

Content

Chapter 1 Commands for Local AP	1-1
1.1 ap authentication	1-1
1.2 ap database	1-1
1.3 ap validation.....	1-2
1.4 clear wireless ap failed.....	1-2
1.5 clear wireless ap failure list	1-2
1.6 location.....	1-3
1.7 management ip	1-3
1.8 mode	1-4
1.9 password plain.....	1-4
1.10 password encrypted	1-5
1.11 show wireless ap database	1-5
1.12 show wireless ap failure status	1-6
1.13 show wireless ap status.....	1-7
1.14 wireless ap debug.....	1-8
1.15 wireless ap eth-parameter apply	1-9
 Chapter 2 Commands for Enabling and Disabling Wireless	
Characteristic	2-1
2.1 auto-ip-assign	2-1
2.2 enable	2-1
2.3 show wireless	2-2
2.4 static-ip.....	2-3
2.5 statci-ipv6.....	2-4
2.6 wireless	2-4
2.7 ap authentication serial-num	2-5

Chapter 3 Commands for Automatical Discovery and Cluster

Creating	3-1
3.1 debug wireless discovery detail.....	3-1
3.2 debug wireless discovery packet.....	3-1
3.3 discovery ip-list	3-2
3.4 discovery ipv6-list	3-2
3.5 discovery method	3-3
3.6 discovery vlan-list	3-3
3.7 keep-alive-interval	3-3
3.8 keep-alive-max-count	3-4
3.9 peer-group.....	3-4
3.10 show wireless discovery.....	3-5
3.11 show wireless discovery ip-list	3-5
3.12 show wireless discovery vlan-list	3-6
3.13 show wireless peer-switch	3-6
3.14 show wireless peer-switch ap status.....	3-7

Chapter 4 Commands for Automatic Deployment and Duplex

Authentication	4-1
4.1 agetime ap-provisioning-db.....	4-1
4.2 clear wireless ap provisioning.....	4-1
4.3 debug wireless ap authentication detail.....	4-2
4.4 debug wireless ap authentication error.....	4-2
4.5 debug wireless ap fsm	4-2
4.6 debug wireless ap authentication packet.....	4-3
4.7 debug wireless mutual-authentication detail	4-3
4.8 debug wireless mutual-authentication error	4-4
4.9 debug wireless mutual-authentication packet	4-4

Commands for Wireless Cluster Management	Content
4.10 debug wireless provision detail	4-4
4.11 debug wireless provision error.....	4-5
4.12 debug wireless provision packet	4-5
4.13 mutual-authentication-mode.....	4-6
4.14 re-provisioning-unmanaged	4-6
4.15 show wireless ap provisioning status	4-7
4.16 show wireless switch provision status.....	4-7
4.17 switch-provisioning.....	4-8
4.18 wireless ap provision profile	4-9
4.19 wireless ap provision start.....	4-9
4.20 wireless ap provision switch	4-9
4.21 wireless certificate-generate	4-10
4.22 wireless cluster exchange-certificate	4-10
4.23 wireless switch certificate-request	4-11
4.24 wireless switch provision	4-11
Chapter 5 Commands for Automatic Cluster Election.....	5-1
5.1 cluster-priority	5-1
Chapter 6 Commands for Pushing Configuration	6-1
6.1 debug wireless peer-switch configure fsm	6-1
6.2 debug wireless peer-switch configure internal.....	6-1
6.3 debug wireless peer-switch configure packet	6-2
6.4 peer-switch configuration.....	6-2
6.5 show wireless configuration receive status.....	6-3
6.6 show wireless configuration request status	6-4
6.7 show wireless peer-switch configure status.....	6-4
6.8 show wireless peer-switch configuration.....	6-5
6.9 wireless peer-switch configure	6-6

Chapter 7 Commands for AP FLOOD Anti-attack 7-1

7.1 wireless ap anti-flood 7-1

7.2 wireless ap anti-flood interval <1-15> 7-1

7.3 wireless ap anti-flood max-conn-count <1-30> 7-2

7.4 wireless ap anti-flood agetime <0-1440> 7-2

7.5 show wireless ap anti-flood 7-2

7.6 show wireless ap anti-flood status 7-3

7.7 clear wireless ap anti-flood 7-3

Chapter 8 Commands for Cluster Maintaining and Debugging

..... 8-1

8.1 debug wireless cluster internal 8-1

8.2 debug wireless cluster packet 8-1

8.3 debug wireless ssl detail 8-2

8.4 debug wireless ssl error 8-2

8.5 debug wireless ssl internal 8-2

8.6 debug wireless ssl packet 8-3

8.7 debug wireless ssl timer 8-3

8.8 show wireless syslogflags 8-3

8.9 show wireless trapflags 8-4

8.10 snmp-server enable traps wireless 8-5

8.11 syslogflags 8-5

8.12 trapflags 8-6

Chapter 1 Commands for Local AP

1.1 ap authentication

Command: `ap authentication {noe | mac | pass-phrase}`

Function: Configure the authentication mode of AP.

Parameters: **none:** Authentication mode of register automatically.

mac: Authentication mode of mac address.

pass-phrase: Authentication mode of password.

Command Mode: Wireless Global Mode.

Default: The default authentication mode of AP is mac authentication.

Usage Guide: If none is chosen, ap database does not need to be added by manual operation on AC. As long as AC or AP can find opposite, they can join to the cluster. If mac is chosen, ap database should be added by manual operation to let AP join to the cluster. If pass-phrase is chosen, AP and AC must be through the Pass-PHRASE authentication to join to the cluster after they set up the connect of TLS.

Example: Configure the authentication mode as the automatic registration.

```
AC(config-wireless)#ap authentication none
```

1.2 ap database

Command: `ap database <macaddr>`

`no ap database <macaddr>`

Function: Add a log to the table of Valid AP and enter the configuration mode of AP. The no command deletes the appointed AP from the table of Valid AP.

Parameters: **<macaddr>**: the MAC address of AP.

Command Mode: Wireless Global Mode.

Default: None.

Usage Guide: Add AP appointed by macaddr to the table of Valid AP through this command and enter the configuration mode of AP. Under the configuration mode of AP, the parameter of the appointed AP can be reworked. If AP has been under the state of managed, AP should be replaced to make the configuration reworked be application.

Example: Add AP whose address is 00-03-0f-02-45-40 to the table of Valid AP.

```
AC(config-wireless)#ap database 00-03-0f-02-45-40
```

1.3 ap validation

Command: ap validation {local | radius}

Function: Designate the authentication for AP adopting local authentication or throughing the server of RADIUS.

Parameters: {local | radius}: the AP authentication mode which needs to be appointed; local: the local authentication; radius: the authentication through the server of RADIUS.

Command Mode: Wireless Global Mode.

Default: Local authentication.

Usage Guide: The default authentication mode is local authentication on AC. Rework the authentication mode to be the mode through the server of RADIUS by reworking the parameter of radius.

Example: Configure the authentication mode to be the mode through the server of RADIUS on AC.

```
AC(config-wireless)#ap validation radius
```

1.4 clear wireless ap failed

Command: clear wireless ap failed [<macaddr>]

Function: Delete the failing AP in the table of managed AP.

Parameters: <macaddr>: the MAC address of AP.

Command Mode: Admin Mode

Default: None.

Usage Guide: AP is not deleted from the table of Managed AP after it is failing in authentication. So it should be deleted through this command. If the parameter is input, the appointed log of AP will be deleted, otherwise all the failing log of AP will be deleted.

Example: Delete the AP whose MAC address is 00-03-0f-02-45-40 from the table of Managed AP.

```
AC#clear wireless ap failed 00-03-0f-02-45-40
```

1.5 clear wireless ap failure list

Command: clear wireless ap failure list

Function: Delete all the log of the failing AP in authentication on the local AC.

Parameters: None.

Command Mode: Admin Mode

Default: None.

Usage Guide: Through this command, all the log of the failing AP in authentication on the

AP Failure List of AC.

Example:

```
AC#clear wireless ap failure list
```

```
Are you sure you want to clear the entire AP failure list? (y/n)  y
```

```
All AP failure entries cleared.
```

1.6 location

Command: `location <value>`

`no location`

Function: Add the position description for AP. The no command deletes the current position information of AP.

Parameters: `<value>`: it is a character string with 32 characters at least. It does not include quotation mark, blank and other special characters.

Command Mode: AP Configuration Mode.

Default: No position description.

Usage Guide: After inputting the command of location, AC will save the position description of AP.

Example: Add the position description—"here" for the AP whose mac address is 00-03-0f-02-45-40.

```
AC(config-wireless)#ap database 00-03-0f-02-45-40
```

```
AC(config-ap)#location here
```

```
AC(config-ap)#exit
```

```
AC(config-wireless)#
```

1.7 management ip

Command: `management {ip A.B.C.D/M|ipv6 X:X::X:X/M}`

`no management {ip|ipv6}`

Function: Configure the management ip address of ap. The no command deletes this ip address.

Parameters: ip A.B.C.D/M is the ip address and mask of ipv4; ipv6 X:X::X:X/M is the ip address and prefix of ipv6.

Command Mode: AP Configuration Mode.

Default: None.

Usage Guide: When AP associated with AC, the management ip address of AP can be modified. Issue to be effective through `wireless ap eth-parameter apply <APMacaddr>` command.

