Content

Chapter 1 Commands for RFPing..1-1

1.1 wireless link-test <client-MAC> (count <1-100>|) (timeout <1000-5000>|)..1-1

1.2 [no] debug wireless link-test msg 1-2

Chapter 2 Commands for Wireless Packet capture................2-1

2.1 wireless capture mode 2-1

2.2 wireless capture promiscuous-mode 2-1

2.3 wireless capture duration 2-1

2.4 wireless capture packet-num...2-1

2.5 wireless capture start ap <macaddr> interface............................2-2

2.6 wireless capture filter-mac 2-2

2.7 wireless capture stop...2-3

2.8 wireless capture file-transfer...2-3

2.9 show wireless capture status...2-3

2.10 debug wireless capture..2-4

Chapter 3 Commands for Spectral Analysis 3-1

3.1 spectral-scan 3-1

3.2 spectral-scan gui-report...3-1

3.3 spectral-scan-report-interval <1-300>...3-1

3.4 agetime spectral-scan <0, 300>...3-2

3.5 show wireless ap profile <1-1024> radio <1-2>............................3-2

3.6 show wireless ap spectrum monitors..3-3

3.7 show wireless ap <macaddr> radio <1-2> spectral-scan channel status 3-3

3.8 show wireless ap <macaddr> radio <1-2> spectral-scan interference status..3-4

3.9 clear wireless ap [<macaddr> [radio <1-2>]] spectral-scan list..3-5
3.10 debug wireless ap <macaddr> spectral-scan-report {trace| receive|dump} 3-5
3.11 debug wireless ap <macaddr> spectral-scan-report-interval {trace |send|dump} 3-5
Chapter 4 Commands for SMTP 4-1
4.1 smtp 4-1
4.2 receiver rule <rule-id> 4-1
4.3 receiver description <desc> 4-1
4.4 receiver address <email-addr> 4-2
4.5 receiver severity [critical| warnings| informational |dubugging]4-2
4.6 receiver time-range from <start-time> to <end-time> [monday| tuesday| wednesday| thursday| friday| saturday| sunday| weekend| weekday| everyday] 4-2
4.7 smtp server (ipv4 <ipaddr>) [port <port-num>] 4-4
4.8 smtp sender address <email-addr> 4-4
4.9 smtp server authentication username <username> password <password> 4-4
4.10 smtp server (source-ipv4 <ipaddr>) 4-5
4.11 smtp test-mail-send 4-5
4.12 show smtp status 4-5
4.13 show smtp receiver rule [<rule-id>] status 4-6

Chapter 1 Commands for RFPing

1.1 wireless link-test <client-MAC> (count <1-100>|) (timeout <1000-5000>|)

Command: wireless link-test <client-MAC> (count <1-100>|) (timeout <1000-5000>|)

Function: Configure to start the link quality testing of the client.

Parameters: <client-MAC>: configure the client MAC which needs to be tested.

count <1-100>: configure the number of the ping packets which are sent by radio to each kind of rate.

timeout <1000-5000>: the maximum internal that the radio interface waits the response of each ping packet, the range is ms.

Command Mode: Admin Mode.

Default: The default count value is 5, and the default timeout value is 1000ms.

Usage Guide: When user inputs this command, the AC will send message to AP. The AP will start to test the link according to the rate that the client supports after receiving the message. In the testing, user can stop the test at any time by using ctrl+c.

Example: Configure the times of sending packets of each kind of rate of the client as 5 and configure the timeout as 3000ms:

```
AC#wireless link-test e0-46-9a-b1-fa-ef count 5 timeout 3000
Testing link to client e0-46-9a-b1-fa-ef, press CTRL_C to break......
                         link Status
  RTT:Round trip time
----------------------------------------------------------------
  Client MAC Address:e0-46-9a-b1-fa-ef
----------------------------------------------------------------
  No./MCS    Rate(Mbps)    Txcnt    RxCnt    RSSI    Retries    RTT(ms)
----------------------------------------------------------------
       6           12         5        5      54         0          0
       7           18         5        5      53         0          0
       8           24         5        5      53         0          0
       9           36         5        5      53         0          0
      10           48         5        5      53         0          0
      11           54         5        5      52         0          0
    MCS-0         6.5         5        5      52         0          0
    MCS-1          13         5        5      53         0          0
```

```
   MCS-2        19.5       5       5     53        0        0
   MCS-3          26       5       5     53        0        0
   MCS-4          39       5       5     53        0        0
   MCS-5          52       5       5     53        0        0
   MCS-6        58.5       5       5     53        0        0
   MCS-7          65       5       5     53        0        0
   MCS-8          13       5       5     53        0        0
   MCS-9          26       5       5     53        0        0
  MCS-10          39       5       5     52        0        0
  MCS-11          52       5       5     52        0        0
  MCS-12          78       5       5     52        0        0
  MCS-13         104       5       5     52        0        0
  MCS-14         117       5       5     52        0        0
  MCS-15         130       5       5     52        0        0
No more Rate, link-test complete!
```

Stop the RFPing configuration:

```
AC#wireless link-test c0-cb-38-3e-13-9e count 5 timeout 3000
Testing link to client c0-cb-38-3e-13-9e, press CTRL_C to break......
                        link Status
 RTT:Round trip time
-----------------------------------------------------------------
 Client MAC Address:c0-cb-38-3e-13-9e
-----------------------------------------------------------------
 No./MCS   Rate(Mbps)   Txcnt   RxCnt   RSSI   Retries   RTT(ms)
-----------------------------------------------------------------
      3        11         5       1      63       4         0
      6        12         5       1      62       0         0
      7        18         5       4      64       0         0
      8        24         5       1      67       0         0
      9        36         5       3      64       0         0
     10        48         5       3      64       0         0
     11        54         5       3      64       0         0
```

1.2 [no] debug wireless link-test msg

Command: [no] debug wireless link-test msg

Function: Enable/disable the debug information of RFPing.

