad hoc STAs, and wireless bridges need to be monitored.

An AP working in monitoring or hybrid mode can identify types of neighboring wireless devices according to detected 802.11 management frames and data frames. The wireless device identification process is as follows:

1. The AP working mode is set to monitoring or hybrid on the AC.
2. The AC delivers the configuration to the AP.
3. The AP listens on frames sent from neighboring wireless devices to collect information about wireless devices. The AP determines frame types and device types according to MAC headers in received 802.11 MAC frames.

A monitor AP listens on the following frames to collect information about neighboring clients, Ad hoc STAs, and wireless bridges:

- Beacon
- Association Request
- Association Response
- Reassociation Request
- Reassociation Response
- Probe Response
- Data frame

When the AP receives an 802.11 MAC frame, it checks the frame type and network type according to the 802.11 protocol.

The Frame Control field in the MAC header of a frame indicates the frame type. Figure 1-2 shows the subfields of the Frame Control field.

Figure 1-2 Frame Control field

	Protocol Version	Type	Subtype	To DS	From DS	More Frag	Retry	More Data	Protected Frame	Order
Bits	2	2	4	1	1	1	1	1	1	1

If the Type subfield is 00, the AP checks the Subtype subfield. The values of the Subtype subfield and corresponding frame types are as follows:

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

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

To DS	From DS	Meaning
0	0	Data frame sent between two stations that are not APs in a basic service set
0	1	Data frame sent from a wireless station in a basic service set
1	0	Data frame sent to a wireless station in a basic service set
1	1	Data frame sent between two wireless bridges

An AP identifies device types in the following way:

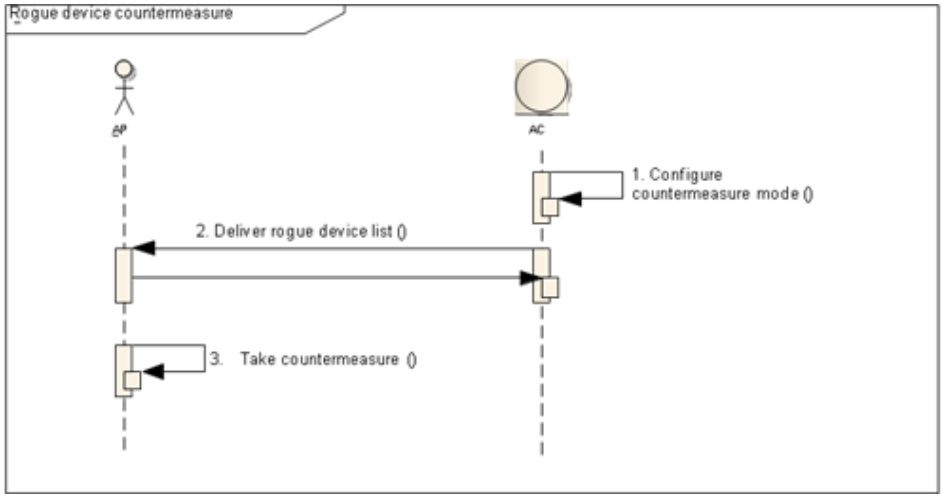
- When receiving a Probe Request, Association Request, or Reassociation Request frame, the AP determines whether the sender is an Ad hoc device or STA according to the network type specified in the Frame Body field of the 802.11 MAC frame.
  - Ad hoc device: The network type is IBSS.
  - STA: The network type is basic service set (BSS).
- When receiving a Beacon, Probe Response, Association Response, or Reassociation Response frame, the AP determines whether the sender is an Ad hoc device or AP according to the network type specified in the Frame Body field of the 802.11 MAC frame.
  - Ad hoc device: The network type is IBSS.
  - AP: The network type is BSS.
- 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, wireless bridge, STA, or AP.
  - Ad hoc device: Both the To DS and From DS subfields are 0.
  - Wireless bridge: Both the To DS and From DS subfields are 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.

1.3.3 Rogue Device Countermeasure (WIPS)

The attack defense and countermeasure functions can be enabled to reject access from detected rogue devices. The attack defense function restricts access from rogue APs or clients using a blacklist. The countermeasure function prevents a specified type of rogue devices from operating, depending on the configured countermeasure mode. Monitor APs download the countermeasure list from the AC and take countermeasures to the rogue devices.

