Content

Chapter 1 Commands for AP Threat Detection

1.1 debug wireless wids internal-info

Command: debug wireless wids internal-info

no debug wireless wids internal-info

Function: Enable the debug information of the WIDS threat detection, the no command will disable the information.

Parameter: None.

Default: None.

Command Mode: Admin mode.

Usage Guide: Use this command to check the debug information of the WIDS threat detection function when you need. The information includes AP MAC of sending RF Scan Report, AP MAC and VAP MAC of threat detection, the result of the detection steps, printing the received Neighor AP Info & Neighor AP Info Part2 of RF Scan Report Message.

Example: Enable the debug information of the WIDS threat detection.

AC#debug wireless wids internal-info

1.2 show wireless ap rf-scan rogue-classification

Command: show wireless ap <*macaddr*> rf-scan rogue-classification

Function: Show the threat detection log summary information of the appointed AP.

Parameter: <*macaddr*> Rogue AP MACaddress.

Default: None.

Command Mode: Admin mode.

Usage Guide: Use this command to show the threat detection log summary information of AP.

Example: MAC address as 00-03-0f-01-02-03, show the threat detection log summary information of AP.

AC #show wireless ap 00-03-0f-01-02-03 rf-scan rogue-classification

Test ID	Cond Detect	MAC Addr (radio)	Test Config	Test Result	Time Since 1st Report	Time Since Last Report

WIDSAPROGUE01 False 00-00-00-00-00-00(0) Enable 0d:00:00:00 0d:00:00:00
WIDSAPROGUE02 True 00-03-0f-01-02-03(1) Enable Rogue 0d:08:18:41 0d:00:29:18
WIDSAPROGUE03 False 00-00-00-00-00-00(0) Enable 0d:00:00:00 0d:00:00:00
WIDSAPROGUE04 False 00-00-00-00-00-00(0) Enable 0d:00:00:00 0d:00:00:00
WIDSAPROGUE05 False 00-00-00-00-00-00(0) Enable 0d:00:00:00 0d:00:00:00
WIDSAPROGUE06 False 00-00-00-00-00-00(0) Enable 0d:00:00:00 0d:00:00:00
WIDSAPROGUE07 False 00-00-00-00-00-00(0) Enable 0d:00:00:00 0d:00:00:00
WIDSAPROGUE08 False 00-00-00-00-00-00(0) Enable 0d:00:00:00 0d:00:00:00
WIDSAPROGUE09 False 00-00-00-00-00-00(0) Enable 0d:00:00:00 0d:00:00:00
WIDSAPROGUE10 False 00-00-00-00-00-00(0) Enable 0d:00:00:00 0d:00:00:00
WIDSAPROGUE11 False 00-00-00-00-00-00(0) Enable 0d:00:00:00 0d:00:00:00

WIDSAPROGUE01..... Administrator configured rogue AP
WIDSAPROGUE02..... Managed SSID from an unknown AP
WIDSAPROGUE03..... Managed SSID from a fake managed AP
WIDSAPROGUE04..... AP without an SSID
WIDSAPROGUE05..... Fake managed AP on an invalid channel
WIDSAPROGUE06..... Managed SSID detected with incorrect security
WIDSAPROGUE07..... Invalid SSID from a managed AP
WIDSAPROGUE08..... AP is operating on an illegal channel
WIDSAPROGUE09..... Standalone AP with unexpected configuration
WIDSAPROGUE10..... Unexpected WDS device detected on network
WIDSAPROGUE11..... Unmanaged AP detected on wired network

Table 1-1 description of the AP threat detection log summary information

Parameter name	Explain
Test ID	Number of 11 kinds of AP rogue-detection (WIDSAPROGUE11)
Cond Detect	whether detected a threat occurrence
MAC Addr(radio)	MAC address this RF scanning AP (radio serial)
Test Config	Whether enable the threat detection(Enable&Disable)
Test Result	The equipment whether illegal
Time Since 1st Report	The first time of this case
Time Since Last Report	The last found of this case

1.3 show wireless wids-security

Command: show wireless wids-security

Function: Show the configured AP threat detection parameters.

Parameter: None.

Default: None.

Command Mode: Admin mode.

Usage Guide: Show the configured AP threat detection detailed parameters, including: the detection whether enabled, the shortest waiting time of each round detection, and other parameters.

Example: Show the configured AP rogue-detection parameters.

AC#show wireless wids-security

Rogue - admin configured Rogue AP's..... Enable
Rogue - AP's on an illegal channel..... Enable
Rogue - fake managed AP / invalid channel..... Enable
Rogue - fake managed AP / no SSID..... Enable
Rogue - managed AP / invalid SSID..... Enable
Rogue - managed SSID / invalid security..... Enable
Rogue - standalone AP / unexpected config..... Enable
Rogue - unknown AP / managed SSID..... Enable
Rogue - fake managed AP / managed SSID..... Enable
Rogue - unmanaged AP on a wired network..... Enable
Rogue - unexpected WDS devices..... Enable
OUI Database mode..... Local
Rogue detected trap interval..... 60 seconds
Wired network detection interval..... 60 seconds
AP De-Authentication Attack..... Disable

Table 1-2 description of the AP threat detection parameters

Parameter name	Explain
Rogue detected trap interval	The interval of detect the Rogue AP whether existing
Wired network detection interval	The interval of detect unmanaged AP connecting to wired network

1.4 show wireless wids-security rogue-test-descriptions

Command: show wireless wids-security rogue-test-descriptions

Function: Show the explanation of AP threat detection.

Parameter: None.

Default: None.

Command Mode: Admin mode.

Usage Guide: Show the explanation of AP threat detection.

Example: Show the explanation of AP threat detection.

AC#show wireless wids-security rogue-test-descriptions

WIDSAPROGUE01..... Administrator configured rogue AP
WIDSAPROGUE02..... Managed SSID from an unknown AP
WIDSAPROGUE03..... Managed SSID from a fake managed AP
WIDSAPROGUE04..... AP without an SSID
WIDSAPROGUE05..... Fake managed AP on an invalid channel
WIDSAPROGUE06..... Managed SSID detected with incorrect security
WIDSAPROGUE07..... Invalid SSID from a managed AP
WIDSAPROGUE08..... AP is operating on an illegal channel
WIDSAPROGUE09..... Standalone AP with unexpected configuration
WIDSAPROGUE10..... Unexpected WDS device detected on network
WIDSAPROGUE11..... Unmanaged AP detected on wired network

1.5 trapflags rogue-ap

Command: trapflags rogue-ap

no trapflags rogue-ap

Function: Enable the detection of illegal AP trap, if it detects illegal AP, the AC will immediately send the trap; the no Command disables this function.

Parameter: None.

Default: Disable the function.

Command Mode: Wireless global configuration mode.

Usage Guide: Illegal AP Trap can be detected by this Command: AC Controller runs AP risk detection, if the threat is detected, put the AP as the Rogue, and send Trap to notify network administrator.

Example: Enable the detection of illegal AP trap.

AC(config-wireless)# trapflags rogue-ap

1.6 wired-detection-vlan

Command: wired-detection-vlan <0-4094>

no wired-detection-vlan

Function: Set VLAN ID of the detection packet of unmanaged AP access to wired network, this no command will restore the default VLAN ID value of 1.

Parameter: *<0-4094>* VLAN ID, range is 0~4094, 0 means the test frame is without tag.

Default: 1.

Command Mode: AP Profile configuration mode.

Usage Guide: Unmanaged AP connects to the wired network detection, AP which is in sentry mode monitors the radio in full-time, every 1 second to switch to the new channel to monitor, if enabled the detection function, after switching to the new channel, send multicast frames address with mac address of 01-02-BC-00-12-00 to the wired network. the VLAN ID of Multicast frames tag is the configuration value in this command, if configured as 0, multicast frames with no VLAN flags. If this command is not configured, the multicast frame tag VLAN ID is 1.

Example: Set the VLAN ID as VLAN 2 of detection package of unmanaged AP access to wired network.

AC(config-wireless)#ap profile 1

AC(config-ap-profile)#wired-detection-vlan 2

AC(config- ap-profile)#no wired-detection-vlan

1.7 wids-security admin-config-rogue

Command: wids-security admin-config-rogue

Function: Enable the illegal AP detection configured by network administrator.

Parameter: None.

Default: Enable this function.

