Content

Chapter 1 Commands for Wireless Client Access and Authentication

1.1 Commands for AC

1.1.1 agetime

Command：agetime {ad-hoc | ap-failure | rf-scan | detected-client} *<0-168>*
no agetime {ad-hoc | ap-failure | rf-scan | detected-client}

Function：Configure the keeping time of data in AC database. The no command recovers to be default.

Parameters： ad-hoc：client status timeout. This value determines how much time that an Ad Hoc client should be kept in the relevance Ad Hoc client status list after disassociated. Every Ad Hoc client table entry in Ad Hoc client status list has a time, when this time achieves the client timeout configured by user, this Ad Hoc client table entry will be deleted from Ad Hoc client status list.

ap-failure：AP failure status timeout. This value determines how much time that an AP will be kept in AP authentication failure status list. Every AP table entry in AP authentication failure status list has a time. When this time achieves the AP failure status timeout configured by user, this AP table entry will be deleted from AP authentication failure status list.

rf-scan：rf-scan status timeout. This value determines how much time that a table entry will be kept in rf-scan status list. Every table entry in rf-scan status list has a time, when this time achieves the rf-scan status timeout configured by user, this table entry will be deleted from rf-scan status list.

detected-client：detected client status timeout. This value determines how much time that a table entry will be kept in detected client status list. Every table entry in detected client status list has a time, when this time achieves the detected client status timeout configured by user, this table entry will be deleted from detected client status list.

Notice: The ranges of the above four timeout are 0 to 168 hours. When it is configured as 0, it means that there is no timeout.

Default：24 hours.

Command Mode：Wireless Global Mode.

Usage Guide：Configure the keeping time of data in AC database through this command.

Example：Configure the keeping time of rf-scan as 2 hours.

AC(config-wireless)# agetime rf-scan 2

1.1.2 client roam-time

Command：client roam-time *<1-65535>*

no client roam-time

Function：Configure the longest time that AC will keep record related to client in associated client list after client disassociated. The no command recovers to be default.

Parameters：*<1-65535>*, the unit is second.

Default：30 seconds.

Command Mode：Wireless Global Mode.

Usage Guide：When client roams, it will disassociated with AP related to it before and connect new AP in roam-time. Than it can be considered roaming.

Example：Configure the keeping time as 100 seconds.

AC(config-wireless)# client roam-time 100

1.1.3 known-client

Command：known-client *<macaddr>* [action {global-action | grant | deny}] [name *<name>*]

no known-client *<macaddr>*

Function：Configure client in Known client database. The no command deletes the appointed client.

Parameters：*<macaddr>* [name *<name>*] [action {global-action | grant | deny}], it includes three fields, they are MAC address of client, client name and action of client. MAC address is necessary. Action appoints allowing, refusing or using MAC authentication of global configuration to judge if allowing this client to associate.

Default：None.

Command Mode：Wireless Global Mode.

Usage Guide：Add or delete a rule table of client in Known client database through this command.

Example：Add the client table whose MAC address is e0-91-f5-42-f5-68. Its rule is allowing as default.

AC(config-wireless)# known-client e0-91-f5-42-f5-68 grant

1.1.4 mac-authentication-mode

Command：mac-authentication-mode {white-list|black-list}

no mac-authentication-mode

Function：Configure MAC authentication mode of AC. Appoint client in Known client database is allowed to associate or refused. The no command recovers to be default.

Parameters：{white-list|balck-list}, if it is defined to be white-list, client in Known client database is allowed to associate; if it is defined to be black-list, client in Known client database is refused to associate.

Default：white-list.

Command Mode：Wireless Global Mode.

Usage Guide：If there is a small part of client are allowed to associate with network through MAC authentication, it should be configured as white-list; if all the default client can associate with network through MAC authentication, only a small part of dangerous client cannot pass by, it should be configured as black-list.

Example：Configure it as black-list mode.

AC(config-wireless)# mac-authentication-mode balck-list

1.1.5 Radius server-name

Command：**radius server-name {auth | acct} *<name>***

no radius server-name {auth | acct}

Function：Configure radius groups used for client authentication or billing. The no command recovers to be default group.

Parameters：*<name>*，appoint radius groups of authentication or billing.

Default：Default-RADIUS-Server.

Command Mode：Wireless Global Mode.

Usage Guide：When network does not use the radius server configured by this network, it will use the radius server of global configuration to authenticate. The default is no using the radius server of wireless global to authenticate or billing. This command can configure to choose the radius group of wireless global.

Example：Configure “radius-server-1” as the radius server of wireless global for authentication; Configure “radius-server-2” as the radius server of wireless global for billing.

AC(config-wireless)# Radius server-name auth radius-server-1

AC(config-wireless)# Radius server-name acct radius-server-2

1.1.6 show wireless agetime

Command：**show wireless agetime**

Function：Show the maximum time of keeping database configured by AC.

Parameters：None.

Default：None.

Command Mode：Admin Mode.

Usage Guide：Inquiry the maximum time of keeping database configured by AC through this command.

Example：Show the maximum time of keeping database items.

AC# show wireless agetime

Ad Hoc Client Statue Age (hours)..... 24

AP Failure Status Age (hours)..... 24

RF Scan Status Age (hours)..... 24

Detected Clients Age (hours)..... 24

agetime client-failure..... 24

AP Provisioning Database Age Time (hours)..... 72

Table 1-1 explanation of the maximum time of keeping database

Parameters	Explanation
Ad Hoc Client Status Age	The maximum keeping time of ad hoc client in status list
AP Failure Status Age	The maximum keeping time of failed AP in status list
RF Scan Status Age	The maximum keeping time of AP scanned by RF in status list
Detected Clients Age	The maximum keeping time of Detected Client in database
AP Provisioning Database Age	The maximum keeping time of AP in AP Provisioning Database

1.1.7 show wireless mac-authentication

Command：show wireless mac-authentication

Function：Show MAC authentication mode configured for AC.

Parameters：None.

Default：None.

Command Mode：Admin Mode.

Usage Guide：Inquire MAC authentication mode configured for AC through this command.

Example：Show MAC authentication mode.

AC# show wireless mac-authentication

mac-authentication-mode..... black-list

1.1.8 show wireless Known-client

Command：show wireless Known-client [<*macaddr*>]

Function：Show information of all client or the client which is appointed MAC address in local known client database.

Parameters：*<macaddr>*，MAC address of client.

Default：None.

Command Mode：Admin Mode.

Usage Guide：Inquire information of all client or the client which is appointed MAC address in local known client database through this command.

Example：Show information of all client in local known client database.

AC# show wireless Known-client

MAC Address Name Action

----------------- -------------------------------- ----------------

5c-ac-4c-3b-73-73 global-action

74-ea-3a-10-bb-94 global-action

信息的具体解释如下所示：

Table 1-2 explanation of the maximum time of keeping database

Parameters	Explanation
Mac Address	MAC address of client in local Known Client database.
Nickname	Another name of Client, it length is less then 32charecters.
Action	Appoint the rule of this client in MAC authentication: allowing, refusing or using the default rule of global configuration.

1.1.9 show wireless radius

Command：show wireless radius

Function：Show the relevant information of wireless global radius server configured for users.

Parameters：None.

Default：None.

Command Mode：Admin Mode.

Usage Guide：Inquire the relevant information of wireless global radius server configured for users through this command.

Example：Show the relevant information of wireless global radius server configured for users.

AC# show wireless radius

RADIUS Authentication Server Name..... Default-RADIUS-Server

RADIUS Authentication Server Status..... Not Configured

RADIUS Accounting Server Name..... Default-RADIUS-Server

RADIUS Accounting Server Status..... Not Configured

RADIUS Accounting..... Disable

1.1.10 UCS

Command: UCS { enable| disable }

Function: It is the universal character configuration on-off. When AC supports the Chinese ssid, this UCS function should be enabled first, the parameter can be configured as Chinese. When this function is disabled, only English or other defined characters can be configured.

Parameters: None.

Default: Disable. The Chinese characters cannot be configured.

Command Mode: Config mode.

Usage Guide: When needs to configure the Chinese characters, this UCS function should be enabled first.

Example: Enable the UCS function.

AC(config)# ucs enable

1.2 Commands for Wireless Network

1.2.1 clear

Command：clear

Function：Recover the network configuration to default.

Parameters：None.

Default：None.

Command Mode：Network Configuration Mode.

Usage Guide：Recover the network configuration to default through this command.

Example：Recover the network configuration to default.

AC(config-network)# clear

1.2.2 dot1x bcast-key-refresh-rate

Command：dot1x bcast-key-refresh-rate <*0-86400*>

no dot1x bcast-key-refresh-rate

Function：Configure the update rate of broadcast key; the no command recovers to be default.

Parameters：*<0-86400>*，the unit is second and 0 means it does not update.

Default：300 second.

Command Mode：Network Configuration Mode.

Usage Guide：Configure the update rate of broadcast key through this command.

Example：Configure the update rate as 1000 second.

AC(config-network)# dot1x bcast-key-refresh-rate 1000

1.2.3 dot1x session-key-refresh-rate

Command：**dot1x session-key-refresh-rate *<0，30-86400>***

no dot1x session-key-refresh-rate

Function：Configure the interval of the re-authentication for client; the no command recovers to be default.

Parameters：***<0，30-86400>***，the unit is second.

Default：0s, it means no re-authentication. Generally, this value should not be too small, otherwise, it will bring the frequent client authentication.

Command Mode：Network Configuration Mode.

Usage Guide：Configure the interval of the re-authentication for client through this command.

Example：Configure the interval of the re-authentication for client as 1000s.

AC(config-network)# dot1x session -key-refresh-rate 1000

1.2.4 hide-ssid

Command：**hide-ssid**

no hide-ssid

Function：Configure SSID of hidden network. If configure it as hiding, there is not SSID in beacon frame of AP. The no command is no hiding SSID.

Parameters：None.

Default：disable, it means it does not hide SSID.

Command Mode：Network Configuration Mode.

Usage Guide：Sometimes, use this command to hide SSID of network for safety.

Example：Hide SSID of some network.

AC(config-network)# hide-ssid

1.2.5 network

Command：network *<1-1024>*

no network *<1-1024>*

Function：If this network does not exist, add a network configuration. Enter network configuration mode to modify its parameters. The no command deletes a network configuration. If this network is used by VAP, it cannot be deleted. The first 16 networks cannot be deleted forever as default.

Parameters：*<1-1024>*，number of network.

Default：Network 1 to network 16 are created as default.

Command Mode：Wireless Configuration Mode.

Usage Guide：When user wants to enter network configuration mode to configure for network, use this command; when the existed network is not enough to use, add the new network configuration through this command.

Example：Add network with number 20.

AC(config-wireless)# network 20

1.2.6 mac authentication

Command：mac authentication {local | radius}

no mac authentication

Function：Enable client MAC authentication and configure MAC authentication way as local or Radius authentication. The no command disables client MAC authentication.

Parameters：{local | radius}，appoint mac authentication way, local is local authentication, Radius uses Radius server authentication.

Default：Disable mac authentication.

Command Mode：Network Configuration Mode.

Usage Guide：Enable MAC authentication through this command and configure MAC authentication way.

Example：Enable MAC authentication and configure it as local authentication.

AC(config-network)# mac authentication local

1.2.7 radius server-name

Command：radius server-name {auth | acct} *<name>*

no radius server-name {auth | acct}

Function：Configure radius groups used for client authentication or billing in network. The

no command recovers to default of Default-RADIUS-Server.

Parameters：{auth | acct}，appoint radius groups recovered authentication or billing.

Default：Default-RADIUS-Server.

Command Mode：Network Configuration Mode.

Usage Guide：If not using global Radius server to authenticate or billing , configure radius groups used for client authentication or billing in this network through this command.

Example：Configure radius groups used for client authentication and billing.

AC(config-network)# radius server-name auth authradius

AC(config-network)# radius server-name acct acctradius

1.2.8 radius use-network-configuration

Command：**radius use-network-configuration**

no radius use-network-configuration

Function：Configure if using radius server configured against network. The no command configures network to use radius server of wireless global configuration.

Parameters：None.

Default：Use radius server configured by network as default.

Command Mode：Network Configuration Mode.

Usage Guide：If not using global Radius server to authenticate and billing , configure radius server against this network through this command.

Example：Configure radius server against this network.

AC(config-network)# radius use-network-configuration

1.2.9 security mode

Command：**security mode {none | static-wep | wep-dot1x | wpa-enterprise | wpa-personal}**

no security mode

Function：Configure authentication and encryption supported by network. The no command recovers to be laws.

Parameters：{none | static-wep | wep-dot1x | wpa-enterprise | wpa-personal}，none means laws, there is no wireless authentication encryption. Others are wireless safety access ways defined by 802.11.

Default：none, it is laws.

Command Mode：Network Configuration Mode.

Usage Guide：Configure all kinds of authentication and encryption ways for network through this command.

Example：Configure authentication and encryption of network as wpa-personal.

AC(config-network)# security mode wpa-personal

1.2.10 show wireless network

Command：**show wireless network [*<1-1024>*]**

Function：Show the detailed configuration of the appointed network. If it is not appointed, show the main configuration of all network.

Parameters：*<1-1024>*, number of network.

Default：None.

Command Mode：Admin Mode.

Usage Guide：Inquire network configuration through this command and show parameters.

Example：Inquire configuration of network1 and show parameters.

AC(config-network)# exit

AC(config-wireless)# exit

AC(config)# exit

AC# show wireless network 1

Network ID..... 1

SSID..... Guest Network

Interface ID..... 11000

Default VLAN..... 1

Hide SSID..... Disable

Deny Broadcast..... Disable

Redirect Mode..... None

Redirect URL..... -----

L2 Distributed Tunneling Mode..... Disable

Bcast Key Refresh Rate..... 300

Session Key Refresh Rate..... 0

Wireless ARP Suppression..... Disable

Security Mode..... None

MAC Authentication..... Disable

RADIUS Authentication Server Name..... Default-RADIUS-Server

RADIUS Authentication Server Status..... Not Configured

RADIUS Accounting Server Name..... Default-RADIUS-Server

RADIUS Accounting Server Status..... Not Configured

RADIUS Use Network Configuration..... Enable

RADIUS Accounting..... Disable

WPA Versions..... WPA/WPA2

WPA Ciphers..... TKIP/CCMP

WPA Key Type..... ASCII

WPA Key.....

WPA2 Pre-Authentication..... Enable

WPA2 Pre-Authentication Limit..... 0

WPA2 Key Caching Holdtime (minutes)..... 10

WEP Authentication Type..... Open System

WEP Key Type..... HEX

WEP Key Length (bits)..... 128

WEP Transfer Key Index..... 1

WEP Key 1.....

WEP Key 2.....

WEP Key 3.....

WEP Key 4.....

Client QoS Mode..... Disable

Client QoS Bandwidth Limit Down..... 0

Client QoS Bandwidth Limit Up..... 0

Client QoS Access Control Down..... -----

Client QoS Access Control Up..... -----

Client QoS Diffserv Policy Down..... -----

Client QoS Diffserv Policy Up..... -----

1.2.11 ssid

Command：ssid <*name*>

Function：Configure SSID of wireless network, a network must be configured with an SSID of more than one character, this SSID can be modified but deleted.

Parameters：*<name>*，network SSID shown by strings. The length is 1 to 32 strings.

Default：The default of Network1 is “Guest Network”; the default of others is “Managed SSID ID”. ID is network ID of SSID.

Command Mode：Network Configuration Mode.

