Content

Chapter 1 Wireless Security

IEEE 802.11 networks are vulnerable to under the impact of a variety of network threats, such as the user of the unauthorized AP (Access Point), Ad-hoc network, flooded attack, etc. Rogue equipment for the enterprise network security is very serious threat. WIDS (Wireless Intrusion Detection System) is used for the early detection of a malicious user attacks and wireless network intrusion. WIPS (Wireless Intrusion Prevention System) can protect the enterprise network and user from the access of unauthorized devices on the wireless network. Wireless security function not only can be the early detection of malicious user attacks and wireless network intrusion, but also can take anti-attack measures for active defense, to ensure that the devices to access the enterprise network and users are not on the wireless network on unauthorized.

The following is a description of the wireless security message:

1. RF Scan Report Message

Managed AP will periodically send RF Scan Report Message to the AC-Controller, which records the neighbors AP and client information. According to the neighbor information, WIDS module will do corresponding threat detection, in order to identify whether the existence of illegal equipment around there. (Can either be the unknow deviceds or rogue)

2. Client-Threat-Deauthenticate Message

When the “legitimate Client related to illegal AP” is detected and identified as Rogue equipment, if the protection function of known client is opened, AC Controller will send this message to Managed AP. The AP will pretend the client and send this Client solution authentication message to its associated AP, to relieve the connection of the Known Client and Unknown AP.

3. WIDS-Configuration Message

When the configuration or Rogue AP attack table changed, AC Controller sends this message to AP, which fields are optional except the AP MAC Address.

Table 1-1 message format of WIDS-Configuration-Message

Description	Element ID	Element Length	Content
AP MAC Address	0x0021	6 bytes	AP MAC Address
Enable Wired Network Detection	0x7001	1 byte	0—Disable Detection 1—Enable Detection

Minimum Wired Network Detection Interval	0x7002	2 bytes	0—Network detection is performed on every RF Scan sweep. 1–3600—Number of seconds between detection attempts.
AP Attack Interval	0x7003	2 bytes	Number of seconds between transmissions of de-authentication frames by operational mode radios.
Number of BSSIDs in the attack list.	0x7004	2 bytes	Number of BSSID for which the AP will execute a de-authentication attack. Set to 0 for an empty list.
BSSID Attack List	0x7005	7 to 112 bytes	6-byte BSSID followed by 1 byte channel number. The list size depends on number of entries.

Chapter 2 AP Threat Detection

2.1 Introduction to AP Threat Detection

AP real-time monitoring the surrounding RF environment, including the neighbor Client and AP information, and periodically send the monitored information to the associated AC. If AC is not the Controller of the whole cluster, the RF Scan Report Message needs to be forwarded to the AC Controller. AC Controller will then analyze the RF Scan Report Message neighbor information, to monitor abnormal device in the entire WLAN network through the established rules illegal device for detecting.

The working state of AP can be divided into four and shown in the table below, which the AP Radio of AP-ended RF Scanning can be configured in two models: Active and Sentry. Radio in Active mode processing use traffic normally, just periodic scan, in a set interval of time. But it can only scan their own working band, such as 2.4G or 5G; Radio in Sentry mode dose not process any user traffic, which is dedicated to scan the monitoring information and monitor all the channels within the bands of 2.4G and 5G in turn. Because the Radio of Sentry mode specifically used to RF scanning and monitoring all the channels of 2.4G and 5G bands at the same time, it can be more comprehensive, accurate and rapid to get RF information. Therefore, some threats must be a sentry mode reported by RF Scan Report Message can be detected, including the ap working in illegal channel, ummanged AP access wired network.

Table 2-1 AP’s four state

Status	Explanation
Managed	In the AC Management (thin AP) state.
Standalone	In the independent operation (fat AP) state, the administrator must manually set this AP to standalone status in the Valid.
Unknown	Unrecognized no state, neither managed or standalone, but not been determined to be illegal AP.
Rogue	Illegal AP, it was identified as a threat by correlative detection.

According to the hacker used illegal AP usage, this product has developed 11 kinds of detection to monitor the abnormal AP in WLAN network: the network management settings of illegal AP; illegal AP pretend to be legitimate SSID; Vendor field in the Beacon is not legitimate; Beacon frame does not have a SSID field; managed AP Beacon frame received in the wrong channel; managed AP sends invalid SSID; AP works in illegal channel; legitimate fat AP configuration error and unmanaged AP access to wired network; AP use a incorrect security authentication; AP works in WDS mode. AC Controller runs the 11 kinds of tests, if a threat is detected; put the AP characterized as Rogue, and send Trap to inform network management.

At the same time, if AC Controller opens the anti-attack function, will send WIDS-Configuration-Message, Rogue AP list sent to Managed AP, then Managed AP rogue AP anti-attack, while sending “wsRFScanRogueAPDetected” Trap to inform network management.

The following will introduce 11 kinds of defensive rule:

1. Network Management Setting of Illegal AP

Network management can be set up in Valid-AP database authentication of local or Radius server. The administrator can manually configure AP into three stats in the Valid-AP database: Managed, Standalone, Rogue. The setting of the illegal AP is the local or Radius server’s Valid-AP database configuration for Rogue AP.

2. Illegal AP pretend to be Legitimate SSID

The network configuration of the AC controller SSID enquire system records the legitimacy of the SSID, sometimes illegal AP pretend to be the legitimate of the SSID to deceive customers access to Client, thereby stealing customer information.

3. Vendor Field in the Beacon Frame is not legitimate

Some hackers pose as Mac of Managed AP and sent the situation of Managed SSID. The managed AP beacon frame agreement of the product must carry the vendor field, then Mac address of the Rogue AP by detecting vendor field it can be detected out of the Managed AP(If there is no vendor field, the AP MAC Address of the Neighbor AP Info of RF Scan Report Message is 00-00-00-xx-xx-xx).

4. Beacon Frame does not have a SSID Field

In order to avoid being detected, the hacker may not contain a SSID field in the beacon frame, but it can still send probe response frame to the Client, who sent the probe request, in order to deceive the client access, to obtaining security information.

5. Managed AP Beacon Frame received in the Wrong Channel

Due to the Managed AP channel is assigned by the AC, so AC knows working the channel of the Managed AP, the hacker fakes Managed AP mac to send beacon frames used by the channel, but may be in the wrong channel.

6. AP uses a false sense of security authentication

AP’s beacon frame contains its security authentication methods (open, WEP, WPA), so by detection of beacon frame carrying the safety authentication method and AC Controller recorded in the AP configuration consistency, can detect such rogue AP.

7. Managed AP Sends an Invalid SSID

If Managed AP sent an invalid SSID, the AP, which detected the Managed AP will sent RF Scan Report Message to AC Controller, the message will contain the illegal SSID.

8. AP Works in Illegal Channel

Different countries have different regulations for RF resources, some channels in some countries are legal, but in some other countries are illegal. If the AP is in the illegal channel, this step can be detected. Due to the interception of all channel beacon frame, only the RF Scan Report information of sentry mode Radio to detect this threat.

9. Legitimate Fat AP Configuration Error

If the initial state of AP is standalone, and the checked scan configuration and AC Controller saved configuration is consistent with the AP as the legitimate AP. Otherwise is Rogue AP. Note: To check the configuration of working channel, SSID security authentication mode ,WDS mode and whether access to the wired network.

10. AP Works in WDS Mode

WDS (Wireless Distribution System) wireless distributed systems is access point (AP) through a wireless connection agreement. Run each other connected by a bridge or repeater AP in WDS mode, reduced the dependence of the wired network and improve the structure of the network flexibility and convenience.

If AP is connect to the AC and managed by AC through the way of WDS, and the faked AP was detected in WDS mode does not work, it can be considered a threat.

11. Unmanaged AP accesses to wired network

Because only managed AP access to the wired network, so if AP’s state is Unknown and was detected connected to the wired network, then testing for Rogue AP.

2.2 AP Threat Detection Configuration

1. Network management configures illegal AP

Command	Explanation
Wireless Global Mode	
wids-security admin-config-rogue	Enable illegal AP detection network management configured.

2. Configuration of illegal AP palming off lawful SSID

Command	Explanation
Wireless Global Mode	
wids-security unknown-ap-managed-ssid **no wids-security unknown-ap-managed-ssid**	Enable/disable the detection of illegal AP palming off lawful SSID.

3. Configuration of illegal Vendor field in Beacon frame

Command	Explanation
Wireless Global Mode	
wids-security fakeman-ap-managed-ssid **no wids-security fakeman-ap-managed-ssid**	Enable/disable the detection of illegal Vendor field in Beacon frame.

4. Configuration of no SSID field in Beacon frame

Command	Explanation
Wireless Global Mode	
wids-security managed-ap-ssid-invalid **no wids-security managed-ap-ssid-invalid**	Enable/disable the detection of no SSID field in Beacon frame.

5. Configuration of Beacon frame which received managed AP in the wrong channel

Command	Explanation
Wireless Global Mode	
wids-security fakeman-ap-chan-invalid **no wids-security fakeman-ap-chan-invalid**	Enable/disable the Beacon frame detection which received managed AP in the wrong channel.

6. Configuration of AP using the wrong security authentication method

Command	Explanation
Wireless Global Mode	
wids-security managed-ssid-secu-bad **no wids-security managed-ssid-secu-bad**	Enable/disable the detection of AP using the wrong security authentication method.