Example : Configure the management ip address of ap with mac address of 00-03-0f-02-45-40 as 192.168.1.1.

```
AC(config-wireless)#ap database 00-03-0f-02-45-40
```

```
AC(config-ap)#management ip 192.168.1.1/24
```

```
AC #wireless ap eth-parameter apply 00-03-0f-02-45-40
```

1.8 mode

Command: mode {ws-managed | standalone | rogue}

Function: Configure the managed mode for AP.

Parameters: **ws-managed:** It is the mode of management which has been done; **standalone:** It is the independent mode; **rogue:** It is the illegal mode.

Command Mode: AP Configuration Mode.

Default: The default managed mode is ws-managed.

Usage Guide: The managed mode of AP can be reworked after AP is related to AC. AP should be restarted to make the configuration mode become effective after reworking the mode of AP. Through the command of **show wireless ap database**, all configuration of the managed mode of AP can be seen.

Example: Configure the managed mode of AP whose MAC address is 00-03-0f-02-45-40 as standalone.

```
AC(config-wireless)#ap database 00-03-0f-02-45-40
```

```
AC(config-ap)# mode standalone
```

AP mode has been changed. The change will not take effect until the AP is reset.

1.9 password plain

Command: password plain <word>
no password

Function: Configure the authentication password for the connection of AP and AC. The no command cancels the password configuration of AP on AC.

Parameters: <word> the configuration password, its length is 8 to 63 characters.

Command Mode: AP Configuration Mode.

Default: No password.

Usage Guide: User will be prompted to input a password after inputting the command of password. The password must make up of letters and numbers, the length is from 8 to 63. AC will encrypt the password character string and save the cryptograph after user inputting the password. This password can become effective only when AC enable the function of authentication.

Example: Configure the cleartext password for 00-03-0f-02-45-40 as qwertyui.

```
AC(config-wireless)#ap database 00-03-0f-02-45-40
```

```
AC(config-ap)#password plain qwertyui
```

1.10 password encrypted

Command: `password encrypted <word>`
`no password`

Function: Appoint a cryptography password for AP on AC. The no command cancel the password.

Parameters: `<word>`: cryptography password, its length is not more than 128 characters.

Command Mode: AP Configuration Mode.

Default: No cryptography password.

Usage Guide: The hexadecimal cryptography password character string can be configured for AP on AC through this command. Its length is not more than 128 characters.

Example : Configure the cryptography password for 00-03-0f-02-45-40 as 1234567890abcdef1234567890abcdef1234567890abcdef1234567890abcdef1234567890abcdef1234567890abcdef1234567890abcdef.

```
AC(config-wireless)#ap database 00-03-0f-02-45-40
```

```
AC(config-ap)#password encrypted  
1234567890abcdef1234567890abcdef1234567890abcdef1234567890abcdef1234567890abcdef1234567890abcdef
```

1.11 show wireless ap database

Command: `show wireless ap database [<macaddr>]`

Function: Show the particular information of Valid AP.

Parameters: `<macaddr>`: the MAC address of AP.

Command Mode: Admin Mode.

Default: None.

Usage Guide: If macaddr is appointed, the particular information of AP of the appointed MAC address will be shown; If macaddr is not appointed, all the particular information of Valid AP will be shown.

Example:

1. Show the information of the AP whose MAC address is 00-03-0f-56-32-80:

```
AC#show wireless ap database 00-03-0f-56-32-80
```

```
AP MAC Address..... 00-03-0f-56-32-80
Location..... net-30
AP Mode..... ws-managed
Password Configured..... No
Profile..... 1 - Default
Radio 1 Channel..... 6
Radio 1 Power..... Auto
```

2. Show all the particular information of Valid AP:

AC#show wireless ap database

MAC Address	Location	AP Mode
-----	-----	-----
00-03-0f-02-45-40	net-30	ws-managed
00-03-0f-04-01-00		ws-managed
00-03-0f-11-22-30		ws-managed

1.12 show wireless ap failure status

Command: show wireless ap [*<macaddr>*] failure status

Function: Show the the particular failing authentication information of AP on AC.

Parameters: *<macaddr>*: Appoint the MAC address of AP which should be shown.

Command Mode: Admin Mode.

Default: None.

Usage Guide:

1. If the parameter is input, show the information of the appointed AP. Otherwise show all the failing authentication information of AP.
2. If the AC which carries out this command is not AC Controller, show the failing authentication information of AP; If the AC is AC Controller, show the failing authentication information of AP of other AC, and the the failing authentication information of AP of the AC which is not local will have a asterisk^{“**”} to distinguish.

Example: Show the failing authentication information of AP whose MAC address is 00-03-0f-13-26-00.

AC#show wireless ap 00-03-0f-13-26-00 failure status

```
MAC address..... 00-03-0f-13-26-00
IP Address..... 192.168.1.100
```

```
Reporting Switch..... Local Switch
Switch MAC Address..... 00-03-0f-14-8f-6b
Switch IP Address..... 192.168.1.1
Last Failure Type..... No Database Entry
Validation Failure Count..... 5
Authentication Failure Count..... 0
Vendor ID..... Digital China (Shanghai) Network
Protocol Version..... 2
Software Version..... 0.0.0.19
Hardware Type..... 1 - DCWL-7952AP(R3), Indoor Single Radio a/b/g/n
Age..... 0d:00:00:23
```

1.13 show wireless ap status

Command: show wireless ap [*<macaddr>*] status

Function: Show the information of Managed AP.

Parameters: *<macaddr>*: the MAC address of AP.

Command Mode: Admin Mode.

Default: None.

Usage Guide: If the parameter is input, show the information of the appointed AP. Otherwise show all the information of Managed AP.

Example : Show the particular information of AP whose MAC address is 00-03-0f-13-26-00.

```
AC#show wireless ap 00-03-0f-13-26-00 status
```

```
MAC address..... 00-03-0f-13-26-00
Location.....
IP Address..... 192.168.1.100
IP Subnet Mask..... 255.255.255.0
Managing Switch..... Local Switch
Switch MAC Address..... 00-03-0f-14-8f-6b
Switch IP Address..... 192.168.1.1
Status..... Managed
Configuration Status..... Success
Last Failing Configuration Element..... None
Configuration Failure Error.....
Debug Mode..... Disable
Code Download Status..... Not Started
```

Reset Status..... Not Started
Profile..... 1 - Default
Vendor ID..... Cisco-Linksys, LLC
Protocol Version..... 2
Software Version..... 0.0.0.19
Hardware Type..... 1 - DCWL-7952AP(R3), Indoor Single Radio a/b/g/n
Serial Number..... E6WL0330B707000001
Discovery Reason..... L2 Poll Received
Authenticated Clients..... 0
L2 Tunnel Interface..... ----
System Up Time..... 0d:00:04:49
Age..... 0d:00:00:00
CPU Type..... CN5010p1.1-400-SCP
CPU Usage(5s)..... 2%
CPU Usage(30s)..... 14%
CPU Usage(5min)..... 7%
Memory Size Total(KB)..... 56580
Memory Size Used(KB)..... 40884

1.14 wireless ap debug

Command: `wireless ap debug <macaddr>`
`no wireless ap debug <macaddr>`

Function: Enable the debug mode on AC and configure a password for it. The no command disables the debug mode of the appointed AP.

Parameters: `<macaddr>`: the MAC address of AP.

Command Mode: Admin Mode.

Default: Disable.

Usage Guide: The debug mode of the appointed AP can be enabled and configure the password of telnet by this command. When the debug mode of AP is enabled, it is allowed to connect to the AP which is managed by AC for debugging through telnet. If AC Controller carries out this command and the appointed AP is not managed directly, the information of enabling the debug mode of AP is passed to the AC which manages the AP by AC Controller. Then the information is transmitted to the appointed AP by the relevant AC. When AP is discovered, the debug mode is invalidation and it must be enable over again.

Example: Enable the debug mode of AP whose MAC address is 00-03-0f-13-26-00.

AC#wireless ap debug 00-03-0f-13-26-00

1.15 wireless ap eth-parameter apply

Command: wireless ap eth-parameter apply [macaddr | profile<1-1024>]

Function: Issue the configuration parameter to the associated AP.

Parameters: <macaddr> is MAC address of AP; profile<1-1024> is AP profile ID.

Command Mode: Admin Mode.

Default: None.

Usage Guide: If the parameter is not input, this command issues the configuration parameter to all managed AP; if inputting macaddr, issue the configuration parameter to one managed ap; if inputting profile id, issue the configuration parameter to all APs associated with the profile.

Example : Configure the managed ip address of the ap with mac address of 00-03-0f-02-45-40 as 192.168.1.1

```
AC(config-wireless)#ap database 00-03-0f-02-45-40
```

```
AC(config-ap)#management ip 192.168.1.1/24
```

```
AC #wireless ap eth-parameter apply 00-03-0f-02-45-40
```

Chapter 2 Commands for Enabling and Disabling Wireless Characteristic

2.1 auto-ip-assign

Command: auto-ip-assign

no auto-ip-assign

Function: Appoint the IP address for the wireless function of AC automatically. The no command disables the function of automatic selection of the IP address.

Parameters: None.

Command Mode: Wireless Global Mode.