Usage Guide：Configure an SSID of wireless network through this command. Notice: SSID can have space, if there is space, “” does not need to be used.

Example：Configure an SSID for network 20.

AC(config-network)# ssid ssidname 20

1.2.12 wep authentication

Command：wep authentication {open-system | share-key}

no wep authentication

Function：Configure the link authentication ways used by network when it is using static wep authentication. The no command recovers to be default of open system.

Parameters：{open-system | share-key}, link authentication ways defined by 802.11. The detailed introduction refers to wireless authentication and access configuration document.

Default：Open System.

Command Mode：Network Configuration Mode.

Usage Guide：Configure using open system and share key in network which is uing static wep authentication through this command.

Example：Configure using share key in network which is using static wep authentication.

AC(config-network)# wep authentication share-key

1.2.13 wep key

Command：wep key <*1-4*> [encrypted] <*value*>

no wep key <*1-4*>

Function：Configure share keys of network which is using static wep. 4 is most and the key characters number is affected by wep key type and wep length. The no command deletes this share keys.

Parameters：*<1-4>* <*value*>，Configure key related to key sequence. The key characters number is affected by wep key type and wep length. The correspondence relationship is the following:

64bit-ASCII：5 characters；Hex：10 characters；

128bit-ASCII：13 characters；Hex：26 characters；

[encrypted]，it is optional. Configure the password as a lawful encryption wep key, the maximum length of it is 128 characters.

Default：None.

Command Mode：Network Configuration Mode.

Usage Guide：Configure share keys of network which is using static wep through this command.

Example：Configure 2 share keys for a network. Notice: In this example, key type is ascii, the length is 64bit. So configure the key characters as 5.

AC(config-network)# wep key 1 wepk1

AC(config-network)# wep key 2 wepk2

1.2.14 wep key length

Command：wep key length {64 | 128}

no wep key length

Function：Configure the key length of network which is using static wep. The no command recovers to be default.

Parameters：{64 | 128}，the length of WEP key.

Default：128.

Command Mode：Network Configuration Mode.

Usage Guide：Configure the key length of network which is using static wep through this command.

Example：Configure the key length as 64bit.

AC(config-network)# wep key length 64

1.2.15 wep key type

Command：wep key type {ascii | hex}

no wep key type

Function：Configure the key encoding type of network which is using static wep. The no command recovers to be default.

Parameters：{ascii | hex}, the key encoding type of wep key, they are shown by ASCII and Hexadecimal

Default：HEX.

Command Mode：Network Configuration Mode.

Usage Guide：Configure the key encoding type of network which is using static wep through this command.

Example：Configure the key encoding type as ASCII.

AC(config-network)# wep key type ascii

1.2.16 wep tx-key

Command：wep tx-key *<1-4>*

no wep tx-key

Function：Configure which wep-key is used for data transmission encryption when network is using static wep. The no command recovers to be default of 1.

Parameters：*<1-4>*, Configure 4 wep key, choose any one to use for data transmission encryption between client and AP.

Default：1, it means the first wep-key is the key using for data transmission encryption between client and AP.

Command Mode：Network Configuration Mode.

Usage Guide：Configure which wep-key is used for data transmission encryption when network is using static wep through this command. Notice: The appointed wep key must have been configured and it is not free.

Example：Configure share key 2 as the key for data transmission encryption.

AC(config-network)# wep tx-key *2*

1.2.17 wpa ciphers

Command：**wpa ciphers {ccmp [tkip] | tkip }**

no wpa ciphers

Function：Configure the encryption algorithm used by network. The no command recovers to be default.

Parameters：{ccmp [tkip] | tkip }, it can be free or ccmp, tkip. Ccmp and tkip can also exist at the same time. Ccmp and tkip are encryption algorithm of 802.11i standard. When they are existing at the same time, users who has TKIP key and AEC-CCMP key can associate with AP.

Default：tkip and ccmp are existing at the same time as default.

Command Mode：Network Configuration Mode.

Usage Guide：Configure wpa encryption algorithm supported by network through this command. The encryption algorithm of WPA or WPA2 can choose ccmp or tkip, they can also exist at the same time.

Example：Configure wap encryption algorithm of wap2.

AC(config-network)# wpa ciphers ccmp

1.2.18 wpa key

Command：**wpa key <*value*>**

Function：Configure WPA share key of network.

Parameters：<*value*>, it is a string with 8 to 84 characters.

Default： none.

Command Mode：Network Configuration Mode.

Usage Guide：Configure WPA share key of network through this command.

Example：Configure WPA share key of network.

AC(config-network)# wpa key wpakey110

1.2.19 wpa versions

Command：wpa versions {wpa [wpa2] | wpa2}

no wpa versions

Function：Configure WPA version used by network. The no command recovers to be default of wpa/wpa2.

Parameters：{wpa [wpa2] | wpa2}, it can be free or wpa, wpa2. wpa and wpa2 can also coexist. When they are coexisting, for client which supports wpa2, system uses wpa2 authentication; for client which does not support wpa2, system uses wpa authentication.

Default：wpa/wpa2.

Command Mode：Network Configuration Mode.

Usage Guide：When using wpa-enterprise or wpa-personal safety authentication mode, wpa version should be sure. This command can configure wpa version.

Example：Configure wpa version as wpa2.

AC(config-network)# wpa versions wpa2

1.2.20 wpa2 key-caching holdtime

Command：wpa2 key-caching holdtime <*1-1440*>

no wpa2 key-caching holdtime

Function：Configure the maximum time of PMK that AP caches the client under WPA2.

Parameters：*<1-1440>,* the unit is minute. It is the maximum time of PMK that AP caches the client under WPA2.

Default：10 minutes.

Command Mode：Network Configuration Mode.

Usage Guide：Configure the maximum time of PMK that AP caches the client under WPA2. This PMK is produced when consulting with radius server in pre-authentication

Example：Configure holdtime as 20.

AC(config-network)# wpa2 key-caching holdtime 20

1.2.21 wpa2 pre-authentication

Command：wpa2 pre-authentication

no wpa2 pre-authentication

Function：Enable WPA2 pre-authentication function of client roaming. The no command disables this function.

Parameters：None.

Default：Disable.

Command Mode：Network Configuration Mode.

Usage Guide：When client connected to AP1 discovers AP2 whose signal is better, client will disassociate with AP1 and roam to AP2. If enabling WPA2 pre-authentication function, client can pass by AP1 agency and request to check identity to AP2 in advance. When client associates to AP2, it disassociates to AP1. It improves the roaming speed and achieves seamless roaming.

Example：Enable WPA2 pre-authentication function.

AC(config-network)# wpa2 pre-authentication

1.2.22 wpa2 pre-authentication limit

Command：**wpa2 pre-authentication limit *<0-192>***

no wpa2 pre-authentication limit

Function：Configure how many client most can be checked identity in advance with an AP network allows. The no command recovers to be default.

Parameters：*<0-192>*，it means how many client most can be checked identity in advance with an AP.

Default：0, it means there is no limitation.

Command Mode：Network Configuration Mode.

Usage Guide：If enabling WPA2 pre-authentication function, configure how many client most can be checked identity in advance with an AP network allows through this command.

Example：Configure the maximum number as 100.

AC(config-network)# wpa2 pre-authentication limit 100

1.3 Commands for VAP

1.3.1 enable

Command：**enable**

no enable

Function：Enable VAP of radio. The no command disables VAP of radio. VAP0 cannot be disabled. If user wants to disable VAP0, radio power must be broken.

Parameters：None.

Default：It enables for VAP0 and disables for VAP 1 to 5.

Command Mode： VAP Configuration Mode.

Usage Guide：Enable VAP of radio through this command.

Example：Enable VAP2 of radio1.

AC(config-ap-profile)#radio 1

AC(config-ap-profile-radio)# vap *2*

AC(config-ap-profile-vap)# enable

1.3.2 network

Command：**network *<1-1024>***

Function：Configure network configuration applied to VAP. A VAP must be appointed which network it belongs, if VAP is applied, this network cannot be deleted.

Parameters：*<1-1024>*，network ID.

Default：network 1 to 16 are applied to VAP0 to VAP15 in order as default.

Command Mode：VAP Configuration Mode.

Usage Guide：A VAP must be appointed which network it belongs. Configure VAP belonging to a network through this command.

Example：Appoint VAP 2 to belong to network 3.

AC(config-ap-profile-radio)# vap *2*

AC(config-ap-profile-vap)# network *3*

1.3.3 vap

Command：**vap *<0-15>***

Function：Entering VAP configuration mode can modify VAP parameters.

Parameters：*<0-15>*，VAP ID.

Default：None.

Command Mode： Radio Configuration Mode.

Usage Guide：If modifying VAP parameters, there is need to enter AP profile VAP configuration mode. Enter this mode through this command.

Example：Enter VAP configuration mode and configure VAP2 parameters.

AC(config-ap-profile-radio)# vap *2*

1.4 Commands for Load-balance

1.4.1 client-reject rssi-threshold <0-100>

Command：**client-reject rssi-threshold <0-100>**

no client-reject rssi-threshold

Function：Enable the weak signal accessing function. Configure the RSSI value to reject tthe weak signal. The client RSSI which is lower than the value will be rejected accessing and the client which is higher than the value will be allowed. The no command allows all the signals accessing.

Parameters：<0-100>: the range of RSSI threshold.

Default：0.

Command Mode：Radio Configuration Mode.

Usage Guide：When the client RSSI is lower than the configured threshold, it will be rejected accessing.

Example：Configure the RSSI threshold as 50.

AC(config-ap-profile-radio)#client-reject rssi-threshold 50

1.4.2 load-balance

Command：**load-balance [utilization <*1-100*>]**

no load-balance [utilization]

Function：Enable load-balance function of system. Configuring radio loading with utilization can achieve total loading percentage of every radio. The no command disables this function. Do not disable load-balance function with utilization, recover to be default.

Parameters：[utilization <*1-100*>], Define the percentage that the maximum value which radio loading achieved occupys every total radio loading.

Default：disable, it is 60% with utilization.

Command Mode：Radio Configuration Mode.

Usage Guide：Enable load-balance function and loading percentage parameters of system through this command to use load-balance function flexibility.

Example：Enable load-balance function and configure the percentage as 70%.

AC(config-ap-profile-radio)# Load-balance utilization 70

1.4.3 max-client

Command：**max-client <*0-200*>**

no max-client

Function：Configure the most number of clients which is allowed to associate with every radio interface at same time. The no command recovers to be default.

Parameters：*<0-200>*，the most number of client.

Default：200.

Command Mode：Radio Configuration Mode.

Usage Guide：Configure the most number of client which is allowed to associate with every radio interface at same time through this command.

Example：Configure the most number of client as 200.

AC(config-ap-profile-radio)# Max-client 200

1.5 Commands for Client Disassociation and Viewing

1.5.1 show wireless client neighbor ap status

Command：**show wireless client <*macaddr*> neighbor ap status**

Function：Show all AP scanned by client whose MAC address is appointed in RF area. For associated client, client roaming to AP can be see.

Parameters：<*macaddr*>, MAC address of client.

Default：None.

Command Mode：Admin Mode.

Usage Guide：Inquire local client neighbor APs table through this command.

Example：Show AP table scanned by client whose MAC address is e0-91-f5-42-f5-68.

AC# show wireless client e0-91-f5-42-f5-68 neighbor ap status

1.5.2 show wireless client statistics

Command：**show wireless client <*macaddr*> statistics [{association | session}]**

Function：Show client association or session statistic information associated with managed AP. If client roams, session statistic information will show the accumulative statistic information which client associates. When the optional parameter is not configured, show session statistic information as default.

Parameters：<*macaddr*>, MAC address of client;

[{association | session}], Appoint that it is the information shown association once or shown the whole session.

Default：None.

Command Mode：Admin Mode.

Usage Guide：Inquire client statistic information in associated client table through this command.

Example：Show the session statistic information of client whose MAC address is b0-48-7a-1e-dd-16.

AC# show wireless client b0-48-7a-1e-dd-16 statistics

MAC address..... b0-48-7a-1e-dd-16

Packets Received..... 41

Packets Transmitted..... 0

Bytes Received..... 6556

Bytes Transmitted..... 0

Packets Receive Dropped..... 0

Packets Transmit Dropped..... 0

Bytes Receive Dropped..... 0

Bytes Transmit Dropped..... 0

Duplicate Packets Received..... 1

Packet Fragments Received..... 463

Packet Fragments Transmitted..... 5

Transmit Retry Count..... 1

Failed Retry Count..... 0

TS Violate Packets Received..... 0

TS Violate Packets Transmitted..... 0

Table 1-3 explanation of Client session statistic information

Parameters	Explanation
Mac Address	MAC address of Client.
Packets Received	Packets sum received.
Bytes Received	Data characters number received.
Packets Transmitted	Packets sum transmitted.
Bytes Transmitted	Data characters number transmitted.
Packets Received Dropped	Packets sum received dropped.
Bytes Received Dropped	Data characters number received dropped.
Packets Transmitted Dropped	Packets sum transmitted dropped.
Bytes Transmitted Dropped	Data characters number transmitted dropped.
Duplicate Packets Received	Repeated packets sum received.
Packets Fragments Received	Packets fragments sum received.
Packets Fragments Transmitted	Packets fragments sum transmitted.
Transmitted Retry Count	Successful count of repeated transmission.
Transmitted Retry Failed Count	Failed count of repeated transmission.
TS Violate Packets	Illegal packets sum received in Tranfic stream allowing

Received	control.
TS Violate Packets Transmitted	Illegal packets sum transmitted in Tranfic stream allowing control.

1.5.3 show wireless client status

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

Function：Show the detailed information of client that appointing local association with managed AP. If AC is controller, show all associated client information of peer-group only.

Parameters：*<macaddr>* is MAC address of client.

Default：None.

Command Mode：Admin Mode.

Usage Guide：Examine the detailed information of client appointed MAC address or all associated client information of peer-group through this command.

Example：Show all associated client information of peer-group.

AC# show wireless client status

Notice: when AC is controller, the client information associated with other AC will has “*”.

MAC Address

(*) Peer Managed VAP MAC Address SSID Status Network Time

---------- ---------- ---------- --------- ----------

*b0-48-7a-1e-dd-16 00-03-0f-18-ed-b0 Guest Network Auth 0d:00:04:54

Total Clients Associated with Local Switch..... 0

Total Clients Associated with Peer Switches..... 1

Table 1-4 explanation of detailed client information

Parameters	Explanation
Mac Address	MAC address of Client.
Detected IP Address	IP address of Client.
Tunnel IP Address	Tunnel IP of Tunneled Clients.
Associating Switch	AC that AP associated with client is in.
Switch MAC Address	MAC address of AC associated with Client.
Switch IP Address	IP address of AC associated with Client.
SSID	SSID of network connected to Client.
NETBIOS Name	NETBIOS of Client.
VAP MAC Address	MAC address of VAP associated with Client.
Channel	Channel of associated Client.

Status	Appoint client status: associate, authenticate or disassociate.
AP MAC Address	MAC address of Managed AP.
Location	Location of Managed AP.
Radio	Radio of managed AP associated with Client.
VLAN	VLAN distributed by VAP associated with Client.
Transmit Data Rate	Rate of Client sending data.
802.11n-Capable	If Client supports 802.11n.
STBC Capable	If Client supports time and space grouping code.
Inactive Period	Non-working period.
Age	The time interval from client status update to now. The unit is second.
Network Time	Online time of Client.