Figure 1-3 shows the process of rogue device countermeasure. Rogue device identification must be configured before the countermeasure function take effect.

Figure 1-3 Process of rogue device countermeasure



1. The countermeasure function is enabled and the countermeasure mode is specified on the AC.
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 takes countermeasure to the rogue devices in the rogue device list sent from the AC.

When a rogue device is moved to the historical list, the AC sends an instruction to the monitor AP, requesting the AP to stop countermeasure to the rogue device.

The countermeasure function is valid only for rogue APs, rogue clients, and Ad hoc devices.

- Countermeasure to rogue APs: When detecting a rogue AP, a monitor AP uses the rogue AP's address to send broadcast Deauthentication frames and then unicast Deauthentication frames. After receiving the Deauthentication frames, STAs disassociate from the rogue AP.
- Countermeasure to rogue clients and Ad hoc devices: After detecting a rogue client or Ad hoc device, a monitor AP uses the BSSID and MAC address of the rogue device to send a unicast Deauthentication frame to the rogue device, preventing the rogue device from connecting to the wireless network. The rogue client countermeasure function can also prevent an authorized client from associating with rogue APs.

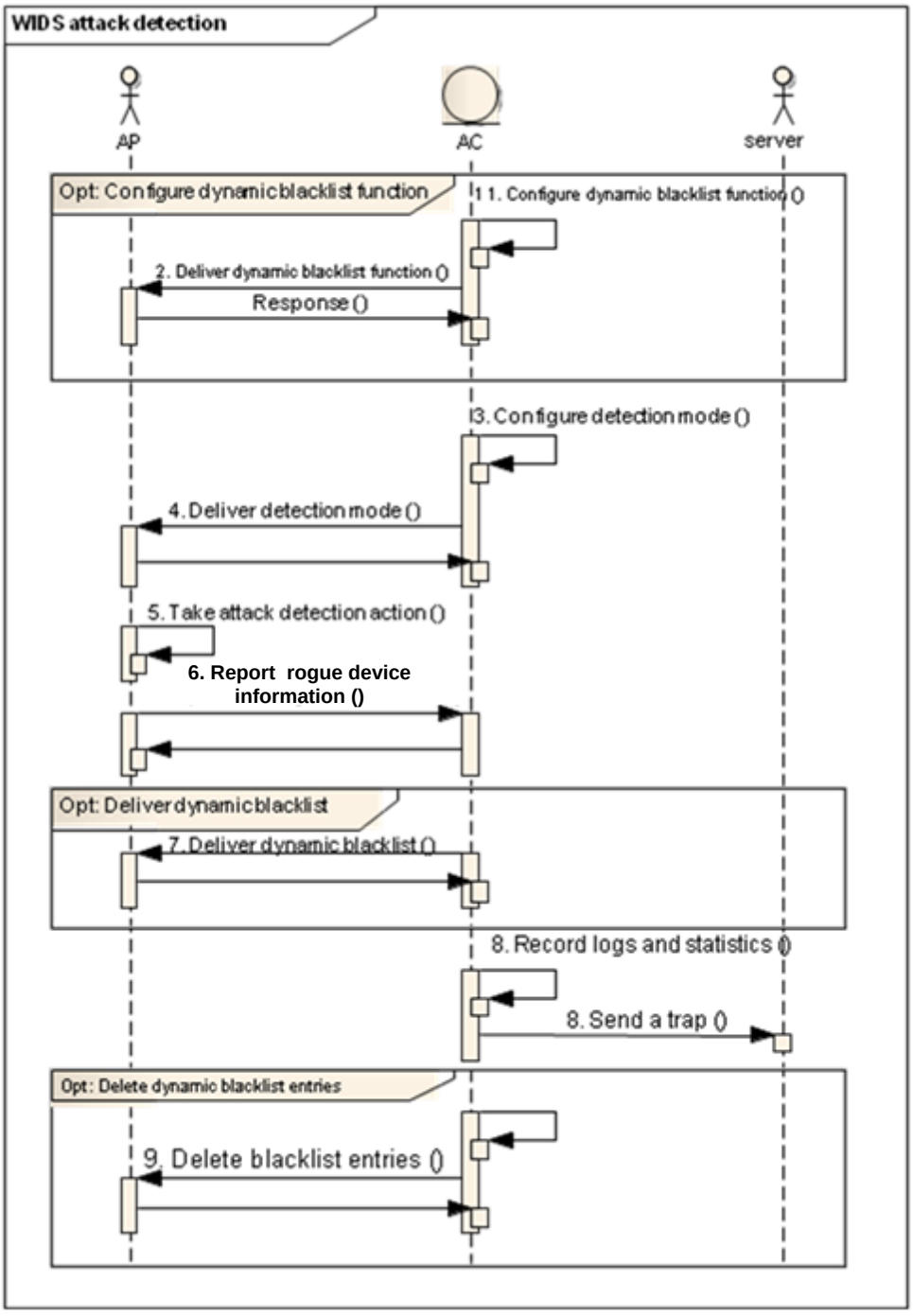
Monitor APs take countermeasures periodically on channels of rogue devices using the configured probing mode.