7. Configuration of Managed AP sending invalid SSID

Command	Explanation
Wireless Global Mode	
wids-security managed-ap-ssid-invalid **no wids-security managed-ap-ssid-invalid**	Enable/disable the detection of Managed AP sending invalid SSID.

8. Configuration of AP working in illegal channel

Command	Explanation

Wireless Global Mode	
wids-security ap-chan-illegal **no wids-security ap-chan-illegal**	Enable/disable the detection of AP working in illegal channel.

9. Configuration of lawful fat AP configured incorrectly

Command	Explanation
Wireless Global Mode	
wids-security standalone-cfg-invalid **no wids-security standalone-cfg-invalid**	Enable/disable the detection of lawful fat AP configured incorrectly.

10. Configuration of AP working in WDS mode

Command	Explanation
Wireless Global Mode	
wids-security wds-device-unexpected **no wids-security wds-device-unexpected**	Enable/disable the detection of AP working in WDS mode.

11. Configuration of Unmanaged AP accessing wired network

1) Enable/disable the detection of Unmanaged AP accessing wired network

Command	Explanation
Wireless Global Mode	
wids-security unmanaged-ap-wired **no wids-security unmanaged-ap-wired**	Enable/disable the detection of Unmanaged AP accessing wired network
wids-security wired-detection-interval <*interval*> **no wids-security wired-detection-interval**	Configure the shortest waiting time of each round of detection; recover the waiting time to be default.

2) Configure VLAN ID of multicast frame detection

Command	Explanation
AP Profile Configuration Mode	

wired-detection-vlan <0-4094> **no wired-detection-vlan**	Configure VLAN ID of multicast frame detection; recover the VLAN ID to be default.

12. Relevant configuration of Debug

Command	Explanation
Admin Mode	
debug wireless wids internal-info **no debug wireless wids internal-info**	Enable/disable debug information in WIDS rogue-detection.

2.3 AP Threat Detection Configuration Examples

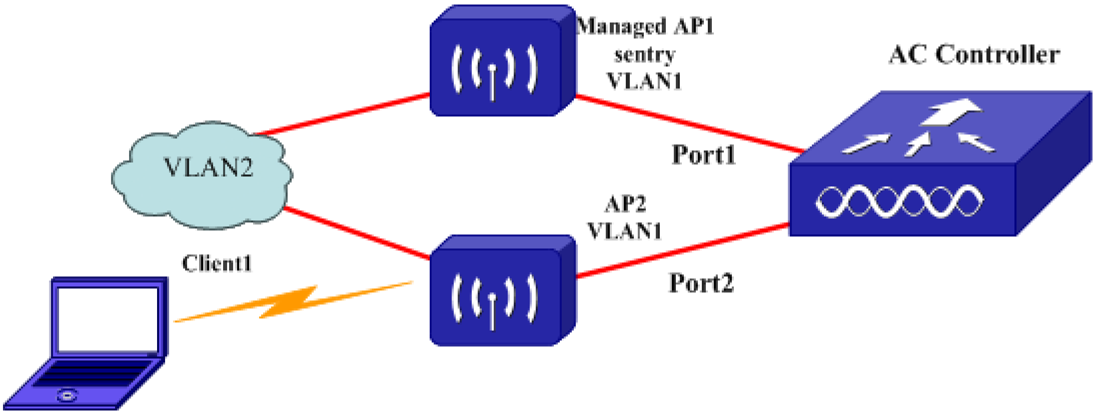


Figure 2-1 case of the Unmanaged AP access wired network

As shown above is an AC network, Managed AP1 connected to AC controller through port1, periodically send the RF scan report message to AC controller for processing. AP1's status is set to sentry mode, AP2 to be testing equipment in the network. To detect whether the network have the existence of Unmanaged AP access the wired network, one needs to configure the AC controller and AP1 as follows:

```
AC>enable
AC#config
AC(config)#wireless
AC(config-wireless)#wids-security unmanaged-ap-wired
AC(config-wireless)#wids-security wired-detection-interval 120
AC(config-wireless)#ap profile 1
AC(config- AP Profile)#vlan 2
```

2.4 AP Threat Detection Troubleshooting

When configure, use the AP threat detection. If AP threat detection failed to normal operation or test result was error. Please check whether the reasons are as follows:

- Please check whether the physical connection is correct.
- Please check whether the AP threat detection has already started.
- AP works in the detection of illegal channels and unmanaged AP, access to the wired network, to confirm the operating mode of scanning AP is sentry mode.
- If illegal AP pretend to be legitimate SSID, threat detection items appear detection result error, please check whether the AP in the AP detection, which is not this cluster, use the same SSID or not. If it is exist, please modify the SSID of the AP that is not in this cluster.
- If Beacon frame does not appear detection result error of a SSID field detection, please check whether configured Hidden SSID for VAP in Internet. If it is exist, please turn off this detection.
- If the AP using the wrong security authentication mode detection items and appear detection results error, please check whether the AC controller is in phase with the AP secure manner in the cluster.
- If Managed AP sends an invalid SSID detection items and appear detection error, please check whether the AC Controller is in phase with the AP network configuration in the cluster.

Chapter 3 Client Threat Detection

3.1 Introduction to Client Threat Detection

The Client state is divided into four kinds as follows:

Table 3-1 Client's four states

Status	Explanation
Authenticated	Client passed the authentication
Detected	The detected Client, did not pass the authentication but have not been identified as illegal
Black-Listed	Client in blacklist
Rogue	Illegal Client

According to the common used method of Illegal Client, this product has made 7 kinds of detection rules to monitor abnormal Client in WLAN network. OUI is not legitimate; Known Client Database to determine illegal authentication request frame flooded attacks; probe request frame flooded attacks; solution of authentication frame flooded attacks; authentication failure and maximum number more than threshold; legitimate Client connected to unknown AP. AC Controller runs the 7 kinds of detection rules, if a threat is detected, put the Client characterized as the Rogue, and send Trap network. At the same time, if it is legitimate Client related to unknown AP and found Rogue Client, it will execute Known Client protection mechanism.

AC Controller supports the Client threat detection which had mentioned above can be configured separately whether to open the corresponding detection. The detection algorithm runs on AC Controller only, extract a neighbor Client information from the received RF Scan report in the following order of threat detection:

1. OUI is illegal

The network management can set legitimate OUI in the AC Controller OUI table, thus once can enquire to target Client Mac address OUI field (three bytes) is in the OUI table with entries, to detect such threats

2. Known the Client Database to determined illegal

The network management can configures AC Controller to read the Known Client Database from a local or Radiu server, if it's a legitimate Client, Known Client Database will have the corresponding client entry. Therefore, according to the configuration of Known Client Database, it can detect whether the client is legitimate.

If network management configures AC controller to read the Known Client Database from a local server, then the AC will read Known Client Database from the local Known

Client Cache.

If the serve preset to Radius server, the AC is actually read Client table entry from the local Known Client Cache. When the Client table is not related to this client, it will put this client into the Detected Clients Database, and AC will send request to the Radius server, read the corresponding entry in the Known Client Database, after Radiu server returns the result, according to the returned result to change the client state of Detected local Known Client Cache.

3. Flooding attack of association request frame

Flooding attack refers to the WLAN equipment will receive a lot of the same type of message in a short time. Then WLAN equipment will be inundated by flooding attack message and can not to deal with the real wireless terminal message.

Association request frame flooded attack refers to Rogue Client send a large number request frame to an AP device in a short period of time, the AP device will be inundated by flooding attack message and can not to deal with the real wireless terminal message. In response to this threat, this product through judge whether the association request frame is beyond the configuration of the frame transmission rate to detect, that is, if sent the association frame exceeds the threshold in detected time, detected as a threat.

4. Flooding attack of disassociation request frame

Disassociation request frame flooded attack refers to Rogue Client send a large number request frame to an AP device in a short period of time, the AP device will be inundated by flooding attack message and can not to deal with the real wireless terminal message. In response to this threat, this product through judge whether the disassociation request frame is beyond the configuration of the frame transmission rate to detect, that is, if sent the disassociation frame exceeds the threshold in detected time, detected as a threat.

5. Flooding attack of Authentication request frame

Flooding attack refers to the WLAN equipment will receive a lot of the same type of message in a short time. Then WLAN equipment will be inundated by flooding attack message and can not to deal with the real wireless terminal message.

Authentication request frame flooded attack refers to Rogue Client send a large number request frame to an AP device in a short period of time, the AP device will be inundated by flooding attack message and can not to deal with the real wireless terminal message. In response to this threat, this product through judge whether the authentication request frame is beyond the configuration of the frame transmission rate to detect, that is, if sent the Authentication Frame exceeds the threshold in detected time, detected as a threat. If enable dynamic blacklist, and should be added to the dynamic blacklist.

6. Flooding attack of Probe request frame

Probe request frame flooded attack refers to Rogue Client sends a large number of probe request frame to AP device in a short period of time. In response to the threat, the product by deterring whether the probe request frame is beyond the configuration of the frame transmission rate to detect, that is, if sent the Probe Request Frame exceeds the threshold in detected time the detection as a threat.

7. Flooding attack of Solution of Authentication Request Frame

Solution of authentication request frame flood attack refer to Rogue Client sends a large number of authentication request frame to a AP device in a short period of time. In response to this threat, the product by judging whether the solution authentication request frame is beyond the configuration of the frame transmission rate to detect, that is , if send the De-Authentication Request Frame exceeds the threshold in detected time. Then detect it as a threat. It is authentication failure maximum number.