1.5.4 show wireless client summary

Command：show wireless client summary

Function：Show the main information of client associated with managed AP in local AC. If this AC is controller, show the main information of all associated client in peer-group.

Parameters：None.

Default：None.

Command Mode：Admin Mode.

Usage Guide：Inquire the main information of client associated with managed AP in local AC or the main information of all associated client in peer-group through this command.

Example：Show the main information of all associated client in peer-group.

Notice: When AC is controller, the client information associated with other AC will has "*".

AC#show wireless client summary

```
      MAC Address
 (*) Peer Managed     IP Address            VAP MAC Address     NetBIOS Name
------------------ ----------------- ----------------- -----------------
*b0-48-7a-1e-dd-16 169.254.119.175     00-03-0f-18-ed-b0 SHIXF
```

Table 1-5 explanation of detailed client information

Parameters	Explanation
Mac Address	MAC address of Client.
IP Address	IP address of Client.
NETBIOS Name	NETBIOS of Client.

1.5.5 show wireless client status ssid

Command：show wireless client status ssid [<*ssid*>]

Function： Show the main information of associated client in all managed SSID. When SSID is appointed, show client information of SSID only.

Parameters： <*ssid*>, SSID with string, it is optional.

Default： None.

Command Mode： Admin Mode.

Usage Guide： Inquire local SSID-Client Mapping table and Associated client table through this command.

Example： Show the main information of associated client in all managed SSID.

AC# show wireless client status ssid

SSID	Client MAC Address
Guest Network	b0-48-7a-1e-dd-16

Table 1-6 explanation of client information

Parameters	Explanation
Mac Address	MAC address of Client.
SSID	SSID of network connected to Client.

1.5.6 show wireless client status switch

Command：show wireless client status switch [<*ipaddr*>]

Function： Show the main information of associated client in all AC. When appoint AC is controller, show all associated client information in peer-group. Other AC show the relevant client information of the appointed AC only.

Parameters： <*ipaddr*>, IP address of AC.

Default： None.

Command Mode： Admin Mode.

Usage Guide： Inquire local Switch-Client Mapping table and Associated client table through this command.

Example： Show the relevant client information of AC whose IP address is 192.168.37.60.

AC#show wireless client status switch 192.168.37.60

Switch IP Address Client MAC Address

---------- ----------

192.168.21.254 b0-48-7a-1e-dd-16

Table 1-7 explanation of client information

Parameters	Explanation
IP Address	IP address of AC or AC groups in wireless system.
Mac Address	MAC address of Client.

1.5.7 show wireless client status vap

Command：show wireless client status vap [<*macaddr*>]

Function：Show the main information of associated client in all managed VAP. When appoint MAC address of VAP, show client information in VAP only.

Parameters：<*macaddr*>, MAC address of VAP.

Default：None.

Command Mode：Admin Mode.

Usage Guide：Inquire local VAP-Client Mapping table through this command.

Example：Show the relevant client information in VAP whose MAC address is 00-03-0f-18-ed-b0.

AC#show wireless client status vap 00-03-0f-18-ed-b0

VAP MAC Address AP MAC Address Location Radio Client MAC Address

---------- ---------- ---------- ----- ----------

00-03-0f-18-ed-b0 00-03-0f-18-ed-b0 1 b0-48-7a-1e-dd-16

The explanation of information is the following:

Table 1-8 explanation of client information

Parameters	Explanation
VAP MAC Address	MAC address of VAP associated with Client.
Mac Address	MAC address of Client.

1.5.8 wireless client disassociate

Command：wireless client disassociate [<*macaddr*>]

Function：Disassociate AC and client appointed MAC address forcibly. This client is associated with managed AP. When MAC address is not appointed, disassociate all client managed in local. If local AC is controller, disassociate all clients in system.

Parameters：<*macaddr*>, MAC address of client.

Default：None.

Command Mode：Admin Mode.

Usage Guide：Disassociate client which is appointed MAC address or all client managed in local through this command.

Example：Disassociate AC and client whose MAC address is e0-91-f5-42-f5-68 Client.

AC# wireless client disassociate e0-91-f5-42-f5-68

1.5.9 wireless client disassociate ap

Command：**wireless client disassociate ap <*macaddr*>**

Function：Disassociate all clien of managed AP which is appointed MAC address forcibly.

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

Default：None.

Command Mode：Admin Mode.

Usage Guide：Disassociate all clien of managed AP which is appointed MAC address through this command.

Example：Disassociate all clien of managed AP whose MAC address is 00-03-0f-01-02-00.

AC# wireless client disassociate ap 00-03-0f-01-02-00

1.5.10 wireless client disassociate ssid

Command：**wireless client disassociate ssid<*name*>**

Function：Disassociate all clien of network which is appointed ssid forcibly.

Parameters：<*name*>, ssid of network.

Default：None.

Command Mode：Admin Mode.

Usage Guide：Disassociate all clien of network which is appointed ssid through this command.

Example：Disassociate all clien of ssid-1.

AC# wireless client disassociate ssid ssid-1

1.5.11 wireless client disassociate vap

Command：**wireless client disassociate vap <*macaddr*>**

Function：Disassociate all clien of VAP which is appointed MAC address forcibly.

Parameters：<*name*>, MAC address of VAP.

Default：None.

Command Mode：Admin Mode.

Usage Guide：Disassociate all clien of VAP which is appointed MAC address through this command.

Example：Disassociate all clien of VAP whose MAC address is 00-03-0f-01-02-03.

AC# wireless client disassociate vap 00-03-0f-01-02-03

1.6 Commands for Ad Hoc Client List

1.6.1 clear wireless client adhoc list

Command：**clear wireless client adhoc list**

Function：Delete all records in Ad Hoc client list.

Parameters：None.

Default：None.

Command Mode：Admin Mode.

Usage Guide：Delete all records in Ad Hoc client list through this command.

Example：Delete all records in Ad Hoc client list.

AC# clear wireless client adhoc list

1.6.2 show wireless client adhoc status

Command：**show wireless client [<*macaddr*>]adhoc status**

Function：Show the main information of all ad-hoc clients discovered by managed AP or the detailed information of the appointed client.

Parameters：<*macaddr*>, MAC address of client.

Default：None.

Command Mode：Admin Mode.

Usage Guide：Inquire the client information in Ad Hoc client list through this command.

Example：Inquire the client information in Ad Hoc client list.

AC#show wireless client adhoc status

MAC Address AP MAC Address Location Radio Det. Mode Age

00-1e-64-6e-dd-98 00-03-0f-80-50-20 here 1 Beacon Rogue 0d:05:52:01

20-68-9d-f2-e8-b2 00-03-0f-80-50-20 here 1 Beacon Rogue 0d:00:54:51

70-1a-04-44-08-c5 00-03-0f-80-50-20 here 1 Beacon Rogue 0d:03:24:57

c8-3a-35-ca-f8-86 00-03-0f-80-50-20 here 1 Beacon Rogue 0d:00:00:24

ca-28-00-00-00-00 00-03-0f-80-50-20 here 1 Data Rogue 0d:07:40:47
d8-2a-7e-e6-48-f1 00-03-0f-80-50-20 here 1 Beacon Rogue 0d:00:08:41

Table 1-9 explanation of Ad hoc client information

Parameters	Explanation
MAC Address	MAC address of Client
AP Mac Address	MAC address of AP which discovers this client
Location	Location of this managed AP
Radio	Radio of AP which discovers this client
Detection Mode	Work mode of discovery client: Beacom Frame, Data Frame
Age	The time interval from discovering this ad hoc network to now. the unit is second.

1.7 Commands for Detected Client Database

1.7.1 clear wireless detected-client non-auth

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

Function：Delete all authentication failure records in detected client or client with appointed MAC address.

Parameters：***<macaddr>***, MAC address of client.

Default：None.

Command Mode：Admin Mode.

Usage Guide：Delete all authentication failure records in detected client or client of appointed MAC address through this command.

Example：Delete client information of appointed MAC address of 00-24-2c-3c-88-5b.

AC# clear wireless detected-client 00-24-2c-3c-88-5b non-auth

1.7.2 clear wireless detected-client preauth-history

Command：clear wireless detected-client [<*macaddr*>] preauth-history

Function：Delete the advance identity authentication history of all clients or the appointed client from Detected Clients Pre-Auth History list.

Parameters：***<macaddr>,*** MAC address of client.

Default：None.

Command Mode：Admin Mode.

Usage Guide：Delete information from Detected Clients Pre-Auth History list through this command.

Example：Delete client information whose MAC address is 00-24-2c-3c-88-5b from Detected Clients Pre-Auth History list.

AC# clear wireless detected-client 00-24-2c-3c-88-5b preauth-history

1.7.3 clear wireless detected-client roam-history

Command：**clear wireless detected-client [<*macaddr*>] roam-history**

Function：Delete roaming history of all clients or the appointed clients from Detected Clients Roam History list.

Parameters：***<macaddr>*,** MAC address of client.

Default：None.

Command Mode：Admin Mode.

Usage Guide：Delete information from Detected Clients Roam History list through this command.

Example：Delete client information whose MAC address is 00-24-2c-3c-88-5b from Detected Clients Roam History list.

AC# clear wireless detected-client 00-24-2c-3c-88-5b roam-history

1.7.4 show wireless client detected-client pre-auth-history

Command：**show wireless client [<*macaddr*>] detected-client pre-auth-history**

Function：Show the advance identity authentication history of all clients in Detected Clients Pre-Auth History list or the appointed client. 10 is most.

Parameters：***<macaddr>*,** MAC address of client.

Default：None.

Command Mode：Admin Mode.

Usage Guide：Inquire advance identity authentication history of all failure authentication clients or the clients appointed MAC address in Detected Clients Pre-Auth History list through this command.

Example：Show advance identity authentication history of all clients in Detected Clients Pre-Auth History list.

AC# show wireless client detected-client pre-auth-history

1.7.5 show wireless client detected-client status

Command：show wireless client [<*macaddr*>] detected-client status

Function：Show status information of clients in Detected client list. If MAC address is not appointed, show the main information of all clients. Otherwise, show the detailed status information of the appointed client.

Parameters：*<macaddr>*，MAC address of client.

Default：None.

Command Mode：Admin Mode.

Usage Guide：Inquire status information of all clients or the clients appointed MAC address in Detected client list through this command.

Example：Show the main information of all clients in Detected client list.

AC# show wireless client detected-client status

MAC Address	Client Name	Client Status	Age	Create Time
00-24-2c-3c-88-5b		Detected	0d:00:00:38	0d:16:08:14
00-24-2c-35-88-56		Detected	0d:00:00:38	0d:16:08:14
00-12-f0-db-9f-98		Detected	0d:00:01:07	0d:16:07:13
f8-db-7f-4d-f6-61		Detected	0d:00:17:21	0d:01:50:58

Total Detected Clients..... 4

AC#show wireless client f8-db-7f-4d-f6-61 detected-client status

MAC address..... f8-db-7f-4d-f6-61
OUI..... ouiname
Client Status..... Detected
Auth Status..... Not Authenticated
Time Since Last Updated..... 0d:00:20:09
Threat Detection..... Not Detected
Threat Mitigation..... Not Done
Client Name.....
Time Since Created..... 0d:01:53:46
Channel..... 11
Auth RSSI..... 18
Auth Signal..... -78
Auth Noise..... -71

Probe Req..... 0

Probe Collection Interval..... 0d:00:00:14

Highest Num Probes..... 0

Auth Req..... 0

Auth Collection Interval..... 0d:00:00:14

Highest Num Auth Msgs..... 0

DeAuth Req..... 0

DeAuth Collection Interval..... 0d:00:00:14

Highest Num DeAuth Msgs..... 0

Num Auth Failures..... 0

Total Probe Msgs..... 2

Broadcast BSSID Probes..... 1

Broadcast SSID Probes..... 1

Specific BSSID Probes..... 0

Specific SSID Probes..... 0

Last Non-Broadcast BSSID..... 00-00-00-00-00-00

Last Non-Broadcast SSID.....

Threat Mitigation Sent..... 0d:00:00:00

Notice: If MAC address of client is not appointed, show client MAC, client Name, status, age and create time only.

Table 1-10 explanation of status information of client

Parameters	Explanation
MAC Address	MAC address of Client.
OUI	OUI of Client.
Client Status	Status of Client.
Auth Status	Show if client is authenticated.
Time Since Last Updated	The time interval from table updating to now.
Threat Detection	Show if enable 7 kinds of threat detection.
Threat Mitigation	Show if mitigate client.
Client Name	Show name of Client.
Time Since Created	The creating time of table entry.
Channel	The work channel of Client.
Auth RSSI	RSSI of client which is scanned by AP.
Auth Signal	The RF signal strength of client which is scanned by AP. The range is dBm.
Auth Noise	The noise strength of client which is scanned by AP. The range is dBm.

Probe Req	The number of times that scanning the probing requisition frame.
Probe Collection interval	The remainder time of scanning.
Highest Num Probes	The threshold of scanning the probing requisition frame.
Auth Req	The number of recording 802.11 authentication when scanning.
Auth Collection Interval	Scanning is over and make sure the remainder time before client is illegal or not.
Highest Num Auth Msgs	The authentication threshold which is done by AC when scanning.
DeAuth Req	The number of recording 802.11 relieving authentication when scanning.
DeAuth Collection Interval	Scanning is over and make sure the remainder time before client is illegal or not.
Highest Num DeAuth Msgs	The maximum number of AC dealing with relieving authentication in interval of statistic set.
Num Auth Failures	The failure 802.1X authentication number of client.
Total Probe Messages	The total number of probing of the last RF scanning.
Broadcast BSSID Probes	The broadcast BSSID probing number of the last RF scanning.
Broadcast SSID Probes	The broadcast SSID probing number of the last RF scanning.
Specific BSSID Probes	The unicast BSSID probing number of the last RF scanning.
Specific SSID Probes	The unicast SSID probing number of the last RF scanning.
Last Non-Broadcast BSSID	The last non-broadcast BSSID in RF scanning.
Last Non-Broadcast SSID	The last non-broadcast SSID in RF scanning.
Threat Mitigation Sent	The time from the last sending mitigation message to client to now.

1.7.6 show wireless client detected-client triangulation

Command：show wireless client *<macaddr>* detected-client triangulation

Function： Show the signal triangulation status of the appointed client.

Parameters： *<macaddr>*，MAC address of client.

Default： None.

Command Mode： Admin Mode.

Usage Guide： Inquire the appointed client information in Detected clients list and show

the signal triangulation status of client through this command.

Example：Show the signal triangulation status of the client whose MAC address is f8-db-7f-4d-f6-61 in Detected client list.

AC# show wireless client f8-db-7f-4d-f6-61 detected-client triangulation

AP Function	AP MAC Address	Radio	RSSI (%)	Signal (dBm)	Noise (dBm)	Age
Non-Sentry	00-03-0f-04-02-c0	1	18	-78	-71	0d:00:22:23
Non-Sentry	00-03-0f-04-02-00	1	16	-79	-88	0d:00:28:23

Table 1-11 explanation of signal triangulation status of client

Parameters	Explanation
AP Function	Appoint if this AP works in sentry mode.
AP Mac Address	MAC address of this AP.
RSSI	The RSSI value of Client receiving signal.
Signal	The RF signal strength of AP scanning client. The range is dBm.
Noise	The noise strength of AP scanning client. The range is dBm.
Detected Time	The time from AP discovering this client signal. The range is second.