1.3.4 WIDS Attack Detection

On small and medium WLAN networks, WIDS can be enabled to detect security threats, including flooding attacks, weak initialization vector (IV), and spoofing attacks. This function enables an AP to add attackers to the dynamic blacklist and send attacker information to the AC. The AC then sends trap messages to the network management system (NMS) to alert the administrators.

Figure 1-4 shows the WIDS attack detection process.

Figure 1-4 WIDS attack detection process



1. The dynamic blacklist function is enabled and the blacklist entry aging time is set on the AC.
2. The AC sends the dynamic blacklist enabled flag and blacklist entry aging time to the AP.
3. The WIDS attack detection mode, detection period, and detection threshold (number of packets detected within the specified period to identify an attack) are configured on the AC.

4. The AC sends the detection mode, detection period, and detection threshold to the AP.
5. The AP performs attack detection according to the configuration.
6. When the AP detects an attack, it reports the attack information to the AC, including the rogue device MAC address and attack type. The AC receives the attack information and adds the received information to the attack record. If the AP does not detect attacks from this rogue device again in the next three attack detection periods, it requests the AC to delete the corresponding attack record.
7. The AP determines whether to add the rogue device to the dynamic blacklist. If the AP adds the rogue device to the dynamic blacklist, the AP reports the dynamic blacklist entry to the AC. The AC adds this entry to the dynamic blacklist cache. The AP drops packets sent from blacklisted devices.
8. The AC records attack types and sends trap messages to report the attack types to the NMS.
9. When a blacklist entry is deleted manually on the AC, the AC sends an instruction to the AP, requesting the AP to delete the corresponding blacklist entry.

WIDS can detect 802.11 packet flooding attacks, spoofing attacks, and weak IV. Attack information reported by an AP includes the rogue device MAC address, channel, attack type, and received signal strength indicator (RSSI).

- Flooding attack detection

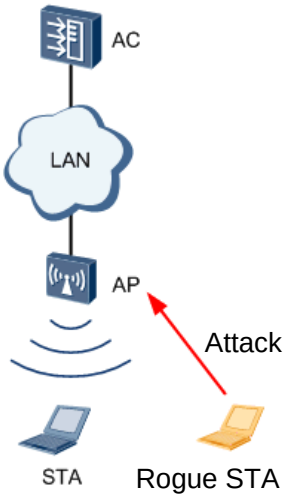
  A flooding attack occurs when an AP receives a large number of management packets or null data packets of the same type from a source MAC address within a short period. These attack packets consume many system resources of the AP, and therefore the AP cannot process packets from authorized STAs.

  Flooding attack detection allows an AP to keep monitoring the traffic rate of each STA to prevent flooding 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 AP adds the detected attack STA to the dynamic blacklist. The AP drops all the packets from this STA to prevent the network from a flooding attack, until the dynamic blacklist entry ages.