Command Mode: Wireless global configuration mode.

Usage Guide: The network administrator can set the authentication in Valid-AP database of local or Radius server, administrator can manually configure the three states of AP: managed, Standalone and Rogue. The illegal AP administrator configured is the rogue AP of Valid-AP database of local or Valid Radius server. use this command to enable this detection to detect the Rogue AP.

Example: Enable the illegal AP detection configured by network administrator.

AC(config-wireless)#wids-security admin-config-rogue

1.8 wids-security ap-chan-illegal

Command: wids-security ap-chan-illegal

no wids-security ap-chan-illegal

Function: Enable the illegal channel detection of AP, the no command will disable this function.

Parameter: None.

Default: Enable the illegal channel detection.

Command Mode: Wireless global configuration mode.

Usage Guide: Different counties have different prescripts for radio resources, so the lawful channel in one county may be illegal in another county, if the AP worked in the illegal channel, use this command to detect this rogue AP.

Example: Enable the illegal channel detection.

AC(config-wireless)# wids-security ap-chan-illegal

1.9 wids-security fakeman-ap-chan-invalid

Command: wids-security fakeman-ap-chan-invalid

no wids-security fakeman-ap-chan-invalid

Function: Enable the Beacon frame detection of received Managed AP in the wrong channel, the no command will disable this detection.

Parameter: None.

Default: Enable Beacon frame detection.

Command Mode: Wireless global configuration mode.

Usage Guide: The Managed AP channels are distributed by the AC, so the AC know which channel the Managed AP should work in, the hacker will fake managed AP MAC, but the channel used to send beacon frames may be in the wrong channel. Use this Command to detect such rogue AP.

Example: Enable the Beacon frame detection receiving managed AP in the wrong channel.

AC(config-wireless)# wids-security fakeman-ap-chan-invalid

1.10 wids-security fakeman-ap-managed-ssid

Command: wids-security fakeman-ap-managed-ssid

no wids-security fakeman-ap-managed-ssid

Function: Enable the illegal Vendor field detection in Beacon frames, the no command will disable this function.

Parameter: None.

Default: Enable the Vendor field illegal detected.

Command Mode: Wireless global configuration mode.

Usage Guide: Some hackers poses as the managed AP's MAC and send managed SSID, vendor field is must carried in the beacon frame of managed AP of this product, so by detecting vendor field, the Rogue AP of the managed AP MAC address can be detected (if there is no vendor field, the AP MAC Address will be 00:00:00:xx:xx:xx in Neighbor AP Info of RF the Scan Report Message). Use this Command to enable this function.

Example: Enable the illegal Vendor field detection in Beacon frames.

AC(config-wireless)#wids-security fakeman-ap-managed-ssid

1.11 wids-security fakeman-ap-no-ssid

Command: wids-security fakeman-ap-no-ssid

no wids-security fakeman-ap-no-ssid

Function: Enable detection of no SSID field in the Beacon frame, the no Command will disable this detection.

Parameter: None.

Default: Enable detection of no SSID field in the Beacon frame.

Command Mode: Wireless global configuration mode.

Usage Guide: In order to avoid being detected, the hacker may not contain the SSID field in benacon frames, but it can still send the probe response frame to the Client sent probe request to deceive the client to access in order to obtain security information. Use this Command to detect such rogue AP.

Example: Enable detection of no SSID field in the Beacon frame.

AC(config-wireless)#wids-security fakeman-ap-no-ssid

1.12 wids-security managed-ap-ssid-invalid

Command: wids-security managed-ap-ssid-invalid

no wids-security managed-ap-ssid-invalid

Function: Enable invalid SSID detection of managed AP, this no Command will disable the detection.

Parameter: None.

Default: Enable invalid SSID detection of managed AP.

Command Mode: Wireless global configuration mode.

Usage Guide: The AP which detects managed AP will send the RF Scan Report Message to the AC controller if the managed AP sends invalid SSID, the information will include

illegal SSID. Use this Command to detect the invalid SSID, and determine as the rogue AP.

Example:

AC(config-wireless)# wids-security managed-ap-ssid-invalid

1.13 wids-security managed-ssid-secu-bad

Command: wids-security managed-ssid-secu-bad

no wids-security managed-ssid-secu-bad

Function: Enable the detection that AP has used a wrong security authentication method, the no command will disable this detection.

Parameter: None.

Default: Enable the detection that AP has used a wrong security authentication method.

Command Mode: Wireless global configuration mode.

Usage Guide: Security authentication method (open, WEP, WPA) of AP in the beacon frame, AC Controller also record AP configuration. This command is used to detect whether the two security authentication methods are consistent, to detect this rogue AP.

Example: Enable the detection that AP has used a wrong security authentication method.

AC(config-wireless)# wids-security managed-ssid-secu-bad

1.14 wids-security rogue-det-trap-interval

Command: wids-security rogue-det-trap-interval <*60-3600*>

no wids-security rogue-det-trap-interval

Function: Set the time interval of detecting rogue AP. The no command will restore the default value.

Parameter: <*60-3600*> time interval, unit is second.

Default: 300s.

Command Mode: Wireless global configuration mode.

Usage Guide: Configure that system checks whether there is a rogue AP every regular interval, if there is, AC controller will send “wsRoguesPresent” Trap to remind the users there is current existing rogue AP. This command is used to configure the time interval.

Example: Set the interval of detection for rogue AP as 1000s.

AC(config-wireless)#wids-security client rogue-det-trap-interval 1000

1.15 wids-security standalone-cfg-invalid

Command: wids-security standalone-cfg-invalid

no wids-security standalone-cfg-invalid

Function: Enable the error detection of the lawful fat AP configuration, the no command will disable this detection.

Parameter: None.

Default: Enable the error detection of the legislation standalone AP configuration.

Command Mode: Wireless global configuration mode.

Usage Guide: If the AP is in standalone state, and the scanned AP configuration (working channel, SSID, security authentication mode, WDS mode, and whether access to the wired network) is detected different to the AC Controller, use this command to detect this rogue AP.

Example: Enable the error detection of the lawful fat AP configuration.

AC(config-wireless)# wids-security standalone-cfg-invalid

1.16 wids-security unknown-ap-managed-ssid

Command: wids-security unknown-ap-managed-ssid

no wids-security unknown-ap-managed-ssid

Function: Enable the detection of unknown AP posing as legal SSID, the no command will disable this detection.

Parameter: None.

Default: Enable the detection of unknown AP posing as legal SSID.

Command Mode: Wireless global configuration mode.

Usage Guide: The network configuration of AC controller SSID inquiry system records the legal SSID, unknown AP maybe poses as the legal SSID to deceive Client access to theft customer information. Use this command to detect this rogue AP.

Example: Enable the detection of unknown AP posing as legal SSID.

AC(config-wireless)#wids-security unknown-ap-managed-ssid

1.17 wids-security unmanaged-ap-wired

Command: wids-security unmanaged-ap-wired

no wids-security unmanaged-ap-wired

Function: Enable the detection of the unmanaged AP accessed to wired network, the no command will disable this detection.

Parameter: None.

Default: Enable the detection of unmanaged AP accessed to wired network.

Command Mode: Wireless global configuration mode.

Usage Guide: Only the Managed AP can access to wired network, so if the unknown AP accessed to wired network, this command can detect this rogue AP.

Example: Enable the detection of unmanaged AP accessed to wired network.

AC(config-wireless)# wids-security unmanaged-ap-wired

1.18 wids-security wds-device-unexpected

Command: wids-security wds-device-unexpected

no wids-security wds-device-unexpected

Function: Enable the detection of AP working in WDS mode, the no command will disable this detection.

Parameter: None.

Default: Enable the detection of AP works in WDS mode.

Command Mode: Wireless global configuration mode.

Usage Guide: WDS (Wireless Distribution System) is the protocol of AP connecting through wireless network. The AP running in WDS mode connected each other by bridge or repeater, it reduces the dependence of the wired network and improves the flexibility and convenience of the entire network structure. Use this command to detect whether the AP WDS state is the same as the AP WDS state in AC database, if they are not the same, then confirmed the AP as rogue AP.

Example: Enable the detection of AP working in WDS mode.

AC(config-wireless)# wids-security wds-device-unexpected

1.19 wids-security wired-detection-interval

Command: wids-security wired-detection-interval <*interval*>

no wids-security wired-detection-interval

Function: Set the shortest idle waiting time of each detection, the no command will restore the waiting time to default value as 60s.