8. Client Authentication failure times threshold

Some unknown Client in order to access a protected wireless network will send the authentication request until the request is allowed. In response to this threat, the product by judging whether the number of Client authentication exceeds the configured threshold, that is, if exceeded the configured maximum authentication failure number, the detection as a threat.

9. Lawful Client connected to unknown AP

The legitimate Client may guided by unknown AP to connected to the network through unknown AP, so that the legitimate Client's all kinds of information would be exposed the Hackers who use the unknown AP, with respect to this problem, if AC detected that AP's state is unknown, legitimate Client connected to this AP and detected as a threat.

3.2 Client Threat Detection Configuration

1. Rogue-detection configuration of illegal OUI

Command	Explanation
Wireless Global Mode	
wids-security oui-database-mode {both | local |read-only}	Configure the OUI database type used in configuring OUI lawful detection.
wids-security client oui-database **no wids-security client oui-database**	Enable/disable detection of illegal OUI.
oui database <*ouival*> <*oui*> **no oui database <*ouival*>**	Add/detele OUI database.

2. Configuration of Known Client Database judged illegal

Command	Explanation
Wireless Global Mode	
wids-security client known-client-database **no wids-security client known-client-database**	Enable/disable the detection of Known Client Database judged illegal.

3. Flooding attack of association request frame

Command	Explanation
Wireless Global Mode	
wids-security client configured-assoc-rate **no wids-security client configured-assoc-rate**	Enable flooding attack detection of association request frame.
wids-security client threshold-interval-assoc <1-3600> **no wids-security client threshold-interval-assoc <1-3600>**	Configure the detection time of client sending 802.11 association request frame.
wids-security client threshold-value-assoc <1-99999> **no wids-security client threshold-value-assoc**	Configure the threshold of client sending 802.11 association request frame.

4. Flooding attack of disassociation request frame

Command	Explanation
Wireless Global Mode	
wids-security client configured-disassoc-rate **no wids-security client configured-disassoc-rate**	Enable flooding attack detection of disassociation request frame.
wids-security client threshold-interval-disassoc <1-3600> **no wids-security client threshold-interval-disassoc**	Configure the detection time of client sending 802.11 disassociation request frame.
wids-security client threshold-value-disassoc <1-99999> **no wids-security client threshold-value-disassoc**	Configure the threshold of client sending 802.11 disassociation request frame.

5. Flooding attack of authentication requisition frame

Command	Explanation

Wireless Global Mode	
wids-security client configured-auth-rate **no wids-security client configured-auth-rate**	Enable/disable the detection of authentication requisition frame flooding attacking.
wids-security client threshold-interval-auth <*1-3600*> **no wids-security client threshold-interval-auth**	Configure detection time of authentication requisition frame; recover this time to be default of 60.
wids-security client threshold-value-auth <*1-99999*> **no wids-security client threshold-value-auth**	Configure authentication requisition frame threshold; recover this threshold to be default of 120.

6. Flooding attack of probe requisition frame

Command	Explanation
Wireless Global Mode	
wids-security client configured-probe-rate **no wids-security client configured-probe-rate**	Enable/disable the detection of exploring requisition frame flooding attacking.
wids-security client threshold-interval-probe <*1-3600*> **no wids-security client threshold-interval-probe**	Configure the detection time of exploring requisition frame; recover this time to be default of 60.
wids-security client threshold-value-probe <*1-99999*> **no wids-security client threshold-value-probe**	Configure exploring requisition frame threshold; recover this threshold to be default of 120.

7. Flooding attack of relieving authenticating requisition frame

Command	Explanation
Wireless Global Mode	

wids-security client configured-deauth-rate **no wids-security client configured-deauth-rate**	Enable/disable the detection of relieving authenticating requisition frame flooding attacking.
wids-security client threshold-interval-deauth <*1-3600*> **no wids-security client threshold-interval- deauth**	Configure the detection time of relieving authenticating requisition frame; recover this time to be default of 60.
wids-security client threshold-value-deauth <*1-99999*> **no wids-security client threshold-value- deauth**	Configure relieving authenticating requisition frame threshold; recover this threshold to be default of 120.

8. Maximum times of authentication failure

Command	Explanation
Wireless Global Mode	
wids-security client max-auth-failure **no wids-security client max-auth-failure**	Enable/disable the detection of maximum times of authentication failure.
wids-security client threshold-auth-failure <1-99999> **no wids-security client threshold-auth-failure**	Configure maximum times threshold of authentication failure; recover this threshold to be default of 5.

9. Lawful Client associates with unknown AP

Command	Explanation
Wireless Global Mode	
wids-security client auth-with-unknown-ap **no wids-security client auth-with-unknown-ap**	Enable/disable function of lawful client associating with unknown AP.

10. Relevant configuration of Debug

Command	Explanation
Admin Mode	

debug wireless wids known-client internal-info **no debug wireless wids known-client internal-info**	Enable/disable debug information of configuring Known client database.

3.3 Client Threat Detection Examples

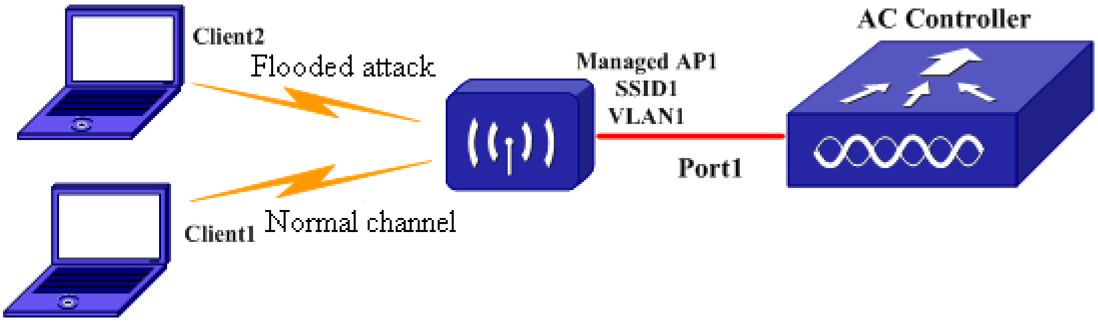


Fig 3-1 case of authentication request frame flood attack

As shown above, Client 1 and Client 2 connected to wireless network. AP1 Client communicates normally, Client 2 is the flood attacker of the flood attack authentication request frame, and it continued to send authentication request to AP1. In order to detect the Client 2 is the Rogue Client of the authentication request frame flooded attack in the network, needs to configure AC controller as follows:

```
AC>enable
AC#config
AC(config)#wireless
AC(config-wireless)#no wids-security client threshold-interval-auth
AC(config-wireless)#wids-security client threshold-value-auth 6000
AC(config-wireless)#wids-security client configured-auth-rate
```

3.4 Client Threat Detection Troubleshooting

When configure, use the Client threat detection, may be due to the physical connection, configuration errors and other reasons led to the detection could not run correctly or error detection. Please check whether the reasons are as follows:

- Ensure the physical connection is correct
- Confirm to start the Client threat detection
- Confirm that the corresponding threshold (authentication request frame flooded attack, the probe request frame flooded attack, the solution of the authentication request frames flooded attack and the maximum number of authentication failure) are

settings appropriately.

Chapter 4 Anti-attack

4.1 Introduction to Anti-attack

After the Rogue AP is detected, if enable the Rogue AP anti-attack, AC Controller will send attack list to Managed AP, Managed AP takes measures to Rogue equipment. Anti-attack measures are divided into 2 types: Rogue AP Anti-attack Function and Known Client Protection Function. Once start the anti-attack function, Sentry Mode Radio will pretend to be the Client to send the solution of authentication message to Rogue AP. And Active Mode Radio will send the solution of authentication message to related Rogue AP Client, to release the connection of Rogue AP and Client. But the following solution will not add to the attack list:

- AP's Mac address is Managed AP Mac (no matter it's fake or real).
- AP works in ad-hoc mode.
- AP works in illegal channel.
- AP attack list is full (up to 16 Rogue AP)

1. Rogue AP Anti-attack Function

After AC Controller detected Rogue AP, if Rogue AP Anti-attack function is opened, then it will be added to Rogue AP attack list, and send list to all the Managed AP through the WIDS-Configuration-Message. Sentry mode Radio will pretend to be the Client to send the solution of authentication message to Rogue AP, and Active Mode Radio will send the solution of authentication message to related Rogue AP Client.

2. Known Client Protection Function

If AC Controller opens legitimate Client associated Rogue AP detection and to detect a threat. After open the threat Rogue identification, the Client is marked as Rogue Client, while Rogue Client information (including mac, channel, associated AP mac, associated AP Radio, etc.) will be treat as a message send to client-security task. The task message queue capacity is 128, therefore to receive up to 128 messages. After received the message of the WIDS module, client-security task will sent Client-Deauthenticate Message to managed AP, Sentry mode Radio will pretend to be the Client sent solution of authentication message to related AP, in order to release the connection with the rogue AP.

4.2 Anti-attack Configuration

1. Anti-attack function configuration of Rogue AP

1) Enable/disable Rogue AP anti-attack function

Command	Explanation
Wireless Global Mode	
wids-security ap-de-auth-attack **no wids-security ap-de-auth-attack**	Enable/disable Rogue AP anti-attack function.