1.7.7 show wireless detected-client roam-history

Command：show wireless detected-client [<*macaddr*>] roam-history

Function：Show the roaming history of the appointed clients or all clients in detected client list. One client shows 10 at most.

Parameters：**<*macaddr*>,** the MAC address of client. If the MAC address is not appointed, show client MAC and AP MAC only.

Default：None.

Command Mode：Admin Mode.

Usage Guide：Inquire the roaming history of the appointed clients or all clients in Detected Clients Roam History list through this command.

Example：Show the roaming history of all clients in Detected Clients Roam History list.

AC#show wireless client detected-client roam-history

MAC Address AP MAC Address

---------- ----------

e0-05-c5-90-1c-54 <- 00-03-0f-04-02-00

AC#show wireless client e0-05-c5-90-1c-54 detected-client roam-history

Client MAC Address..... e0-05-c5-90-1c-54

AP MAC Addr(Radio) VAP MAC Address SSID Auth Time since

Status Event

---------- ---------- ---------- -------- ----------

00-03-0f-04-02-00(1) 00-03-0f-04-02-00 xuwf1 Roam 0d:00:01:39

Table 1-12 explanation of client roaming history

Parameters	Explanation
Macaddr	The MAC address of Client.
AP Mac Address	The MAC address of dealing with the advance identity test to AP of client.
Radio	Radio of AP.
VAP Mac Address	The MAC address of Client roaming to the new VAP.
SSID	RF noise of AP scanning client.
Auth Status	Show client is the new authentication or roaming.
Time Since Roam	The time from the entries updating to now.

1.8 Radius Configuration

1.8.1 aaa enable

Command：aaa enable

no aaa enable

Function：This command is used for configuring to enable global authentication function. The no command disables this function.

Parameters：None.

Default：Disable.

Command Mode：Global Configuration Mode.

Usage Guide：Only when configuring this command, the controller will send authentication requesting packets to radius authentication server.

Example：Enable global authentication function.

AC(Config)# aaa enable

1.8.2 aaa-accounting enable

Command：**aaa-accounting enable**

no aaa-accounting enable

Function：This command is used to configure to enable global accounting function, the no command disables this function.

Parameters：None.

Default：Disable.

Command Mode：Global Configuration Mode.

Usage Guide：Only when configuring this command, the controller will send accounting requesting packets to radius accounting server.

Example：Enable global accounting function.

AC(Config)# aaa-accounting enable

1.8.3 aaa group server radius

Command：**aaa group server radius WORD**

no aaa group server radius WORD

Function：Use this command to configure an aaa radius server group name and enter the aaa radius server group configuration mode. The no command deletes this aaa radius server group.

Parameters:WORD：the name of aaa group server radius. It is a string with 32 characters most.

Default：None.

Command Mode：Global Configuration Mode.

Usage Guide：Use this command to configure an aaa radius server group

Example：Use this command to configure an aaa radius server group and its name is group1.

AC(Config)# aaa group server radius group1

1.8.4 deadtime

Command：deadtime <*1-255*>

no deadtime

Function：Use this command to configure deadtime of aaa radius server group, the no command recovers to be default.

Parameters: <*1-255*>：deadtime value, the range is 1 to 225 and the unit is minute.

Default： 5 minutes.

Command Mode：aaa Radius Server Group Configuration Mode.

Usage Guide：Use this command to configure deadtime of aaa radius server group.

Example：Use this command to configure deadtime of aaa radius server group1.

AC(Config)# aaa group server radius group1

AC (config-sg-radius)# deadtime 2

1.8.5 nas-identifier

Command: nas-identifier<*string*>

no nas-identifier

Function: Configure nas device to send nas-identifier property in packets to radius server. This property is used for supporting roaming accounting, settlement and position server. The no command recovers to be default.

Parameters: <*string*>*,* the range is no more than 32 characters. The format is HST.CTY.PRO.OPE.NAT (the "." among the number is just used for convenient to mark, in the actual parameter configuration and packets transmission, 16 numbers are needed only). WLAN access device needs to configure different WLAN access place number for different hotspot areas.

Command Mode: Radius Group Configuration Mode

Default: The CPU MAC address of switch pluses 1, MAC address is broke up by "-".

Usage Guide: This command is used to mark the position and range switch of nas device belongs to. This value can be configured according to different requirements; it can be configured as numbers and can be also string.

Example: Configure nas-identifier as number or string.

AC(config-sg-radius)#nas-identifier 1234001010000460

AC(config-sg-radius)#nas-identifier abcdgethfgshtrjhfdf

1.8.6 nas-port-type

Command: nas-port-type *{virtual | ethernet | wireless-other | wireless-802-11| wireless-802-16 | pppoa | pppoeoa |pppoeoe | pppoeovlan |pppoeoqinq |value <int-value>}*

no nas-port-type

Function: This command is used to configure access port types of interface. The no command deletes the interface type.

Parameters: *virtual* | *ethernet* | *wireless-other* | *wireless-802-11*| *wireless-802-16* | *pppoa* | *pppoeoa* |*pppoeoe* | *pppoeovlan* |*pppoeoqinq* |*value <int-value>:* it is used to mark different interface types;

Virtual: Virtual interface type, the related number value is 5;

Ethernet: Ethernet interface type, the related number value is 15;

wireless-other: Wireless-other interface type, the related number value is 18;

wireless-802-11: It meets the interface type of Wireless-IEEE 802.11 standard, the related number value is 19;

Wireless-IEEE-802-16: Air Interface for Fixed and Mobile Broadband Wireless Access Systems, the related number value is 27;

Pppoa: PPP over ATM, the related number value is 30;

pppoeoa: PPP over Ethernet over ATM, the related number value is 31;

pppoeoe - PPP over Ethernet over Ethernet, the related number value is 32;

pppoeovlan - PPP over Ethernet over VLAN, the related number value is 33;

pppoeoqinq - PPP over Ethernet over IEEE 802.1QinQ, the related number value is 34;

Value <int-value>, the other values except the number value of the above parameters, the range is 1 to 128, for example, the value of int-value is 17, it means the interface type is Cable.

Command Mode: Radius Group Configuration Mode.

Default: The interface type is Ethernet.

Usage Guide: This command is used to mark the authentication type interface adopts of client. The value can be configured as characters and can be also configured as numbers; some numbers and string are corresponding.

Example: Configure the interface type of client as wireless-other and configure the value as 12.

AC(config-sg-radius)#nas-port-type wireless-other

AC(config-sg-radius)#nas-port-type value 12

1.8.7 nas-port

Command: nas-port *<int-value>*

no nas-port

Function: This command is used to mark the physical port connected between client and switch.

Parameters: <int-value>, it means nas-port value and the range is 0 to 65535.

Command Mode: Radius Group Configuration Mode.

Default: 1.

Usage Guide: This command is used to mark the physical port connected between client and switch.

Example: Configure the physical port connected between client and switch as 17.

AC(config-wireless)# nas-port 17

1.8.8 radius-attribute vlan-id format

Command：radius-attribute vlan-id format {integer|string}

Function： Use this command to configure the vlan-id type issued by radius on AC.

Parameters：integer is integer type;

string is string type.

Default： integer.

Command Mode： aaa radius server group configuration mode.

Usage Guide： Use this command to configure the vlan-id type issued by radius on AC. Make the vlan-id type of radius match to the vlan-id type of AC.

Example： Configure the vlan-id type issued by radius on AC as string.

AC(config-sg-radius)#radius-attribute vlan-id format string

1.8.9 radius nas-ipv4

Command：radius nas-ipv4 *<A.B.C.D>*

no radius nas-ipv4

Function： Appoint source address of radius packets, the no command deletes the appointed source address of radius packets.

Parameters：A.B.C.D：the source IP address of radius packets.

Default： Do not appoint the source address as default.

Command Mode： Global Configuration Mode.

Usage Guide： Use this command to configure a radius source address.

Example：Appoint the source IP address of radius packets as 192.168.40.2.

AC(Config)# radius nas-ipv4 192.168.40.2

1.8.10 radius-server accounting host

Command：**radius-server accounting host <*A.B.C.D*> [port <*0-65535*>] [key WORD] [primary]**

no radius-server accounting host <*A.B.C.D*>

Function：This command is used to configure the appointed radius accounting server host. The no command deletes the appointed radius accounting server host.

Parameters：**<*A.B.C.D*>**：IP address of RADIUS accounting server host.

port <*0-65535*>：port number of RADIUS accounting server host. The range is 0 to 65535.

WORD：the key of RADIUS accounting server, it is a string with 16 characters most.

primary：judge if this server is the master server, if configureing this parameter, it is master server, otherwise, it is backup server.

Default：The default of port value is 1813 and it is free for the key value.

Command Mode：Global Configuration Mode.

Usage Guide：Use this command to configure a radius accounting server.

Example：Configure radius accounting server and the IP address is 192.168.10.1, the port is 19, the key is test. And it is master server.

AC(Config)# radius-server accounting host 192.168.10.1 port 19 test primary

1.8.11 radius-server authentication host

Command：**radius-server authentication host <*A.B.C.D*> [port <*0-65535*>] [key WORD] [primary]**

no radius-server authentication host <*A.B.C.D*>

Function：This command is used to configure the appointed radius authentication server host. The no command deletes the appointed radius authentication server host.

Parameters: <*A.B.C.D*>：the IP address of RADIUS authentication server.

port <*0-65535*>：the UDP port number of RADIUS authentication server and the range is 0 to 65535.

WORD：define the shared password of the controller communicating to radius authentication server. it is a string with 16 characters most.

primary：judge if this server is the master server, if configureing this

parameter, it is master server, otherwise, it is backup server.

Default：The default of port value is 1812, the default of key is free and it is false for primary.

Command Mode：Global Configuration Mode.

Usage Guide：Use this command to appoint radius authentication server host. The no command deletes the radius authentication server host. In order to achieve AAA authentication service by using radius, radius authentication server must be configured. **radius-server authentication host** command can be used to define one or more radius authentication server.

Example：Configure radius authentication server, the IP address is 192.168.10.1, the port number is 18, the key is test and it is master server.

AC(Config)# radius-server authentication host 192.168.10.1 port 18 test primary

1.8.12 radius-server dead-time

Command：**radius-server dead-time <*1-255*>**

no radius-server dead-time

Function：After user sending packets, if there is no response in the time of t, the server is considered dead. Then t will be called dead-time. Use this command to configure radius dead-time. The no command recovers to be default.

Parameters：<*1-255*>：deadtime value. The range is 1 to 255 and the unit is minute.

Default：5 minutes.

Command Mode：Global Configuration Mode.

Usage Guide：Use this command to configure radius dead-time.

Example：Configure radius dead-time as 8 minuts.

AC(Config)# radius-server dead-time 8

1.8.13 radius-server key

Command：**radius-server key WORD**

no radius-server key

Function：This command is used to configure the global shared password of the controller communicating to radius authentication server. The no command recovers to be default of free.

Parameters：WORD: The shared password of the controller communicating to radius authentication server. It is a string with 16 characters most.

Default：Free.

Command Mode：Global Configuration Mode.

Usage Guide：If radius server is not configured the shared password, use this command to configure the global shared password as it.

Example：Configure the global shared password of the controller communicating to radius authentication server as test.

AC(Config)# radius-server key test

1.8.14 radius-server retransmit

Command：**radius-server retransmit <*0-100*>**

no radius-server retransmit

Function：Use this command to configure the times of retransmitting packets before radius safety server does not have reaction. The no command recovers to be default.

Parameters：**<*0-100*>**：times of timeout retransmission. The range is 0 to 100.

Default：3 times.

Command Mode：Global Configuration Mode.

Usage Guide：The premise of AAA using next way to authenticate to user is that the current safety server of authentication does not have reaction. The standard of equipment judging that the safety server does not have reaction is that the safety server does not have reaction when equipment retransmits the appointed times radius packets and there is timeout between retransmission.

Example：Configure radius timeout retransmission times as 5.

AC(Config)# radius-server retransmit 5

1.8.15 radius-server timeout

Command：**radius-server timeout <*1-1000*>**

no radius-server timeout

Function：Use this command to configure time of retransmission radius packets waiting for reaction of safety server. The no command recovers to be default.

Parameters: <*1-1000*>：timeout. The range is 1 to 1000 and the unit is second.

Default：3 seconds.

Command Mode：Global Configuration Mode.

Example：Configure radius timeout as 2 seconds.

AC(Config)# radius-server timeout 2

1.8.16 server

Command：server <*A.B.C.D*> [auth-port <*0-65535*> | acct-port <*0-65535*>]

no server <*A.B.C.D*> [auth-port <*0-65535*> | acct-port <*0-65535*>]

Function：Use this command to add the server of aaa radius server group. The no command deletes this server.

Parameters: <*A.B.C.D*>：IP address of server.

auth-port <*0-65535*>: port number of authentication server. the range is 0 to 65535.

acct-port <*0-65535*>： port number of accounting server. the range is 0 to 65535.

Default：The default of auth-port value is 1812 and it is 1813 for acct-port value.

Command Mode：Aaa Radius Server Group Configuration Mode.

Usage Guide：Use this command to add radius server to aaa radius server group. The authentication server and accounting server in this radius server must exist in global configuration.

Example：Use this command to add a radius server to aaa radius server group1. The IP address is 192.168.10.1, the authentication UDP port is 123 and the accounting UDP port is 456.

AC(Config)# aaa group server radius group1

AC (config-sg-radius)# server 192.168.10.1 auth-port 123 acct-port 456

1.9 Commands for User Offline Based on Flow

1.9.1 offline-detect

Command: offline-detect

no offline-detect

Function: Enable the offline-detect function based on flow on AC. The no command disables this function. When the on-off of the offline-detect function is changed, it should be issued to AP manually and AP detects the flow.

Parameters: None.

Default: Disable.

Command Mode: Network Config Mode.

Usage Guide: After enabled this function, AP detects the user flow. After used the no command, the offline-detect function can be disabled, AP cannot detect the user flow any more. At the same time, the idle-timeout and flow threshold will be recovered to be default

values.

Example: Enable/disable the offline-detect function based on flow of network1.

AC(config-wireless)#network 1

AC(config-network)#offline-detect

AC(config-network)#no offline-detect

1.9.2 offline-detect (idle-timeout [seconds]|) (threshold [bytes]|)

Command: offline-detect (idle-timeout [seconds]|) (threshold [bytes]|)

Function: Configure the idle-timeout and flow threshold of the offline-detect function. When the parameters are changed, they should be issued to AP manually.

Parameters: <seconds>: the maximum interval that the user is allowed being free after online, the range is from 60 to 7200 seconds.

<bytes>: the minimum data flow (the sum of uplink and downlink flow) that the user is allowed being free, the range is from 0 to 33554432 Bytes (32M).

Default: The default idle-timeout is 300s; the default flow threshold is 0KB.

Command Mode: Network Config Mode.

Usage Guide: After enabled this command, the ranges of seconds and bytes will be detected. If they are not in the lawful ranges, there will be the prompt of error; if they are in the lawful ranges, the idle-timeout and flow threshold on AC are effective.

When enabled the offline-detect function, if the idleTimeout or threshold is not the default value, the format of show run is offline-detect idletimeout <vlaue> threshold <value>; if they are both the default values, the format of show run is offline-detect.

Example: Configure the idle-timeout as 400s and configure the flow threshold as 1000bytes.

AC(config-network)#offline-detect idle-timeout 400 threshold 1000

1.10 Commands for Debug

1.10.1 debug wireless auth wdm

Command：debug wireless auth wdm *<macaddr>*

no debug wireless auth wdm *<macaddr>*

Function：Enable client authentication in wireless module or the WDM debug information in AP authentication.