Parameter: <*interval*> is the shortest idle waiting time of each detection for AP, range is 1~3600s.

Default: 60s.

Command Mode: Wireless global configuration mode.

Usage Guide: In order to avoid the AP sending the detection data packet in high frequency, set the shortest idle waiting time then the AP must wait for the next time after the completion of a round of detection (in this time, the RF Scan function is as usual). Use

this Command to set the shortest idle waiting time.

Example:

AC(config-wireless)# wids-security wired-detection-interval 360

Chapter 2 Commands for Client Threat Detection Parameter

2.1 debug wireless wids known-client

Command: debug wireless wids known-client

no debug wireless wids known-client

Function: Enable the debug information of Known-client database, the no command will disable this information.

Parameter: None.

Default: None.

Command Mode: Admin mode.

Usage Guide: Use this command to check the debug information of Known-client database, to show the information of added, deleted and checked known-client.

Example: Enable the debug information of Known-client database.

AC#debug wireless wids known-client

2.2 oui database

Command: oui database <*ouival*> [<*oui*>]

no oui database <*ouival*>

Function: Add OUI entries to OUI database, used to show and detect; the no command will delete the entries from the local OUI database corresponding oui value.

Parameter: <*ouival*> is the OUI value of AP or Client company; **<*oui*>** is the company name of this OUI.

Default: None.

Command Mode: Wireless global configuration mode.

Usage Guide: Use this command to add / delete OUI entries, in order to advanced the detection which uses the OUI list to detect threaten.

Example: Add OUI entry with the OUI value as 00-03-0f to company vendorname.

AC(config-wireless)#oui database 00-03-0f “vendorname”

2.3 show wireless client detected-client rogue-classification

Command: show wireless client <*macaddr*> detected-client rogue-classification

Function: Show the Client threat detection log.

Parameter: <*macaddr*> is Client MAC address.

Default: None.

Command Mode: Admin mode.

Usage Guide: Use this command to show the Client threat detection log.

Example: Show the threat detection log of Client with MAC as 00-03-0f-01-02-03.

AC#show wireless client 00-03-0f-01-02-03 detected-client rogue-classification

Test ID	Cond Detect	MAC Addr (radio)	Test Config	Test Result	Time Since 1st Report	Time Since Last Report
WIDSCLNTROGUE1	False	00-00-00-00-00-00(0)	Disable		0d:08:40:54	0d:08:40:54
WIDSCLNTROGUE2	False	00-03-0f-01-02-03(1)	Enable		0d:08:40:54	0d:00:00:01
WIDSCLNTROGUE3	False	00-00-00-00-00-00(0)	Disable		0d:08:40:54	0d:08:40:54
WIDSCLNTROGUE4	False	00-03-0f-01-02-03(1)	Enable		0d:08:40:54	0d:00:00:01
WIDSCLNTROGUE5	False	00-00-00-00-00-00(0)	Disable		0d:08:40:54	0d:08:40:54
WIDSCLNTROGUE6	False	00-03-0f-01-02-03(1)	Enable		0d:08:40:54	0d:00:00:01
WIDSCLNTROGUE7	False	00-00-00-00-00-00(0)	Disable		0d:08:40:54	0d:08:40:54

WIDSCLNTROGUE1..... Client not in Known Client Database

WIDSCLNTROGUE2..... Client exceeds configured rate for auth msgs

WIDSCLNTROGUE3..... Client exceeds configured rate for probe msgs

WIDSCLNTROGUE4..... Client exceeds configured rate for de-auth msgs

WIDSCLNTROGUE5..... Client exceeds max failing authentications

WIDSCLNTROGUE6..... Known client authenticated with unknown AP

WIDSCLNTROGUE7..... Client OUI not in the OUI Database

Table 2-1 Client threat detection log parameters

Parameter name	Explain
Test ID	Client threat test ID (WIDSCLNTROGUEnn)
Detect	whether a threat occured is detected
MAC Addr(radio)	MAC address of this RF scanning AP (radio number)
Config	Show the threat detection Enable or Disable
Result	Show the equipment whether the illegal equipment
1st Report	Show the time stamp of this threat first occured
Last Report	Show the time stamp of threat last occured

2.4 show wireless oui database

Command: show wireless oui database [<*ouival*>]

Function: Show OUI database.

Parameter: <*ouival*> is OUI value of AP or Client company.

Default: None.

Command Mode: Admin mode.

Usage Guide: Use this command to show the specified OUI company information, if not specified oui, then show all oui database content.

Example: Show the OUI database with company OUI value as 00-03-0f.

AC#show wireless OUI database 00-03-0f

OUI Value..... 00-03-0F

OUI.....

Table 2-2 OUI database Parameter explain

Parameter name	Explain
Ouival	AP/Client company OUI value
Oui	company name of this OUI value

2.5 show wireless wids-security client

Command: show wireless wids-security client

Function: Show the configured Client threat detection parameters.

Parameter: None.

Default: None.

Command Mode: Admin mode.

Usage Guide: Use this command to check the configured Client threat detection parameters.

Example: Show the configured Client threat detection parameters.

AC#show wireless wids-security client

Rogue detected trap interval..... 300 seconds
Rogue-Not in OUI database..... Disable
Rogue-Not in Known Client list..... Disable
Rogue-Exceeds Auth Req ..... Enable
Rogue-Exceeds DeAuth Req ..... Enable
Rogue-Exceeds Probe Req ..... Disable
Rogue-Exceeds Failed auth ..... Disable
Rogue-Auth with unknown AP..... Enable
Client Threat Mitigation..... Disable
De-auth threshold interval..... 300 seconds
De-auth threshold value..... 10
Auth threshold interval..... 300 seconds
Auth threshold value..... 10
Probe threshold interval..... 300 seconds
Probe threshold value..... 10
Auth failure threshold..... 5
Known DB Location..... Local
Known DB RADIUS Server Name..... Default-RADIUS-Server
Known DB Radius Server Status..... Not Configured

Table 2-3 Client threat detection parameters explain

Parameter name	Explain
Rogue Detected Trap Interval	The interval of system testing whether Rogue Client is being
De-auth threshold interval	Interval of Client sending 802.11 delete authentication frame
De-auth threshold value	Threshold of Client sending 802.11 delete authentication frame
Auth threshold interval	Interval of Client sending 802.11 authentication frame
Auth threshold value	Threshold of Client sending 802.11 authentication frame

Probe threshold interval	Interval of Client sending 802.11 exploration frame
Probe threshold value	Threshold of Client sending 802.11 exploration frame
Auth failure threshold	Threshold of Client failure authentication numbers
Known DB Location	Known Client database location (local or Radius server)
Known DB Radius Server Name	Radius server name, when Known Client database location as Radius server
Known DB Radius Server Status	Show whether set Known Client database location as Radius server

2.6 show wireless wids-security client rogue-test-descriptions

Command: show wireless wids-security client rogue-test-descriptions

Function: Show Client threat detection description.

Parameter: None.

Default: None.

Command Mode: Admin mode.

Usage Guide: Use this command to show Client threat detection description.

Example: Show Client threat detection description.

AC#show wireless wids-security client rogue-test-descriptions

WIDSCLNTROGUE1..... Client not in Known Client Database
WIDSCLNTROGUE2..... Client exceeds configured rate for auth msgs
WIDSCLNTROGUE3..... Client exceeds configured rate for probe msgs
WIDSCLNTROGUE4..... Client exceeds configured rate for de-auth msgs
WIDSCLNTROGUE5..... Client exceeds max failing authentications
WIDSCLNTROGUE6..... Known client authenticated with unknown AP
WIDSCLNTROGUE7..... Client OUI not in the OUI Database

2.7 wids-security client auth-with-unknown-ap

Command: wids-security client auth-with-unknown-ap

no wids-security client auth-with-unknown-ap

Function: Enable the detection of legal Client associate with illegal AP, the no command will disable this detection.

Parameter: None.

Default: Enable the detection of legal Client associate with illegal AP.

Command Mode: Wireless global configuration mode.

Usage Guide: Legal Client maybe access to network through illegal AP, then the legal Client information will be disclosed to the hacker using this rouge AP. Use this command to detect this type Rogue Client.