Default: Disable.

Usage Guide: When enable the function of automatic distribution of IP address of the wireless function, AC will appoint an IP address for the wireless module automatically. The gist of the selection of this IP address is: if there is loopback connector on AC, the IP address of the connector whose index number of loopback connector is the smallest should be chosen to be the wireless function address; If there is the layer 3 connector, the smallest IP address should be chosen to be the wireless function address. If the static IP address has bond to AC, the function of automatic selection does not rework the binding address.

Example:

```
AC(config-wireless)#auto-ip-assign
```

2.2 enable

Command: enable

no enable

Function: Enable the wireless characteristic on AC. The no command disables the wireless characteristic of AC.

Parameters: None.

Command Mode: Wireless Global Mode.

Default: Disable.

Usage Guide: The wireless function can be configured and used after enable the wireless characteristic of AC by this command.

Example:

```
AC(config-wireless)#enable
```

2.3 show wireless

Command: show wireless

Function: Show the wireless global configuration of AC.

Parameters: None.

Command Mode: Admin Mode.

Default: None.

Usage Guide: Achieve the wireless global configuration information of AC and show it through this command. The information shown includes the content below:

Field	Description
Administrative Mode	Show if the state of the global management mode enables.
WLAN Switch Operational Mode	Show if the wireless function of AC enables.
WS IP Address	Show the IP address of AC
WS Auto IP Assign Mode	Show if the automatic IP distribution mode of AC enables
WS Switch Static IP	Show the static IP address of AC
AP Authentication Mode	Show the authentication mode of the relationship of AP and AC
AP Auto Upgrade Mode	Show if the automatic removing mode of AP enables
AP Validation Method	Show if AP is accredited through local/radius database
Client Roam Timeout (Sec)	Show the overtime that client roam is authenticate again
Country Code	Show the country code of WLAN
Peer Group ID	Show Peer Group ID
Cluster Priority	Show the PRI that this machine participates in the cluster election
Cluster Controller	Show if this machine is Cluster Controller
Cluster Controller IP Address	Show the IP address of Cluster Controller
AP Client QoS Mode	Show if AP Client QoS enables
Switch Provisioning	Show if the function of automatic deployment of AC enables
Network Mutual Authentication Mode	Show if the function of both direction authentication enables
Unmanaged AP Re-provisioning	Show if the function of automatic deployment of

Mode	AP which is not managed enables
Network Mutual Authentication Status	Show the state of both direction authentication
Regenerate X.509 Certificate Status	Show the state of X.509 certificate that is created newly

Example: Show the wireless global configuration information.

AC#show wireless

```

Administrative Mode..... Enable
Operational Status..... Enabled
WS IP Address..... 192.168.1.1
WS Auto IP Assign Mode ..... Enable
WS Switch Static IP ..... 0.0.0.0
AP Authentication Mode..... mac
AP Auto Upgrade Mode..... Disable
AP Validation Method..... Local
Client Roam Timeout (secs)..... 30
Country Code..... CN - China
Peer Group ID..... 1
Cluster Priority..... 1
Cluster Controller..... Yes
Cluster Controller IP Address..... 192.168.1.1
Wireless System IP control port..... 57775
AP Client QoS Mode..... Disable
Switch Provisioning..... Enable
Network Mutual Authentication Mode..... Disable
Unmanaged AP Re-provisioning Mode..... Enable
Network Mutual Authentication Status..... Not Started
Regenerate X.509 Certificate Status..... Not In Progress
    
```

2.4 static-ip

Command: `static-ip <ipaddr>`

`no static-ip`

Function: Bind IP to the wireless characteristic of AC. The no command deletes the wireless characteristic IP address which is bond in static state.

Parameters: `<ipaddr>`: the IP address bond to the wireless characteristic

Command Mode: Wireless Global Mode

Default: The default IP address is 0.0.0.0.

Usage Guide: Make sure the bond IP is the same as the IP address of some loopback port or layer 3 port on AC when binding address to the wireless characteristic of AC in static state. Otherwise, the wireless characteristic will fail to enable. And disable the automatic choice function of IP address of AC through the **no auto-ip-assign** command.

Example: Bind the IP address of 10.1.1.5 to the wireless characteristic of AC.

```
AC(config-wireless)#static-ip 10.1.1.5
```

2.5 statci-ipv6

command: **static-ipv6** <ipv6addr>
no static-ipv6

Function: Bind the IPv6 address for the wireless property of AC. The no command deletes the static IPv6 address.

Parameters: <ipv6addr> is the IPv6 address bond for the wireless property.

Command Mode: Wireless Global Mode

Default: The default IPv6 address is ::0.

Usage Guide: When binding the address for the wireless property of AC with static method, ensure the IPv6 address is the same as the IPv6 address of one loopback interface or layer3 interface, otherwise, the wireless property will fail to enable. Use **no auto-ip-assign** command to disable the automatic IPv6 address selection function of AC.

Example: Bind the IPv6 address of 2001:1::5 for the wireless property of AC.

```
AC(config-wireless)#static-ip 2001:1::5
```

2.6 wireless

Command: **wireless**

Function: Enter the wireless global mode of AC.

Parameters: None.

Command Mode: Global Mode.

Default: The controller is not in the wireless global mode.

Usage Guide: Enter the wireless global mode of AC by this command. In this mode, the wireless function of AC can be configured.

Example: Enter the wireless global mode.

```
AC(config)#wireless
```

2.7 ap authentication serial-num

Command: ap authentication serial-num

Function: Configure the authentication method that AP connects to AC. There are mac, none, pass-phrase, serial-num currently. The method of serial-num means to authenticate based on the serial number of AP. This serial number is carried from factory, and it can be shown through using the command of **get system** under the console mode of AP.

Parameters: serial-num: it is the authentication method that AP connects to AC.

Command Mode: Wireless Global Mode.

Default: mac authentication.

Usage Guide: The default authentication method of AP is mac. If use the command of serial-num, it means that AP sends the serial number to AC when authenticating. AC finds the serial number of that AP in the configuration, if finds it, the authentication is successful, if it is not found or no matching, the authentication fails.

Example: Configure the authentication method between AC and AP as serial-num.

```
AC(config-wireless)# ap authentication serial-num
```

Chapter 3 Commands for Automatical Discovery and Cluster Creating

3.1 debug wireless discovery detail

Command: debug wireless discovery detail

no debug wireless discovery detail

Function: Open the particular debugging information discovered automatically. The no command disables the particular debugging information discovered automatically.

Parameters: None.

Command Mode: Admin Mode.

Default: None.

Usage Guide: The particular course discovered automatically can be inspected, debugged and diagnosed by this command.

Example: Enable the particular debugging information discovered automatically.

AC#debug wireless discovery detail

3.2 debug wireless discovery packet

Command: debug wireless discovery packet {all | receive | send | dump}

no debug wireless discovery packet {all | receive | send | dump}

Function: Enable the print debugging information of the automatically finding packets. The no command disables the information.

Parameters: **all:** Print the receiving and sending debugging information of all packets;

receive: Print the debug information of the receiving direction; **send:** Print the debug information of the sending direction; **dump:** Print the content of the packets.

Command Mode: Admin Mode.

Default: The debug function is disabled.

Usage Guide: The packets of the course discovered automatically can be inspected by this command, it is good at system debugging and diagnosing.

Example: Enable the function of debug and print the content of the packets.

AC#debug wireless discovery packet dump

3.3 discovery ip-list

Command: `discovery ip-list <ipaddr>`

`no discovery ip-list [<ipaddr>]`

Function: Add the new IP address to the IP address table that UDP found it automatically. The no command clears IP address in the table.

Parameters: `<ipaddr>`: the address of AP or AC which needs to be added to the IP address table.

Command Mode: Wireless Global Mode.

Default: The IP address table is empty.

Usage Guide: After adding a new IP address to the IP address table through this command, AC will send discovery message to the IP address in the table and does finding automatically for the relevant AP or AC when AC does finding automatically. The no command does not appoint the parameters and it deletes all the IP address in the IP address table discovered automatically. Otherwise, it deletes the appointed IP address.

Example : Add the IP address of 10.1.1.22 to the IP address table discovered automatically.

```
AC(config-wireless)#discovery ip-list 10.1.1.22
```

3.4 discovery ipv6-list

command: `discovery ipv6-list <ipv6addr>`

`no discovery ip-list [<ipaddr>]`

Function: Add the new IPv6 address to the IPv6 address table that UDP found it automatically. The no command clears IPv6 address in the table.

Parameters: `<ipv6addr>`: the address of AP or AC which needs to be added to the IPv6 address table.

Command Mode: Wireless Global Mode.

Default: The IPv6 address table is empty.

Usage Guide: After adding a new IPv6 address to the IPv6 address table through this command, AC will send discovery message to the IPv6 address in the table and does finding automatically for the relevant AP or AC when AC does finding automatically. The no command does not appoint the parameters and it deletes all the IPv6 address in the IPv6 address table discovered automatically. Otherwise, it deletes the appointed IPv6 address.

Example: Add the IPv6 address of 2001:1::22 to the IPv6 address table discovered automatically.