Parameters：<*macaddr*>: the MAC address of client or AP. Examine the WDM information of an user or AP authentication.

Default：Disable.

Command Mode：Admin Mode.

Usage Guide：Enable/disable WDM debug information of client or AP authentication through this command.

Example：Enable WDM debug information of client authentication whose MAC address is 00-03-0f-01-02-03.

AC# debug wireless auth wdm 00-03-0f-01-02-03

1.10.2 debug wireless client-association packet

Command： **debug wireless client-association packet {all| receive | dump} *<macaddr>***

no debug wireless client-association packet {all | receive | dump} *<macaddr>*

Function：Enable the receiving and sending packets debug information in all client association requesting of the appointed AP. Examine the packets debug information which is dealt by AC.

Parameters：receive：Enable the debug information of receiving packets from AP in client association.

dump：Enable the debug information of Client association and load balancing packet dumps.

all：Enable the debug information of receiving and sending packets in client association.

<*macaddr*>：the MAC address of AP that AC receives and sends packets to. One AP can be choose to debug.

Default：Disable.

Command Mode：Admin Mode.

Usage Guide：Enable/disable the packets debug information in client association requesting through this command.

Example：Enable the receiving and sending packets debug information in all client association requesting of the appointed AP whose MAC address is 00-03-0f-01-02-00.

AC# debug wireless client-association packet all 00-03-0f-01-02-00

1.10.3 debug wireless client-association internal-info

Command：**debug wireless client-association internal-info *<macaddr>***

no debug wireless client-association internal-info *<macaddr>*

Function：Enable the internal debug information of all client association requesting under

the appointed AP. Examine the internal debug information.

Parameters：*<macaddr>*： the MAC address of AP which is associated with client. One AP can be choose to debug.

Default： Disable.

Command Mode： Admin Mode.

Usage Guide： Enable/disable the internal debug information in client association requesting through this command.

Example： Enable the detailed internal debug information in all client association requesting of the appointed AP whose MAC address is 00-03-0f-01-02-00.

AC# debug wireless client-association internal-info 00-03-0f-01-02-00

1.10.4 debug wireless client-auth error

Command：debug wireless client-auth error

no debug wireless client-auth error

Function： Enable the error debug information in wireless module. Examine the error debug information when AC deals with client association, authentication, advance identity test, disassociation and load balance.

Parameters： None.

Default： Disable.

Command Mode： Admin Mode.

Usage Guide： Enable/disable the error debug information in wireless module through this command.

Example： Enable the error debug information in wireless module.

AC#debug wireless client-auth error

1.10.5 debug wireless client-auth radius-info

Command：debug wireless client-auth radius-info *<macaddr>*

no debug wireless client-auth radius-info *<macaddr>*

Function： Enable radius debug information of client authentication in wireless module.

Parameters： *<macaddr>*：the MAC address of client. Examine radius debug information of user authentication.

Default： Disable.

Command Mode： Admin Mode.

Usage Guide： Enable/disable radius debug information of client authentication through this command.

Example： Enable radius debug information of client authentication access module whose

MAC address is 00-1b-77-22-75-27.

AC#debug wireless client-auth radius-info 00-1b-77-22-75-27

1.10.6 debug wireless client-auth internal-info

Command：debug wireless client-auth internal-info <*macaddr*>

no debug wireless client-auth internal-info <*macaddr*>

Function：Enable the internal debug information of all client authentication requesting under the appointed AP. Examine the detailed internal debug information.

Parameters：<*macaddr*>：the MAC address of AP which is authenticated by AC. One AP can be choose to debug.

Default：Disable.

Command Mode：Admin Mode.

Usage Guide：Enable/disable the internal debug information of client association through this command.

Example：Enable the detailed internal debug information of all client authentication requesting dealt by AC and the MAC address of AP is 00-03-0f-01-02-03.

AC# debug wireless client-auth internal-info 00-03-0f-01-02-03

1.10.7 debug wireless client-auth packet

Command：debug wireless client-auth packet {all | receive | send | dump} <*macaddr*>

no debug wireless client-auth packet {all | receive | send | dump} <*macaddr*>

Function：Enable the receiving and sending packets debug information of all client authentication requesting under the appointed AP. Examine the packets debug information.

Parameters：send：enable the sending packets debug information of client authentication.

receive：enable the receiving packets debug information of client authentication.

dump：enable the packet dump information of client authentication.

all：enable the all debug information of client authentication.

<*macaddr*>：the MAC address of AP which sends or receives packets. One AP can be choose to debug.

Default：Disable.

Command Mode：Admin Mode.

Usage Guide：Enable/disable the sending and receiving packets debug information of

clien authentication requesting dealt by AC through this command.

Example：Enable the sending and receiving packets debug information of all client authentication requesting dealt by AC and the MAC address of AP is 00-03-0f-01-02-03.

AC# debug wireless client-auth packet 00-03-0f-01-02-03

1.10.8 debug wireless client-disasso packet

Command：**debug wireless client-disasso packet {all | receive | send } <*macaddr*>**

no debug wireless client-disasso packet {all | receive | send } <*macaddr*>

Function：Enable the receiving and sending packets debug information of all client disassociation under the appointed AP. Examine the packets debug information.

Parameters：send：enable the sending packets debug information that AC send enforcement relieving client command to AP.

receive：enable the receiving packets debug information that AC deals with client disassociation message from AP.

all：enable all sending and receiving packets debug information of client disassociation.

<*macaddr*>：the MAC address of AP which sends or receives packets. One AP can be choose to debug.

Default：Disable.

Command Mode：Admin Mode.

Usage Guide：Enable /disable the packets debug information of client disassociation dealt by AC through this command.

Example：Enable the receiving and sending packets debug information of all client disassociation under the appointed AP whose MAC address is 00-03-0f-01-02-03.

AC# debug wireless client-disasso packet all 00-03-0f-01-02-03

1.10.9 debug wireless client-pmk

Command：**debug wireless client-pmk <*macaddr*>**

no debug wireless client-pmk <*macaddr*>

Function：Enable debug information of the appointed client PMK auth. Examine the packets debug information when AC deals with client PMK authentication.

Parameters：<*macaddr*>：the MAC address of client. One PMK authentication of user can be choose to debug.

Default：Disable.

Command Mode：Admin Mode.

Usage Guide：Enable/disable the debug information of client PMK authentication dealt by AC through this command.

Example：Enable the debug information of client PMK authentication whose MAC address is 00-22-fa-25-dc-a0.

AC# debug wireless client-pmk 00-22-fa-25-dc-a0

1.10.10 debug wireless client-preauth

Command：**debug wireless client-preauth <*macaddr*>**

no debug wireless client-preauth <*macaddr*>

Function：Enabling debug information of advance identity authentication of the appointed client can examine the debug information that AC deals with advance identity authentication of client.

Parameters：<*macaddr*>：MAC address of client, debug against to an user who does the advance identity authentication.

Default：Disable.

Command Mode：Admin Mode.

Usage Guide：Enable/disable debug information that AC deals with advance identity authentication of client through this command.

Example：Enable/disable debug information that AC deals with advance identity authentication of client whose MAC address is 00-22-fa-25-dc-a0.

AC# debug wireless client-preauth 00-22-fa-25-dc-a0

Chapter 2 Commands for Captive Portal Authentication

2.1 Commands for Authentication Function

2.1.1 ac-name

Command: ac-name <word>

no ac-name

Function: Configure the parameter of wlanacname in the redirect url. The no command deletes it.

Parameters: <word>, it is the value of wlanacname including 32 characters at most.

Command Mode: Captive Portal Instance Mode.

Default: None.

Usage Guide: This command is used to configure the parameter of wlanacname in the redirect url. Some portal servers can pass the authentication only with the specific wlanacname. So this command should be configured according to the requirement of the portal server.

Example: Configure the wlanacname in the redirect url as 0100.0010.010.00 according to the standard of the mobile portal server, and the format is ACN.CTY.PRO.OPE.

AC(config-cp-instance)#ac-name 0100.0010.010.00

2.1.2 authentication-mode

Command: authentication-mode {pap|chap}

no authentication-mode

Function: This command is used to configure the encryption method used in authentication between client and authentication server. Use pap method or chap method.

Command Mode: Captive Portal Global Configuration Mode.

Default: chap authentication.

Usage Guide: This command is used to configure the encryption method used in authentication between client and authentication server.

Example: Configure the authentication method as chap, delete chap configured to recover it to be default.

AC(config-cp)# authentication-mode chap

AC(config-cp)# no authentication-mode

2.1.3 authentication-type

Command: authentication-type {internal | external}

Function: This command to configure the type of portal server, when it is configured as external, select the external portal server to launch the redirection page; when it is configured as internal, select built-in portal server to launch the redirection page. Built-in portal server function is provided by portal server module within AC.

Parameter: internal: internal portal server.

external: external portal server.

Default: external portal server.

Command Mode: Captive Portal global configuration mode.

Usage Guide: Set the portal server type.

Example: Configure the portal server type as external.

AC(config-cp)# authentication-type external

2.1.4 authentication timeout

Command: authentication timeout <*timeout*>

no authentication timeout

Function: Configure the Captive Portal authentication timeout, within the timeout period the user does not input a valid authentication credentials, the authentication page will be timeout, the user needs to reconnect to open the authentication page. the no command will restore the default configuration.

Parameter: <*timeout*> Portal authentication timeout, range is 60 to 600.

Default: 300s.

Command Mode: Captive Portal global configuration mode.

Usage Guide: Set the timeout of Captive Portal authentication.

Example: Set the timeout of Captive Portal authentication.

AC(config-cp)# authentication timeout 100

2.1.5 block

Command: block

no block

Function: Block all communications in the Captive Portal configuration. The users who have passed portal authentication will be forced offline, and disassociated with wireless

authentication access point, client which does not pass the portal authentication can not be redirected and authenticated, and it will disassociate with the wireless controller and wireless authentication access point. The no command will disable this function and restore the normal user authentication function.

Parameter: None.

Default: None.

Command Mode: Captive Portal Instance configuration mode.

Usage Guide: Block all communications of Captive Portal configuration.

Example: Block all communications of Captive Portal configuration.

AC(config-cp-instance)# block

2.1.6 captive-portal

Command: captive-portal

Function: Use this command to enter Captive Portal configuration mode.

Parameter: None.

Default: None.

Command Mode: Global configuration mode.

Usage Guide: Use this command to enter Captive Portal configuration mode.

Example: Enter captive portal configuration mode for configuring.

AC(config)#captive-portal

2.1.7 clear

Command: clear

Function: This command sets the configuration of the routine to be the default value.

Parameter: None.

Default: None.

Command Mode: Captive Portal Instance configuration mode.

Usage Guide: Set the configuration of the portal routine to be the default value.

Example: Set the configuration of the routine to be the default value.

AC(config-cp-instance)# clear

2.1.8 configuration

Command: configuration <*cp-id*>

no configuration <*cp-id*>

Function: Use this command to enter Captive Portal routines Mode. The no command

will delete the Portal Captive routine configuration..

Parameter: <*cp-id*> is the number of Captive Portal routines, range is 1 to 10.

Default: None.

Command Mode: Captive Portal global configuration mode.

Usage Guide: This configuration is used to configure Captive Portal routines. Each routine represents a class of users, users under the same routine have the same flow and rate configuration, etc., and vice versa. No command will delete a captive portal configuration. If there is an interface associated with a routine, then the no command will be invalid.

Example: Set the ID parameter as 4.

AC(config-cp)#configuration 4

2.1.9 debug captive-portal packet

Command: debug captive-portal packet {send|receive|dump|all}

no debug captive-portal packet {send|receive|dump|all}

Function: Enable the packet debugging on-off of the captive portal authentication. The no command disables it.

Parameters: send: enables the debugging information of sending packet of captive portal;

receive: enables the debugging information of receiving packet of captive portal;

dump: enables the debugging information of dumping packet of captive portal;

all: enables the debugging information of sending, receiving and dumping packet of captive portal.

Command Mode: Admin Mode.

Default: Disable.

Usage Guide: This command is used to enable the packet debugging on-off of the captive portal authentication.

Example: Enable all the packets debugging information of the captive portal authentication.

AC#debug captive-portal packet all

2.1.10 debug captive-portal-cluster packet

Command: debug captive-portal-cluster packet {send|receive|dump|all}

no debug captive-portal-cluster packet {send|receive|dump|all}

Function: Enable the roaming packet debugging on-off of the captive portal

authentication. The no command disables it.

Parameters: send: enables the debugging information of roaming sending packet of captive portal;

receive: enables the debugging information of roaming receiving packet of captive portal;

all: enables the debugging information of roaming sending and receiving packet of captive portal.

Command Mode: Admin Mode.

Default: Disable.

Usage Guide: This command is used to enable the roaming packet debugging on-off of the captive portal authentication.

Example: Enable all the roaming packets debugging information of the captive portal authentication.

AC#debug captive-portal-cluster packet all

2.1.11 debug captive-portal trace

Command: debug captive-portal trace

no debug captive-portal trace

Function: Enable the tracing debugging of the captive portal authentication. The no command disables it.

Parameters: None.

Command Mode: Admin Mode.

Default: Disable.

Usage Guide: This command is used to enable the tracing debugging of the captive portal authentication.

Example: Enable the tracing debugging of the captive portal authentication.

AC#debug captive-portal trace

2.1.12 debug captive-portal detail event

Command: debug captive-portal detail event

no debug captive-portal detail event

Function: Enable the packet detail debugging of the captive portal authentication. The no command disables it.

Parameters: None.

Command Mode: Admin Mode.

Default: Disable.

Usage Guide: This command is used to enable the packet detail debugging of the captive portal authentication.

Example: Enable the packet detail debugging of the captive portal authentication.

AC#debug captive-portal detail event

2.1.13 debug captive-portal-cluster info

Command: debug captive-portal-cluster info

no debug captive-portal-cluster info

Function: Enable the roaming tracing debugging of the captive portal authentication. The no command disables it.

Parameters: None.

Command Mode: Admin Mode.

Default: Disable.

Usage Guide: This command is used to enable the roaming tracing debugging of the captive portal authentication.

Example: Enable the roaming tracing debugging of the captive portal authentication.

AC#debug captive-portal-cluster info

2.1.14 debug captive-portal error

Command: debug captive-portal error

no debug captive-portal error

Function: Enable the error debugging of the captive portal authentication. The no command disables it.

Parameters: None.

Command Mode: Admin Mode.

Default: Disable.

Usage Guide: This command is used to enable the error debugging of the captive portal authentication.

Example: Enable the error debugging of the captive portal authentication.

AC#debug captive-portal error

2.1.15 enable (global)

Command: enable

disable

Function: Use this command to enable the Captive Portal function of the controller

globally, use disable function to disable the Captive Portal function of the controller globally.

Parameter: None.

Default: Disable.

Command Mode: Captive Portal global configuration mode.

Usage Guide: Use this command to enable global Captive Portal characteristics on the controller.

Example: Enable the global Captive Portal function on the controller.

AC(config-cp)#enable

2.1.16 enable (routine)

Command: enable

disable

Function: Enable Captive Portal configuration.

Parameter: None.

Default: Enable Captive Portal configuration.

Command Mode: Captive Portal Instance configuration mode.

Usage Guide: disable command will disable the captive-portal function, after disabling this command, the portal users will be forced offline.

Example: Enable captive-portal function.