Example: Enable the detection of legal Client associate with illegal AP.

AC(config-wireless)#wids-security client auth-with-unknown-ap

2.8 wids-security client configured-assoc-rate

Command: wids-security client configured-assoc-rate

no wids-security client configured-assoc-rate

Function: Enable flooding attack detection of association request frame. The no command disables it.

Parameters: None.

Default: Enable.

Command Mode: Wireless global configuration mode.

Usage Guide: 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. Use this command to enable this detection to detect this class of Rogue Client.

Example: Enable flooding attack detection of association request frame; disable this detection.

AC(config-wireless)#wids-security client configured-assoc-rate

AC(config-wireless)#no wids-security client configured-assoc-rate

2.9 wids-security client configured-auth-rate

Command: wids-security client configured-auth-rate

no wids-security client configured-auth-rate

Function: Enable authentication request frame flood attack detection, the no command will disable this command.

Parameter: None.

Default: Enable authentication request frame flood attack detection.

Command Mode: Wireless global configuration mode.

Usage Guide: Authentication request frame flooding attack refers to the Rogue Client send a large number of authentication request frame to the AP devices in a short time, the AP device will be flooded by attack packets and can not handle the message of the

wireless terminal. Enable this Command to detect such Rogue Client.

Example: Enable authentication request frame flood attack detection

AC(config-wireless)#wids-security client configured-auth-rate

2.10 wids-security client configured-deauth-rate

Command: wids-security client configured-deauth-rate

no wids-security client configured-deauth-rate

Function: Enable the deletion authentication request frame flooding attack detection, the no command will disable this detection.

Parameter: None.

Default: Enable the deletion authentication request frame flooding attack detection.

Command Mode: Wireless global configuration mode.

Usage Guide: Deletion authentication request frame flood attack is the Rogue Client sends a large number of authentication request frame in a short time to an AP device. Use this Command to enable the OUI not legitimate detection, to detect such Rogue Client.

Example: Enable the deletion authentication request frame flooding attack detection.

AC(config-wireless)#wids-security client configured-deauth-rate

2.11 wids-security client configured-disassoc-rate

Command: wids-security client configured-disassoc-rate

no wids-security client configured-disassoc-rate

Function: Enable flooding attack detection of disassociation request frame. The no command disables it.

Parameters: None.

Default: Enable.

Command Mode: Wireless global configuration mode.

Usage Guide: 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. Use this command to enable this detection to detect this class of Rogue Client.

Example: Enable flooding attack detection of disassociation request frame; disable this detection.

AC(config-wireless)# wids-security client configured-disassoc-rate

AC(config-wireless)# no wids-security client configured-disassoc-rate

2.12 wids-security client configured-probe-rate

Command: wids-security client configured-probe-rate

no wids-security client configured-probe-rate

Function: Enable probe request frame flooding attack detection, the no command will disable this detection.

Parameter: None.

Default: Enable probe request frame flooding attack detection.

Command Mode: Wireless global configuration mode.

Usage Guide: Probe request frame flooding refers Rogue Client sends a large number probe request frame to the AP device in a short time. This command can detect such Rogue Client.

Example: Enable probe request frame flooding attack detection.

AC(config-wireless)#wids-security client configured-probe-rate

2.13 wids-security client known-client-database

Command: wids-security client known-client-database

no wids-security client known-client-database

Function: Enable Known Client Database detection, the no command will disable this detection.

Parameter: None.

Default: Disable Known Client Database detection.

Command Mode: Wireless global configuration mode.

Usage Guide: Set AC controller read Known Client Database from local or Radius server, the Known Client Database notes the appropriate client entry if the Client is legitimate, otherwise the Client is not legitimate. Use this command to detect such Rogue Client.

Example: Enable Known Client Database detection.

AC(config-wireless)#wids-security client known-client-database

2.14 wids-security client max-auth-failure

Command: wids-security client max-auth-failure

no wids-security client max-auth-failure

Function: Enable the maximum authentication failure number detection, the no command will disable this detection.

Parameter: None.

Default: Enable the maximum authentication failure number detection.

Command Mode: Wireless global configuration mode.

Usage Guide: Some illegal Client in order to access the protected wireless network, will always try to send authentication requests until the certification request be allowed. The command can detect such Rogue Client.

Example: Enable the maximum authentication failure number detection.

AC(config-wireless)#wids-security client max-auth-failure

2.15 wids-security client oui-database

Command: wids-security client oui-database

no wids-security client oui-database

Function: Enable OUI illegal detection, the no command will disable this detection.

Parameter: None.

Default: Disable OUI illegal detection.

Command Mode: Wireless global configuration mode.

Usage Guide: The legal OUI set in AC controller OUI database, check the OUI field (the first three bytes) of the destination Client MAC address whether in the OUI database. Use this command to detect such Rogue Client.

Example: Enable OUI illegal detection.

AC(config-wireless)#wids-security client oui-database

2.16 wids-security client rogue-det-trap-interval

Command: wids-security client rogue-det-trap-interval <*60-3600*>

no wids-security client rogue-det-trap-interval

Function: Set the interval of detection Rogue Client. The no command will restore the interval to the default value.

Parameter: <*60-3600*> time interval, in seconds.

Default: 300s.

Command Mode: Wireless global configuration mode.

Usage Guide: Set at a regular intervals, the system will check whether there is the Rogue Client, if exists, the AC controller sends "wsRogueClientPresent" Trap to alert the user, use this command to set the time interval.

Example: Set the interval of detection Rogue Client as 1000 seconds.

AC(config-wireless)#wids-security client rogue-det-trap-interval 1000

2.17 wids-security client threshold-auth-failure

Command: wids-security client threshold-auth-failure <*1-99999*>

no wids-security client threshold-auth-failure

Function: Set the threshold of Client authentication failure number. The no command will restore the threshold to the default value.

Parameter: <*1-99999*> threshold of Client authentication failure number.

Default: 5.

Command Mode: Wireless global configuration mode.

Usage Guide: Detect the Rouge AP by the number of Client certification whether beyond the configured threshold, use this command to set the threshold of Client authentication failure number.

Example: Set the threshold of Client authentication failure number as 1000.

AC(config-wireless)# wids-security client threshold-auth-failure 1000

2.18 wids-security client threshold-interval-assoc

Command: wids-security client threshold-interval-assoc <1-3600>

no wids-security client threshold-interval-assoc <1-3600>

Function: Configure the detection time of client sending 802.11 association request frame. The no command recovers to be default.

Parameters: <1-3600> is the detection time of client sending association request frame. Unit is second.

Default: 60s.

Command Guide: Wireless Config.

Usage Guide: Judge whether it is flooding attack of association request frame through the number of association request frames detected in the configured time. Use this command to configure the detection time of association request frame.

Example: Configure the detection time of client sending 802.11 association request frame as 360s.

AC(config-wireless)# wids-security client threshold-interval-assoc

2.19 wids-security client threshold-interval-auth

Command: wids-security client threshold-interval-auth <*1-3600*>

no wids-security client threshold-interval-auth

Function: Set the detection interval of Client sending 802.11 authentication request frame. The no command will restore the interval to the default value.

Parameter: <*1-3600*> interval of client sending authentication request frame, in seconds.

Default: 60s.

Command Mode: Wireless global configuration mode.

Usage Guide: Judged by the number of authentication request frame whether exceeds the threshold to determine there is not an authentication request frame flood attack. Can use this command to set the authentication request frame detection time.

Example: Set the detection interval of Client sending 802.11 authentication request frame as 360s.

AC(config-wireless)#wids-security client threshold-interval-auth 360

2.20 wids-security client threshold-interval-deauth

Command: wids-security client threshold-interval- deauth <*1-3600*>

no wids-security client threshold-interval- deauth

Function: Set the detection interval of Client sending 802.11 deletion authentication request frame. The no command will restore the interval to the default value.

Parameter: <*1-3600*> is detection interval of Client sending 802.11 deletion authentication request frame, in seconds.

Default: 60s.

Command Mode: Wireless global configuration mode.

Usage Guide: Judged by the number of deletion authentication request frame whether exceeds the threshold to determine there is not a deletion authentication request frame flood attack. Can use this command to set the deletion authentication request frame detection time.

Example: Set the detection interval of Client sending 802.11 deletion authentication request frame as 100 seconds.