Parameters: None.

Default: Disable.

Command Mode: Privileged EXEC.

Example: Enable/disable the debug information of RFPing.

```
AC#debug wireless link-test msg
AC#no debug wireless link-test msg
```

Chapter 2 Commands for Wireless Packet capture

2.1 wireless capture mode

Command: wireless capture mode {file | remote [<*2002-2006*>]}

no wireless capture mode

Function: Configure the wireless packet capturing mode of AP. The no command clears this configuration.

Parameters: file is the file capturing mode;

remote is the remote capturing mode;

<2002-2006> is the port number of remote capturing, the range is 2002-2006and the default value is 2002.

Command Mode: Admin Mode.

Default: The packet capturing mode is not configured as default.

Usage Guide: If configures as file mode, AP can enable the file capturing mode and use the blocking TCP protocol to pack the captured packet as the .pcap file and upload it to AC. If configures as remote mode, AP can redirect the captured packet to the PC of Wireshark. The remote capturing is suitable for the cooperative work with Wireshark, the AP does not save any captured data into the local file system. If in the process of capturing packets, the parameters are modified, they will be effective next time to enable this function and it is same for the following configuration about wireless packet capture.

Example: Configure the packet capturing mode of AP as file.

```
AC#wireless capture mode file
```

Configure the packet capturing mode of AP as remote and the port is 2005.

```
AC#wireless capture mode remote 2005
```

In remote mode, the capture duration and packet numbers parameters will be ignored by Capture AP.

2.2 wireless capture promiscuous-mode

Command: wireless capture promiscuous-mode

no wireless capture promiscuous-mode

Function: Enable the promiscuous mode of packet capturing. The no command disables this mode.

Parameters: None.

Command Mode: Admin Mode.

Default: Disable.

Usage Guide: After enabled the promiscuous mode of packet capturing, the capture AP can capture all the flow on the channel which is same to its channel. If the promiscuous mode is not enabled, the capture AP can only capture the packet whose destination address is itself.

Example: Enable the promiscuous mode of packet capturing.

```
AC#wireless capture promiscuous-mode
```

2.3 wireless capture duration

Command: wireless capture duration <*60-3600*>

no wireless capture duration

Function: Configure the duration of packet capturing under the file capturing mode. The no command recovers it to be the default value.

Parameters: <60-3600> is the duration and the range is 60-3600, the unit is second.

Command Mode: Admin Mode.

Default: 3600s.

Usage Guide: The file mode is one of the conditions that AP stops the packet capturing. The duration of packet capturing can be configured through this command. If the duration achieves the configured value, AP will stop the packet capturing and upload the captured packet to AC. Under the remote mode, AP captures the packets all the time and it cannot be affected by this command.

Example: Configure the duration of packet capturing as 1000s.

```
AC#wireless capture duration 1000
```

2.4 wireless capture packet-num

Command: wireless capture packet-num <*1-10000*>

no wireless capture packet-num

Function: Under the file capturing mode, configure the maximum value of the captured packets. The no command recovers it to be the default value.

Parameters: <*1-10000*> is the number of the captured packets, the range is 1-10000.

Command Mode: Admin Mode.

Default: 10000.

Usage Guide: The file mode is one of the conditions that AP stops the packet capturing. The number of packets can be configured through this command. If the number achieves the configured value, AP will stop the packet capturing and upload the captured packet to AC. Under the remote mode, AP captures the packets all the time and it cannot be affected by this command.

Example: Configure the maximum value of the captured packets as 5000.

```
AC#wireless capture packet-num 5000
```

2.5 wireless capture start ap <macaddr> interface

Command: wireless capture start ap <*macaddr*> interface {radio <1|2>|ethernet }

Function: Configure the MAC address of the capture AP and the interface of the packet capturing. At the same time, control the AP to capture the packets.

Parameters: <macaddr> is the MAC address of the capturing AP. AP must be managedby the AC currently and the default value is 00-00-00-00-00-00.

interface is the interface of the packet capturing. Radio 1 means to capture the packet in 2.4G, radio 2 means to capture the packet in 5G. The AP must support the dual-band when configure this parameter.

ethernet is the wired packet capturing of AP and the default value is empty.

Command Mode: Admin Mode.

Default: The wireless packet capture is not enabled.

Usage Guide: After configured the packet capturing mode (necessary) and its parameters, the administrator can use this command to configure the MAC address of the capture AP and choose the interface. At the same time, this command is the start command of the wireless packet capture. The capture AP will configure the parameters first after received the message and then start to capture the packets.

Example: Configure the AP whose MAC address is 00-03-0f-09-51-30 to capture the packets on radio1.

```
AC#wireless capture start ap 00-03-0f-09-51-30 interface radio 1
```

Configure the AP whose MAC address is 00-03-0f-08-09-40 to capture the packets on wired interface.