AC(config-cp-instance)#enable

2.1.17 external portal-server server-name

Command: external portal-server server-name <*name*> {ipv4 | ipv6} <*ipaddr*> [port <*1-65535*>]

no external portal-server {ipv4 | ipv6}server-name <*name*>

Function: Configure the external portal server. Launch the redirect page through this server, after inputting the correct user name and password, the authentication is successful and the wireless client can access the outside network.

Parameter: <*name*> is name of external portal server.

<*ipaddr*> is ip address of external portal server.

ipv4 the configured portal server address is ipv4 address.

ipv6 the configured portal server address is ipv6 address.

<*1-65535*> is number of portal server.

Default: None.

Command Mode: Captive Portal global configuration mode.

Usage Guide: Configure external portal servers, 10 can be configured at most. Each cp configuration can be bound to one portal server.

Example: Configure a external portal server.

AC(config-cp)# external portal-server server-name x1 ipv4 1.0.0.1 port 11111

2.1.18 http port

Command: http port *<port-num>*

no http port

Function: Use this command to add additional HTTP port. The no command will restore the default http port configuration.

Parameter: *<port-num>* the effective port range is 0 to 65535, port 80 and 443 are reserved. HTTP default port is 0, which means that there is no additional port added and the default port (80) has been used.

Default: 0.

Command Mode: Captive Portal Instance configuration mode.

Usage Guide: This command can add or delete additional HTTP authentication port, the client can launch authentication to the added port and be responded, **no http port** command will delete the added additional http port, the user's http request will be responded automatically through port 80.

Example: Add HTTP port 88.

AC(config-cp-instance)#http port 88

2.1.19 interface ws-network

Command: interface ws-network *<1-1024>*

no interface ws-network *<1-1024>*

Function: The command can bind the Captive Portal interface and the captive configuration. The no command will remove the configuration.

Parameter: *<1-1024>* is network ID.

Default: None.

Command Mode: Captive Portal Instance configuration.

Usage Guide: The command can bind the Captive Portal interface and the captive configuration.

Example: Bind the network of interface 4 to the Captive Portal routine.

AC(config-cp-instance)# interface ws-network 4

2.1.20 listen portal-server-port

Command: listen portal-server-port <1-65535>

no listen portal-server-port

Function: Configure AC to listen the portal server packet port. This port is also the source port that AC sends packets to portal server. The no command recovers it to be the default port.

Parameters: <1-65535>, it is the configured port number.

Command Mode: Captive Portal Instance Mode.

Default: The default port is 2000.

Usage Guide: This command is used to listen the portal server packet port. This port is also the source port that AC sends packets to portal server. Configures the port for listening on AC according to the destination port of the portal server packet, AC can deal with the packet from portal server normally.

Example: Configure AC to listen the portal server packet port of 7749.

AC(config-cp-instance)#listen portal-server-port 7749

2.1.21 max-bandwidth-down

Command: max-bandwidth-down <*0-536870911*>

no max-bandwidth-down

Function: Use this command to define the maximum downlink data rate of client network. The no command will restore the rate to the default state.

Parameter: <*0-536870911*> is the maximum downlink data rate of client network, the unit is byte.

Default: 0.

Command Mode: Captive Portal Instance configuration mode.

Usage Guide: This command defines the maximum rate of the downlink data, the unit is bps, the user's downlink maximum rate cannot exceed the set value when set the parameter.

Example: Define the maximum data rate that client can receive from network as 4096.

AC(config-cp-instance)#max-bandwidth-down 4096

2.1.22 max-bandwidth-up

Command: max-bandwidth-up <*0-536870911*>

no max-bandwidth-up

Function: This command defines the maximum data rate client can send to the network. The no command will restore the rate limit to the default state.

Parameter: ***<0-536870911>***, the maximum data rate client can send to the network, the unit is byte.

Default: 0.

Command Mode: Captive Portal Instance configuration mode.

Usage Guide: This command defines the maximum rate of the uplink data, the unit is bps, the user's uplink maximum rate cannot exceed the set value when set the parameter.

Example: Define the maximum data rate client can send to the network as 4096.

AC(config-cp-instance)#max-bandwidth-up 4096

2.1.23 max-input-octets

Command: max-input-octets *<0-4294967295>*

no max-input-octets

Function: This command defines the maximum bytes which allows users to transmit, after reaching the restriction defined, the user will be disconnected. The no command means the rate is not limited.

Parameter: ***<0-4294967295>***, the maximum bytes which allows users to transmit, unit is byte, the value of 0 means that the restriction function does not take effect.

Default: 0.

Command Mode: Captive Portal Instance configuration mode.

Usage Guide: This command limits the maximum bytes of user inputting, the maximum inputting bytes cannot exceed the restriction threshold in using of network resources, if it exceeds, user will be disassociated.

Example: Define the maximum bytes which allows users to transmit as 4096.

AC(config-cp-instance)# max-input-octets 4096

2.1.24 max-output-octets

Command: max-output-octets *<0-4294967295>*

no max-output-octets

Function: This command defines the maximum bytes which user can receive, after reaching the restriction defined, the user will be disconnected. The no command means the rate is not limited.

Parameter: ***<0-4294967295>***, the maximum bytes user can receive, unit is byte, the value of 0 means that the restriction function does not take effect.

Default: 0.

Command Mode: Captive Portal Instance configuration mode.

Usage Guide: The command limits the maximum bytes of user outputting, the maximum outputting bytes cannot exceed the restriction threshold in using of network resources, if it exceeds, user will be disassociated.

Example: Define the maximum bytes user can receive as 1024.

AC(config-cp-instance)# max-output-octets 1024

2.1.25 max-total-octets

Command: max-total-octets <*0-4294967295*>

no max-total-octets

Function: This command defines the maximum number of bytes which allows user to send and receive. after reaching the restriction defined, the user will be disconnected. The no command means the rate is not limited.

Parameter: <*0-4294967295*>, the maximum number of bytes which allows user to send and receive, unit is byte, the value of 0 means that the restriction function does not take effect.

Default: 0.

Command Mode: Captive Portal Instance configuration mode.

Usage Guide: The command limits the maximum number bytes of user inputting and outputting, the maximum inputting and outputting bytes number cannot exceed the restriction threshold in using of network resources, if it exceeds, user will be disassociated.

Example: The maximum number of bytes which allows user to send and receive as 1024.

AC(config-cp-instance)# max-total-octets 1024

2.1.26 name

Command: name <*cp-name*>

no name

Function: Define the name of Captive Portal configuration.

Parameter: <*cp-name*>, the name of Captive Portal configuration, 32 characters can be included at most and they can be numbers and letters.

Default: None.

Command Mode: Captive Portal Instance configuration mode.

Usage Guide: Define the name of Captive Portal configuration.

Example: Define the name of Captive Portal configuration as abc123.

AC(config-cp-instance)#name abc123

2.1.27 portal-server

Command: portal-server {ipv4 | ipv6} <*name*>

no portal-server {ipv4 | ipv6}

Function: This command can bind specific external portal server for the CP configuration. Networks under this CP configuration all redirect authentication through this portal server.

Parameter: <name> binding Portal server name.

ipv4 the bond portal server address is ipv4 address.

ipv6 the bond portal server address is ipv6 address.

Default: None.

Command Mode: Captive Portal Instance configuration mode.

Usage Guide: Use this command to bind specific external portal server for the CP configuration; it can also unbind the specific external portal server.

Example: Bind specific external portal server for the CP configuration.

AC(config-cp -instance)#portal-server ipv4 x1

2.1.28 protocol

Command: protocol {http | https}

Function: Configure a protocol mode Captive Portal supports.

Parameter: http: select http mode.

https: select https mode.

Default: https mode.

Command Mode: Captive Portal Instance configuration mode.

Usage Guide: Configure a protocol mode Captive Portal supports.

Example: Configure a protocol mode Captive Portal supports.

AC(config-cp-instance)# protocol https

2.1.29 radius-auth-server

Command: radius-auth-server <*server-name*>

no radius-auth-server

Function: Use this command to define the RADIUS authentication server of the Captive Portal configuration. The no command deletes the configuration.

Parameter: <*server-name*>, RADIUS authentication server name of Captive Portal configured.

Default: None.

Command Mode: Captive Portal Instance configuration mode.

Usage Guide: Define the RADIUS authentication server of the Captive Portal configuration.

Example: Define the RADIUS authentication server of the Captive Portal configuration as radius_aaa_1.

AC(config-cp-instance)#radius-auth-server radius_aaa_1

2.1.30 redirect attribute apmac enable

Command: redirect attribute apmac enable

no redirect attribute apmac enable

Function: Enable the function that the mac address of AP associated with the client is carried in the redirect url address. The no command disables it.

Parameters: None.

Command Mode: Captive Portal Instance configuration mode.

Default: As default, the mac address of AP associated with the client is not carried in the redirect url address.

Usage Guide: Configure the function that the mac address of AP associated with the client is carried in the redirect url address.

Example: Configure the function that the mac address of AP associated with the client is carried in the redirect url address.

AC(config-cp-instance)#redirect attribute apmac enable

2.1.31 redirect attribute apmac name

Command: redirect attribute apmac name<apmac-name>

no redirect attribute apmac name

Function: Configure the direct url address to carry the name of apmac. The no command recovers it to be the default value.

Parameters: <apmac-name>, it is the name of the configured apmac.

Command Mode: Captive Portal Instance configuration mode.

Default: The default name is apmac.

Usage Guide: This command can configure the direct url address to carry the name of apmac.

Example: Modify the the name of apmac which is carried in the direct url address to be vap.

AC(config-cp-instance)#redirect attribute apmac name vap

2.1.32 redirect attribute usermac enable

Command: redirect attribute usermac enable

no redirect attribute usermac enable

Function: Enable the function that the parameter of usermac is carried in the redirect url address. The no command cancels it.

Parameters: None.

Command Mode: Captive Portal Instance configuration mode.

Default: As default, the parameter of usermac is not carried in the redirect url address.

Usage Guide: Enable the function that the mac address of client is carried in the redirect url address.

Example: Configure the function that the mac address of client is carried in the redirect url address.

AC(config-cp-instance)#redirect attribute usermac enable

2.1.33 redirect attribute usermac name

Command: redirect attribute usermac name<usermac-name>

no redirect attribute usermac name

Function: Configure the direct url address to carry the name of usermac. The no command recovers it to be the default value.

Parameters: <usermac-name>, it is the name of the configured usermac.

Command Mode: Captive Portal Instance configuration mode.

Default: The default name is usermac.

Usage Guide: This command can configure the direct url address to carry the name of usermac.

Example: Modify the the name of usermac which is carried in the direct url address to be vap.

AC(config-cp-instance)#redirect attribute apmac name vap

2.1.34 redirect attribute custom-string name

Command: redirect attribute custom-string name<custom-string>

no redirect attribute custom-string name

Function: Configure the direct url address to carry the custom string. The no command cancels it.

Parameters: <custom-string>, it is the configured custom string.

Command Mode: Captive Portal Instance configuration mode.

Default: As default, the custom string is not carried in the redirect url address.

Usage Guide: Configure the direct url address to carry the custom string.

Example: Configure the direct url address to carry the custom string of workgroup.

AC(config-cp-instance)#redirect attribute custom-string name workgroup

2.1.35 redirect url-head

Command: redirect url-head <word>

no redirect url-head

Function: Configure the redirect url-head including transmission protocol, host name, port and path. The no command deletes it.

Parameters: <word>, It is the redirect url-head such as https://200.101.13.4:8080/index.jsp or http:// www.portal.com/index.jsp. 128 characters can be input at most.

Command Mode: Captive Portal Instance Mode.

Default: None.

Usage Guide: This command is used to configure the redirect url-head including transmission protocol, host name, port and path. Configures according to the redirect url of the portal server. The transmission protocol, host name, port and path should be same for redirecting.

Example: Configure the redirect url-head as http://17.16.1.26/control.

AC(config-cp-instance)#redirect url-head http://17.16.1.26/control

2.1.36 redirect attribute ssid enable

Command: redirect attribute ssid enable

no redirect attribute ssid enable

Function: Configure the redirect url to carry the parameter of ssid. The no command disables this function.

Parameters: None.

Command Mode: Captive Portal Instance Mode.

Default: Disable.

Usage Guide: This command is used to configure the redirect url to carry the parameter of ssid. After enabled this command, the redirect url will carry the ssid associated with client when the client conducts the redirection.

Example: Configure the redirect url to carry the parameter of ssid.

AC(config-cp-instance)#redirect attribute ssid enable

2.1.37 redirect attribute ssid name

Command: redirect attribute ssid name <word>

no redirect attribute ssid name

Function: Configure the name of the parameter of ssid carried in the redirect url. The no command recovers it to be the default value.

Parameters: <word>, it is the ssid name including 32 characters at most.

Command Mode: Captive Portal Instance Mode.

Default: ssid.

Usage Guide: This command is used to configure the name of the parameter of ssid carried in the redirect url.

Example: Configure the name of the parameter of ssid carried in the redirect url as wlanssid.

AC(config-cp-instance)#redirect attribute ssid name wlanssid

2.1.38 redirect attribute nas-ip enable

Command: redirect attribute nas-ip enable

no redirect attribute nas-ip enable

Function: Configure the redirect url to carry the parameter of nas-ip. The no command disables this function.

Parameters: None.

Command Mode: Captive Portal Instance Mode.

Default: Disable.

Usage Guide: This command is used to configure the redirect url to carry the parameter of nas-ip. After enabled this command, the redirect url will carry the wireless IP address of AC associated with client when the client conducts the redirection.

Example: Configure the redirect url to carry the parameter of nas-ip.

AC(config-cp-instance)#redirect attribute nas-ip enable

2.1.39 redirect attribute nas-ip name

Command: redirect attribute nas-ip name <word>

no redirect attribute nas-ip name

Function: Configure the name of the parameter of nas-ip carried in the redirect url. The no command recovers it to be the default value.

Parameters: <word>, it is the nas-ip name including 32 characters at most.

Command Mode: Captive Portal Instance Mode.

Default: wlanacname.

Usage Guide: This command is used to configure the name of the parameter of nas-ip carried in the redirect url.

Example: Configure the name of the parameter of nas-ip carried in the redirect url as wlannasip.

AC(config-cp-instance)#redirect attribute nas-ip name wlannasip

2.1.40 show captive-portal

Command: show captive-portal

Function: Shows the characteristics status of the Captive Portal.

Parameter: None.

Default: None.

Command Mode: Admin mode

Usage Guide: Show the relevant state parameters of the captive portal function on this AC.

Example: Show Captive Portal status of enable and disable.

captive portal enable:

AC#show captive-portal

Administrative Mode..... Enable

Operational Status..... Enabled

CP IP Address..... 101.1.1.3

captive portal disable:

AC#show captive-portal

Administrative Mode..... Disable

Operational Status..... Disabled

Disable Reason..... Administrator Disabled

CP IP Address..... 0.0.0.0

2.1.41 show captive-portal status

Command: show captive-portal status

Function: Shows the status of all the Captive Portal routine in the system.

Parameter: None.

Default: None.

Command Mode: Admin mode

Usage Guide: This command shows the captive portal configuration and the supported

property parameters on this AC.

Example: Show the Captive Portal status of the controller.

AC#show captive-portal status

Peer Switch Statistics Reporting Interval..... 120

Authentication Timeout..... 300

Authentication Type..... External

Supported Captive Portals..... 10

Configured Captive Portals..... 9

Active Captive Portals..... 0

Local Supported Users..... 128

Configured Local Users..... 0

System Supported Users..... 1024

Authenticated Users..... 0

2.1.42 show captive-portal trapflags

Command: show captive-portal trapflags

Function: Shows the available captive-portal SNMP traps.