AC(config-wireless)# wids-security client threshold-interval- deauth 100

2.21 wids-security client threshold-interval-disassoc

Command: wids-security client threshold-interval-disassoc <1-3600>

no wids-security client threshold-interval-disassoc

Function: Configure the detection time of client sending 802.11 disassociation request frame. The no command recovers to be default.

Parameters: <1-3600> is the detection time of client sending disassociation request frame. Unit is second.

Default: 60s.

Command Guide: Wireless Config.

Usage Guide: Judge whether it is flooding attack of disassociation request frame through the number of disassociation request frames detected in the configured time. Use this command to configure the detection time of disassociation request frame.

Example: Configure the detection time of client sending 802.11 disassociation request frame as 100s.

AC(config-wireless)# wids-security client threshold-interval-disassoc100

2.22 wids-security client threshold-interval-probe

Command: wids-security client threshold-interval-probe *<1-3600>*

no wids-security client threshold-interval-probe

Function: Set the detection interval of Client sending 802.11 probe request frame. The no command will restore the interval to the default value.

Parameter: *<1-3600>* is detection interval of Client sending 802.11 probe request frame, in seconds.

Default: 60s.

Command Mode: Wireless global configuration mode.

Usage Guide: Judged by the number of probe request frame whether exceeds the threshold to determine there is not a probe request frame flood attack. Can use this command to set the probe request frame detection time.

Example: Set the detection interval of Client sending 802.11 probe request frame as 100 seconds.

AC(config-wireless)# wids-security client threshold-interval-probe 100

2.23 wids-security client threshold-value-assoc

Command: wids-security client threshold-value-assoc <1-99999>

no wids-security client threshold-value-assoc

Function: Configure the threshold of client sending 802.11 association request frame. The no command will restore the threshold to the default value.

Parameters: <1-99999> the threshold of Client sending 802.11 association request frame.

Default: 120

Command Mode: Wireless global configuration mode.

Usage Guide: Use this command to set the maximum number of Client sending 802.11 association request frame in the threshold-interval-assoc time.

Example: Set the maximum number of Client sending 802.11 association request frame as 100.

AC(config-wireless)#wids-security client threshold-value-assoc 100

2.24 wids-security client threshold-value-auth

Command: wids-security client threshold-value-auth <*1-99999*>

no wids-security client threshold-value-auth

Function: Set the threshold of Client sending 802.11 authentication request frame. The no command will restore the threshold to the default value.

Parameter: <*1-99999*> the threshold of Client sending 802.11 authentication request frame.

Default: 120.

Command Mode: Wireless global configuration mode.

Usage Guide: Use this command to set the maximum number of Client sending 802.11 authentication request frame in the threshold-interval-auth time.

Example: Set the threshold of Client sending 802.11 authentication request frame as 100.

AC(config-wireless)# wids-security client threshold-value-auth 100

2.25 wids-security client threshold-value-deauth

Command: wids-security client threshold-value- deauth <*1-99999*>

no wids-security client threshold-value- deauth

Function: Set the threshold of Client sending 802.11 deletion authentication request frame. The no command will restore the threshold to the default value.

Parameter: <*1-99999*> threshold of Client sending 802.11 deletion authentication request frame.

Default: 120.

Command Mode: Wireless global configuration mode.

Usage Guide: Use this command to set the maximum number of Client sending 802.11 deletion authentication request frame in the threshold-interval-deauth time.

Example: Set the threshold of Client sending 802.11 deletion authentication request frame as 100.

AC(config-wireless)# wids-security client threshold-value- deauth 100

2.26 wids-security client threshold-value-disassoc

Command: wids-security client threshold-value-disassoc <1-99999>

no wids-security client threshold-value-disassoc

Function: Configure the threshold of client sending 802.11 disassociation request frame.

The no command will restore the threshold to the default value.

Parameters: <1-99999> the threshold of Client sending 802.11 disassociation request frame.

Default: 120

Command Mode: Wireless global configuration mode.

Usage Guide: Use this command to set the maximum number of Client sending 802.11 disassociation request frame in the threshold-interval-disassoc time.

Example: Set the maximum number of Client sending 802.11 disassociation request frame as 1100.

AC(config-wireless)# wids-security client threshold-value-disassoc 1100

2.27 wids-security client threshold-value-probe

Command: wids-security client threshold-value-probe <*1-99999*>

no wids-security client threshold-value-probe

Function: Set the threshold of Client sending 802.11 probe request frame. The no command will restore the threshold to the default value.

Parameter: <*1-99999*> threshold of Client sending 802.11 probe request frame.

Default: 120.

Command Mode: Wireless global configuration mode.

Usage Guide: Use this command to set the maximum number of Client sending 802.11 probe request frame in the threshold-interval-probe time.

Example: Set the threshold of Client sending 802.11 probe request frame as 1100.

AC(config-wireless)# wids-security client threshold-value-probe 1100

Chapter 3 Commands for Anti-attack Function

3.1 clear wireless detected-client non-auth

Command: clear wireless detected-client [<*macaddr*>] non-auth

Function: Clear the Client from detected-client database.

Parameter: <*macaddr*> MAC address of Client.

Default: None.

Command Mode: Wireless global configuration mode.

Usage Guide: Use this command to clear the specified Client from detected-client database, if the client MAC address is not specified, clear the whole detected-client database, if the Client state is Authenticated, it will not be deleted.

Example: Clear the Client with MAC of 00-03-0f-01-02-03 from detected-client database.

AC(config-wireless)#clear wireless detected-client 00-03-0f-01-02-03 non-auth

3.2 debug wireless wids msg

Command: debug wireless wids msg

no debug wireless wids msg

Function: Enable the debug information of WIDS sending messages (Client-Threat-Deauthenticate Message and WIDS-Configuration Message), the no command will disable the information.

Parameter: None.

Default: None.

Command Mode: Admin mode.

Usage Guide: Use this command to enable the debug information of WIDS sending messages including the message content and the sending result.

Example: Enable the debug information of WIDS sending message.

AC#debug wireless wids msg

3.3 show wireless wids-security de-authentication

Command: show wireless wids-security de-authentication

Function: Show the Rogue AP attacking list.

Parameter: None.

Default: None.

Command Mode: Admin mode.

Usage Guide: Use this command to show the Rogue AP attacking list.

Example: Show the Rogue AP attacking list.

AC#show wireless wids-security de-authentication

BSSID	Channel	Attack Time	Age
00-03-0f-18-ed-30	11	0d:00:00:13	0d:00:00:13
00-03-0f-18-ed-31	11	0d:00:00:12	0d:00:00:12

Table 3-1 Rogue AP attacking list explanation

Parameter name	Explanation
BSSID	Rogue AP BSSID
Channel	Rogue AP work channel
Attack Time	Anti-attack start time
Age	Time of receiving this Rogue AP RF report

3.4 wids-security ap-de-auth-attack

Command: wids-security ap-de-auth-attack

no wids-security ap-de-auth-attack

Function: Enable Rogue AP anti-attack function, the no command will disable this function.

Parameter: None.

Default: Disable.

Command Mode: Wireless global configuration mode.

Usage Guide: After AC Controller detected Rogue AP, it will add this AP to the Rouge AP attacking list if enable this function, and send this list to all managed APs through WIDS-Configuration-Message. Radio of Sentry Mode imitates the Client to send relieving authentication message to the Rouge AP, the Radio of Active Mode will send the relieving authentication message to the Client associated with the Rogue AP. Use this command to enable the anti-attack.

Example: Enable Rogue AP anti-attack function.

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

3.5 wids-security client threat-mitigation

Command: wids-security client threat-mitigation

no wids-security client threat-mitigation

Function: Enable Known Client protection function, the no command will disable this function.

Parameter: None.

Default: Disable Known Client protection.

Command Mode: Wireless global configuration mode.

Usage Guide: If the AC Controller enable detection of lawful Client associating with rogue AP, and detect such threats, the Client will be signed as Rogue Client, then send this message of Rogue Client information to the client-security task, this task message queue capacity is 128, so 128 messages can be received at most. The client-security task constructs Client-Threat-Deauthenticate Message to send it to managed AP when received the message from WIDS module, Radio of Sentry mode imitates this Client to send relieving authentication message to its associated AP to relive the connection with the rogue AP. use this command to protect the Known Client .

Example: Enable Known Client protection function.