2) Recover Rogue AP to the previous status

Command	Explanation
Admin Mode	
wireless acknowledge-rogue [<*macaddr*>]	If the Rogue AP with appointed mac address has been cleared rogue by network management, recover it to the previous status.
wireless acknowledge-rogue	Change all Rogue APs to the previous status.

2. Known Client protection function configuration

1) Enable/disable Known Client protection function

Command	Explanation
Wireless Global Mode	
wids-security client threat-mitigation **no wids-security client threat-mitigation**	Enable/disable Known Client protection function

2) Clear client from Detected Clients Database

Command	Explanation
Admin Mode	
clear wireless detected-client [<*macaddr*>] non-auth	Clear the client of non-authenticated status appointed MAC address from Detected Clients Database.
clear wireless detected-client non-auth	Clear all clients from detected-client database.

3) Change the status of Rogue Client

Command	Explanation
Admin Mode	
wireless detected-client [<*macaddr*>] ack-rogue	Change the status of Rogue Client appointed MAC address.

wireless detected-client ack-rogue	Change the status of all Rogue Clients.

Notice: If client is authenticated before it is treated as Rogue, its status will change to authenticated; otherwise, its status will change to Detected.

3. Relevant configuration of Debug

Command	Explanation
Admin Mode	
debug wireless wids msg **no debug wireless wids msg**	Enable/disable the debug information of WIDS sending messages.

4.3 Anti-attack Examples

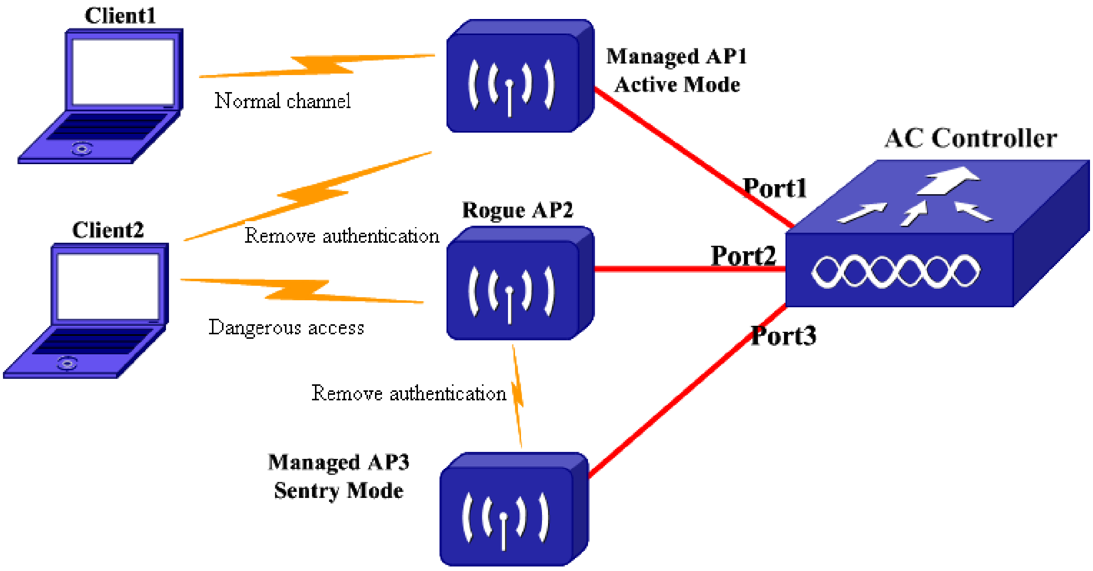


Fig 4-1 case of Rogue AP Anti-attack Function

As shown above, Client1 and Client2 connected to the network by AP1 and AP2 respectively. After testing, we found that:

- AP1 is a legitimate AP of Active mode in the state of Managed
- AP2 is Rogue AP
- AP3 is legitimate AP of Managed state Sentry mode
- Client2 through Rogue AP2 to access network.

In view of this situation, the Rogue AP Anti-attack function should be opened, AC Controller adds AP2 to Rogue AP attack list, and sent list to all the AP1 and AP3 through

WIDS-Configuration-Message. AP1 Radio will send solution of authentication message to Client2. AP3 Radio will pretend to be Client2 and sent solution of authentication message to AP2. In order to achieve the above anti-attack process need to configure AC Controller as follows:

```
AC>enable
AC#config
AC(config)#wireless
AC(config-wireless)#wids-security ap-de-auth-attack
```

When AP without threat, the network management need to change the Rogue status to its previous state:

```
AC(config-wireless)#wireless acknowledge-rogue 00-03-0f-01-02-03
AC(config-wireless)#no wids-security ap-de-auth-attack
```

4.4 Anti-attack Troubleshooting

When configure, use the anti-attack function, may be due to the physical connection, configuration errors, cause the anti-attack to unmoral operation or error anti-attack. Please check whether the reasons are as follows:

- Ensure the physical connection is correct.
- Confirm start anti-attack function
- Confirm has clear threat to Rogue AP whether restore the previous state

Chapter 5 User Isolation

5.1 Introduction to User Isolation

In the operation of the WLAN network, users are mutual distrust, so it is necessary to use the user isolation technology to prevent the user from attacking or trapping each other. At the same time, if user uses the LAN to access each other and send data will take up network resources as well and cause network congestion, so in some cases, it also must be use the user isolation to prohibit users mutually visit. Specific strategies are as follows:

⑴ By MAC internal control principle isolate the user visits. To ensure that user under the same AP cannot be second floor of the same, only connected to uplink port.

⑵ AP with MAC address access control or network aggregation equipment Layer 2 isolation between technology such as VLAN/of PVLAN/PVC isolation, to ensure that users can not communicate directly under different AP.

⑶ AC uses the same port isolation to isolate user. When the AC of the same port is a message input and output, the AC packet is discarded.

According to the AP's different ways of working, user isolation is divided into 2 categories: Centralized forwarding mode and Distributed forwarding mode.

1. Centralized forwarding mode

In Centralized forwarding mode, the AP-driven layer will not do any processing to 802.11 packet, and will only directly transfer it into the 802.3 encapsulated tunnel sent to AC to deal with. Therefore, the user isolation is all realized in AC. Here the main uses of the controller chip L2 Port Bridge function.

At normal circumstances, the controller look-up table in the second floor and find that the input port and output port are the same, will discard the message. But if you open the Port L2Port Bridge function, then allows the layer2 forwarding, and then sent back from the receiving port, each Port can configure L2 Port Bridge function separately, typical application is in the WLAN network, as shown in the figure below, the same AP to communicate with each other belong to the same VLAN Client, you must open the corresponding AC Port L2 Port Bridge function (as shown in the following picture):

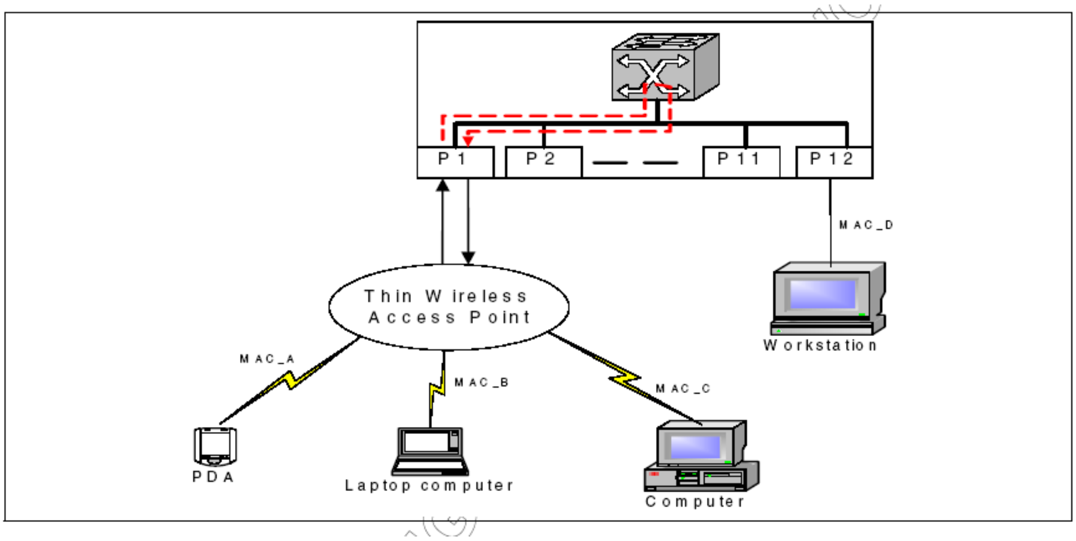


Fig 5-1 application of L2 Port Bridge function

Of course, if you turn off the L2 Port Bridge function, the AP under the same VLAN cannot affect the Layer3 forwarding between different VLAN, the look-up table after L3 forwarding packets sent from the receiving port. Therefore, the use of L2 Port Bridge function can isolate the wireless users under the same VLAN, and dose not affect the 3 layer between different VLAN.

According to user's different situation, centralized forwarding mode's user isolation can be divided into 4 circumstances as follows:

⑴ The same AP under different SSID users between two layers network isolation: Under normal circumstances, the same AP under different SSID users belongs to different VLAN, through the VLAN to undergo the isolation layer2 network.Otherwise, if the same AP under different SSID distribution of the same VLAN, the situation is equivalent to B.