  An AP can detect flooding attacks of the following frames:

  - Authentication Request
  - Deauthentication
  - Association Request
  - Disassociation
  - Probe Request
  - Action
  - EAPOL Start
  - EAPOL-Logoff
  - PS-Poll
  - 802.11 Null frame

Figure 1-5 Flooding attack

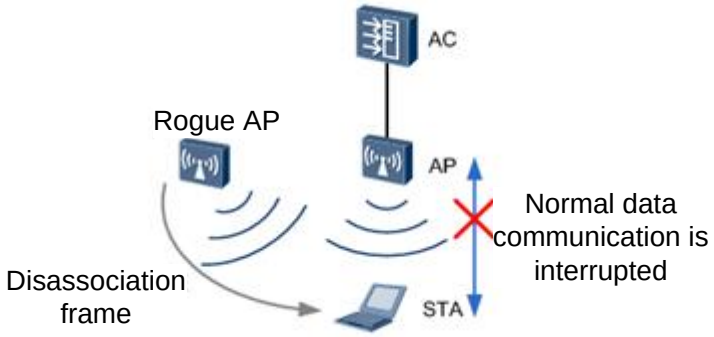


- Spoofing attack detection

  A spoofing attack is also called a man-in-the-middle 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 Disassociation frames and Deauthentication frames, which are broadcast 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.

Figure 1-6 Spoofing attack



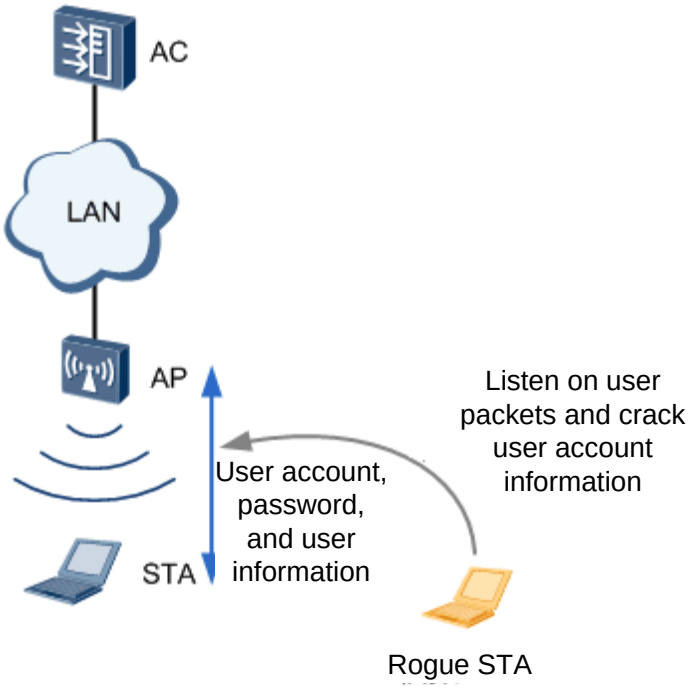
- Weak IV detection

  The wired equivalent privacy (WEP) standard uses a random 3-byte IV and a fixed shared key to encrypt every packet to be sent. This encryption algorithm ensures that packets are encrypted into different strings although the same key is used. If an AP uses a weak IV (the first byte of the IV ranges from 3 to 15 and the second byte is 255), attackers can easily crack the shared key because STAs send 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 the AP detects a packet carrying a weak IV, the AP 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 1-7 User account cracking through weak IVs



Spoofing attack detection cannot add attackers to the dynamic blacklist, whereas weak IV detection can prevent user information cracking without the need of a blacklist.

1.3.5 PSK Brute Force Attack Defense

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. In theory, the brute force method can crack any password. The only problem is how to shorten the time used to crack a password. When a WLAN uses the WPA/WPA2-PSK, WAPI-PSK, or WEP-Shared-Key security policy, attackers can use the brute force method to crack the password.