AC(config-wireless)# wids-security client threat-mitigation

3.6 wireless acknowledge-rogue

Command: wireless acknowledge-rogue [<*macaddr*>]

Function: when clear the Rogue AP threats, change the AP Rogue state.

Parameter: <*macaddr*> Rogue AP MAC address.

Default: None.

Command Mode: Wireless global configuration mode.

Usage Guide: When the Rogue AP threat has been cleared, you should restore the AP state to the state before it is judged as Rogue in RF Scan database. Use this command to change such Rogue AP state, if the MAC address is specified, change the AP state with this MAC address; if it is not specified, then change all the rogue AP status.

Example: Change the Rouge AP state with MAC address of 00-03-0f-01-02-03.

AC#wireless acknowledge-rogue 00-03-0f-01-02-03

3.7 wireless detected-client ack-rogue

Command: wireless detected-client [<*macaddr*>] ack-rogue

Function: when clear the Rogue client threats, change the state of this Rogue Client.

Parameter: <*macaddr*> Client MAC address.

Default: None.

Command Mode: Wireless global configuration mode.

Usage Guide: Use this command to change the Rogue Client state, the principle is: If the Client is Authenticated state before it is identified as the Rogue, then change state to the Authenticated; Otherwise, the status will be changed to Detected. If the MAC address is specified, then change the Client status with specified MAC address, if the MAC address is specified, then change all the Rogue Client states.

Example: Change all the Rouge Client states.

AC(config-wireless)#wireless detected-client ack-rogue

Chapter 4 Commands for User Isolation

4.1 l2tunnel station-isolation allowed vlan

Command: l2tunnel station-isolation allowed vlan {WORD | add WORD | except WORD | remove WORD}

no l2tunnel station-isolation allowed vlan

Function: Enable the user isolation in centralized forwarding mode, the no command will disable this isolation.

Parameter: WORD: add a vlanList as allow vlan, and overwrite the old configuration.

add WORD: add a vlanList to the existed allow vlanList.

except WORD: set all VLAN as allow vlan except vlanList.

remove WORD: delete the VLAN specified by vlanList from the existed allow vlanList.

Default: Disable this user isolation.

Command Mode: Wireless global configuration mode.

Usage Guide: Use this command to enable the user isolation function in centralized forwarding mode.

Example: Enable the users isolation function of vlan100 in centralized forwarding mode.

AC#l2tunnel station-isolation allowed vlan 100

4.2 station-isolation (network mode)

command: station-isolation

no station-isonation

Function: Configure to make the wireless users associated with the same VAP achieve the isolation. No command disables this function.

Parameter: None.

Default: Disable the user isolation.

Command Mode: Network configuration mode.

Usage Guide: For safety, the network operator may need to isolate the wireless users associated with the same VAP, this can be achieved by configuring this command. After configured this command, the users associated with the same VAP cannot communicate to each other, but they can communicate to the users under the other VAP. After configured this command, the profile must be issued again to become effective, and the configured user isolation should be used under the locale forwarding mode.

Example: Configure the user isolation under VAP1 (network 18 is assumed).

ac(config-wireless)#network 18

ac(config-network)#station-isolation

ac#wireless ap profile apply 1

4.3 station-isolation (radio mode)

command: station-isolation

no station-isonation

Function: Configure to enable the user isolation function for all the VAP under the radio mode. No command disables this function.

Parameter: None.

Default: Disable the user isolation.

Command Mode: Radio configuration mode.

Usage Guide: This command can enable the wireless user isolation of all VAP under the radio mode. Two users under the same any VAP cannot communicate to each other; the users under the different VAP can communicate. After configured this command, the profile must be issued again to become effective, and the configured user isolation should be used under the locale forwarding mode.

Example: Enable the user isolation of all VAP under the radio 1 of profile 1.

ac(config)#wireless

ac(config-wireless)#ap profile 1

ac(config-ap-profile)#radio 1

ac(config-ap-profile-radio)#station-isolation

ac#wireless ap profile apply 1

4.4 station-isolation (profile mode)

command: station-isolation allowed vlan {[add | remove] <vlan id>}

no station-isolation allowed vlan

Function: 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.

Parameters: add: add a isolation VLAN; Remove: delete a isolation VLAN; <vlan id>: the VLAN number which need to be added, and the range is from 1 to 4094, more than one can be added. If there is no add or remove parameter, it will clear the configured isolation VLAN and add the new VLAN.

Default: Disable the user isolation.

Command Mode: Profile configuration mode.

Usage Guide: This command can enable the wireless user isolation function under the

different VAP of the same VLAN of AP. But the users associated with the same VAP are not isolated. For example, client1 joins up the SSID1 network of VAP1 under the AP, and client2 joins up the SSID2 network of VAP2 under the AP; the SSID1 and SSID2 belong to the same VLAN. If enabled the user isolation of this VLAN on profile, client1 and client2 cannot communicate to each other. If client1 and client2 are both associated with SSID1 or SSID2, they can communicate to each other. After configured this command, the profile must be issued again to become effective, and the configured user isolation should be used under the locale forwarding mode.

Example: Enable the user isolation among the VAP which belongs to VLAN 100 under the AP of profile 1.

ac(config)#wireless

ac(config-wireless)#ap profile 1

ac(config-ap-profile)# station-isolation allowed vlan 100

ac#wireless ap profile apply 1

Chapter 5 Commands for ARP Suppression and ARP Agency

5.1 arp-suppression

Command: arp-suppression

no arp-suppression

Function: Enable the ARP suppression function of the AP, then enable ARP Broadcast-to-unicast, DHCP packet inspection function automatically. The no command will disable this function, and disable the other detection function automatically.

Parameter: None.

Default: Disable.

Command Mode: Network configuration mode.

Usage Guide: This function uses the DHCP function to record the IP and MAC mapping table of all the local Authenticated Clients. It can reduce empty ARP broadcast packets through ARP Broadcast-to-unicast to save the Client electricity. Use this command to enable the ARP suppression function.

Example: Enable the ARP suppression function of the AP.

AC(config-wireless)#network 1

AC(config-network)# arp-suppression

5.2 proxy-arp

Command: proxy-arp

no proxy-arp

Function: Enable ARP agency function of the AP, then enable ARP agency, DHCP packet inspection function automatically. The no command will disable this function, and disable the other detection function automatically.

Parameters: None.

Default: Disable.

Command Mode: Network configuration mode.

Usage Guide: This function uses the DHCP function to record the IP and MAC mapping table of all the local Authenticated Clients. AP received ARP-Request, AP will send mac address in maintenance table to ARP-Reply (there is real client address, not AP mac address that filled in traditional agency), and do not need to transfer ARP-Request to Client. It can reduce empty ARP broadcast packets and save the Client electricity. Use this

command to enable the ARP agency function.

Example: Enable ARP agency function of the AP.

AC(config-wireless)#network 1

AC(config-network)# proxy-arp

5.3 show wireless ap statistics

Command: show wireless ap <*macaddr*> statistics

Function: Show ARP suppression and ARP agency information.

Parameter: None.

Default: None.

Command Mode: Admin mode.

Usage Guide: Use this command to show the ARP suppression and ARP agency information.

Example: Show ARP suppression and ARP agency information.

AC#show wireless ap 00-03-0f-01-02-03 statistics

MAC address..... 00-03-0f-01-02-03

Location.....

WLAN Packets Received..... 657165

WLAN Packets Transmitted..... 22491

WLAN Bytes Received..... 53895600

WLAN Bytes Transmitted..... 2106411

WLAN Packets Receive Dropped..... 0

WLAN Packets Transmit Dropped..... 0

WLAN Bytes Receive Dropped..... 0

WLAN Bytes Transmit Dropped..... 0

Ethernet Packets Received..... 34983

Ethernet Packets Transmitted..... 665519

Ethernet Bytes Received..... 3098387

Ethernet Bytes Transmitted..... 91636961

Ethernet Multicast Packets Received..... 11217

Total Transmit Errors..... 0

Total Receive Errors..... 0

Central L2 Tunnel Bytes Received..... 353162

Central L2 Tunnel Packets Received..... 57

Central L2 Tunnel Multicast Packets Received... 4035

Central L2 Tunnel Bytes Transmitted..... 44695300

Central L2 Tunnel Packets Transmitted..... 654775

Central L2 Tunnel Multicast Packets Transmitt.. 2391

ARP Reqs Converted from Bcast to Ucast..... 0

Filtered ARP Requests..... 0

Broadcasted ARP Requests..... 0

Proxy ARP Requests..... ...0

Table 5-1 ARP suppression and ARP agency information parameter explanation

Parameter name	Explanation
Filtered ARP Requests	Discarded ARP requests number of ARP Broadcast-to-unicast
Broadcasted ARP Requests	ARP requests number of ARP Broadcast-to-unicast
Proxy ARP Requests	ARP requests number of ARP agency

Chapter 6 Commands for Dynamic Blacklist

6.1 dynamic-blacklist

Command: dynamic-blacklist

no dynamic-blacklist

Function: Enable dynamic blacklist function. The no command disables this function.