⑵ The same AP under the same SSID user between 2 layer network isolation: The same AP under the same SSID user belonging to the same VLAN, under normal circumstances, it can be carried out 2 forwarding through AC layer, but must turn on the AC, the corresponding physical Port L2 Port Bridge function. If turned off L2 Port Bridge, the same AP under the same SSID cannot be exchanged.

⑶ Under different AP and different SSID users between 2 layers network isolation: In general, under different AP and different SSID between users belonging to the different VLAN. Through the VLAN isolation layer 2 network, same with A; if different APs under different SSID are assigned the same VLAN, it is equivalent to D.

⑷ Under different AP and same SSID user between 2 layer network isolation: Different AP under same SSID between a user may set different VLAN configuration, so you can use VLAN To isolate the 2 layer network; but in general, the VLAN setting is same, so you cannot use VLAN to isolate the 2 layer network, but due to the concentrated forward manner, AP must put data VP to AC to deal with, different AP and AC established VP is possible through the same physical port, may also be through different physical port access, so different AP under the same SSID, user layer 2 network isolation must be considered when the following 2 cases:

- If different AP and AC established the VP through the same physical port access, turn off the corresponding port L2 Port Bridge function of AC.
- If different AP and AC established the VP through different physical port access, you can open between different physical port layer2 isolation to isolate different physical port layer 2 network.

2. Distributed Forwarding Mode

In distributed forwarding mode, AP-driver layer needs to analysis the 802.11 data packet. If the destination address is the client under the same BSSID,then will forwarded directly, otherwise converted to 802.3 format and sent to the internal bridge to forwarding, then sent to the wired network, it is similar to the wired network. Therefore, the user isolation requires AP and connected wired network to complete. Among them, User isolation under the same AP is controlled by the AP. user isolation under different AP; AP connected to wired network control it.

According to use’s different situation, user isolation in distributed forwarding mode can be divided into 4 circumstances as follows:

⑴ The same AP under different SSID users between 2 layers network isolation: Under the normal circumstances, the same AP under different SSID users belong to different VLAN, through the VLAN isolation layer2 network interworking, If the same AP under different SSID distribution of the same WLAN, do not do isolation processing temporary.

⑵ The same AP under the same SSID between users’ 2 layers network isolation: the same AP under the same SSID between user 2 layer network isolation to achieve through internal bridge.

- When it is not open the user isolation, the same BSSID user access layer 2 messages driven at 802.11 layer forwarding.
- Open user isolation, that is, turn off the 802.11 driver layer forwarding function, the same BSSID user access layer 2 messages to 802.3 formats to AP internal bridge processing, by internal bridge to isolate the same between the same VLAN layer2 messages.

(3) Under different AP and different SSID users between 2 layers network isolation: In general, the user belongs between the different AP with different SSID's WLAN network through VLAN isolation the second floor of interoperability between them. Different AP under different SSID are assigned the same VLAN, it equivalent to D.

(4) Under different AP and same SSID user between 2 layer network isolation: Different AP under different SSID, user may set different VLAN configuration, it equivalent to C. But in general, the VLAN setting is same, so you cannot use VLAN to isolate the 2

layer network. You must use the AP connected to the AC port isolation layer2 network isolation. Relatively, the simple method is isolated all controller lower export only on the uplink sharing, but may not suitable for some application.

5.2 User Isolation Configuration

1. Enable/disable the layer 2 user isolation of the port which is appointed by AC

Command	Explanation
Wireless Global Mode	
l2tunnel station-isolation allowed vlan {WORD | add WORD | except WORD | remove WORD} **no l2tunnel station-isolation allowed vlan**	Enable user isolation status under centralized forwarding mode. The no command disables this isolation.

2. Configure the user isolation under the same VAP

Command	Explanation
Network Configuration Mode	
station-isolation **no station-isonation**	Configure to make the wireless users associated with the same VAP achieve the isolation. No command disables this function.

3. Configure the user isolation of all the VAP under the RADIO mode

Command	Explanation
Radio Configuration Mode	
station-isolation **no station-isonation**	Configure to enable the user isolation function for all the VAP under the radio mode. No command disables this function.

4. Configure the user isolation among different VAP under the same VLAN

Command	Explanation
Profile Configuration Mode	
station-isolation allowed vlan {[add | remove|] <vlan id>} **no station-isolation allowed vlan**	Configure the isolation among the VAP which belongs to the same VLAN under the AP. No

	command deletes the isolation VLAN and disables this function.

5.3 User Isolation Examples

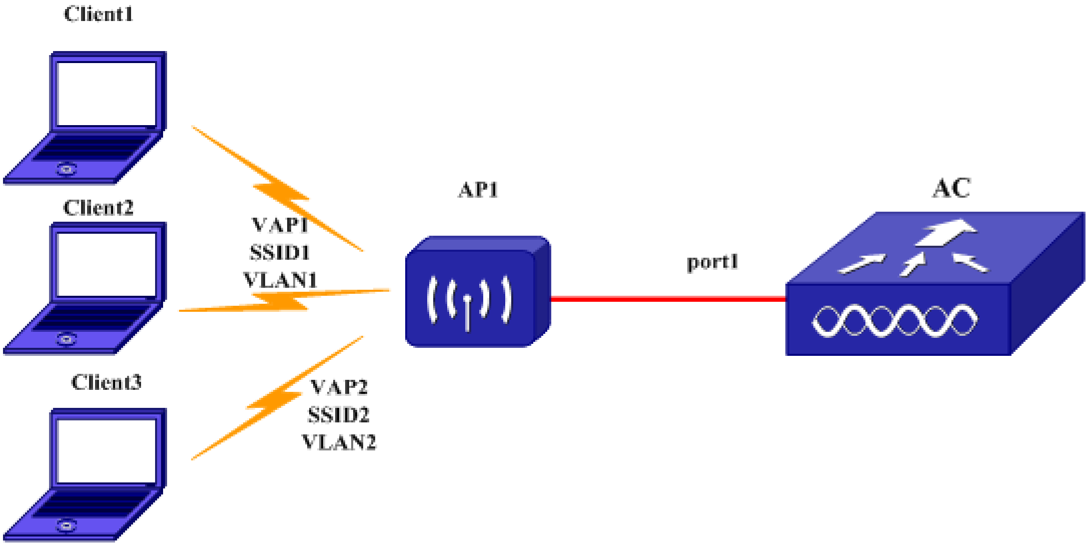


Fig 5-2 example of user isolation in centralized forwarding mode

As shown in the network, client1 and client2 access to AP1, both of them belong to VLAN1; Client3 access to AP1, but belongs to VLAN2; AP1 works in the centralized forwarding mode. Clinet1 and client3 do not belong to the same vlan, they are not interoperable. Client2 and client3 do not belong to the same vlan neither, they are not interoperable. Because Client1 and Client2 belong to VLAN1, both of them layer 2 is interoperable. If you want to isolation, you must turn off port1 L2 port bridge function of AC, the received package from Port1 will not be able to back to Port1, thereby isolating all Client layer 2 network under AP of AC access through the Port1. To achieve this purpose, you need to use the controller to specify the port layer 2 user isolation function and the corresponding configuration:

```
AC>enable
AC#config
AC(config)#wireless
AC(config-wireless)#l2tunnel station-isolation allowed vlan 1
```

5.4 User Isolation Troubleshooting

During configure and use the user isolation, may be due to the physical connection, configuration errors, cause the isolation failed to normal operation or error filtering. Please check whether the reasons are as follows:

- ☞ First, ensure that physical connection is correct.
- ☞ Second, confirm whether belonging to the same VLAN. If it does, in the case of centralized forwarding, please make sure that the controller is turned on the second floor of user isolation; in the case of using distributed forwarding, make sure whether open a user isolation of the AP.

Chapter 6 ARP Suppression and ARP Agency

6.1 Introduction to ARP Suppression and ARP Agency

ARP suppression and ARP agency in AP is a function of detecting DHCP packet, record address got by DHCP and the address mapping of IP and MAC of no roaming client. Through ARP broadcast to change into a unicast or a ARP agent, reduce the empty ARP broadcast reported message in order to save Client electricity.

The ARP suppression and ARP agency process is as follows:

1. DHCP

When enable ARP suppression function, for update IP information of Client, it needs to detect DHCP packet of local wireless users in AP, then get IP information of Client, and saved to local ARP table of related Client.

2. ARP suppression

ARP suppression (ARP broadcast switch to unicast): AP received ARP Request packet, use the destination IP query associated with the local Client ARP table, if it match, then put the purpose of the mac change the 0xffffffff into purpose of Client to Mac address, change the broadcast message to the unicast message, and sent to the destination Client. If it cannot be found, do nothing.

3. ARP agency

ARP Agent: DHCP makes the AP to safeguard access to the Client MAC and IP address mapping. When turned on the ARP agent, received ARP-Request, AP will safeguard the mac address of the table and return the ARP-Reply (here is the real Client address, not the filled AP mac address in the traditional agency) instead of forwarding the ARP-Request to Client. When open ARP suppression and ARP agency at the same time, AP deal with the ARP broadcasting packet in the form of ARP agency.

6.2 ARP Suppression and ARP Agency Configuration

1. ARP suppression configuration

Command	Explanation
Network Configuration Mode	

arp-suppression **no arp-suppression**	Enable/disable ARP suppression function on AP.

2. ARP agency configuration

Command	Explanation
Network Configuration Mode	
proxy-arp **no proxy-arp**	Enable/disable ARP agency function on AP.