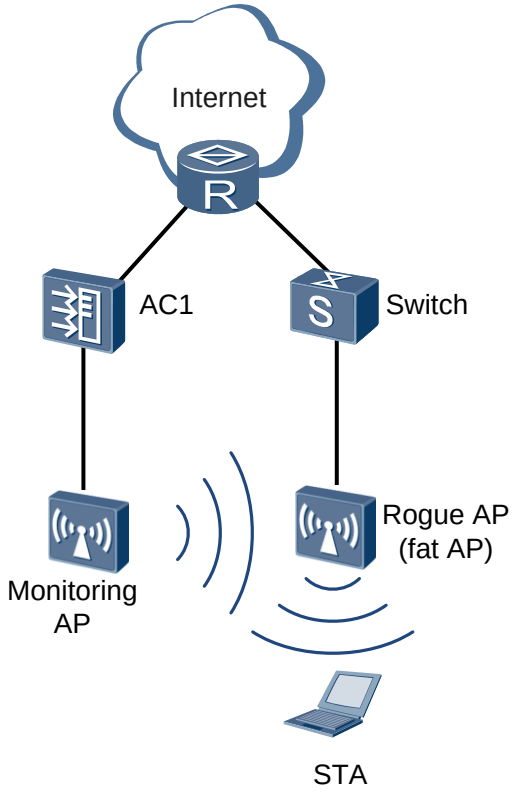
To improve key security, enable PSK brute force attack defense to prolong the time used to crack passwords. An AP checks whether the number of key negotiation attempts during WPA/WPA2-PSK, WAPI-PSK, or WEP-Shared-Key authentication exceeds the configured threshold. If so, the AP considers that a user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

1.4 References

Document	Description
802.11-2007	IEEE Standard for Information technology Telecommunications and information exchange between systems Local and metropolitan area networks Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications

2 WIDS/WIPS Application

Figure 2-1 WIDS/WIPS networking



As shown in Figure 2-1, an employee connects to a rogue fat AP from the campus network or uses simulation software to simulate a fat AP. After WIDS and WIPS are configured on AC1, the monitor AP collects neighbor information and reports it to AC1. When AC1 identifies the rogue AP, AC1 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 countermeasure prevents STAs from associating with the rogue AP.

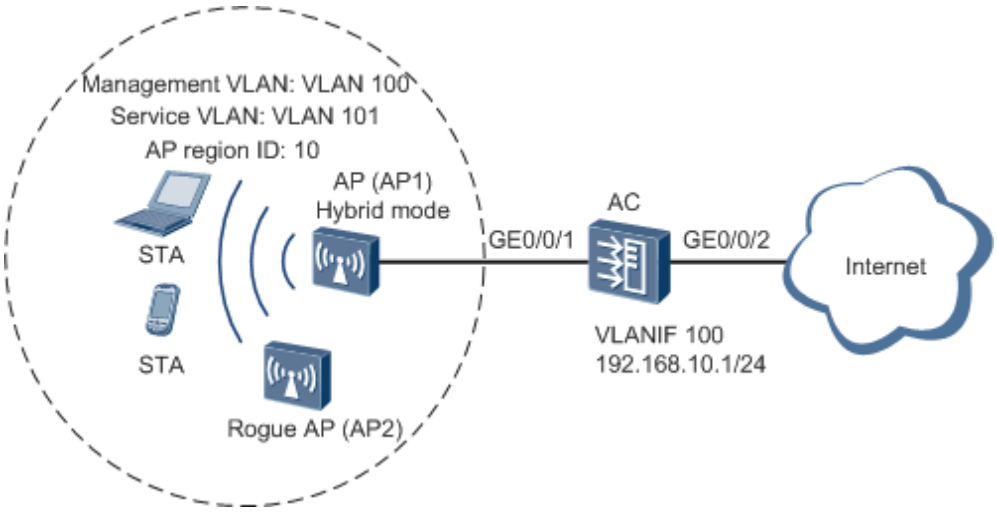
3 Configuration Example

3.1 Networking Requirements

AP1 directly connects to the AC. The enterprise needs to deploy basic WLAN services to enable mobile users to connect to the enterprise network from anywhere at any time. The WLAN SSID is test, and STAs must be able to automatically obtain IP addresses.

A rogue AP (AP2) is deployed on the WLAN and attempts to steal enterprise business information by establishing connections with STAs. This rogue AP threatens information security on the enterprise network. To protect the enterprise network against intrusion from such rogue APs, configure WIDS and WIPS on the AC so that the AC can detect AP2 and prevent STAs from associating with AP2.

Figure 3-1 Rogue AP detection and countermeasure



3.2 Configuration Roadmap

1. Configure basic WLAN services to enable STAs to connect to the WLAN.
2. Configure WIDS and WIPS functions: Set the working mode of AP1 to monitor or hybrid so that AP1 can report neighboring wireless device information and report the

collected neighbor information to the AC. Then enable the AC to take countermeasures to rogue APs, so that STAs can disassociate from the rogue AP (AP2).