Parameters: None.

Command Mode: Wireless Global Mode.

Default: Disable.

Usage Guide: This command is used to enable dynamic blacklist. When detected the threat conforms dynamic blacklist and it is considered as Rogue client, put the mac address of this client into dynamic blacklist and send it to managed AP to prevent the flooding attack of this client.

Example: Enable dynamic blacklist function.

AC(config-wireless)# dynamic-blacklist

6.2 dynamic-blacklist lifetime <60-3600>

Command: dynamic-blacklist lifetime <60-3600>

no dynamic-blacklist lifetime

Function: Configure aging time of dynamic blacklist. The no command recovers to be default.

Parameters: 60-3600: the aging time and unit is second, one hour is the most.

Command Mode: Wireless Global Mode.

Default: 300s.

Usage Guide: This command is used to configure the aging time of dynamic blacklist. When adding the new table entry to dynamic blacklist, the aging time will be configured at the same time. In this time, AP will drop the data frame of this rogue client. After it is time to the aging time, the relevant table entry will be deleted and the data frame of this client will be received again.

Example: Configure aging time of dynamic blacklist as 600s.

AC(config-wireless)# dynamic-blacklist lifetime 600

6.3 clear dynamic-blacklist (FF-FF-FF-FF-FF-FF|)

Command: clear dynamic-blacklist (FF-FF-FF-FF-FF-FF|)

Function: Delete the MAC address record of wireless terminal in dynamic blacklist manually.

Parameters: FF-FF-FF-FF-FF-FF : delete one record of wireless terminal MAC address.

None: delete all wireless terminal records in dynamic blacklist.

Command Mode: Privileged EXEC Mode.

Default: None.

Usage Guide: This command is used to delete one or all the MAC address records of wireless terminal in dynamic blacklist manually, delete the relevant table entry and receive the data frame of this client again.

Example: Delete the MAC address record of 30-46-9a-30-2b-e4 of wireless terminal in dynamic blacklist manually.

AC#clear wireless dynamic-blacklist 30-46-9a-30-2b-e4

6.4 show wireless dynamic-blacklist

Command: show wireless dynamic-blacklist

Function: Show all wireless terminal records in dynamic blacklist, including MAC address, keep-alive time, the time from last updating and anti-flooding attack detection type of wireless terminal.

Parameters: None.

Command Mode: Privileged EXEC Mode.

Default: None.

Usage Guide: This command is used to show all wireless terminal records in dynamic blacklist.

Example: Show all wireless terminal records in dynamic blacklist.

AC#show wireless dynamic-blacklist

Client MAC Address	LifeTime (seconds)	Time Since Last Report	Rogue Classification
54-e6-fc-0b-a8-36	300	0d:00:00:25	Exceed Configured Probe Rate
20-7c-8f-7c-8f-73	300	0d:00:00:25	Exceed Configured Probe Rate
00-22-5f-5a-22-93	300	0d:00:00:25	Exceed Configured Probe Rate
00-23-4e-e1-a7-d2	300	0d:00:00:25	Exceed Configured Probe Rate
e0-05-c5-8e-10-2f	300	0d:00:00:25	Exceed Configured Probe Rate
20-7c-8f-7c-90-4c	300	0d:00:00:25	Exceed Configured Probe Rate

18-f4-6a-00-e2-eb	300	0d:00:00:25	Exceed Configured Probe Rate
74-ea-3a-10-bb-ab	300	0d:00:00:25	Exceed Configured Probe Rate
08-10-74-ad-93-c8	300	0d:00:00:25	Exceed Configured Probe Rate
18-f4-6a-00-14-62	300	0d:00:00:25	Exceed Configured Probe Rate
00-21-00-cf-f0-e0	300	0d:00:00:25	Exceed Configured Probe Rate
fc-25-3f-d8-d0-b8	300	0d:00:00:25	Exceed Configured Probe Rate
8c-7b-9d-fb-b4-51	300	0d:00:00:25	Exceed Configured Probe Rate
00-0b-c0-02-9d-ac	300	0d:00:00:25	Exceed Configured Probe Rate
e0-b9-ba-dd-b8-c8	300	0d:00:00:25	Exceed Configured Probe Rate
30-46-9a-30-2b-e4	300	0d:00:00:25	Exceed Configured Probe Rate

Dynamic-blacklist entries Count..... 16

Chapter 7 Wireless SAVI

7.1 clear wireless savi binding

Command: clear wireless savi binding {dhcp|dhcpv6|slaac|static|mac <client-mac>|}

Function: Clear the wireless SAVI whose binding type is appointed or clear all the wireless SAVI entries.

Parameters: dhcp：delete the binding of SAVI DHCP type.

dhcpv6：delete the binding of SAVI DHCPV6 type.

slaac：delete the binding of SAVI SLAAC type.

static：delete the binding of SAVI STATIC type.

client-mac：delete the SAVI dynamic binding entry with the appointed client MAC.

Notice: When the configured parameters are empty, all the wireless SAVI entries will be deleted including static and dynamic entries.

Default: None.

Command Mode: Previlidged EXEC Mode.

Usage Guide: Use this command to delete the wireless SAVI whose binding type is appointed or clear all the wireless SAVI entries. After the SAVI entry is deleted, the corresponding client cannot access the network. When the configured parameters are empty, all the wireless SAVI entries will be deleted. When using this command to delete the SAVI binding entry with the appointed client MAC, the static entry will not be deleted; if user wants to delete the static entry, please use the following command: **no savi binding <ipv4|ipv6> <client-ip>**.

Example: Delete all the entries of the wireless SAVI.

AC#clear wireless savi binding

7.2 debug wireless savi packet

Command: debug wireless savi packet {send|receive|dump|all} <ap-mac>

no debug wireless savi packet {send|receive|dump|all} <ap-mac>

Function: Enable the packet debug on-off of the wireless SAVI function. The no command disables it.

Parameters: send：enable the debug information of sending packets of wireless SAVI;

receive：enable the debug information of receiving packets of wireless SAVI;

dump：enable the debug information of dumping packets of wireless SAVI;

all：enable the debug information of sending, receiving and dumping packets of wireless SAVI;

ap-mac：the MAC address of the AP which sends or receives the packet, user can debug an AP.

Default: Disable.

Command Mode: Previlidged EXEC Mode.

Usage Guide: Use this command to enable the packet debug on-off of the wireless SAVI function.

Example: Enable the debug information of sending, receiving and dumping packets of the wireless SAVI of the AP with the MAC address of 00-03-0f-10-30-40.

AC#debug wireless savi packet all 00-03-0f-10-30-40

MAC:00-03-0f-10-30-40 packet WD_LEVEL_SAVI_PKT_RX debug is on

MAC:00-03-0f-10-30-40 packet WD_LEVEL_SAVI_PKT_TX debug is on

MAC:00-03-0f-10-30-40 packet WD_LEVEL_SAVI_PKT_DUMP debug is on

7.3 debug wireless savi trace

Command: debug wireless savi trace <ap-mac>

no debug wireless savi trace <ap-mac>

Function: Enable the tracing debug on-off of the wireless SAVI function. The no command disables it.

Parameters: ap-mac：the MAC address of the AP which sends or receives the packet, user can debug an AP.

Default: Disable.

Command Mode: Previlidged EXEC Mode.

Usage Guide: Use this command to enable the tracing debug on-off of the wireless SAVI function.

Example: Enable the tracing debug information of sending, receiving and dumping packets of the wireless SAVI of the AP with the MAC address of 00-03-0f-10-30-40.