AC#wireless capture start ap 00-03-0f-08-09-40 interface ethernet

2.6 wireless capture filter-mac

Command: wireless capture filter-mac <*macaddr*>

no wireless capture filter-mac

Function: Configure the filtration conditions of MAC address of the packet capturing. The no command clears the configuration.

Parameters: <macaddr> is the filtered MAC address.

Command Mode: Admin Mode.

Default: Disable.

Usage Guide: The administrator can configure the packet capturing about one device and use its MAC address as the filtration condition of the AP packet capturing, they can be STA MAC, VAP MAC. If the captured packet is the wired packet, AP can filter it after matching the source MAC and destination MAC addresses. If it is the wireless packet, AP can filter it after matching the source MAC address, destination MAC address and BSSID.

Example: Configure AP to capture the packets with the MAC address of 00-26-82-60-89-E6.

AC#wireless capture filter-mac 00-26-82-60-89-E6

2.7 wireless capture stop

Command: wireless capture stop

Function: Control the AP to stop the packet capturing.

Parameters: None.

Command Mode: Admin Mode.

Default: None.

Usage Guide: Use this command to stop the wireless packet capturing of the Capture AP manually. If it is the file mode, AP will upload the captured packet to AC after stopping the packet capturing.

Example: Control the AP to stop the packet capturing.

AC#wireless capture stop

2.8 wireless capture file-transfer

Command: wireless capture file-transfer

Function: Control the AP to upload the captured packet manually.

Parameters: None.

Command Mode: Admin Mode.

Default: None.

Usage Guide: The administrator can control the Capture AP to upload the captured packet to AC manually. After issued this command, AP will upload the last captured packet under the file mode. This command can be only used when the packet capturing is not started or stopped.

Example: Control the AP to re-upload the captured packet.

```
AC#wireless capture file-transfer
```

2.9 show wireless capture status

Command: show wireless capture status

Function: View the parameters configuration of the wireless packet capture and the current capturing status.

Parameters: None.

Command Mode: Admin Mode.

Default: None.

Usage Guide: View the parameters configuration of the wireless packet capture and the current capturing status through this command. The main content is as below:

Field	Description
Wireless capture status	Status of wireless capturing (Enable/Disable)
Capture ap MAC	The MAC address of the AP which is used for capturing.
Capture running status.	Status of the current packet capturing: 1- wireless packet capture not start 2- wireless packet capture in progress 3- wireless packet capture stop
Capture stop reason	If the capturing is stopped, the reason will be shown.
Download status	Under the file mode, the downloading status of the file

	is as below: 1- not start 2- Wireless packet capture file is transferring 3- Download success 4- Download failure
Capture file real size	Shows the real size of the capture file after the successful downloading.
Capture mode	The mode of wireless capturing (file/remote)
Remote port	It is the port of the remote capturing under the remote mode.
Capture interface	The interface of wireless capturing (radio1/radio2/Ethernet)
Capture duration	It is the duration of wireless capturing, the unit is second.
Capture packet number	It is the maximum number of the captured packets.
Capture Filter MAC	It is the MAC address which needs to be filtered if enables the filter mode.
Capture promiscuous mode	Status of promiscuous mode (Enable/Disable)

Example: Show the current capturing status.

```
AC#show wireless capture status

wireless capture status......................... Enable
Capture ap MAC................................. 00-03-0f-09-51-30
wireless capture running status................ wireless capture stop
wireless capture stop reason................... -----
wireless download status....................... -----
wireless capture mode.......................... remote
Remote port.................................... 2002
wireless capture interface..................... radio 1
wireless capture duration...................... 3600
wireless capture packet number................. 5000
wireless capture filter mac.................... 00-26-82-60-89-e6
wireless capture promiscuous mode.............. Enable
```

2.10 debug wireless capture

Command: debug wireless capture {all|event|packet}

no debug wireless capture {all|event|packet}

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

Parameters: all means all the data packets and events information of printing the wireless packet capture; event is the event information of printing the wireless packet capture; packet is the received and sent data packet of printing the wireless packet capture.

Command Mode: Admin Mode.

Default: Disable.

Usage Guide: This command can be used to control the AC to show the detailed information of the data packets and events in the wireless packet capture.

Example: Enable the on-off of the received and sent data packets showing of the wireless packet capture.

```
AC#debug wireless capture packet
wireless capture packet debug is on
```

Chapter 3 Commands for Spectral Analysis

3.1 spectral-scan

Command: spectral-scan

no spectral-scan

Function: Enable/disable the spectral analysis function.

Parameters: None.

Command Mode: Radio1 Configuration Mode.

Default: Disable.

Usage Guide: This command can be used to enable or disable the spectral analysis function of all the APs under the profile. And then the configuration is issued to AP, AP will run the spectral analysis. Only the radio of 2.4GHz can enable the spectral analysis function currently, and please ensure that only the vap0 under the radio1 is enabled when enable this function.

Example: Enable the spectral analysis function of the ap under profile1.

```
AC(config-ap-profile)#radio 1
AC(config-ap-profile-radio)#spectral-scan
AC(config-ap-profile-radio)#end
AC#wireless ap profile apply 1
```

3.2 spectral-scan gui-report

Command: spectral-scan gui-report

no spectral-scan gui-report

Function: Enable/disable the spectral analysis data function.

Parameters: None.

Command Mode: Radio1 Configuration Mode.

Default: Disable.