6.3 ARP Suppression Examples

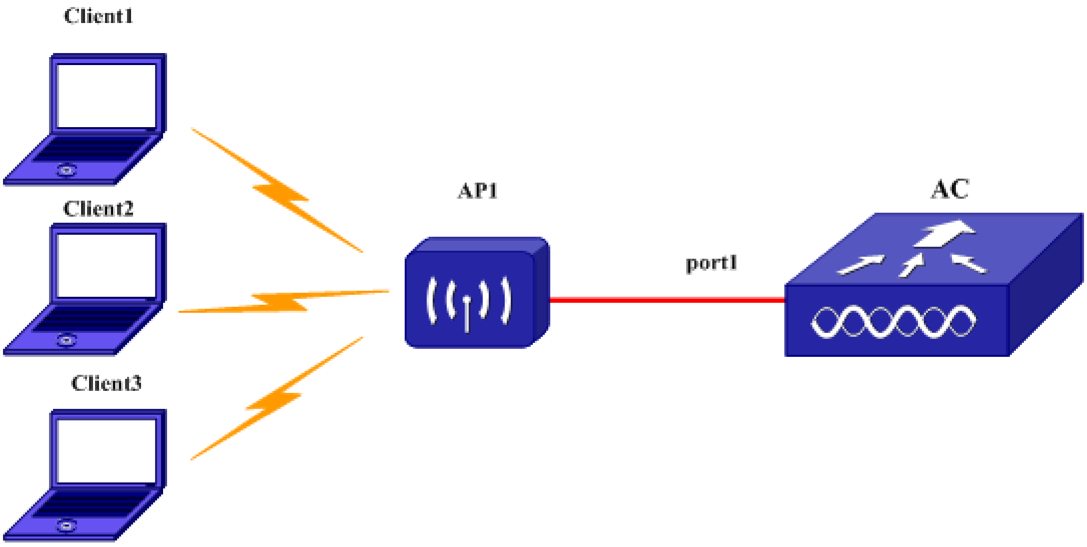


Fig 6-1 ARP agent

As shown in the network, Client1, Client2 and Client3 all access network through AP1. Now suppose Client1 wants to connect with Client3, but don't know the Client mac address. Client1 will send ARP Request signal to all customers in the form of broadcasting, such a serious impact on the efficiency of network communications. If AP1 opens the ARP suppression the corresponding auto-enable the ARP broadcast-to-unicast, DHCP frame detection, AP1 will record all the Authenticated Client IP and Mac mapping table (Client1, 2 and 3), after AP1 received ARP request signal, using destination IP to check local related ARP table of Client and change destination mac from 0xffffffff to Client3 mac address, changing broadcast packet to unicast packet to send to Client3.In order to achieve this purpose, you need to use ARP agent function and corresponding configuration:

```
AC>enable
AC#config
```

```
AC(config)# wireless
AC(config-wireless)#network 1
AC(config-network)# arp-suppression
```

If open the ARP suppression mode as ARP agent at the same time, the AP1 received the Client1 of ARP the request signal, the AP will return the napping table Client3 mac address to the ARP-Reply, without broadcasting ARP-Request to all Client. In order to achieve this purpose, you need to use ARP agent function and corresponding configuration:

```
AC>enable
AC#config
AC(config)# wireless
AC(config-wireless)#network 1
AC(config-network)# proxy-arp
```

6.4 ARP Suppression and ARP agency Troubleshooting

When configure, use ARP suppression and ARP agency, may be due to the physical connection, configuration errors cause the isolation failed to normal operation, Please check whether the reasons are as follows:

- ☞ First, ensure the physical connection is correct.
- ☞ Second, ensure whether Client belongs to IPv4 Client.
- ☞ Then, ensure whether AP is working on WDS mode.
- ☞ Last, confirm open ARP suppression or ARP agency.

Chapter 7 Dynamic Blacklist

7.1 Overview of Dynamic Blacklist

Dynamic Blacklist belongs to anti-DOS attacks of wireless security module. Dynamic blacklist includes the MAC address of the terminal device of frame which will be dropped. AP uses this list, drops the data frames sent by the terminal device in this list. When the flooding packets sent by the terminal device are detected exceeding the security threshold, add the terminal device into the dynamic blacklist.

In wireless security function, when add a new wireless terminal record, it should check whether it conforms the condition. When enabled dynamic blacklist function, if it conforms the condition, add the MAC address of wireless terminal and the type of flooding attack into dynamic blacklist. After a new record is added successfully in dynamic blacklist, inquire the AP IP address that the wireless terminal with the MAC address belongs to (if inquire successfully, it means that this wireless terminal has been online), issue the disconnection command with this wireless terminal to this IP address; for the wireless terminal which is not connected to AP, authentication module will inquire the dynamic blacklist when the terminal requests for connection; check if the MAC address of this wireless terminal is in this blacklist, if inquire successfully, refuse the authentication requisition from this wireless terminal.

This list includes the MAC address of the terminal device dropped. When the flooding packets sent by the terminal device are detected and it causes the network congestion, add it into the dynamic blacklist through WIDS.

The flooding attacks which conform to be added into dynamic blacklist include:

(1) Configured Authentication Rate Test

(2) Configured Probe Request Rate Test

(3) Configured De-Authentication Requests Rate Test

(4) Maximum Authentication Failures Test

After enabled dynamic blacklist function, AC will add the MAC addresses of Rogue devices which conform the above conditions into the dynamic blacklist to configure the aging time of the table entry (this time can be configured). After it is time to aging time, delete this table entry.

There are 128 table entries in dynamic blacklist at most, when there is not free table entry, it will not be added into the dynamic blacklist.

7.2 Dynamic Blacklist Configuration

1. Dynamic Blacklist Configuration

Command	Explanation
Wireless Config	
dynamic-blacklist **no dynamic-blacklist**	Enable/disable dynamic blacklist function.

2. Configure the aging time of dynamic blacklist

Command	Explanation
Wireless Config	
dynamic-blacklist lifetime <60-3600> **no dynamic-blacklist lifetime**	Configure the aging time of dynamic blacklist; the no command recovers to be default of 300s.

3. Clear the wireless terminal configuration in dynamic blacklist manually

Command	Explanation
Privileged EXEC	
clear dynamic-blacklist (FF-FF-FF-FF-FF-FF|)	Clear the wireless terminal MAC address record in dynamic blacklist manually. If the MAC is not appointed, clear the MAC address records of all wireless terminal.

4. Relevant showing configuration

Command	Explanation
Admin Mode	
show wireless dynamic-blacklist	Show the wireless terminal record in dynamic blacklist.

7.3 Dynamic Blacklist Examples

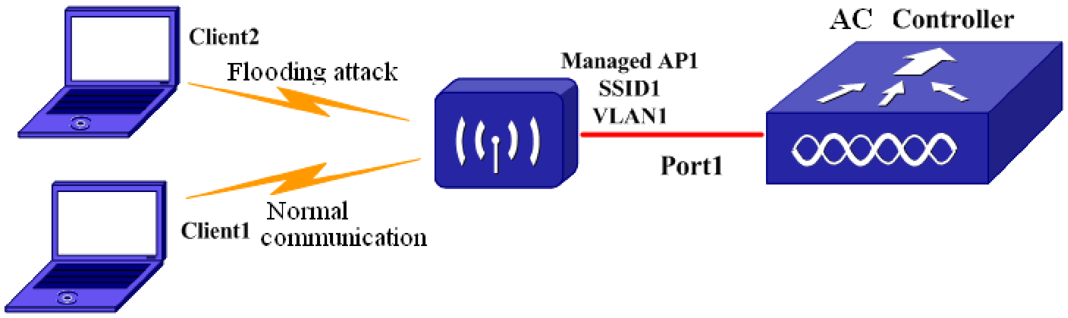


Fig 7-1 case of dynamic blacklist

As shown in the above picture, client1 and client2 connect to wireless network through AP1. Client1 communicates normally; client2 sends the flooding attack packets of authentication requisition frame and sends authentication requisition to AP1 constantly. If user wants to add the client which sent the flooding attack frame into dynamic blacklist, should configure for AC Controller:

Enable anti-flooding attack detection first:

```
AC > enable
AC # config
AC (config)# wireless
AC (config-wireless)# no wids-security client threshold-interval-auth
AC (config-wireless)# wids-security client threshold-value-auth 6000
AC (config-wireless)# wids-security client configured-auth-rate
```

Second, enable dynamic blacklist function and local MAC authentication function:

```
AC(config-wireless)#dynamic-blacklist
AC(config-wireless)#dynamic-blacklist lifetime 600
AC(config-wireless)#network 100
AC(config-network)#mac authentication local
```

7.4 Dynamic Blacklist Troubleshooting

When using or configuring dynamic blacklist, the dynamic blacklist maybe run abnormally because of physical connection, wrong configuration or other reasons. The explanation is as below:

Dynamic blacklist runs abnormally:

Ensure the physical connection is correct first;

Second, ensure that the treat detection conformed dynamic blacklist conditions has been enabled (the relevant configuration is as above);

Thirdly, ensure the dynamic blacklist has been enabled and the MAC local authentication under network has been configured (the relevant configuration is as above).

There are wrong records of dynamic blacklist:

Ensure whether the maximum times of Configured Authentication Rate Test, Configured Probe Request Rate Test, Configured De-Authentication Requests Rate Test and Maximum Authentication Failures Test are suitable and whether the relevant devices are all detected as rogue.