AC(config-wireless)#discovery ipv6-list 2001:1::22

3.5 discovery method

Command: `discovery method [ip-poll | I2-multicast]`
`no discovery method [ip-poll | I2-multicast]`

Function: Appoint the automatic discovery mode. The no command disables the function of automatic discovery.

Parameters: `ip-poll | I2-multicast`: the automatic discovery mode. ip-poll means doing automatic discovery by the IP address table; I2-multicast means doing layer 2 broadcast discovery.

Command Mode: Wireless Global Mode.

Default: The two functions of automatic discovery are enabled.

Usage Guide: If the parameters are not input, the two functions are enabled/disabled at the same time. Otherwise, enable/disable the appointed function.

Example: Enable the automatic discovery function of layer 2 on AC.

AC(config-wireless)#discovery method I2-multicast

3.6 discovery vlan-list

Command: `discovery vlan-list <1-4094>`
`no discovery vlan-list [<1-4094>]`

Function: Add a VLAN to the VLAN table discovered by layer 2 broadcast. The no command deletes the VLAN in the VLAN table discovered by layer 2 broadcast.

Parameters: `<1-4094>`: the VLAN ID discovered by layer 2 automatically, the range is 1 to 4094.

Command Mode: Wireless Global Mode.

Default: `discovery vlan-list` includes vlan 1 only.

Usage Guide: Add a VLAN to the VLAN table discovered by layer 2 broadcast by this command. When inputting the no command and appointing the parameter, the relevant VLAN will be delete from discovery vlan-list. Otherwise, all VLAN will be delete. The layer 2 broadcast discovery does not go along in the VLAN deleted from the vlan-list.

Example: Add vlan 100 to discovery vlan-list.

AC(config-wireless)#discovery vlan-list 100

3.7 keep-alive-interval

Command: `keep-alive-interval <5000-60000>`

Function: Configure the time interval of AC sending keep alive message.

Parameters: <5000-60000> is the keep-alive time interval input, unit is ms.

Command Mode: Wireless Global Mode.

Default: 10000.

Usage Guide: Configure the keep-alive time interval between AC or between AC and AP according to the actual situation. The interval can be flexible to be shortened or extended. After configured this command, it is effective in local and in the AP managed by it. It is effective in local immediately and it is effective on AP after the local AC sending keep-alive to AP next time. If the interval is configured too short, it can cause that AP dropped line or AP cannot be on-line. This is determined by the situation of AP.

Example: Configure the keep-alive time interval as 1 minute.

```
AC(config-wireless)#keep-alive-interval 60000
```

3.8 keep-alive-max-count

Command: `keep-alive-max-count<1-15>`

Function: Configure the maximum sending times of AC sending keep alive message.

Parameters: <1-15> is the maximum sending times of keep-alive.

Command Mode: Wireless Global Mode.

Default: 3.

Usage Guide: Configure the maximum keep-alive times. If there is still no response when the times has exceeded the maximum value, the keep-alive is failure.

Example: Configure the maximum keep-alive sending times as 2.

```
AC(config-wireless)# keep-alive-max-count 2
```

3.9 peer-group

Command: `peer-group <1-255>`

`no peer-group`

Function: Configure the cluster mark-Group ID for AC. The no command deletes the Group ID of AC.

Parameters: <1-255>: the value of Group ID, the range is 1 to 255.

Command Mode: Wireless Global Mode.

Default: The default Group ID of AC is 1.

Usage Guide: Configure the Group ID for AC by this command. The AC which have the same Group ID can make up a wireless cluster and the information can be transmitted between AC and AC. The AC have different Group ID can not communicate. When delete the Group ID of AC by the no command, the Group ID of AC will recover the default of 1.

Example: Configure the Group ID of 2 for AC.

```
AC(config-wireless)#peer-group 2
```

```
AC(config-wireless)#
```

3.10 show wireless discovery

Command: show wireless discovery

Function: Show the automatic discovery mode.

Parameters: None.

Command Mode: Admin Mode.

Default: None.

Usage Guide: By inputting this command, show the automatic discovery of IP and the discovery of layer 2 broadcast are enabled or not.

Example:

```
AC#show wireless discovery
```

```
IP Polling Mode.....Enabled
```

```
L2 Multicast Discovery Mode.....Enabled
```

3.11 show wireless discovery ip-list

Command: show wireless discovery ip-list

Function: Show all content of the IP address table which does the automatic discovery of AC.

Parameters: None.

Command Mode: Admin Mode.

Default: None.

Usage Guide: By inputting this command, show all IP address and their states (Not Polled、Unreachable、Discovered) of the IP address table which does the automatic discovery of AC.

Example:

```
AC#show wireless discovery ip-list
```

IP Address	Status
-----	-----
1.1.1.1	Not Polled

3.12 show wireless discovery vlan-list

Command: show wireless discovery vlan-list

Function: Show the VLAN ID which does the layer 2 broadcast discovery of AC.

Parameters: None.

Command Mode: Admin Mode.

Default: None.

Usage Guide: By inputting this command, show the VLAN's ID and names of layer 2 broadcast discovery.

Example:

```
AC#show wireless discovery vlan-list
```

```
VLAN List
```

```
-----
```

```
1 - default
```

3.13 show wireless peer-switch

Command: show wireless peer-switch [*<ipaddr>*]

Function: Show the information of the cluster member-AC.

Parameters: *<ipaddr>*: the Ipv4 address of AC.

Command Mode: Admin Mode.

Default: None.

Usage Guide: If the parameter is not appointed, show all the AC's information in the cluster; If the parameter is appointed, show the specific AC's information in the cluster.

Example:

1. Show the information of peer-switch whose IP address is 10.1.1.1:

```
AC#show wireless peer-switch 30.1.1.6
```

```
IP Address..... 30.1.1.6
Vendor ID..... Digital China (Shanghai) Network
Software Version..... 6.1.100.18
Protocol Version..... 2
Discovery Reason..... IP Poll
Managed AP Count..... 0
L2 Tunnel Interface..... ----
Age..... 0d:00:00:11
```

3.14 show wireless peer-switch ap status

Command: show wireless peer-switch [*<ipaddr>*] ap [*<macaddr>*] status

Function: Show the state information of the AP which has been managed in the cluster.

Parameters: *<ipaddr>*: the appointed Ipv4 address of AC; *<macaddr>*: the appointed MAC address of AC.

Command Mode: Admin Mode.

Default: None.

Usage Guide: If the parameters of *<ipaddr>* and *<macaddr>* are not appointed, show all AP which has been managed in the cluster; If the IP address of AC is appointed only, show all AP's information which is managed by this AC; If the MAC address is appointed only, show the information of this IP.

Example:

1. Show the state information of all AP which are managed:

AC(config)#show wireless peer-switch ap status

Peer Switch				
MAC Address	IP Address	Location	Profile	HwType
00-03-0f-02-45-40	200.1.1.3		1-Default	1

2. Show the state information of all AP which are managed and whose IP address is 200.1.1.3:

AC(config)#show wireless peer-switch 200.1.1.3 ap status

Peer Switch				
MAC Address	IP Address	Location	Profile	HwType
00-03-0f-02-45-40	200.1.1.3		1-Default	1

3. Show the state information of AP whose MAC address is 00-03-0f-02-45-40:

AC(config)#sho wireless peer-switch ap 00-03-0f-02-45-40 status

```
MAC address..... 00-03-0f-02-45-40
Peer Switch IP Address..... 200.1.1.3
IP Address..... 200.1.1.201
```

IP Subnet Mask..... 255.255.255.0
Location.....
Profile..... 1-Default
Hardware Type..... 1

Chapter 4 Commands for Automatic Deployment and Duplex Authentication

4.1 agetime ap-provisioning-db

Command: `agetime ap-provisioning-db <0-240>`
`no agetime ap-provisioning-db`

Function: Configure the ageing time for the record of AP Provisioning table. The `no` command recovers the ageing time to be default.

Parameters: `<0-240>`: the value of ageing time, the unit is an hour. 0 means that the record in AP Provisioning table is not ageing.

Command Mode: Wireless Global Mode.

Default: The default ageing time of AP Provisioning table is 72 hours.

Usage Guide: When configuring the ageing time, the record in the table will be timed. When the time is up to the ageing time, the record will be delete. When configuring the ageing time as 0, the record in the table will not be ageing and it can be deleted by administrator only.

Example: Configure the ageing time in AP Provisioning table as 24 hours.

```
AC(config-wireless)#agetime ap-provisioning-db 24
```

4.2 clear wireless ap provisioning

Command: `clear wireless ap provisioning [<macaddr>]`

Function: Delete the record of AP in AP Provisioning table.

Parameters: `<macaddr>`: the MAC address of AP.

Command Mode: Admin Mode.

Default: None.

Usage Guide: If the MAC address of AP is not appointed, delete all AP's record in AP Provisioning table; If the MAC address of AP is appointed, delete this AP's record in AP Provisioning table.

Example: Delete the record of AP in AP Provisioning table that its MAC address is 00-03-0f-13-26-00.

```
AC#clear wireless ap provisioning 00-03-0f-13-26-00
```

4.3 debug wireless ap authentication detail

Command: debug wireless ap authentication detail
no debug wireless ap authentication detail

Function: Enable the particular debugging information of AP authentication. The no command disables the information.

Parameters: None.

Command Mode: Admin Mode.

Default: The particular debugging information of AP authentication is disabled.