Usage Guide: This command can be used to enable or disable send the spectral analysis function to network management of all the APs under the profile. And then the configuration is issued to AP, AP will send the spectral analysis data to network management. Only the radio of 2.4GHz and the ap only can work on 5 and 11 channel can enable the function of sending the spectral analysis data to network management currently, and please ensure that only the vap0 under the radio1 is enabled when enable this function.

Example: Enable the function of sending the spectral analysis data to network management of the ap under profile1.

```
AC(config-ap-profile)#radio 1
AC(config-ap-profile-radio)# spectral-scan gui-report
AC(config-ap-profile-radio)#end
AC#wireless ap profile apply 1
```

3.3 spectral-scan-report-interval <1-300>

Command: spectral-scan-report-interval <1-300>
no spectral-scan-report-interval

Function: Configure the reporting interval of the spectral analysis result from AP to AC. For different profiles, different intervals can be configured. The no command recovers to be the default value.

Parameters: <1-300>: the reporting interval of the spectral analysis result from AP to AC, unit is second.

Command Mode: Profile Configuration Mode.

Default: 5s.

Usage Guide: This command can be used to modify the reporting interval of the spectral analysis result from AP. After issued to AP, it will be effective. Use the command of **show wireless ap profile profile_ID** to view it.

Example: Configure the reporting interval of the spectral analysis result from AP under the profile1 as 30s and issue it.

```
AC(config-ap-profile)#spectral-scan-report-interval 30
AC(config-ap-profile)#end
AC#wireless ap profile apply 1
AC#sh wireless ap profile 1

AP Profile ID................................. 1
redundancy mode............................... normal
Profile Name.................................. Default
Hardware Type................................. 22 - DCWL-7962AP(R5), Indoor Dual Radio a/n,
b/g/n
Load-balance Template ID...................... -----
Disconnected AP Data Forwarding Mode........... Disable
Disconnected AP Management Mode................ Enable
Wired Network Detection VLAN ID................ 1
```

```
AeroScout Engine Protocol Support............. Disable
Profile Status................................ Associated
Valid APs Configured.......................... 1
Managed APs Configured........................ 1
AP Escape..................................... Disable
Spectral Scan Report Interval(seconds)......... 30
NTP Server Status............................. Disable
NTP Server.................................... -----
NTP Synchronization Interval.................. 0d:00:01:04
Primary DNS Server............................ -----
BackUp DNS Server............................. -----
Management Vlan............................... 1
Management Vlan Priority...................... 0
Station-isolation Allowed Vlan................ -----
band-select................................... Disable
band-select cycle count....................... 30
band-select cycle threshold................... 1000
band-select client RSSI....................... 0
Profile Savi Mode............................. Disable
Profile Savi Ipv6-Slaac Mode.................. Disable
Maximum Savi Binding-Limit.................... 240
Maximum Savi Dyn-Mac-Binding-Limit............ 8
```

3.4 agetime spectral-scan <0, 300>

Command: agetime spectral-scan <0-300>

no agetime spectral-scan

Function: Configure the agetime of the spectral analysis result. The no command recovers it to be the default value.

Parameters: <0-300> is the interval of clearing the history, range is 1-300 and unit is minute. 0 means no aging.

Command Mode: wireless Configuration Mode.

Default: 15 minutes.

Usage Guide: Under the wireless Configuration Mode, this command can be used to modify the agetime of the spectral analysis result of all APs. Use the command of show wireless agetime to view.

Example: Configure the agetime of the spectral analysis result as 2 hours.

```
AC(config)#wireless
AC(config-wireless)#agetime spectral-scan 120
AC#sh wireless agetime

Ad Hoc Client Status Age (hours)............... 24
AP Failure Status Age (hours).................. 24
RF Scan Status Age (hours)..................... 24
Detected Clients Age (hours)................... 24
AP Provisioning Database Age Time (hours)...... 72
Spectral Scan Status Age Time (minutes)........ 120
```

3.5 show wireless ap profile <1-1024> radio <1-2>

Command: show wireless ap profile <1-1024> radio <1-2>

Function: Show the spectral analysis status.

Parameters: <1-1024>:profile ID

<1-2>: radio ID

Command Mode: Admin Mode.

Default: None.

Usage Guide: This command can be used to view whether the spectral analysis function of AP under the profile is enabled. Only the radio1 supports this function currently. For the selection of radio, user can only choose radio1.

Example: View the spectral analysis status under the profile1.

```
AC#show wireless ap profile 1 radio 1
AP Profile ID.................................. 1
Profile Name................................... Default
Radio.......................................... 1 - 802.11b/g/n
Status......................................... On
Mode........................................... 802.11b/g/n
RF Scan - Other Channels Mode.................. Enable
RF Scan - Other Channels Scan Interval......... 86400
RF Scan - Sentry Mode.......................... Disable
RF Scan - Sentry Scan Channels................. 802.11b/g
RF Scan - Scan Duration........................ 10
Spectral Scan Mode............................. Enable
Enable Broadcast/Multicast Rate Limiting....... Disable
Broadcast/Multicast Rate Limit................. 50
Broadcast/Multicast Rate Limit Burst........... 75
Beacon Interval................................ 100
```

```
DTIM Period.................................. 1
Fragmentation Threshold....................... 2346
```

3.6 show wireless ap spectrum monitors

Command: show wireless ap spectrum monitors

Function: Show the AP list which is enabled the spectral analysis.

Parameters: None.

Command Mode: Admin Mode.

Default: None.