AC#debug wireless savi trace 00-03-0f-10-30-40

MAC:00-03-0f-10-30-40 internal WD_LEVEL_SAVI_TRACE debug is on

internal WD_LEVEL_SAVI_TRACE debug is on

7.4 debug wireless savi error

Command: debug wireless savi error

no debug wireless savi error

Function: Enable the error debug on-off of the wireless SAVI function. The no command

disables it.

Parameters: None.

Default: Disable.

Command Mode: Previlidged EXEC Mode.

Usage Guide: Use this command to enable the error debug on-off of the wireless SAVI function.

Example: Enable the error debug on-off of the wireless SAVI function.

AC#debug wireless savi error

error WD_LEVEL_SAVI_ERROR debug is on

7.5 savi binding

Command: savi binding <*client-mac*> <*ipv4|ipv6*> <*client-ip*>

no savi binding <*ipv4|ipv6*> <*client-ip*>

Function: Create the SAVI static binding entry globally. The no command deletes the entry.

Parameters: <client-mac>: Configure the client MAC address of the SAVI binding entry;

<client-ip>: Configure the client ipv4 or ipv6 address of the SAVI binding entry.

Default: None.

Command Mode: Wireless Config Mode.

Usage Guide: Use this command to create the SAVI static binding entry. The type of the entry is STATIC. After the static binding entry is created, issue this entry to the AP which is associated with that client. AC will notify the AP to add the entry and the rules are as below: if the static binding entry with the same IP address has existed, it will cover the entry; if the MAC is matching, the type will be updated as STATIC; if that IP entry does not exist, add the new entry. The no command deletes the SAVI binding entry and the type can be static or dynamic. When delete the entry through this command, AC will issue to AP immediately to notify the AP to delete the entry.

Example: Configure the static binding ipv4 address of the client with the MAC of 00-0d-0a-30-9a-0e as 192.168.1.3.

AC(config-wireless)#savi binding 00-0d-0a-30-9a-0e ipv4 192.168.1.3

7.6 savi ipv6-nd lifetime

Command: savi ipv6-nd lifetime *<1-31536000>*

no savi ipv6-nd lifetime

Function: Configure the lifetime of the SAVI SLAAC static binding. The no command

recovers to be the default value.

Parameters: <*1-31536000*>: the range of the lifetime is 1-31536000, the unit is second and it can be configured as one year at most.

Default: 4 hours (14400s).

Command Mode: Wireless Config Mode.

Usage Guide: Configure the lifetime of the SAVI SLAAC static binding. The no command recovers to be the default value.

Example: Configure the lifetime of the SAVI SLAAC static binding as 31536000s.

AC(config-wireless)#savi ipv6-nd lifetime 31536000

7.7 savi enable

Command: savi enable

no savi enable

Function: 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.

Parameters: None.

Default: Disable.

Command Mode: Ap Profile Config Mode.

Usage Guide: Use this command to 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.

Notice: User should configure it when the AP is effective and the configuration should be issued manually.

Example: Enable the SAVI controlling function.

AC(config-ap-profile)#savi enable

7.8 savi ipv6-slaac enable

Command: savi ipv6-slaac enable

no savi ipv6-slaac enable

Function: Enable the monitoring function for DAD NS packet from the managed AP under the ap profile. The no command recovers to disable it.

Parameters: None.

Default: Disable.

Command Mode: Ap Profile Config Mode.

Usage Guide: Use this command to enable the monitoring function for DAD NS packet

from the managed AP under the ap profile. It will be issued to AP immediately, after this function is effective, the SAVI SLAAC binding entry will be created and the packet source address will be tested. The no command recovers to disable it. After this function is effective, the SAVI SLAAC binding entry will not be created, and the existed SLAAC will not be dealt with.

Example: Enable the monitoring function for DAD NS packet.

AC(config-ap-profile)#savi ipv6-slaac enable

7.9 savi dyn-mac-binding-limit

Command: savi dyn-mac-binding-limit *<8-16>*

no savi dyn-mac-binding-limit

Function: Configure the binding-limit number corresponding to the same MAC address on AP. The no command recovers to be the default.

Parameters: *<8-16>*：Configure the binding-limit number corresponding to the same MAC address on AP and the range is 8-16.

Default: 8.

Command Mode: Ap Profile Config Mode.

Usage Guide: Use this command to create the binding-limit number corresponding to the same MAC address on AP. When the value reaches the toplimit, the new dynamic binding cannot be created; user can configure the larger value to meet the demand. The no command recovers to be the default.

Example: Configure the binding-limit number corresponding to the same MAC address on AP as 16.

AC(config-ap-profile)#savi dyn-mac-binding-limit 16

7.10 savi binding-limit

Command: savi binding-limit *<0-320>*

no savi binding-limit

Function: Configure to create the SAVI binding-limit capacity on AP. The no command recovers the configuration to be default.

Parameters: *<0-320>*：it is the binding-limit capacity on the AP and the range is 0-320. If the value is configured as 0, it means not to create any dynamic binding on AP.

Default: 240.

Command Mode: Ap Profile Config Mode.

Usage Guide: Use this command to create the SAVI binding-limit capacity on AP. When the value reaches the toplimit, the dynamic binding cannot be created; user can configure

the larger value to meet the demand. The no command recovers to be the default.

Example: Configure the SAVI binding-limit capacity on AP as 320.

AC(config-ap-profile)#savi binding-limit 320

7.11 show wireless savi binding

Command: show wireless savi binding {ipv4|ipv6|ap-mac <ap-mac>|}

Function: Show the wireless SAVI entry information on AC.

Parameters: ipv4：show the SAVI entry of the ipv4 user;

ipv6：show the SAVI entry of the ipv6 user;

ap-mac：show the user SAVI entry of the AP whose MAC address is appointed.

Notice: When the configured parameters are empty, show all the SAVI entries.

Default: None.

Command Mode: Previlidged EXEC Mode.

Usage Guide: Show the wireless SAVI entry information on AC including MAC address, IP address, binding type and lifetime.

Example: Show all the SAVI entries.

AC#show wireless savi binding

MAC Address IP Address AP MAC Address
Type Expires Lease Expiration
---------- ---------- ---------- ------- -------- ----------
00-00-00-11-22-33 1.1.1.1
STATIC infinite infinite
00-0d-0a-30-9a-0e 192.168.201.2 00-03-0f-10-30-40
DHCP 86400 Wed Jul 31 12:15:00 2013
00-0d-0a-30-9a-0e 2000:101::18 00-03-0f-10-30-40
DHCPV6 2592000 Thu Aug 29 12:15:00 2013
00-0d-0a-30-9a-0e 2000:101::3c3c:6507:511f:857a 00-03-0f-10-30-40
SLAAC 14400 Tue Jul 30 16:15:00 2013
00-0d-0a-30-9a-0e 2000:101::dc4b:1526:40cc:64bc 00-03-0f-10-30-40
SLAAC 14400 Tue Jul 30 16:15:00 2013
00-0d-0a-30-9a-0e 2000:201::11 00-03-0f-10-30-40
DHCPV6 2592000 Thu Aug 29 12:15:00 2013
00-0d-0a-30-9a-0e 2000:201::3c3c:6507:511f:857a 00-03-0f-10-30-40
SLAAC 14400 Tue Jul 30 16:15:00 2013
00-0d-0a-30-9a-0e 2000:201::8161:896b:13a6:e537 00-03-0f-10-30-40

SLAAC 14400 Tue Jul 30 16:15:00 2013

00-0d-0a-30-9a-0e fe80::3c3c:6507:511f:857a 00-03-0f-10-30-40

SLAAC 14400 Tue Jul 30 16:15:00 2013

Chapter 8 Commands for DHCP Suppression

8.1 dhcp-suppression

Command: dhcp-suppression

no dhcp-suppression

Function: Enable dhcp suppression function of the AP, it will enable DHCP OFFER/ACK packet Broadcast-to-unicast function automatically. The no command disable the suppression.

Parameters: None.

Default: Disable.

Command Mode: Network configuration mode.

Usage Guide: DHCP suppression function in AP is according to FLAGS field in DHCP packets to turn DHCP OFFER/ACK packets broadcast to unicast, reduce empty DHCP broadcast packets to save the Client electricity. Use this command to enable the DHCP suppression function.

Example: Enable the DHCP suppression function of the AP.

AC(config-wireless)#network 1

AC(config-network)# dhcp-suppression