Usage Guide: Monitor the unusual circumstances in the procedure of AP authentication by this command. It is good at fault diagnosis.

Example: Enable the particular debugging information of AP authentication.

AC#debug wireless ap authentication detail

4.4 debug wireless ap authentication error

Command: debug wireless ap authentication error
no debug wireless ap authentication error

Function: Enable the anomalous debugging information of AP authentication. The no command disables the information.

Parameters: None.

Command Mode: Admin Mode.

Default: The anomalous debugging information of AP authentication is disabled.

Usage Guide: Monitor the unusual circumstances in the procedure of AP authentication by this command. It is good at fault diagnosis.

Example: Enable the anomalous debugging information of AP authentication.

AC#debug wireless ap authentication error

4.5 debug wireless ap fsm

Command: debug wireless ap fsm [*<macaddr>*]
no debug wireless ap fsm [*<macaddr>*]

Function: Enable the debugging information of AP's state. The no command disables the information.

Parameters: *<macaddr>*: the MAC address of AP.

Command Mode: Admin Mode.

Default: The debugging information of AP's state is disabled.

Usage Guide: Monitor the diversification of the AP's state by this command. It is good at debugging and troubleshooting. If inputting the parameter, enable the state debugging information of the appointed AP. Otherwise, enable the information of all AP.

Example: Enable the state debugging information of AP whose MAC address is 00-03-0f-13-26-00.

```
AC#debug wireless ap fsm 00-03-0f-13-26-00
```

4.6 debug wireless ap authentication packet

Command: `debug wireless ap authentication packet {all | receive | send | dump}`
`no debug wireless ap authentication packet {all | receive | send | dump}`

Function: Enable the packet printer information of AP authentication. The no command disables the information.

Parameters: **all:** Print all the debugging information of Pass-PHARSE authentication packets; **send:** Print the authentication packets information of Pass-PHARSE which are transmitted; **receive:** Print the authentication packets information of Pass-PHARSE which are received; **dump:** Print the detailed content of Pass-PHARSE authentication information.

Command Mode: Admin Mode.

Default: The printing information of AP authentication packets is disabled.

Usage Guide: Monitor the packets in the procedure of AP authentication by this command. It is good at system debugging and fault diagnosis.

Example: Enable the detailed printing information of AP authentication packets.

```
AC#debug wireless ap authentication packet dump
```

4.7 debug wireless mutual-authentication detail

Command: `debug wireless mutual-authentication detail`
`no debug wireless mutual-authentication detail`

Function: Enable the detailed debugging information of mutual authentication. The no command disables the detailed debugging information of mutual authentication.

Parameters: None.

Command Mode: Admin Mode.

Default: The detailed debugging information of mutual authentication is disabled as default.

Usage Guide: Monitor the unusual circumstances in the procedure of mutual authentication by this command. It is good at fault diagnosis.

Example: Enable the detailed debugging information of mutual authentication.

AC#debug wireless mutual-authentication detail

4.8 debug wireless mutual-authentication error

Command: debug wireless mutual-authentication error

no debug wireless mutual-authentication error

Function: Enable the unusual debugging information of mutual authentication. The no command disables the unusual debugging information of mutual authentication.

Parameters: None.

Command Mode: Admin Mode.

Default: The unusual debugging information of mutual authentication is disabled as default.

Usage Guide : Monitor the unusual circumstances in the procedure of mutual authentication by this command. It is good at fault diagnosis.

Example: Enable the unusual debugging information of mutual authentication.

AC#debug wireless mutual-authentication error

4.9 debug wireless mutual-authentication packet

Command: debug wireless mutual-authentication packet

no debug wireless mutual-authentication packet

Function: Enable the packet printing debugging information of mutual authentication. The no command disables the packet printing debugging information of mutual authentication.

Parameters: None.

Command Mode: Admin Mode.

Default: The packet printing debugging information of mutual authentication is disabled as default.

Usage Guide: Monitor the packets in the procedure of mutual authentication by this command. It is good at system debugging and fault diagnosis.

Example: Enable the packet printing debugging information of mutual authentication.

AC#debug wireless mutual-authentication packet

4.10 debug wireless provision detail

Command: debug wireless provision detail

no debug wireless provision detail

Function: Enable the detailed debugging information of automatic disposition. The no

command disables the detailed debugging information of automatic disposition.

Parameters: None.

Command Mode: Admin Mode.

Default: The detailed debugging information of automatic disposition is disabled as default.

Usage Guide: Monitor the detailed procedure of mutual authentication by this command. It is good at system debugging and fault diagnosis.

Example:

```
AC#debug wireless provision detail
```

4.11 debug wireless provision error

Command: `debug wireless provision error`

`no debug wireless provision error`

Function: Enable the unusual information printing function of automatic disposition. The no command disables the unusual information printing function of automatic disposition.

Parameters: None.

Command Mode: Admin Mode.

Default: The unusual information printing function of automatic disposition is disabled as default.

Usage Guide: Monitor the unusual circumstances in the procedure of automatic disposition by this command. It is good at fault diagnosis.

Example: Enable the unusual information printing function of automatic disposition

```
AC#debug wireless provision error
```

4.12 debug wireless provision packet

Command: `debug wireless provision packet {all | receive | send | dump}`

`no debug wireless provision packet {all | receive | send | dump}`

Function: Enable the printing debugging information of automatic disposition. The no command disables the printing debugging information of automatic disposition.

Parameters: **all:** output all private information data of automatic disposition; **send:** print debug information which is at the direction of transmitting; **receive:** print debug information which is at the direction of receiving; **dump:** print the detailed content of the automatic disposition information.

Command Mode: Admin Mode.

Default: The printing debugging information of automatic disposition is disabled as default.

Usage Guide: Monitor the packets in the procedure of automatic disposition by this command. It is good at system debugging and fault diagnosis.

Example: Enable the debug switch of automatic disposition packets and print the detailed content of the automatic disposition information:

```
AC#debug wireless provision packet dump
```

4.13 mutual-authentication-mode

Command: `mutual-authentication-mode`
`no mutual-authentication-mode`

Function: Enable the mutual authentication function in the whole cluster. The `no` command disables the mutual authentication function in the whole cluster.

Parameters: None.

Command Mode: Wireless Global Mode.

Default: The mutual authentication function in the whole cluster is disabled as default.

Usage Guide: Enabling/disabling the mutual authentication function through this command is effective in the whole cluster. After enabling the mutual authentication function, AP and AC need to save the X.509 authentication to NVRAM. Creating the TLS connection between AP and AC should pass the mutual authentication.

Example: Enable the mutual authentication function in the whole cluster.

```
AC(config-wireless)#mutual-authentication-mode
```

4.14 re-provisioning-unmanaged

Command: `re-provisioning-unmanaged`
`no re-provisioning-unmanaged`

Function: Dispose AP which is at the state of unmanaging automatically. The `no` command cancels the automatic disposition.

Parameters: None.

Command Mode: Wireless Global Mode.

Default: The function of disposing AP which is at the state of unmanaging automatically is enabling as default.

Usage Guide: This command is effective only when enabling the function of mutual authentication. After enabling this command, it will be effective in the whole cluster and every AC will save this configuration. When enabling the function of disposing AP which is at the state of unmanaging automatically, the AP which is at the state of unmanaging begins to launch the automatic discovery to the AC which does the automatic disposition to it.

Example: Dispose AP which is at the state of unmanaging automatically.

AC(config-wireless)#re-provisioning-unmanaged

4.15 show wireless ap provisioning status

Command: show wireless ap provisioning [*<macaddr>*] status

Function: Show the disposition information of AP in the AP Provisioning table.

Parameters: *<macaddr>* is the MAC address of AP.

Command Mode: Admin Mode.

Default: None.

Usage Guide: If the MAC address of AP is not appointed, show the disposition information of all AP in the AP Provisioning table; If the MAC address of AP is appointed, show the disposition information of this AP in the AP Provisioning table.

Example : Show the disposition information of AP whose MAC address is 00-03-0f-13-26-00 in the AP Provisioning table:

AC#show wireless ap 00-03-0f-13-26-00 provisioning status

```
MAC address..... 00-03-0f-13-26-00
AP IP Address..... 192.168.1.100
Primary Switch IP..... 0.0.0.0
Backup Switch IP..... 0.0.0.0
Mutual Authentication Mode..... Disabled
Unmanaged AP Re-provisioning Mode..... Disabled
New Primary Switch IP..... 0.0.0.0
New Backup Switch IP..... 0.0.0.0
New Profile ID..... 1 - Default
AP Provisioning Status..... Not Started
AP Profile and Certificate Tx. Status..... Not Started
Time Since Last Update..... 0d:00:00:01
```

4.16 show wireless switch provision status

Command: show wireless switch provision status

Function: Examine the current state of automatic disposition of this switch's AC.

Parameters: None.

Command Mode: Admin Mode.

Default: None.

Usage Guide: After inputting this command, it will show the each other's IP address and

the current state of AC disposition. The states of current disposition are the following:

Provisioning Status	Explanation
Not Started	It is the initial state. It means AC does not begin the automatic disposition.
Requested	It begins the automatic disposition and has launched the requisition of TLS connection to each other.
Certificate Requested	It begins the automatic disposition and has launched the information of Switch Provision Data.
In Progress	It means doing the local processing.
Failed	This time of automatic disposition of AC is failing to the end.
Success	It means this time of automatic disposition of AC is succeeding to the end.
None	It means the state is unusual.