Usage Guide: Show the AP list which is configured as spectrum monitor, the content is as below:

Managed AP Address	Mac address of AP
Radio	Radio ID and physical mode
Channel	The channel that AP works in
Band	The band that AP works in

The channel of the AP which is running the spectral analysis can be shown as 5 and 13 periodically. If AP is enable the spectral analysis function but it is not issued, the channel information will be shown as the normal channel.

Example: Show the AP list which is enabled the spectral analysis.

```
AC#show wireless ap spectrum monitors
Managed AP Address          Radio            Channel   Band
------------------ ----------------- ------- -------
00-03-0f-30-30-00     1 - 802.11b/g/n       5          2.4GHz
```

3.7 show wireless ap <macaddr> radio <1-2> spectral-scan channel status

Command: show wireless ap <macaddr> radio <1-2> spectral-scan channel status

Function: Show the channel status of the spectral scanning by AP.

Parameters: <macaddr>: the mac address of the AP which needs show the spectral analysis.

<1-2>: radio ID.

Command Mode: Admin Mode.

Default: None.

Usage Guide: This command can be used to show the channel status of the spectral scanning by AP, the content is as below:

Channel	The channel which is running the spectral analysis
Center Frequency	The center frequency of the channel

Example: Show the channel status of the spectral scanning by AP whose mac is 00-03-0f-11-11-20.

```
AC#show wireless ap 00-03-0f-11-11-20 radio 1 spectral-scan channel status
MAC address................................... 00-03-0f-11-11-20
Location......................................
Radio......................................... 1 - 802.11b/g/n
 channel    centerFreq          Age
--------- ------------ -----------
1           2.412GHZ       0d:00:00:05
2           2.417GHZ       0d:00:00:05
3           2.422GHZ       0d:00:00:05
4           2.427GHZ       0d:00:00:05
5           2.432GHZ       0d:00:00:05
6           2.437GHZ       0d:00:00:05
7           2.442GHZ       0d:00:00:05
8           2.447GHZ       0d:00:00:05
9           2.452GHZ       0d:00:00:05
10          2.457GHZ       0d:00:00:05
11          2.462GHZ       0d:00:00:05
12          2.467GHZ       0d:00:00:05
13          2.472GHZ       0d:00:00:05
14          2.484GHZ       0d:00:00:05
```

3.8 show wireless ap <macaddr> radio <1-2> spectral-scan interference status

Command: show wireless ap <macaddr> radio <1-2> spectral-scan interference status

Function: Show the spectral analysis result of the AP.

Parameters: <macaddr>: the mac address of the AP which needs to show the spectral analysis.

<1-2>: radio ID.

Command Mode: Admin Mode.

Default: None.

Usage Guide: Use this command to show the information of the microwave interference device that the AP spectral analysis detected, the content is as below:

Device type	Interference device type including Bluetooth, microwave, phone, etc.
Center frequency	Center frequency
Affect-channel	The channel affected

Example: Show the spectral analysis result of the AP whose mac is 00-03-0f-11-11-20.

```
AC# show wireless ap 00-03-0f-11-11-20 radio 1 spectral-scan interference status
MAC address.................................. 00-03-0f-11-11-20
Location.....................................
Radio......................................... 1 - 802.11b/g/n
Device Type 1: Microwave
Device Type 2: Bluetooth
Device Type 3: Cordless Phone
Device Type 4: Tone
Device Type 5: Other

Device Type     centerFreq        Affected Channel         Age
------------- --------------------------- ---------------

No Spectral Scan Interference Info Exits!
```

3.9 clear wireless ap [<macaddr> [radio <1-2>]] spectral-scan list

Command: clear wireless ap [<macaddr> [radio <1-2>]] spectral-scan list

Function: Clear the spectral analysis result of the AP.

Parameters: <macaddr>: the mac address of the AP which needs to show the spectral analysis.

<1-2>: radio ID.

Command Mode: Admin Mode.

Default: None.

Usage Guide: Clear the spectral analysis result of the appointed AP or all APs.

Example: the spectral analysis result of the AP whose mac address is 00-03-0f-11-11-20.

```
AC#clear wireless ap 00-03-0f-11-11-20 radio 1 spectral-scan list
Process with clear wireless managed ap spectral-scan list? [Y/N] y
All Spectral Scan entries cleared.
```

3.10 debug wireless ap <macaddr> spectral-scan-report {trace| receive|dump}

Command: debug wireless ap <macaddr> spectral-scan-report {trace | receive | dump }

no debug wireless ap <macaddr> spectral-scan-report {trace | receive | dump }

Function: Enable/disable the debug on-off of the spectral-scan reporting. It will show the debug information including spectral analysis result.

Parameters: macaddr: the mac address of the AP which reports the spectral analysis result.

trace: Show the tracking information of the packet dealing.

receive: Show the dealing information of received the packet.

dump: Show the detailed content of the packet.

Command Mode: Admin Mode.

Default: Disable.

Usage Guide: This command can be used to check whether the AP reports the spectral analysis result to AC periodically.

Example: Enable the debug on-off of the dealing information for the received packet.

```
AC#debug wireless ap 00-03-0f-11-11-20 spectral-scan-report receive
MAC:00-03-0f-11-11-20 packet WD_LEVEL_SPECTRAL_SCAN_REPORT_RX debug is on
```

3.11 debug wireless ap <macaddr> spectral-scan-report-interval {trace |send|dump}

Command: debug wireless ap <macaddr> spectral-scan-report-interval {trace | send | dump}

no debug wireless ap <macaddr> spectal-scan-report-interval {trace| send | dump}

Function: Enable/disable the debug on-off of dealing the interval message of the spectral analysis reporting. It will show the debug information that AC issues the reporting interval information to ap.