3.3 Procedure

1. Configure the AC as a DHCP server to allocate IP addresses to STAs and APs.

   # Enable the DHCP service on the AC and configure IP address pools on VLANIF 100 and VLANIF 101. The DHCP server allocates IP addresses to APs from the IP address pool on VLANIF 100, and allocates IP addresses to STAs from the IP address pool on VLANIF 101.

   ```
   [AC] dhcp enable
   [AC] interface vlanif 100
   [AC-Vlanif100] ip address 192.168.10.1 24
   [AC-Vlanif100] dhcp select interface
   [AC-Vlanif100] quit
   [AC] interface vlanif 101
   [AC-Vlanif101] ip address 192.168.11.1 24
   [AC-Vlanif101] dhcp select interface
   [AC-Vlanif101] quit
   ```

2. Configure AC system parameters.

   # Configure the country code.

   ```
   [AC] wlan ac-global country-code cn
   ```

   # Configure the source interface.

   ```
   [AC] wlan
   [AC-wlan-view] wlan ac source interface vlanif 100
   ```

3. Manage APs on the AC.

   # Check the AP type ID after obtaining the AP MAC address.

   ```
   [AC-wlan-view] display ap-type all
    All AP types information:
   ID    Type
    --------------------------------------------------------------------------------
    0     WA601
    1     WA631
    6     WA603SN
    7     WA603DN
    8     WA633SN
    11    WA603DE
    12    WA653DE
    14    WA653SN
    17    AP6010SN-GN
    19    AP6010DN-AGN
    21    AP6310SN-GN
    23    AP6510DN-AGN
    25    AP6610DN-AGN
    27    AP7110SN-GN
    28    AP7110DN-AGN
    29    AP5010SN-GN
    30    AP5010DN-AGN
    31    AP3010DN-AGN
    33    AP6510DN-AGN-US
   ```

```
  34    AP6610DN-AGN-US
  ------------------------------------------------------------------------------
  Total number: 20
```

Add the AP offline according to the AP type ID. For example, the AP type is AP6010DN-AGN and MAC address is 5489-9846-1dd4.

```
[AC-wlan-view] ap-auth-mode mac-auth
[AC-wlan-view] ap id 0 type-id 19 mac 5489-9846-1dd4
[AC-wlan-ap-0] quit
# Configure an AP region and add the AP to the region.
[AC-wlan-view] ap-region id 10
[AC-wlan-ap-region-10] quit
[AC-wlan-view] ap id 0
[AC-wlan-ap-0] region-id 10
[AC-wlan-ap-0] quit
```

After powering on the AP, run the **display ap all** command on the AC to check the AP running status. The command output shows that the AP status is normal.

```
[AC-wlan-view] display ap all
  All AP information(Normal-1,UnNormal-0):

------------------------------------------------------------------------------
  AP    AP                AP            Profile   AP            AP
                                        /Region
  ID    Type              MAC            ID       State         Sysname

------------------------------------------------------------------------------
  0     AP6010DN-AGN        5489-9846-1dd4    0/10    normal         ap-0

------------------------------------------------------------------------------
  Total number: 1
```

4. Configure WLAN service parameters.

   # Create a WMM profile **wmm**.

```
[AC-wlan-view] wmm-profile name wmm id 1
[AC-wlan-wmm-prof-wmm] quit
```

   # Create a radio profile **radio** and bind the WMM profile **wmm** to the radio profile.

```
[AC-wlan-view] radio-profile name radio id 1
[AC-wlan-radio-prof-radio] wmm-profile name wmm
[AC-wlan-radio-prof-radio] quit
[AC-wlan-view] quit
```

   # Create WLAN-ESS interface 1.

```
[AC] interface wlan-ess 1
[AC-Wlan-Ess1] port link-type hybrid
[AC-Wlan-Ess1] port hybrid pvid vlan 101
[AC-Wlan-Ess1] port hybrid untagged vlan 101
[AC-Wlan-Ess1] quit
```

   # Create a security profile **security**.

```
[AC] wlan
[AC-wlan-view] security-profile name security id 1
[AC-wlan-sec-prof-security] quit
```