Whether the dynamic blacklist records of the relevant devices exceeds the keep-alive time.

Chapter 8 Wireless SAVI

8.1 Introduction to Wireless SAVI

SAVI means Source Address Validation Improvement. The achieved SAVI in the wired environment is named as wired SAVI, and the achieved SAVI in the wireless environment is named as wireless SAVI. In this manual, we will introduce the wireless SAVI. The fundamental between the wired and wireless SAVI is same which means to create the SAVI entries on the access device and filter the terminal IP packets according to the SAVI entries, only the IP packet which matches the conditions can pass through.

The main purpose of SAVI is to verify the effectiveness of the source MAC and source IP of the STA IPv4/IPv6 packets. For this purpose, the wireless SAVI will make the AP (access point) monitor the process that the terminal uses the DHCP/DHCPv6 to get the address and the IPv6 DAD NS/NA packets that the terminal sends. Two elements entries of STA MAC and IP will be created on the AP and AC through monitoring these packets. And the terminal IP packets will be filtered according to the two elements entries. The IP packets which match the conditions will pass through, the packets which do not match the conditions will be dropped.

Another purpose of SAVI is to prevent the terminal configuring the IP addresses privately. The wireless SAVI always prevent the terminal configuring the IPv4 addresses privately; it can be selective to prevent the terminal configuring the IPv6 addresses privately. For this purpose, the wireless SAVI will make the AP select if monitor the IPv6 DAD NS/NA that the terminal sends for creating the two elements entries of STA MAC and IP.

The wireless SAVI function can also allows the network administrator configuring the static SAVI entry for occupying the terminal with one IP address in a long time. This kind of terminals can use the configured static IP address to access the network.

8.2 Wireless SAVI Configuration

Wireless SAVI configuration task list is as below:

1. Configure the lifetime of the SLAAC dynamic binding
2. Configure the binding-limit number corresponding to the same MAC address on AP
3. Configure to create the SAVI binding-limit capacity on AP
4. Configure to prevent the STA configuring IPv6 address privately
5. Configure the static SAVI entries
6. Enable the SAVI function under the AP profile config mode

7. Apply the AP profile and issue the configuration to the corresponding AP

1. Configure the lifetime of the SLAAC dynamic binding

Command	Explanation
Wireless Config Mode	
savi ipv6-nd lifetime <1-31536000> **no savi ipv6-nd lifetime**	Configure the lifetime of the SAVI SLAAC static binding under the BOUND status. The no command recovers to be the default value. The range of the lifetime is 1-31536000 (365 days) and the default is 4 hours (14400 seconds).

2. Configure the binding-limit number corresponding to the same MAC address on AP

Command	Explanation
AP profile Config Mode	
savi dyn-mac-binding-limit<*8-16*> **no savi dyn-mac-binding-limit**	Configure the binding-limit number corresponding to the same MAC address on AP. The no command recovers to be the default. The default maximum value is 8 and the range is 8-16 (the static entry is not included).

3. Configure to create the SAVI binding-limit capacity on AP

Command	Explanation
AP profile Config Mode	
savi binding-limit <*0-320*> **no savi binding-limit**	Configure to create the SAVI binding-limit capacity on AP. The no command recovers the configuration to be default. The default value is 240 and the range is 0-320 (the static entry is not included).

4. Configure to prevent the STA configuring IPv6 address privately

Command	Explanation
AP profile Config Mode	
savi ipv6-slaac enable **no savi ipv6-slaac enable**	Disable the IPv6 address configuration prevention function. The no command enables it.

5. Configure the static SAVI entries

Command	Explanation
Wireless Config Mode	
savi binding <*client-mac*> <ipv4|ipv6> <*client-ip*> **no savi binding <ipv4|ipv6> <*client-ip*>**	Use this command to create the SAVI static binding entry. The type of the entry is STATIC. The no command deletes the entry. The MAC address of STA does not need to be appointed when deleted.

6. Enable the SAVI function under the AP profile config mode

Command	Explanation
AP profile Config Mode	
savi enable **no savi enable**	Enable the SAVI controlling function of the managed AP under the ap profile for testing the source address of the IP packet effectively. The no command disables the SAVI controlling function.

7. Apply the AP profile and issue the configuration to the corresponding AP

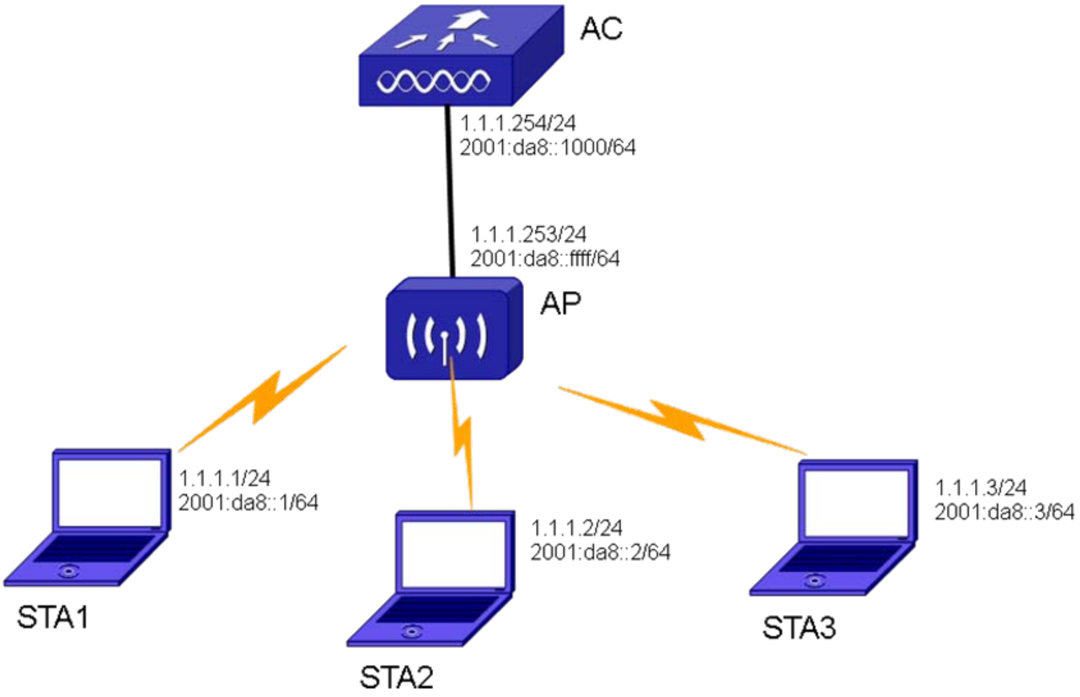
Command	Explanation
Admin Mode	
wireless ap profile apply	When enable/disable the SAVI function, the configuration should be issued manually to be effective. When the SAVI function is enabled, the configuration of modifying **savi ipv6-nd lifetime <1-31536000>** will be issued to AP automatically; when the SAVI function is disabled, the configuration will not be issued to AP automatically. The configuration of modifying other parameters will be issued automatically no matter the SAVI function is enabled or disabled. It does not need to be issued manually.

8.3 Wireless SAVI Examples

Case 1:

Test the effectiveness of the source address of the STA IP packets.

AC uses ap profile 1 to manage the AP, enable the SAVI function on profile 1 and issue the configuration.



(1) AC configuration is as below:

```
Wireless
Ap profile 1
Savi enable
Exit
Exit
Exit
Wireless ap profile apply 1
```

Sta1 is associated with AP, gets the IPv4 address of 1.1.1.1 and the IPv6 address of 2001:da8::1.

Sta2 is associated with AP, gets the IPv4 address of 1.1.1.2 and the IPv6 address of 2001:da8::2.

Sta3 is associated with AP, gets the IPv4 address of 1.1.1.3 and the IPv6 address of 2001:da8::3.

Sta1 can ping 1.1.1.2, 1.1.1.3, 2001:da8::2 and 2001:da8::3.

sta1 uses the sending packets software to send the IP data flow whose source mac is sta1-mac, source IP is 1.1.1.2, destination mac is sta3-mac and destination IP is 1.1.1.3. This flow cannot be gotten on sta3.

sta1 uses the sending packets software to send the IP data flow whose source mac is sta1-mac, source IP is 2001:da8::2, destination mac is sta3-mac and destination IP is 2001:da8::3. This flow cannot be gotten on sta3.

(2) Retry the above configuration on AC after disabled the wireless SAVI function.

AC configuration is as below:

```
Wireless
Ap profile 1
No savi enable
Exit
Exit
Exit
Wireless ap profile apply 1
```

Sta1 is associated with AP, gets the IPv4 address of 1.1.1.1 and the IPv6 address of 2001:da8::1.

Sta2 is associated with AP, gets the IPv4 address of 1.1.1.2 and the IPv6 address of 2001:da8::2.

Sta3 is associated with AP, gets the IPv4 address of 1.1.1.3 and the IPv6 address of 2001:da8::3.

Sta1 can ping 1.1.1.2, 1.1.1.3, 2001:da8::2 and 2001:da8::3.