Parameter: None.

Default: None.

Command Mode: Admin mode

Usage Guide: Shows the tracking status parameters of the portal users.

Example: Show the available captive-portal SNMP traps.

AC#show captive-portal trapflags

Client Authentication Failure Traps..... Enable

Client Connection Traps..... Enable

Client Database Full Traps..... Enable

Client Disconnection Traps..... Enable

2.1.43 show captive-portal configuration

Command: show captive-portal configuration <*cp-id*>

Function: Show the status of Captive Portal configuration.

Parameter: <*cp-id*> is the ID number of captive portal, range is 1 to 10.

Default: None.

Command Mode: Admin mode

Usage Guide: Show the configured parameters of portal routine.

Example: Show the configured situation of captive portal1.

AC#show captive-portal configuration 1
CP ID..... 1
CP Name..... AC2_CP1
Operational Status..... Enabled
Block Status..... Not Blocked
Configured Locales..... 1
Authenticated Users..... 0

2.1.44 show captive-portal configuration interface

Command: show captive-portal configuration <*cp-id*> interface ws-network <*id*>
Function: Shows all the interface information assigned to the captive portal configuration.
Parameter: <*cp-id*>, ID number of cp; **<*id*>** is the ID number of network binding to captive portal routine; **<*cp-id*>** shows the content of a routine, **<id>** shows the content of a network.
Default: None.
Command Mode: Admin mode
Usage Guide: Shows the interface state of the a portal routine.
Example: Shows all the interface information of Captive Portal configuration.
AC#show captive-portal configuration 1 interface ws-network 1
CP ID..... 1
CP Name..... AC2_CP1
Interface..... 11000
Interface Description..... Wireless Network 1
Operational Status..... Enabled
Block Status..... Not Blocked
Authenticated Users..... 0

2.1.45 show captive-portal configuration status

Command: show captive-portal configuration [<*cp-id*>] status
Function: Shows the configuration information of all or specific Captive Portal.
Parameter: <*cp-id*>, ID number of cp, the parameter **<cp-id>** means the content of a routine, without the parameter to show all the current configured routine parameters.
Default: None.
Command Mode: Admin mode
Usage Guide: Show detailed configuration parameters of portal routine.
Example: Show all Captive Portal configuration information.

Show the status of all the routines:

AC# show captive-portal configuration status

CP ID	CP Name	Mode	Protocol Verification
1	AC2_CP1	Enable	HTTP RADIUS
2	Default	Enable	HTTP RADIUS
3	Default	Enable	HTTP RADIUS
10	Default	Enable	HTTP RADIUS

2.1.46 show captive-portal client status

Command: show captive-portal client [<*FF-FF-FF-FF-FF-FF*> { ipv4 | ipv6} <*ip-addr*>] status

Function: This command shows detailed connection information or an overview of users connected to the captive portal.

Parameter: <*FF-FF-FF-FF-FF-FF*> is the MAC address of the user.

ipv4: user address is ipv4 address.

ipv6: user address is ipv6 address.

<*ip-addr*> is user address. Ipv4 address is decimal format with point and ipv6 address is the format of X:X::X:X.

Default: None.

Command Mode: Admin mode

Usage Guide: This command shows the status of all or a portal user.

Example: Show detailed information of the user connected to the captive portal with MAC address as 34-08-04-30-07-ca.

AC#show captive-portal client 34-08-04-30-07-ca status

Client MAC Address..... 34-08-04-30-07-ca

Client IP Address..... 100.1.1.1

Protocol Mode..... HTTP

Verification Mode..... RADIUS

CP ID..... 1

CP Name..... AC2_CP1

Interface..... 11002

Interface Description..... Wireless Network 3

User Name..... a1

Session Time..... 0d:00:00:21

Switch MAC Address..... 00-03-0f-14-8f-85

Switch IP Address..... 110.1.1.2

Switch Type..... Local

2.1.47 show captive-portal configuration client

Command: show captive-portal configuration [<*cp-id*>] client status

Function: This command shows the client information through the portal authentication in an interface.

Parameter: <*cp-id*>, ID number of Captive Portal.

Default: None.

Command Mode: Admin mode

Usage Guide: This command shows the user parameters of a portal routine.

Example: Show all the portal configuration information of the client passed authentication.

AC#show captive-portal configuration 1 client status

CP ID..... 1

CP Name..... AC2_CP1

Client MAC Address	Client IP Address	Interface	Interface Description
34-08-04-30-07-ca	100.1.1.1	11002	Wireless Network 3

2.1.48 show captive-portal ext-portal-server status

Command: show captive-portal ext-portal-server status

Function: Use this command to check the status of the external portal server.

Parameter: None.

Default: None.

Command Mode: Admin mode.

Usage Guide: Check the status of the external portal server.

Example: Check the status of the external portal server.

AC#show captive-portal ext-portal-server status

Server Name	IP Address	port
x1	20.1.1.1	1
x2	20.1.1.2	2
x3	20.1.1.3	3
x4	20.1.1.4	4

x5	20.1.1.5	5
x6	20.1.1.6	6
x7	20.1.1.7	7
x8	20.1.1.8	8
x9	20.1.1.9	9
x10	20.1.1.10	10

2.1.49 show captive-portal interface ws-network client status

Command: show captive-portal interface ws-network *<1-1024>* client status

Function: This command shows the information of all or a specific interface of certified clients.

Parameter: <*1-1024*>, network ID.

Default: None.

Command Mode: Admin mode

Usage Guide: This command shows the information of online portal user of a network.

Example: Show the certified Client information on the specific network.

AC#show captive-portal interface ws-network 3 client status

Interface..... 11002

Interface Description..... Wireless Network 3

Client MAC Address	Client IP Address	CP ID	CP Name	Protocol	Verification
34-08-04-30-07-ca	100.1.1.1	1	AC2_CP1	HTTP	RADIUS

2.1.50 show captive-portal interface configuration status

Command: show captive-portal interface configuration [<*cp-id*>] status

Function: This command shows the interface information of all captive portal configuration or a specific configuration.

Parameter: <*cp-id*>, captive portal ID.

Default: None.

Command Mode: Admin mode

Usage Guide: This command shows the binding relationship of all or a portal routines

with interface.

Example: Show the interface information of all captive portal configuration.

AC#show captive-portal interface configuration status

CP ID	CP Name	Interface	Interface Description	Type
1	AC2_CP1	11000	Wireless Network 1	Wireless
		11001	Wireless Network 2	Wireless
		11002	Wireless Network 3	Wireless
		11003	Wireless Network 4	Wireless
2	Default	11004	Wireless Network 5	Wireless
3	Default	11005	Wireless Network 6	Wireless

2.1.51 show captive-portal interface capability ws-network

Command: show captive-portal interface capability ws-network *<1-1024>*

Function: This command shows all selected captive portal interface information, or specific captive portal interface ability.

Parameter: *<1-1024>* network ID.

Default: None.

Command Mode: Admin mode

Usage Guide: This command shows the property parameters of network which binds to portal supports.

Example: Show the interface information of the specific captive portal.

AC# show captive-portal interface capability ws-network 2

Interface..... 11001

Interface Description..... Wireless Network 2

Interface Type..... Wireless

Session Timeout..... Supported

Idle Timeout..... Supported

Bytes Received Counter..... Supported

Bytes Transmitted Counter..... Supported

Packets Received Counter..... Supported

Packets Transmitted Counter..... Supported

Roaming..... Supported

2.1.52 snmp-server enable traps captive-portal

Command: snmp-server enable traps captive-portal

Function: Enable Captive Portal traps globally; the no command will disable this function.

Parameter: None.

Default: Disable.

Command Mode: Global configuration mode.

Usage Guide: When enabling trap function of captive portal, if portal user authentication is failed, the connection is successful, Controller authentication table is full and disassociation, message can be sent to the configured trap server to inform the server with the above information.

Example: Enable Captive Portal traps.

AC(Config)# snmp-server enable traps captive-portal

2.1.53 statistics interval

Command: statistics interval *<0 | 15-3600>*

no statistics interval

Function: Use this command to configure the interval of controller sending portal user statistics information to the controller in the cluster. The no command will restore the default value.

Parameter: *<0 | 15-3600>*, interval of sending portal user statistics information, unit is second. The parameter 0 means to disable this function.

Default: 120s.

Command Mode: Captive Portal global configuration mode.

Usage Guide: The interval of sending user's information to the controller in the cluster can be changed from 15 to 3600 seconds freely.

Example: Configure the interval of controller sending portal user statistics information to the controller in the cluster as 120s.

AC(config-cp)#statistics interval 120

2.1.54 trapflags

Command: trapflags {client-auth-failure | client-connect | client-db-full | client-disconnect}

no trapflags {client-auth-failure | client-connect | client-db-full | client-disconnect}

Function: Use this command to enable captive the portal SNMP traps. The no command will disable this function.

Parameter: client-auth-failure: allow the SNMP interface routine to send trap when a client failed to pass the captive portal authentication. **client-connect:** allow the SNMP interface routine to send trap when a client passes the captive portal authentication. **client-db-full:** allow the SNMP interface routine to send trap when there is entity which cannot be added because the local database is full. **client-disconnect:** allow the SNMP interface routine to send trap when the client is disconnected from the captive portal.

Default: Disabled

Command Mode: Captive Portal global configuration mode.

Usage Guide: The controller send messages to the snmp server when the user authentication fails, the authentication is successful, the controller state table is full and the user is disconnected. If the parameters are not configured, all traps are enabled, SNMP traps can also use optional parameters by itself.

Example:

AC(config-cp)# trapflags

AC(config-cp)#trapflags client-auth-failure

2.2 Commands for Accounting Function

2.2.1 captive-portal client deauthenticate

Command: captive-portal client deauthenticate {*<1-10>* | *<FF-FF-FF-FF-FF-FF>* { ipv4 | ipv6} *<ip-addr>*}

Function: Use this command to disassociate with the specified Captive Portal Client.

Parameter: ***<1-10>*** Captive Portal ID.

<FF-FF-FF-FF-FF-FF> MAC address of the Client.

ipv4: user address is ipv4 address.

ipv6: user address is ipv6 address.

<ip-addr> is user address. Ipv4 address is decimal format with point and ipv6 address is the format of X:X::X:X.

Default: None.

Command Mode: Admin mode

Usage Guide: Use this command to disassociate with the client of the appointed MAC address; it can also remove all or a single user in the specified captive portal configuration; with no parameters, remove all users.

Example: Disassociate with the specified Captive Portal Client.

AC#captive-portal client deauthenticate (Force the portal user offline on the controller)

The specified clients will be deauthenticated. Are you sure you want to deauthenticated clients? [Y/N]

AC#captive-portal client deauthenticate 1(Force the user offline on the routine 1)

AC#captive-portal client deauthenticate 34-08-04-30-07-ca(Force a user offline)

2.2.2 idle-timeout

Command: idle-timeout *<0-900>*

no idle-timeout

Function: Defines the user idle timeout of the Captive Portal configuration, if exceed the configured value and there is still no network traffic when the user passed portal authentication, the client will be forced offline. The no command is disable this function.

Parameter: *<0-900>* user idle timeout, unit is second, 0 means the function is not effective, the idle time is not limited.

Default: 0.

Command Mode: Captive Portal Instance configuration mode.

Usage Guide: Defines the user idle timeout of the Captive Portal configuration, if configured as 0 means the function is not effective.

Example: Defines the user idle timeout of the Captive Portal configuration as 120s.

AC(config-cp-instance)# idle-timeout 120

2.2.3 radius accounting

Command: radius accounting

no radius accounting

Function: Use this command to enable the accounting function of Captive Portal routine. the no command will disable the function.

Parameter: None.

Default: Disable the function of Captive Portal accounting.

Command Mode: Captive Portal Instance configuration mode.

Usage Guide: Configure Captive Portal accounting function.

Example: Enable the accounting function of a Captive Portal routine.

AC(config-cp-instance)#radius accounting

2.2.4 radius-accounting update interval

Command: radius-accounting update interval *<60-3600>*

no radius-accounting update interval

Function: Configure the accounting updating interval of portal user of AC sent to the radius. the no command will restore the default value.

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

Default: 300s.

Command Mode: Captive Portal Instance configuration mode.

Usage Guide: Configure the accounting updating interval of Captive Portal.

Example: Configure the accounting updating interval of portal user of AC sent to the radius as 60s.

AC(config-cp-instance)# radius-accounting update interval 60

2.2.5 radius-acct-server

Command: radius-acct-server <*server-name*>

no radius-acct-server

Function: Defines the RADIUS accounting server name of the Captive Portal configuration. The no command will delete the configuration.

Parameter: <*server-name*>, RADIUS accounting server name.

Default: None.

Command Mode: Captive Portal Instance configuration mode.

Usage Guide: Define the RADIUS accounting server of Captive Portal configuration.

Example: Define the RADIUS accounting server of Captive Portal configuration as radius_aaa_1.

AC(config-cp-instance)#radius-acct-server radius_aaa_1

2.2.6 session-timeout

Command: session-timeout <*0-86400*>

no session-timeout

Function: Define session timeout of Captive Portal configuration. The no command will disable this function.

Parameter: <*0-86400*>, Session timeout, unit is second, 0 means Timeout Function is not effective.

Default: 86400.

Command Mode: Captive Portal Instance configuration mode.

Usage Guide: Define session timeout of Captive Portal configuration.

Example: Define session timeout of Captive Portal configuration as 100s.

AC(config-cp-instance)# session-timeout 100

2.2.7 show captive-portal client statistics

Command: show captive-portal client <*FF-FF-FF-FF-FF-FF*> { ipv4 | ipv6} <*ip-addr*>] statistics

Function: Show the specific captive portal client statistics.

Parameter: <*FF-FF-FF-FF-FF-FF*>, MAC addresses of users passed portal authentication.

ipv4: user address is ipv4 address.

ipv6: user address is ipv6 address.

<*ip-addr*> is user address. Ipv4 address is decimal format with point and ipv6 address is the format of X:X::X:X.

Default: None.

Command Mode: Admin mode

Usage Guide: This command shows traffic statistics information of a portal user.

Example: Show the client statistics with the MAC address of 34-08-04-30-07-ca.

AC#show captive-portal client 34-08-04-30-07-ca statistics

Client MAC Address..... 34-08-04-30-07-ca

Bytes Received..... 88964

Bytes Transmitted..... 15157

Packets Received..... 1153

Packets Transmitted..... 22

2.3 Commands for Free-resource

2.3.1 free-resource(global)

Command: free-resource <*rule-number*> {destination {any | { ipv4 | ipv6} <*ip-addr*> } | source {any | { ipv4 | ipv6} <*ip-addr*> }}

no portal free-resource {<*rule-number*> | all}

Function: Configure the free-resource rules, the wireless client who conforms the source IP address in rules can access the resources of the destination IP address in rules, the AP does not redirect, the client can access directly without Portal authentication.

Parameter: <*rule-number*> free resource ID.

ipv4 the configured free resource address is ipv4 address

ipv6 the configured free resource address is ipv6 address

<*ip-addr*> free-resource rules interviewees'/visitors' IP addresses.

<*netmask*> free-resource rules interviewees'/visitors' IP addresses.

Default: None.

Command Mode: Captive Portal Global configuration mode.