   # Create a traffic profile **traffic**.

```
[AC-wlan-view] traffic-profile name traffic id 1
```

```
[AC-wlan-traffic-prof-traffic] quit
```

Create a service set **test** and bind the WLAN-ESS interface, security profile, and traffic profile to the service set.

```
[AC-wlan-view] service-set name test id 1
[AC-wlan-service-set-test] ssid test
[AC-wlan-service-set-test] wlan-ess 1
[AC-wlan-service-set-test] security-profile name security
[AC-wlan-service-set-test] traffic-profile name traffic
[AC-wlan-service-set-test] service-vlan 101
[AC-wlan-service-set-test] forward-mode tunnel
[AC-wlan-service-set-test] quit
```

5. Configure WIDS and WIPS.

   Configure WIDS.

```
[AC-wlan-view] ap 0 radio 0
[AC-wlan-radio-0/0] work-mode hybrid
 Warning: Modify the work mode may cause business interruption, are you sure to continue?(y/n)[n]:y
[AC-wlan-radio-0/0] device detect enable
```

   # Enable countermeasures to rogue APs.

```
[AC-wlan-radio-0/0] countermeasures enable
[AC-wlan-radio-0/0] countermeasures mode rogue ap
[AC-wlan-radio-0/0] quit
```

6. Configure a VAP and deliver the VAP configuration to the AP.

   # Configure a VAP.

```
[AC-wlan-view] ap 0 radio 0
[AC-wlan-radio-0/0] radio-profile name radio
 Warning: Modify the Radio type may cause some parameters of Radio resume default value, are you sure to continue?[Y/N]:y
[AC-wlan-radio-0/0] service-set name test
[AC-wlan-radio-0/0] quit
```

   # Commit the configuration.

```
[AC-wlan-view] commit ap 0
  Warning: Committing configuration may cause service interruption,continue?[Y/N]y
```

7. Verify the configuration.

   Run the **display wlan ids countermeasures device all** command on the AC to view information about rogue APs to which countermeasures were taken. Information about AP2 is displayed in the command output.

```
[AC] display wlan ids countermeasures device all
Total number of countermeasures device: 1
Flags: a = adhoc, w = ap, c = client
#AP = number of active APs detecting, Ch = channel number
--------------------------------------------------------------------------------
 MAC address    Type  #AP   Ch   Last Detected Time   SSID
--------------------------------------------------------------------------------
 000b-6b8f-fc6a  -w    1   11   2012-01-22/15:33:21   test
--------------------------------------------------------------------------
```

STAs attempt to connect to the Internet through AP2. Because countermeasure has been taken on AP2, traffic of the STAs is interrupted intermittently.

```
C:\Documents and Settings\huawei>ping www.baidu.com

Pinging www.a.shifen.com [220.181.112.143] with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.
Reply from 220.181.112.143: bytes=32 time=1433ms TTL=255
Reply from 220.181.112.143: bytes=32 time=40ms TTL=255
Reply from 220.181.112.143: bytes=32 time=11ms TTL=255
Reply from 220.181.112.143: bytes=32 time=46ms TTL=255
Request timed out.
Request timed out.
```

3.4 Configuration Files

The following is part of the configuration file on the AC:

```
sysname AC
#
vlan batch 100 to 101
#
dhcp enable
#
interface Vlanif100
 ip address 192.168.10.1 255.255.255.0
 dhcp select interface
#
interface Vlanif101
 ip address 192.168.11.1 255.255.255.0
 dhcp select interface
#
interface WLAN-ESS1
 port hybrid pvid vlan 101
 port hybrid untagged vlan 101
#
wlan
 wlan ac source interface vlanif100
 ap-region id 10
 ap id 0 type-id 19 mac 5489-9846-1dd4 sn AB35015384
  region-id 10
 wmm-profile name wmm id 1
 traffic-profile name traffic id 1
 security-profile name security id 1
 service-set name test id 1
  forward-mode tunnel
  wlan-ess 1
  ssid test
  traffic-profile id 1
  security-profile id 1
```

```
 service-vlan 101
radio-profile name radio id 1
 wmm-profile id 1
ap 0 radio 0
 radio-profile id 1
 service-set id 1 wlan 1
 work-mode hybrid
 device detect enable
 countermeasures enable
 countermeasures mode rogue ap
```