Parameters: macaddr: the mac address of the AP which receives the spectral analysis reporting interval information.

trace: Show the tracking information of sending packet.

send: Show the debug information of sending packet.

dump: Show the detailed content of the packet.

Command Mode: Admin Mode.

Default: Disable.

Usage Guide: This command can be used to check whether AC issues the spectral analysis result reporting interval to AP correctly.

Example: Enable the debug on-off of sending packet.

```
AC#debug wireless ap 00-03-0f-11-11-20 spectral-scan-report-interval send
MAC:00-03-0f-11-11-20 packet WD_LEVEL_SPECTRAL_SCAN_REPORT_INTVL_TX debug is on
```

Chapter 4 Commands for SMTP

4.1 smtp

Command: smtp

no smtp

Function: Enter into the SMTP configuration mode and enable the global SMTP on-off. The no command disables this on-off and does not provide the function of sending emails any more.

Parameters: None.

Default: Disable.

Command Mode: Global Configuration Mode.

Usage Guide: Enter into the SMTP configuration mode, all the configurations of SMTP should be configured under this mode. After disabled the global SMTP on-off, AC does not provide the function of sending mails to SMTP server and all the requirements of sending mails will be ignored.

Example: Enable/disable the smtp function.

```
AC(config)#smtp
AC(config-smtp)#exit
AC(config)#no smtp
```

4.2 receiver rule <rule-id>

Command: receiver rule <rule-id>

no receiver rule <rule-id>

Function: Create the SMTP receiver rule and enter into the SMTP receiver rule configuration mode. The no command deletes the SMTP receiver rule.

Parameters: <rule-id>: the configuration template's ID, the range is from 1 to 8 and it supports 8 rules at most.

Default: The default configuration is null, it means that the receiver rule does not exist.

Command Mode: SMTP Configuration Mode.

Usage Guide: If the rule has existed, enter into this rule configuration mode; if the rule does not exist, enter into the rule configuration mode and create the rule. The created rule does not include any receiver. For the no command, there is no any action if the rule does not exist; the no command will clear all the configurations of the rule if the rule has existed. The mail cannot be sent to the receiver in that rule. If the rule does not exist, there will be the prompt that the smtp receiver rule 2 has not been created.

Example: Create the SMTP receiver rule 1 and enter into the SMTP receiver rule1 configuration mode. And then delete the SMTP receiver rule1 and rule2.

```
AC(config-smtp)#receiver rule 1
AC(config-smtp-rule)#
AC(config-smtp-rule)#exit
AC(config-smtp)#no receiver rule 1
AC(config-smtp)#no receiver rule 2
Smtp receiver rule 2 has not been created!
```

4.3 receiver description <desc>

Command: receiver description <desc>
no receiver description

Function: Configure the description information for the current receiver rule. The no command recovers to be default.

Parameters: <desc>: the description information is the string whose characters are not more than 128. It can include the character of blank.

Default: Null.

Command Mode: SMTP Receiver Rule Configuration Mode.

Usage Guide: Configure the description information for the current receiver rule. The no command recovers to be default.

Example: Configure the description information for SMTP receiver rule 1 as “test” and then delete it.

```
AC(config-smtp)#receiver rule 1
AC(config-smtp-rule)#receiver description test
AC(config-smtp-rule)#no receiver description
```

4.4 receiver address <email-addr>

Command: receiver address <email-addr>

no receiver address <email-addr>

Function: Add the receiver in the current receiver rule. The no command deletes the configured receiver.

Parameters: <email-addr>: the description information is the mail address whose length is not more than 64 characters; the format is like XXXX@domain.com, the detailed format is delimited in RFC2821 and RFC5321.

Default: The default receiver is null, it means that there is no receiver.

Command Mode: SMTP Receiver Rule Configuration Mode.

Usage Guide: 8 different receiver addresses are supported to be added at most currently.

If user adds more than 8 receiver addresses, it will fail. When deleting the receiver, it will fail if the receiver does not exist. After added or deleted the receiver address, the receiver will be added or recovered automatically in the next time of sending mail. If the receiver list is empty, the mail will not be sent. Multiple receiver addresses can be added by using this command multiple times. In the same rule, the same receiver address cannot be added twice.

Example: Add the receiver of test@wifitest.com in the receiver rule; after added the illegal receiver of #, it will show error; delete the receiver of test@wifitest.com and delete it again, it will show error.

```
AC(config-smtp-rule)#receiver address test@wifitest.com
AC(config-smtp-rule)#receiver address #
Input email address is error, the format of email address is xxxx@domain!
AC(config-smtp-rule)#no receiver address test@wifitest.com
AC(config-smtp-rule)#no receiver address test@wifitest.com
The e-mail address "test@wifitest.com" has not been configured!
```

4.5 receiver severity [critical| warnings| informational |dubugging]

Command: receiver severity [critical| warnings| informational |dubugging]
no receiver severity

Function: Configure the severity level of the SMTP receiver rule. Only when the mail's severity level is the configured level or higher than it, this mail needs to be sent to the configured receiver in the rule. The no command recovers to be the default value.