Example: Examine the current state of automatic disposition of this switch's AC.

AC#show wireless switch provision status

```
Provisioning Switch Ip Address.....10.1.1.3
Provisioning Status..... Failed
```

4.17 switch-provisioning

Command: `switch-provisioning`

`no switch-provisioning`

Function: Enable the function of automatic disposition of this switch. The no command disables the function of automatic disposition.

Parameters: None.

Command Mode: Wireless Global Mode.

Default: The function of automatic disposition is enabling as default.

Usage Guide: After enabling/disabling the function of automatic disposition, users can examine switch provisioning that it is enable/disable through show wireless.

Example: Enable the function of automatic disposition of this switch.

AC(config-wireless)#switch-provisioning

4.18 wireless ap provision profile

Command: wireless ap provision <macaddr> profile <1-1024>
no wireless ap provision <macaddr> profile

Function: Appoint profile ID for AP and it becomes effective when disposing automatically. The no command cancels the appointed effective profile ID.

Parameters: <macaddr> is the MAC address of AP; <1-1024> is ID of AP Profile.

Command Mode: Admin Mode.

Default: The profile ID appointed to AP for disposition is 1 as default.

Usage Guide: Appoint the profile ID for the deployed AP through this command, the profile ID will be effective after deploying. Notice: if the deployed AP has been added to the AP database, the profile ID configured in AP database will be used in priority; if the profile ID is not configured in AP database, use the default value of 1. If the deployed AP was not added to AP database and the profile ID was not configured, the effective AP profile ID after the deployment is 1.

Example: Appoint the effective AP Profile ID in disposition as 2 for the AP whose MAC address is 00-00-00-11-22-33.

```
AC#wireless ap provision 00-00-00-11-22-33 profile 2
```

4.19 wireless ap provision start

Command: wireless ap provision start

Function: Begin the automatic disposition of AP on AC Controller.

Parameters: None.

Command Mode: Admin Mode.

Default: It does not carry on the automatic disposition of AP on AC.

Usage Guide: After inputting this command, AC Controller begins to dispose one by one automatically to every AP in AP Provisioning table.

Example: Begin the automatic disposition of AP on AC Controller.

```
AC#wireless ap provision start
```

4.20 wireless ap provision switch

Command : wireless ap provision <macaddr> switch {backup | primary}
{<ipaddr>|<ipv6addr>}

Function: Configure primary and backup AC for AP of automatic disposition.

Parameters: <macaddr>: Appoint the MAC address for AP; <ipaddr>: Appoint the IPv4

address for AC; **<ipv6addr>**: Appoint the IPv6 address for AC..

Command Mode: Admin Mode.

Default: The default IPv4 address of AC is 0.0.0.0 and the default IPv6 address is::0.

Usage Guide: The primary/backup AC configured by this command will be saved to AP Provisioning table.

Example: Configure the primary AC of AP 00-00-00-11-22-33 as 10.1.1.1 and it is 10.1.1.2 for backup AC.

```
AC#wireless ap provision 00-00-00-11-22-33 switch primary 10.1.1.1
```

```
AC#wireless ap provision 00-00-00-11-22-33 switch backup 10.1.1.2
```

4.21 wireless certificate-generate

Command: wireless certificate-generate

Function: Generate X.509 certificate on AC.

Parameters: None.

Command Mode: Admin Mode.

Default: The X.509 certificate exists on AC as default.

Usage Guide: After inputting this command, it will generate the X.509 certificate file of wssl2_cert.pem and the private key file of wssl2_key.pem on AC.

Example: Generate the X.509 certificate on AC.

```
AC#wireless certificate-generate
```

4.22 wireless cluster exchange-certificate

Command: wireless cluster exchange-certificate

Function: Initialize the switch trigger of the X.509 certificate.

Parameters: None.

Command Mode: Admin Mode.

Default: AC does not initialize the switch trigger of the X.509 certificate as default.

Usage Guide: After inputting this command, the switch trigger of X.509 certificate of AC will be initialized. When creating the TLS connection, AC will be certificated with the opposite device of X.509 certificate. This command is effective when enabling the two-way authentication function only.

Example: Initialize the switch trigger of the X.509 certificate.

```
AC#wireless cluster exchange-certificate
```

4.23 wireless switch certificate-request

Command: wireless switch certificate-request {<ipaddr>|<ipv6addr>}

Function: Let AC request the X.509 authentication before AC deploying automatically.

Parameters: <ipaddr> is IPv4 address of the opposite AC; <ipv6addr> is IPv6 address of the opposite AC.

Command Mode: Admin Mode.

Default: AC will not send the requisition of X.509 authentication to the opposite AC.

Usage Guide: After inputting this command, AC will send the requisition of X.509 authentication to the opposite AC appointed by <ipaddr>/<ipv6addr> before AC deploying automatically.

Example: AC sends the requisition of X.509 authentication to the AC whose IP address is 10.1.1.22.

```
AC#wireless switch certificate-request 10.1.1.22
```

4.24 wireless switch provision

Command: wireless switch provision <ip address>

Function: The local AC begins to deploy with the appointed AC automatically. When it succeeded, it will join to the cluster that the other side is in.

Parameters: <ip address> is the IPv4 address of the object deployed automatically.

Command Mode: Admin Mode.

Default: None.

Usage Guide: After inputting this command, the local AC will deploy with the AC appointed by <ip address> automatically. After deploying successfully, the local AC will join to the cluster that the other side is in. At this time, the local AC will create TLS connection with every AC in that cluster.

Example: Let the local AC begin to deploy with the AC whose IP address is 10.1.1.3 automatically.

```
AC#wireless switch provision 10.1.1.3
```

Chapter 5 Commands for Automatic Cluster Election

5.1 cluster-priority

Command: `cluster-priority <0-255>`

`no cluster-priority`

Function: Appoint the priority of electing AC Controller in the cluster for AC. The `no` command recovers the priority of AC to the default value.

Parameters: `<0-255>` is the election priority, the range is 0 to 255.

Command Mode: Wireless Global Mode.

Default: The priority of AC is 1 as default.

Usage Guide: The larger the value of priority is, the higher the priority of AC is. After changing the priority of one AC in the cluster, it will touch off once new election of AC Controller.

Example: Modify the priority of this AC to 5.

```
AC(config-wireless)#cluster-priority 5
```

Chapter 6 Commands for Pushing Configuration

6.1 debug wireless peer-switch configure fsm

Command: debug wireless peer-switch configure fsm

no debug wireless peer-switch configure fsm

Function: Enable the debugging information of the pushing switch configuration. The no command disables the information.

Parameters: None.

Command Mode: Admin Mode.

Default: The debugging information of the pushing switch configuration is disabled as default.

Usage Guide: By configuring this command can monitor the pushing switch. It is good at debugging and fault diagnosis.

Example: Enable the debugging information of the pushing switch configuration.

```
AC#debug wireless peer-switch configure fsm
```

6.2 debug wireless peer-switch configure internal

Command: debug wireless peer-switch configure internal

no debug wireless peer-switch configure internal

Function: Enable the general debugging information of pushing configuration. The no command disables the information.

Parameters: None.

Command Mode: Admin Mode.

Default: The general debugging information of pushing configuration is disabled as default.

Usage Guide: By configuring this command can examine the general debugging information of pushing configuration. It is good at debugging and fault diagnosis.

Example: Enable the general debugging information of pushing configuration.

```
AC#debug wireless peer-switch configure internal
```

6.3 debug wireless peer-switch configure packet

Command: debug wireless peer-switch configure packet {all | receive | send | dump}

no debug wireless peer-switch configure packet {all | receive | send | dump}

Function: Enable the debugging information of configuration pushing packets. The no command disables the information.

Parameters: **all:** Print the debugging information of all configuration pushing packets; **send:** Print the information of the configuration pushing packets which need to be send; **receive:** Print the information of the configuration pushing packets received only; **dump:** Print the detailed information of the configuration pushing packets.

Command Mode: Admin Mode.

Default: The debugging information of configuration pushing packets is disabled as default.

Usage Guide: By configuring this command can monitor the configuration pushing packets. It is good at system debugging and fault diagnosis.

Example: Enable the debugging information of configuration pushing packets and examine the information of the sending packet.

```
AC#debug wireless peer-switch configure packet send
```

6.4 peer-switch configuration

Command: peer-switch configuration [ap-database | ap-profile | captive-portal | channel-power | device-location | discovery | global | known-client | qos-acl | qos-diffserv | radius-client | wds-group]

no peer-switch configuration [ap-database | ap-profile | captive-portal | channel-power | device-location | discovery | global | known-client | qos-acl | qos-diffserv | radius-client | wds-group]

Function: Configure the pushing transmission for AC. The no command configures the pushing no transmission.