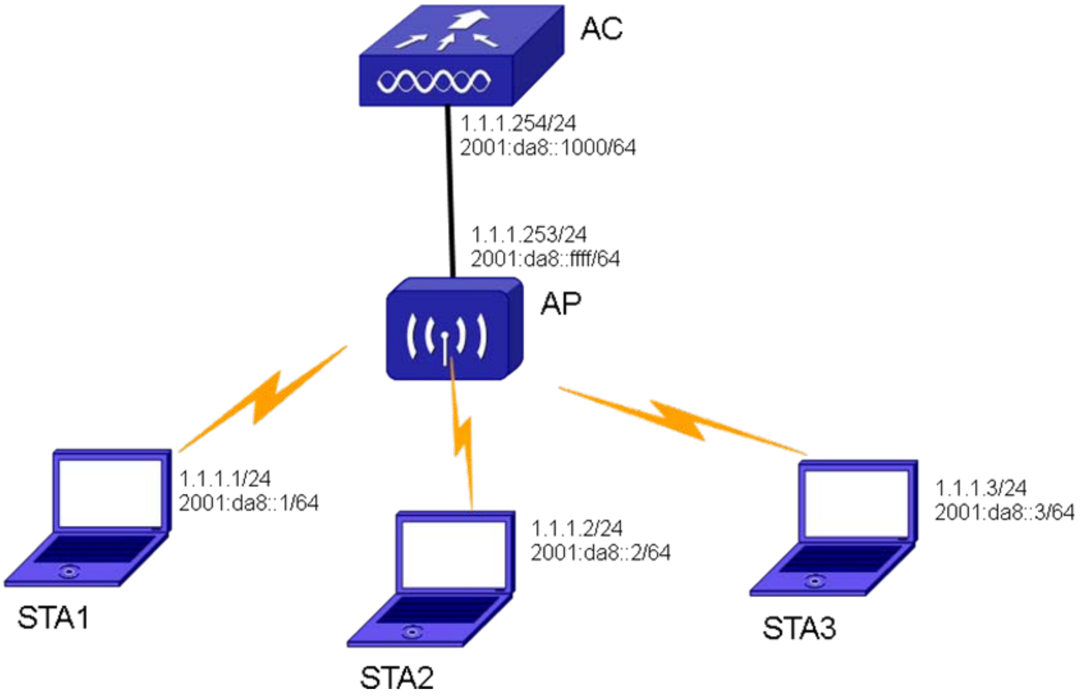
sta1 uses the sending packets software to send the IP data flow whose source mac is sta1-mac, source IP is 1.1.1.2, destination mac is sta3-mac and destination IP is 1.1.1.3. This flow can be gotten on sta3.

sta1 uses the sending packets software to send the IP data flow whose source mac is sta1-mac, source IP is 2001:da8::2, destination mac is sta3-mac and destination IP is 2001:da8::3. This flow can be gotten on sta3.

Case 2:

Prevent the STA configuring the IP address privately.

AC uses ap profile 1 to manage the AP, enable the SAVI function on profile 1 and issue the configuration.



(1) AC configuration is as below:

```
Wireless
Ap profile 1
Savi enable
No savi ipv6-slaac enable
Exit
Exit
Exit
Wireless ap profile appy 1
```

Sta1 configures the static IPv4 address as 1.1.1.1 and the static IPv6 address as 2001:da8::1. It is associated with the AP.

Sta2 is associated with AP, gets the IPv4 address of 1.1.1.2 and the IPv6 address of 2001:da8::2.

Sta3 is associated with AP, gets the IPv4 address of 1.1.1.3 and the IPv6 address of 2001:da8::3.

Sta1 cannot ping 1.1.1.2, 1.1.1.3, 2001:da8::2 and 2001:da8::3.

(3) Retry the above configuration on AC after disabled the function of preventing the IPv6 address configuration.

```
Wireless
Ap profile 1
```

```
savi ipv6-slaac enable
exit
exit
exit
wireless ap profile apply 1
```

Sta1 configures the static IPv4 address as 1.1.1.1 and the static IPv6 address as 2001:da8::1. It is associated with the AP.

Sta2 is associated with AP, gets the IPv4 address of 1.1.1.2 and the IPv6 address of 2001:da8::2.

Sta3 is associated with AP, gets the IPv4 address of 1.1.1.3 and the IPv6 address of 2001:da8::3.

Sta1 cannot ping 1.1.1.2 and 1.1.1.3, but it can ping 2001:da8::2 and 2001:da8::3.

8.4 Wireless SAVI Troubleshooting

If there are problems when using the wireless SAVI function, please check if they are caused by the following reasons:

- The wireless SAVI is enabled with the ap profile as the unit, so please ensure that the SAVI is enabled under the correct ap profile first.
- If the IPv6 address cannot be used to access the network after the STA is associated with the network, please ensure that the IPv6 address configuration prevention function is disabled. Use the command of **ipv6-slaac enable** to disable the IPv6 address configuration prevention function.
- If the IPv6 address cannot be used to access the the network for 4 hours after the STA is associated with the network, please adjust the lifetime of the SLAAC SAVI binding, the corresponding command is **savi ipv6-nd lifetime <1-31536000>**.
- If the ip address cannot be gotten through dhcp afte the STA is associated with the network, please find out if the associated AP has achieved the top limit of the SAVI binding entries capacity. When achieved the top limit, the new dynamic binding cannot be created, user can use the command of savi binding-limit <0-320> to configure the larger value for meeting the requirement.

Chapter 9 DHCP Suppression

9.1 Introduction to DHCP Suppression

According to FLAGS field in DHCP packet, DHCP suppression in AP through DHCP OFFER/ACK packet broadcast to change into a unicast, reduce the empty ARP broadcast reported message in order to save Client electricity.

The DHCP suppression process is as follows:

1. **DHCP**

When enable DHCP suppression function, it needs to detect DHCP packet of local wireless users in AP, then get FLAGS information of DHCP packet.

2. **DHCP suppression method**

DHCP broadcast switch to unicast: AP received DHCP Discover/Request packet, according to FLAGS field in DHCP packet, if FLAGS in packet is 0, put the purpose of the mac change the 0xffffffff into purpose of Client to Mac address, change the broadcast message to the unicast message, and sent to the destination Client. If FLAGS in packet is 1, do nothing.

9.2 DHCP Suppression Configuration

1. DHCP suppression configuration

Command	Explanation
Network configuration mode	
dhcp-suppression **no dhcp-suppression**	Enable/disable DHCP suppression function on AP.

9.3 DHCP Suppression Example

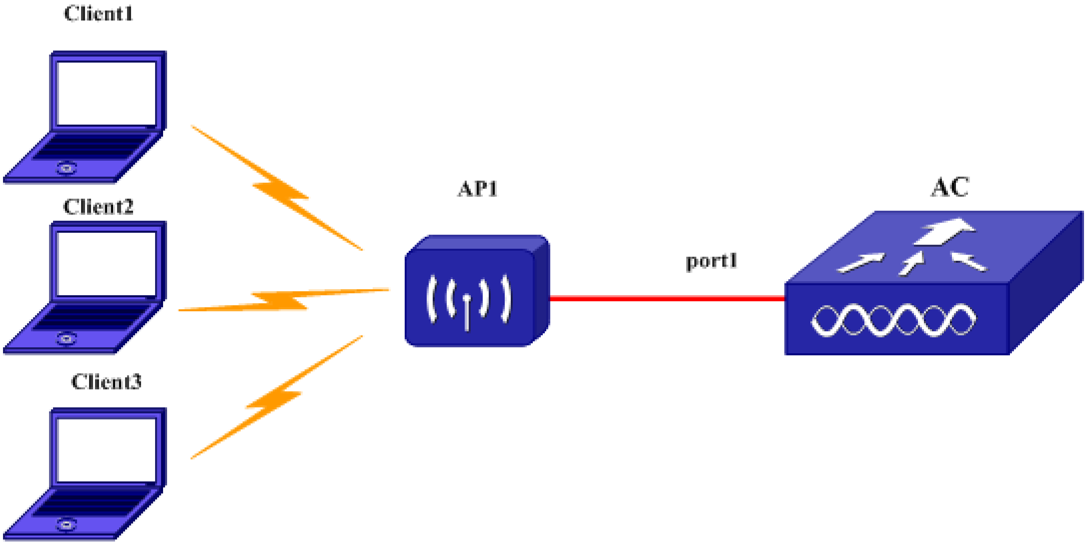


Fig 9-1 DHCP agency

As shown in the network, Client1, Client2 and Client3 all access network through AP1. Now suppose Client1 get address through DHCP, Client1 will send DHCP discover/Request signal to all devices in the form of broadcasting, when DHCP server receive DHCP discover/request packet, it will return packet to all network in the form of broadcasting.If AP1 opens the DHCP suppression, AP1 will inspect FLAGS in DHCP discover/request packet, if FLAGS is 0, AP1 will send DHCP OFFER/ACK packet to Client1 after broadcast-to-unicast, and no longer sending DHCP packet to all Client in the form of broadcasting.

In order to achieve this purpose, you need to use DHCP agent function and corresponding configuration:

```
AC>enable
AC#config
AC(config)# wireless
AC(config-wireless)#network 1
AC(config-network)# dhcp-suppression
```

9.4 DHCP Suppression Troubleshooting

When configure, use DHCP suppression, may be due to the physical connection, configuration errors cause the isolation failed to normal operation, Please check whether the reasons are as follows:

- ☞ First, ensure the physical connection is correct.
- ☞ Second, ensure whether Client get address through IPv4.

☞ Then, ensure whether AP is working on WDS mode.

☞ Last, confirm open DHCP suppression.