Parameters: The severity levels of the receiver rule are defined according to the levels in the syslog module as below:

Critical
Warnings
Informational
Debugging

Default: Critical.

Command Mode: SMTP Receiver Rule Configuration Mode.

Usage Guide: When sending mail, it will be appointed a level according to the information severity. Only when the mail's severity level is the configured level or higher than it, this mail needs to be sent to the configured receiver in the rule. In sending mails, they will be filtered according to the level.

Example: Configure the level of SMTP receiver rule1 as debugging and then use the no command to recover it to be the default value of critical.

```
AC(config)#smtp
AC(config-smtp)#receiver rule 1
AC(config-smtp-rule)#receiver severity debugging
AC(config-smtp-rule)#no receiver severity
```

4.6 receiver time-range from <start-time> to <end-time> [monday| tuesday| wednesday| thursday| friday| saturday| sunday| weekend| weekday| everyday]

Command: receiver time-range from <start-time> to <end-time> [monday| tuesday| wednesday| thursday| friday| saturday| sunday| weekend| weekday| everyday]

no receiver time-range [monday| tuesday| wednesday| thursday| friday| saturday| sunday| weekend| weekday| everyday]

Function: Configure the time-range of receiving mails for the receiver in the current rule. Out of the time-range, AC will not send mails to receiver. The no command recovers to be default.

Parameters:

start-time	The start of the interval, the format is HH:MM and the range is 00:00~23:59.
end-time	The end of the interval, the format is HH:MM and the range is 00:00~23:59.
monday	Monday of each week
tuesday	Tuesday of each week
wednesday	Wednesday of each week
thursday	Thursday of each week
friday	Friday of each week
saturday	Saturday of each week
sunday	Sunday of each week
weekday	Monday to Friday
weekend	Saturday and Sunday
everyday	Monday to Sunday

Default: As default, the mails can be sent anytime. The parameters of start time and end time are both from 00:00 to 23:59; the parameter of everyday means the date.

Command Mode: SMTP Receiver Rule Configuration Mode.

Usage Guide: The device provides various forms of commands for user to configure the time-range of sending mails. When the third parameter is configured as everyday, the whole week will be configured as the time-range; weekday and weekend are used to configure the time-range as Monday to Friday and Saturday to Sunday; other options can be used to configure one day as the time-range. When AC sends mail, it will decide whether sends it to the receiver in the rule according to the time-range. When keeping the configuration, it will be according to the time-range of every day. The options of weekend, weekday and everyday can provide convenience to user but they will not be kept in the configuration. If 00:00~12:00 of the weekend is configured as the time-range of sending mails, the configuration keeping or the show command showing will show two configurations: 00:00~12:00 of Saturday and 00:00~12:00 of Sunday.

The last configuration can cover the forward configurations. If user configured the time-range as 00:00~12:00 of everyday and then configures 12:00~23:59 of Sunday again; the final time-range is 00:00~12:00 of Monday to Saturday and 12:00~23:59 of Sunday. The configuration of 12:00~23:59 of Sunday covered the current configuration of 00:00~12:00 of Sunday.

If the end-time is configured earlier than the start-time, the configuration will invalid, and AC will print the error information.

Example: Configure the time-range of the mails for SMTP receiver rule1 as 9:00~12:00 every day.

```
AC(config-smtp)#receiver rule 1
AC(config-smtp-rule)#receiver time-range from 9:00 to 12:00 everyday
```

4.7 smtp server (ipv4 <ipaddr>) [port <port-num>]

Command: smtp server (ipv4 <ipaddr>) [port <port-num>]

no smtp server

Function: Configure or update the address and port of the smtp severity; the no command deletes the configuration.

Parameters: <ipaddr>: It appoints the IPv4 address of smtp server and this IP address needs to be an effective unicast address.

<port-num>: It is optional and appoints the port which provides the smtp server, the default port is 25.

Default: The port configuration is optional. The default port is 25 and the default ip address is empty.

Command Mode: SMTP Configuration Mode.

Usage Guide: If the smtp server has not been created on AC, this command can be used to configure an SMTP server and create the connection between the server and the appointed server address and port. If the smtp server has been created on AC, this command can be used to update the configuration. If the parameters of ipaddr or port are changed, AC will interrupt the current connection and re-create the connection to the server, it will clear the authentication parameters at the same time. When using the no command, there will be the prompt that the smtp server has not been created and do nothing else if the smtp server does not exist. After deleted the smtp server, the smtp server configuration and parameters can be deleted. If the TCP connection between AC and SMTP server has existed, the connection will be interrupted and AC cannot send mails anymore.

Example: Configure (update) the smtp server address as 200.101.0.56 and configure the port as 30. And use the no command to delete this configuration. And then use the no command to delete the configuration again, there will be the prompt that the smtp server has not been created.

```
AC(config-smtp)#smtp server ipv4 200.101.0.56 port 30
AC(config-smtp)#no smtp server
AC(config-smtp)#no smtp server
The smtp server has not been created!
```

4.8 smtp sender address <email-addr>

Command: smtp sender address <email-addr>

no smtp sender address

Function: Appoint the sender. The no command deletes the sender.

Parameters: <email-addr> is the sender’s address and the length is not more than 64 characters, the format is like XXXX@domain.com. The detailed format is delimited in RFC2821 and RFC5321.

Default: None.

Command Mode: SMTP Configuration Mode.