Parameters: **ap-database:** Transmit the AP data local managed when pushing;

ap-profile: Transmit the AP Profile local saved when pushing;

captive-portal: Transmit the Captive Portal data when pushing;

channel-power: Transmit the channel and power local configured and so on when pushing;

- device-location:** Transmit the device-location data when pushing;
- discovery:** Transmit the local automatical discovery data when pushing;
- global:** Transmit the global configuration data local saved when pushing;
- known-client:** Transmit the client data local saved when pushing;
- qos-acl:** Transmit the qos-acl data when pushing;
- qos-diffserv:** Transmit the qos-diffserv data when pushing;
- radius-client:** Transmit the client data certificated by Radius when pushing.
- wds-group:** Transmit the WDS Group data when pushing;

Command Mode: Wireless Global Mode.

Default: All the configuration will be transmitted or all of them will not be transmitted as default.

Usage Guide: If the parameters are not input, all the configuration will be transmitted by AC when configuring pushing. Otherwise, AC will only transmit the appointed configuration when pushing. The no command is similar.

Example: Configure AC to transmit ap-database configuration when pushing.

```
AC(config-wireless)#peer-switch configuration ap-database
```

6.5 show wireless configuration receive status

Command: show wireless configuration receive status

Function: This command is used to show the state information of configuration pushing for the receiver.

Parameters: None.

Command Mode: Admin Mode.

Default: None.

Usage Guide: Input this command on the receiver AC when configuring pushing, it will show the state information of configuration pushing.

Example: show the state information of configuration pushing for the receiver.

```
AC#show wireless configuration receive status
```

```
Configuration Receive Status..... Success
```

```
Last Configuration Received
```

```
-----
```

```
Peer Switch IP Address..... 30.1.1.2
```

```
Configuration..... AP Database
```

```
AP Profile
```

```
Channel Power
```

Global
Known Client
Captive Portal
QoS ACL
QoS DiffServ

Timestamp..... JAN 01 09:09:42 2006

6.6 show wireless configuration request status

Command: show wireless configuration request status

Function: Configure the pushing sender to show the global state of configuration pushing and show the state information of every AC participated the configuration pushing.

Parameters: None.

Command Mode: Admin Mode.

Default: None.

Usage Guide: After inputting this command, AC will pick up the global state of configuration pushing and the state information of every AC participated the configuration pushing from configuration database and show them.

Example: Configure the pushing sender to show the global state of configuration pushing and show the state information of every AC participated the configuration pushing.

AC#show wireless configuration request status

```
Configuration Request Status..... Complete
Total Count..... 2
Success Count..... 2
Failure Count..... 0
Peer IP Address      Configuration Request Status
-----
30.1.1.6             Success
200.1.1.3            Success
```

6.7 show wireless peer-switch configure status

Command: show wireless peer-switch [*<ipaddr>*] configure status

Function: Show the state information of cluster configuration pushing.

Parameters: *<ipaddr>* is IPv4 address of AC.

Command Mode: Admin Mode.

Default: None.

Usage Guide: *<ipaddr>* is the optional parameter. If the parameter is not input, show the state information of configuration pushing of all AC in the cluster; if the parameter is input, show the information of configuration pushing of the appointed AC.

Example: Show the state information of configuration pushing of the AC whose IP address is 30.1.1.6.

AC#show wireless peer-switch 30.1.1.6 configure status

```
Peer Switch IP Address..... 30.1.1.6
Configuration Switch IP Address..... 30.1.1.2
Configuration Status..... Success
Configuration..... AP Database
                                AP Profile
                                Channel Power
                                Global
                                Known Client
                                Captive Portal
                                QoS ACL
                                QoS DiffServ
Timestamp..... JAN 01 00:10:54 2006
```

6.8 show wireless peer-switch configuration

Command: show wireless peer-switch configuration

Function: Show the data which is synchronous with AC when configuring pushing.

Parameters: None.

Command Mode: Admin Mode.

Default: None.

Usage Guide: Inputting this command will show the data which is synchronous with AC when configuring pushing. These data include AP data, AP Profile data, Channel Power data, automatical discovery configuration data, global configuration data, Know Client data, Captive Portal data, Radius Client data, QoS ACL data and QoS DiffServ data.

Example: Show the data which is synchronous with AC when configuring pushing.

AC#show wireless peer-switch configuration

```
AP Database..... Enable
AP Profile..... Enable
Channel Power..... Enable
Discovery..... Disable
```

Global.....	Enable
Know Client.....	Enable
Captive Portal.....	Enable
RADIUS Client.....	Enable
QoS ACL.....	Enable
QoS DiffServ.....	Enable

6.9 wireless peer-switch configure

Command: wireless peer-switch configure [*<ipaddr>*|*<ipv6addr>*]

Function: Configure pushing for the AC in the cluster.

Parameters: *<ipaddr>* is IPv4 address of other AC in the cluster; *<ipv6addr>* is IPv6 address of other AC in the cluster.

Command Mode: Admin Mode.

Default: Do not configure pushing for the other AC in the cluster as default.

Usage Guide: If the parameter of ipaddr/ipv6addr is not input, configure pushing for all AC in the cluster as default; if the parameter of ipaddr/ipv6addr is input, configure pushing for the AC which is appointed by ipaddr/ipv6addr.

Example: Configure pushing for the AC whose IP address is 100.1.1.120.

AC#wireless peer-switch configure 100.1.1.120

Chapter 7 Commands for AP FLOOD Anti-attack

7.1 wireless ap anti-flood

Command: wireless ap anti-flood

no wireless ap anti-flood

Function: Enable the AP FLOOD anti-attack function. The no command disables this function.

Parameters: None.

Command Mode: Wireless Global Mode.

Default: Enable the AP FLOOD anti-attack function.

Usage Guide: Enable the AP FLOOD anti-attack function through this command. When the TCP connection times of AP with AC are detected exceeding the restriction, make the AP join in the AP FLOOD table to prevent this AP's flooding attack.

Example: Enable the AP FLOOD anti-attack function.

```
AC(config-wireless)# wireless ap anti-flood
```

7.2 wireless ap anti-flood interval <1-15>

Command: wireless ap anti-flood interval <1-15>

no wireless ap anti-flood interval

Function: Configure the detection time of AP FLOOD anti-attack function. The no command recovers it to be the default.

Parameters: <1-15>: detection time, the unit is minute, and 15 minutes are the most.

Command Mode: Wireless Global Mode.

Default: 5 minutes.

Usage Guide: This command is used to configure the detection time of AP FLOOD anti-attack function. In this time, if the connection times are detected as the maximum value, make this AP join in the AP FLOOD anti-attack table.

Example: Configure the detection time of AP FLOOD anti-attack function as 10 minutes.

```
AC(config-wireless)# wireless ap anti-flood interval 10
```

7.3 wireless ap anti-flood max-conn-count <1-30>

Command: wireless ap anti-flood max-conn-count <1-30>

no wireless ap anti-flood max-conn-count

Function: Configure the maximum times of the allowed connection by AP FLOOD anti-attack function. The no command recovers it to be the default.

Parameters: <1-30>: the allowed connection times, the unit is time, and 30 times are most.

Command Mode: Wireless Global Mode.

Default: 4 times.

Usage Guide: This command is used to configure the maximum times of the allowed connection by AP FLOOD anti-attack function. In this detection time, if the connection times are detected as the configured number, make the AP join in the AP FLOOD anti-attack table.

Example: Configure the maximum times of the allowed connection by AP FLOOD anti-attack function as 5.

```
AC(config-wireless)# wireless ap anti-flood max-conn-count 5
```

7.4 wireless ap anti-flood agetime <0-1440>

Command: wireless ap anti-flood agetime <0-1440>

no wireless ap anti-flood agetime

Function: Configure the aging time of the AP FLOOD anti-attack table. The no command recovers it to be the default.

Parameters: <0-1440>: the aging time, the unit is minute and 0 means no aging.

Command Mode: Wireless Global Mode.

Default: 30 minutes.

Usage Guide: This command is used to configure the aging time of the AP FLOOD anti-attack table. The AP is joined in the anti-attack table, it will be deleted after the end of the aging time and it will be allowed to connect to AC.

Example: Configure the aging time of the AP FLOOD anti-attack table as 60 minutes.

```
AC(config-wireless)# wireless ap anti-flood agetime 60
```

7.5 show wireless ap anti-flood

Command: show wireless ap anti-flood

Function: Show the current configuration parameters of the AP FLOOD anti-attack.

Parameters: None.

Command Mode: Admin Mode.

Default: None.

Usage Guide: Show the current configuration parameters of the AP FLOOD anti-attack through this command.

Example: Show the current configuration parameters of the AP FLOOD anti-attack.

```
AC# show wireless ap anti-flood
Operational Status..... Enable
Total Flood Aps..... 0
Detected Interval..... 10
Allowed Max Connect Count..... 5
Age Time..... 60
```

7.6 show wireless ap anti-flood status

Command: show wireless ap anti-flood status

Function: Show all the records in the AP FLOOD anti-attack table.

Parameters: None.

Command Mode: Admin Mode.

Default: None.

Usage Guide: Show all the records in the AP FLOOD anti-attack table through this command.

Example: Show all the records in the current AP FLOOD anti-attack table.

```
AC# show wireless ap anti-flood
MAC Address      Agetime
-----
00-03-0f-cc-cf-20  0d:00:30:33
```

7.7 clear wireless ap anti-flood

Command: clear wireless ap anti-flood

Function: Clear all the records in the AP FLOOD anti-attack table.

Parameters: None.