Usage Guide: This command is used to appoint the sender. If there is a sender, the new one can replace it. In the next time to send mail, the new configured sender will be used to send mail. The no command deletes the configured sender’s address.

Example: Appoint the smtp sender as send@wifitest.com and then delete it.

```
AC(config)#smtp
AC(config-smtp)#smtp sender address send@wifitest.com
AC(config-smtp)#no smtp sender address
```

4.9 smtp server authentication username <username> password <password>

Command: smtp server authentication username <username> password <password>

no smtp server authentication

Function: Configure the authentication user name and password for smtp server. The no command recovers to be default.

Parameters: <username>: it is the user name for smtp server authentication; the length is not more than 64 characters. <password>: it is the password (laws) for smtp server authentication; the length is not more than 64 characters.

Default: The parameters are null.

Command Mode: SMTP Configuration Mode.

Usage Guide: AC is the smtp client. If it does not authenticate to smtp server, after the authentication parameters are configured, it will issue the authentication. If the AC has authenticated to smtp server, it needs to authenticate to the server again. The current connection should be cut before the re-authentication and AC should configure the TCP connection to the server. One TCP connection only allows once successful authentication.

Example: Configure the authentication user name and password for smtp server as test and 123 respectively. And then use the no command to recover them to be default (Null).

```
AC(config-smtp)#smtp server authentication username test password 123
AC(config-smtp)#no smtp server authentication
```

4.10 smtp server (source-ipv4 <ipaddr>)

Command: smtp server (source-ipv4 <ipaddr>)
no smtp server (source-ipv4)

Function: Appoint a source IP address for AC. AC will adopt this IP address as the source IP to create TCP connection to the server. The no command deletes the source IP address.

Parameters: <ipaddr>: it should be the ip address with an effective interface.

Default: None.

Command Mode: SMTP Configuration Mode.

Usage Guide: Some smtp servers can authorize one or more IP addresses, when sending mails to this server through those addresses, the authentication is not needed. The source IP can also appoint the outgoing interface. The packet can only get out from the layer3 interface, so we suggest configuring as lookback interface. Configuring, modifying or deleting the source IP address will make AC re-authenticate to the smtp server, the following mails all need the new connection for sending. If the configured IP address is the one of an invalid interface, AC cannot create TCP connection to smtp server; and the mail sending requirements in this interval will be ignored. The ipv4 and ipv6 addresses can coexist. When creating the TCP connection, AC can choose to use ipv4 or ipv6 address according to that the SMTP server’s address is ipv4 or ipv6.

Example: Appoint a source IP address for AC as 200.101.0.3.

```
AC(config-smtp)#smtp server source-ipv4 200.101.0.3
```

4.11 smtp test-mail-send

Command: smtp test-mail-send

Function: Test if the SMTP can send the mail to receiver successfully according to the current configuration. The theme and content of the mail are both “test”.

Parameters: None.

Default: None.

Command Mode: Admin Mode.

Usage Guide: After enabled this command, AC will send a test mail to SMTP server according to the current configuration, the theme and content of the mail are both “test”. And it will print the interactive information to the console. Then the network administrator can judge if there is problem in the current configuration and if the mail can be sent to the receiver normally.

Example: Test if the SMTP can send the mail to receiver successfully according to the current configuration.

```
AC(config)#smtp
AC(config-smtp)#smtp test-mail-send
```

4.12 show smtp status

Command: show smtp status

Function: Show the configuration of smtp.

Parameters: None.

Default: None.

Command Mode: Admin Mode.

Usage Guide: Show the configuration of smtp including smtp status, server address, port number, server connection status, sender’s address, source IP address of sender, server authentication user name and password.

Example: Show the configuration of smtp.

```
AC#show smtp status
Status ------------------------------------------- Enable
Ipv4 address ----------------------------------- 192.168.2.100
Port -------------------------------------------- 25
Server status ---------------------------------- Authenticated
Mail sender ----------------------------------- heloword@domain.com
Source ipv4 ---------------------------------- 192.168.1.1
```

```
Username ------------------------------------ abcdefg
Password ------------------------------------- 12345678
```

4.13 show smtp receiver rule [<rule-id>] status

Command: show smtp receiver rule [<rule-id>] status

Function: Show the configuration of smtp receiver rule.

Parameters: <rule-id>: the range is from 1 to 8 and it is the ID of the receiver rule.

Default: None.

Command Mode: Admin Mode.

Usage Guide: Show the configuration of smtp receiver rule. If the rule-id is appointed in the command, the detailed information of the rule will be shown; if the parameter is not appointed, only the profiles of all the rules will be shown including rule-id and description information.

Example: Configure the command of **show smtp receiver rule [<rule-id>] status** to show the following information:

A. The rule-id is not appointed, and the profiles of all the rules can be shown.

```
AC#show smtp receiver rule status
Rule ID          Description
------------      -----------------------------------
1                  everyday receiver rule
2                  weekday receiver rule
3                  weekend receiver rule
8                  emergencies receiver rule
```

B. The rule-id is appointed, and the detailed information of the rule can be shown.

```
AC#show smtp receiver rule 1 status
Rule ID --------------------------------- 1
Description ----------------------------- everyday receiver
Receiver email ------------------------- receiver1@domain.com
                                          receiver2@domain.com
                                          receiver3@domain.com
Time range ----------------------------- monday: 18:00~20:00
                                         sunday: 18:00~20:00
Severity --------------------------------- critical
```