Command Mode: Admin Mode.

Default: None.

Usage Guide: Clear all the records in the AP FLOOD anti-attack table through this command.

Example: Clear all the records in the current AP FLOOD anti-attack table.

AC# clear wireless ap anti-flood

Are you sure you want to clear the AP flood list? [Y/N]Y

All AP flood entries cleared.

Chapter 8 Commands for Cluster Maintaining and Debugging

8.1 debug wireless cluster internal

Command: debug wireless cluster internal

no debug wireless cluster internal

Function: Enable the general debugging information of information collection and cluster controlling. The no command disables the general debugging information.

Parameters: None.

Command Mode: Admin Mode.

Default : The general debugging information of information collection and cluster controlling is disabled as default.

Usage Guide: Monitor the general debugging information of information collection and cluster controlling by this command. It is good at system debugging and fault diagnosis.

Example: Enable the general debugging information of information collection and cluster controlling.

```
AC#debug wireless cluster internal
```

8.2 debug wireless cluster packet

Command: debug wireless cluster packet {all | receive | send | dump}

no debug wireless cluster packet {all | receive | send | dump}

Function: Enable the packets printing debugging information of information collection and cluster controlling. The no command disables the information.

Parameters: **all:** Print the debugging information of all packets; **send:** Print the packets information which need to be sent only; **receive:** Print the packets information which are received only; **dump:** Print the detailed content of cluster management information.

Command Mode: Admin Mode.

Default: The packets printing debugging information of information collection and cluster controlling is disabled as default.

Usage Guide: Monitor the packets of information collection and cluster controlling on AC by this command. It is good at system debugging and fault diagnosis.

Example: Enable the packets printing debugging information of information collection and cluster controlling of all AC.

```
AC#debug wireless cluster packet all
```

8.3 debug wireless ssl detail

Command: `debug wireless ssl detail`
`no debug wireless ssl detail`

Function: Enable the detailed debugging information of SSL. The no command disables the information.

Parameters: None.

Command Mode: Admin Mode.

Default: The detailed debugging information of SSL is disabled as default.

Usage Guide: Monitor the detailed debugging information of SSL by this command. It is good at system debugging and fault diagnosis.

Example: Enable the detailed debugging information of SSL.

AC#debug wireless ssl detail

8.4 debug wireless ssl error

Command: `debug wireless ssl error`
`no debug wireless ssl error`

Function: Enable the anomalous debugging information of SSL. The no command disables the information.

Parameters: None.

Command Mode: Admin Mode.

Default: The anomalous debugging information of SSL is disabled as default.

Usage Guide: Monitor the anomalous debugging information of SSL by this command. It is good at fault diagnosis.

Example: Enable the anomalous debugging information of SSL.

AC#debug wireless ssl error

8.5 debug wireless ssl internal

Command: `debug wireless ssl internal`
`no debug wireless ssl internal`

Function: Enable the normal debugging information of SSL. The no command disables the information.

Parameters: None.

Command Mode: Admin Mode.

Default: The normal debugging information of SSL is disabled as default.

Usage Guide: Monitor the normal debugging information of SSL by this command. It is good at system debugging and fault diagnosis.

Example: Enable the normal debugging information of SSL.

```
AC#debug wireless ssl internal
```

8.6 debug wireless ssl packet

Command: `debug wireless ssl packet {all | receive | send}`

`no debug wireless ssl packet {all | receive | send}`

Function: Enable the packets printing debugging information of SSL. The no command disables the information.

Parameters: None.

Command Mode: Admin Mode.

Default: The packets printing debugging information of SSL is disabled as default.

Usage Guide: Monitor the packets information of SSL by this command. It is good at system debugging and fault diagnosis.

Example: Enable the packets printing debugging information of SSL.

```
AC#debug wireless ssl packet receive
```

8.7 debug wireless ssl timer

Command: `debug wireless ssl timer`

`no debug wireless ssl timer`

Function: Enable the timer debugging information of SSL. The no command disables the information.

Parameters: None.

Command Mode: Admin Mode.

Default: The timer debugging information of SSL is disabled as default.

Usage Guide: Monitor the timer debugging information of SSL by this command. It is good at system debugging and fault diagnosis.

Example: Enable the timer debugging information of SSL.

```
AC#debug wireless ssl timer
```

8.8 show wireless syslogflags

Command: `show wireless syslogsflags`

Function: Show whether the syslogflags on-off of AC is enabled.

Parameters: None.

Command Mode: Admin Mode.

Default: None.

Usage Guide: Input this command to show whether the syslogflags on-off of AC is enabled. These on-offs include: syslog of AP failure, syslog of AP state changing, syslog of client authentication failure, syslog of client state changing, AC syslog, Rouge AP syslog, syslog of WIDS state changing, syslog of wireless state changing and syslog of wireless attack.

Example: Show whether the syslogflags on-off of AC is enabled.

```
AC#sho wireless syslogflags
AP Failure Syslogs..... Disable
AP State Change Syslogs..... Disable
Client Failure Syslogs..... Disable
Client State Change Syslogs..... Disable
Peer Switch Syslogs..... Disable
Rogue AP Syslogs..... Disable
WIDS Status Syslogs..... Disable
Wireless Status Syslogs..... Disable
Wireless Attack Syslogs..... Disable
```

8.9 show wireless trapflags

Command: **show wireless trapflags**

Function: Show SNMP Trap on-off of AC is enabled or not.

Parameters: None.

Command Mode: Admin Mode.

Default: None.

Usage Guide: Inputting this command can show every Trap of AC is enabled or not. The Trap on-off includes: the failure Trap of AP, the Trap changed by AP state, the failure authentication Trap of Client, the Trap changed by Client state, AC Trap, RF Scan Trap, Rouge AP Trap, the Trap changed by WIDS state, the Trap changed by wireless state and the trap of attacking event.

Example: Show the SNMP Trap on-off of AC is enabled or not.

```
AC#show wireless trapflags
AP Failure Traps..... Disable
AP State Change Traps..... Disable
Client Failure Traps..... Disable
Client State Change Traps..... Disable
Peer Switch Traps..... Disable
```

RF Scan Traps.....	Disable
Rogue AP Traps.....	Disable
WIDS Status Traps.....	Disable
Wireless Status Traps.....	Disable
Wireless Attack Traps.....	Disable

8.10 snmp-server enable traps wireless

Command: `snmp-server enable traps wireless`

`no snmp-server enable traps wireless`

Function: Enable the wireless SNMP Trap function of AC in the whole cluster. The `no` command disables the SNMP Trap function.

Parameters: None.

Command Mode: Global Mode.

Default: The the wireless SNMP Trap function of AC in the whole cluster is disabled as default.

Usage Guide: After enabling the wireless SNMP Trap function of AC in the whole cluster, SNMP Server can receive the trap message from the cluster.

Example: Enable the wireless SNMP Trap function of AC in the whole cluster.

```
AC(Config)#snmp-server enable traps wireless
```

8.11 syslogflags

Command: `syslogflags [{ap-failure | ap-state | client-failure | client-state | peer-ws | rogue-ap | wids-status | ws-status} attack-event]`

`no syslogflags [{ap-failure | ap-state | client-failure | client-state | peer-ws | rogue-ap | wids-status | ws-status} attack-event]]`

Function: Enable wireless syslog function. The `no` command disables this function.

Parameters: All the parameters are optional.

`ap-failure`: the event that AP failed to authenticate;

`ap-state`: the event that AP status is changed;

`client-failure`: the event that client failed to authenticate;

`client-state`: the event that client status is changed;

`peer-ws`: the event of AC changing in the cluster;

`rogue-ap`: Rouge AP event;

`wids-status`: the event that WIDS status is changed;

`ws-status`: the event that local status is changed;

`attack-event`: attacking event.

Command Mode: Wireless Global Mode.

Default: syslogflags function of AC is disabled.

Usage Guide: If the parameters are not input, enable the syslogflags function of all the above events; otherwise, enable the syslogflags function of the event which is appointed by parameters.

Example: Enable syslog function of ap-state.

```
AC(config-wireless)# syslogflags ap-state
```

8.12 trapflags

Command: trapflags [{ap-failure | ap-state | client-failure | client-state | peer-ws | rf-scan | rogue-ap | wids-status | ws-status| attack-event}]

no trapflags [{ap-failure | ap-state | client-failure | client-state | peer-ws | rf-scan | rogue-ap | wids-status | ws-status| attack-event }]

Function: Enable SNMP Trap function against some events on AC. The no command disables the SNMP Trap function.

Parameters: **ap-failure:** AP authentication failure event;

ap-state: AP state diversification event;

client-failure: Client authentication failure event;

client-state: Client state diversification event;

peer-ws: AC diversification event in the cluster;

rf-scan: RF Scan event;

rogue-ap: Rouge AP event;

wids-status: WIDS state diversification event;

ws-status: Local state diversification event;

attack-event: Attacking event.

Command Mode: Wireless Global Mode.

Default: The SNMP Trap function of AC is disabled as default.

Usage Guide: If the parameters are not input, enable the SNMP Trap function of all events. Otherwise, enable the SNMP Trap function of the events which are appointed by the parameters.

Example: Enable SNMP Trap function of the event of ap-state:

```
AC(config-wireless)#trapflags ap-state
```