Usage Guide: Configure the wireless client address segment (visitor) which can be free to access the resources and the address segment which is free to provide the resource (interviewee).

Example: Set free-resource rules.

AC(config-cp)# free-resource 1 destination ipv4 1.0.0.0/8 source ip 10.0.0.2 /8

2.3.2 free-resource(routine)

Command: free-resource <*rule-number*>

no free-resource <*rule-number*>

Function: Configure free- resource rules for CP configuration. Network binding to this CP configuration can determine whether the flow sent from the client can be directly released without authentication according to this rule.

Parameter: <*rule-number*> free-resource rule number.

Default: None.

Command Mode: Captive Portal Instance configuration mode.

Usage Guide: Bind a free-resource rule to the CP configuration, the CP configuration can bind several rules, a rule can be bound to a number of CP configurations. Rules are distributed to the AP, on AP, the packets in rules sent from the client will be directly released whether the client passed authentication.

Example: Bind free- resource rules.

AC(config-cp -instance)# free-resource 1

2.3.3 show captive-portal free-resource status

Command: show portal free-resource status

Function: Use this command to check the free-resource status.

Parameter: None.

Default: None.

Command Mode: Admin mode.

Usage Guide: Check the free-resource status.

Example: Check the free-resource status.

AC(config-cp-instance)#show captive-portal free-resource status

	Destination	Destination	Source	Source
Rule ID	IP Address	Mask length	IP Address	Mask length

1	1.0.0.0	8	10.0.0.2	8
2	2.0.0.0	8	10.0.0.0	8

2.4 Commands for MAC Portal

2.4.1 mac-portal authentication

Command: mac-portal authentication

no mac-portal authentication

Function: Enable/disable the mac portal function of a portal routine.

Parameter: None.

Default: None.

Command Mode: Captive Portal routine configuration mode.

Usage Guide: Enable the mac portal function of a portal routine.

Example: Enable mac portal function of configuration 1.

AC(config-cp-instance)#mac-portal authentication

2.4.2 mac-portal known-client

Command: mac-portal known-client <*macAddr*>

no mac-portal known-client <*macAddr*>

Function: Add / delete the mac address of client which is as mac portal user.

Parameter: <*macAddr*>: Client mac address.

Default: None.

Command Mode: Captive Portal configuration mode.

Usage Guide: Add a client mac address enabled mac portal function.

Example: Add a client mac address enabled mac portal function.

AC(config-cp)#mac-portal known-client e0-05-c5-8e-10-05

2.5 Commands for User Verification of Internal Portal

2.5.1 verification {local|radius|ladp|none}

Command: verification {local|radius|ladp|none}

Function: Configure the verification method of captive portal instance.

Parameters: local: User needs to pass through the verification of local database; radius:

User needs to pass through the verification of radius server; ldap: Server user needs to pass through the verification of ldap; none: free verification.

Default: Radius.

Command Mode: Captive Portal Instance Mode.

Usage Guide: This command can be used for users who use the captive portal instance to choose the verification method. If user needs to use the local verification, the parameter of local can be chosen. Different captive portal instances can choose different verification methods.

Example: Configure the local verification method for Captive Portal instance 1.

ac(config)# captive-portal

ac(config-cp)#configuration 1

ac(config-cp-instance)#verification local

2.5.2 group<group-name> (Captive Portal Instance Mode)

Command: group<group-name>

no group

Function: Configure a user group for the captive portal instance. The no command cancels this configuration.

Parameters: <group-name>, name of user group, it is a string including 1 to 32 characters and it can only include the letters of [a-z,A-Z], numbers, underlines (_) and dashes (-). It is case sensitive.

Default: None.

Command Mode: Captive Portal Instance Mode.

Usage Guide: Users are divided into different groups. When users conduct the portal access, AC can make the user corresponding to the captive portal instance according to the network. The captive portal instance that user is associated with should be in the same group with user, otherwise, the verification will fail. If they belong to the same group, the password will be checked, if the password is not correct, the verification fails.

Example: Configure the user-group1 for Captive Portal 1.

ac(config)# captive-portal

ac(config-cp)#configuration 1

ac(config-cp-instance)# group user-group1

2.5.3 user<user-name>

Command: user<user-name>

no user<user-name>

Function: Create a local user or enter into the captive portal user mode. The no command deletes the local user.

Parameters: <user-name>: It is the user name which is a string including 1 to 32 characters and it can only include the letters of [a-z,A-Z], numbers, underlines (_), dashes (-), the special character (.) and @.

Default: None.

Command Mode: Captive Portal Global Mode.

Usage Guide: Only when the local user is created and the user information is configured, the user can adopt the local verification. If the local user is not created or the user information is modified illegally, the local verification will fail.

Example: Configure the user1 and enter into the captive portal user mode.

ac(config)# captive-portal

ac(config-cp)#user user1

ac(config-cp-local-user)#

2.5.4 password<user-password>

Command: password<user-password>

no password

Function: Configure the password for the local user. The no command deletes the password.

Parameters: <user-password>: It is the local user password and it is a string including 1 to 64characters and it can include any character.

Default: None.

Command Mode: Captive Portal User Mode.

Usage Guide: The user password is the integrant information which should be configured. If the password is not configured, user cannot pass the verification. After configured the password, the command of show run can show the encrypted password; the command of show captive portal user can show the plaintext.

Example: Configure the password of user1 as user1password.

ac(config)# captive-portal

ac(config-cp)#user user1

ac(config-cp-local-user)#password user1password

2.5.5 password-encrypted<encrypted-pwd>

Command: password-encrypted< encrypted -pwd>

Function: Configure the encrypted password for the local user.

Parameters: <encrypted-pwd>: It is the encrypted password and it is the 128 hexadecimal characters.

Default: None.

Command Mode: Captive Portal User Mode.

Usage Guide: The encrypted password needs the validity check; the random password will be reported error. This command is mainly used for the password configuration saving, it is not suggested using to configured the password generally.

Example: Configure the encrypted password of user1 as user1password.

(Explanation: the encrypted hexadecimal characters are: 93a400e82138adfc2387f5f1d11f02ec5ba290a4ed578d5030af821eacd10dfc000bb5e227775f133185809c345115af437050c65f32204e37aba3649442f238)

ac(config)# captive-portal

ac(config-cp)#user user1

ac(config-cp-local-user)#password-encrypted

93a400e82138adfc2387f5f1d11f02ec5ba290a4ed578d5030af821eacd10dfc000bb5e227775f133185809c345115af437050c65f32204e37aba3649442f238

2.5.6 group< group-name > (Captive Portal User Mode)

Command: group<group-name >

no group

Function: Associate a user group with the local user. The no command deletes the association.

Parameters: <group-name>: It is the name of group which is a string including 1 to 32 characters and it can only include the letters of [a-z,A-Z], numbers, underlines (_) and dashes (-). It is case sensitive and must be the only one globally.

Default: None.

Command Mode: Captive Portal User Mode.

Usage Guide: User must be associated with a group at least. One user can be associated with multiple groups which are 10 at most. After the association between local user and the 10 groups is created, it will fail if associates with the new group.

Example: Associate user1 with usergroup1.

ac(config)# captive-portal

ac(config-cp)#user user1

ac(config-cp-local-user)#group usergroup1

2.5.7 session-timeout<timeout>

Command: session-timeout<timeout>

no session-timeout

Function: Configure the timeout of session for the local user. The no command recovers it to be the default value.

Parameters: <timeout>: It is the timeout of session. The unit is second and the range is 0-86400.

Default: 0, it means there is no limit of the session timeout.

Command Mode: Captive Portal User Mode.

Usage Guide: After the session is timeout, the user is forced to be down line. After modified the session timeout value of the local user, the new timeout value will be adopted to deal with the user terminal. The session timeout value is counted from the user association; it will be recovered to 0 after the user is down line, the value will be re-counted.

Example: Configure the session timeout value of user1 as 10000.

ac(config)# captive-portal

ac(config-cp)#user user1

ac(config-cp-local-user)#session-timeout 10000

2.5.8 max-bandwidth-up <rate>

Command: max-bandwidth-up <rate>

no max-bandwidth-up

Function: Configure the maximum uplink bandwidth of the local user. The no command cancels the uplink bandwidth limit.

Parameters: <rate>: It is the bandwidth and the range is 0-536870911. 0 means there is no limit.

Default: 0, it means there is no bandwidth limit.

Command Mode: Captive Portal User Mode.

Usage Guide: After this command is configured, the maximum uplink bandwidth of the user is the configured value. The maximum bandwidth value should be configured according to the users' requirements; otherwise, it will affect the application.

Example: Configure the maximum uplink bandwidth limit of user1 as 100000.

ac(config)# captive-portal

ac(config-cp)#user user1

ac(config-cp-local-user)#max-bandwidth-up 100000

2.5.9 max-bandwidth-down<rate>

Command: max-bandwidth-down<rate>

no max-bandwidth-down

Function: Configure the maximum downlink bandwidth of the local user. The no command cancels the downlink bandwidth limit.

Parameters: <rate>: It is the bandwidth and the range is 0-536870911. 0 means there is no limit.

Default: 0, it means there is no bandwidth limit.

Command Mode: Captive Portal User Mode.

Usage Guide: After this command is configured, the maximum downlink bandwidth of the user is the configured value. The maximum bandwidth value should be configured according to the users' requirements; otherwise, it will affect the application.

Example: Configure the maximum downlink bandwidth limit of user1 as 100000.

ac(config)# captive-portal

ac(config-cp)#user user1

ac(config-cp-local-user)#max-bandwidth-down 100000

max-input-octets <bytes>

2.5.10 max-input-octets <bytes>

Command: max-input-octets <bytes>

no max-input-octets

Function: Configure the total number of bytes which are allowed to be sent. The no command cancels the limit.

Parameters: <bytes>: It is the number of bytes and the range is 0-4294967295. 0 means there is no limit.

Default: 0, it means there is no bytes limit.

Command Mode: Captive Portal User Mode.

Usage Guide: After configured total number of bytes which are allowed to be sent, the user will be disconnected when the bytes achieve the maximum limit value. This configured value can limit the bytes that user sends one time of connection. After the user is online again, the number of bytes will be re-counted. The parameter will be effective directly after modified.

Example: Configure the total number of user1's bytes which are allowed to be sent as

90000000.

ac(config)# captive-portal

ac(config-cp)#user user1

ac(config-cp-local-user)#max-input-octets 90000000

2.5.11 max-output-octets <bytes>

Command: max-output-octets <bytes>

no max-output-octets

Function: Configure the total number of bytes which are allowed to be received. The no command cancels the limit.

Parameters: <bytes>: It is the number of bytes and the range is 0-4294967295. 0 means there is no limit.

Default: 0, it means there is no bytes limit.

Command Mode: Captive Portal User Mode.

Usage Guide: After configured total number of bytes which are allowed to be received, the user will be disconnected when the bytes achieve the maximum limit value. This configured value can limit the bytes that user receives one time of connection. After the user is online again, the number of bytes will be re-counted. The parameter will be effective directly after modified.

Example: Configure the total number of user1's bytes which are allowed to be received as 90000000.

ac(config)# captive-portal

ac(config-cp)#user user1

ac(config-cp-local-user)#max-output-octets 90000000

2.5.12 max-total-octets <bytes>

Command: max-total-octets <bytes>

no max-total-octets

Function: Configure the total number of bytes which are allowed to be transmitted. The no command cancels the limit.

Parameters: <bytes>: It is the number of bytes and the range is 0-4294967295. 0 means there is no limit.

Default: 0, it means there is no bytes limit.

Command Mode: Captive Portal User Mode.

Usage Guide: After configured total number of bytes which are allowed to be transmitted, the user will be disconnected when the transmitted bytes achieve the maximum limit value.

This configured value can limit the bytes that user transmits one time of connection. After the user is online again, the number of bytes will be re-counted. The parameter will be effective directly after modified.

Example: Configure the total number of user1's bytes which are allowed to be transmitted as 90000000.

ac(config)# captive-portal

ac(config-cp)#user user1

ac(config-cp-local-user)#max-total-octets 90000000

2.5.13 show captive-portal user [<user-name>]

Command: show captive-portal user [<user-name>]

Function: Show the configured local user information of captive portal. This command can show the main information of all the users without the parameter of user-name; it also can show the detailed information of one user with the parameter of user-name.

Parameters: <user-name>: It is the user name which is a string including 1 to 32 characters and it can only include the letters of [a-z,A-Z], numbers, underlines (_), dashes (-), the special character (.) and @.

Default: None.

Command Mode: Admin Mode.

Usage Guide: When the local user cannot pass the verification, this command can be configured to check if the data information is configured and if the password is correct. When the timeout and limit speed are not as expected, the information should be checked first if the configuration is correct.

Example: Show the main information of all the users.

AC#show captive-portal user

User Name	Password	Session Timeout	Group Name
user1	user1password	0	group1 group2
user2	user2password	0	group1

Show the detailed information of user1.

AC#show captive-portal user user1

User Name..... user1

Password Configured..... 'user1password'

Session Timeout..... 0

Max Bandwidth Up (bytes/sec)..... 0

Max Bandwidth Down (bytes/sec)..... 0

Max Input Octets (bytes)..... 90000

Max Output Octets (bytes)..... 0

Max Total Octets (bytes)..... 0

Group Name

---

group1

group2

2.5.14 clear captive-portal users

Command: clear captive-portal users

Function: Delete all the users of the local verification database and make all the users who passed the verification down line.

Parameters: None.

Default: None.

Command Mode: Admin Mode.

Usage Guide: This command should be used carefully. It can delete the configured user information and it can also make the users down line. We suggest making a backup for the configured files before using this command.

Example: Delete all the users of the local verification database.

AC#clear captive-portal users

Are you sure to delete all of the users? [Y/N] y

All CP users deleted!

2.6 Commands for Portal Page of Web Server

2.6.1 ext-web-server enable

Command: ext-web-server enable

no ext-web-server enable

Function: Enable the portal page of web server on AC for the CP instance. The no command disables this function.

Parameters: None.

Default: Disable.

Command Mode: Captive Portal Instance Mode.

Usage Guide: User can decide to use the external page or the internal page of AC for the

portal authentication according to the CP instance.

Example: Enable he internal portal page based on web server on AC for the CP instance.

ac(config)# captive-portal

ac(config-cp)#configuration 1

ac(config-cp-instance)#ext-web-server enable

2.6.2 ext-web-server login-failure-url <word>

Command: ext-web-server login-failure-url <word>

no ext-web-server login-failure-url

Function: Configure the login-failure-url of the web server. The no command cancels this configuration.

Parameters: <word>: it is the login-failure-url such as http://200.101.13.4/loginfail.html. 128 characters can be input at most.

Default: None.

Command Mode: Captive Portal Instance Mode.

Usage Guide: Configure the login-failure-url of the web server and save the configuration. The result can be viewed through the command of **show captive-portal configuration <1-10> status**.

Example: Under the CP instance, configure/delete the login-failure-url of the web server.

ac(config)# captive-portal

ac(config-cp)#configuration 1

ac(config-cp-instance)#ext-web-server login-failure-url http://192.168.105.200/loginfail.html

2.6.3 ext-web-server login-url <word>

Command: ext-web-server login-url <word>

no ext-web-server login-url

Function: Configure the login-url of the web server. The no command cancels this configuration.

Parameters: <word>， it is the login-url such as http://200.101.13.4/login.html. 128 characters can be input at most.

Default: None.

Command Mode: Captive Portal Instance Mode.

Usage Guide: Configure the login-url of the web server and save the configuration. The result can be viewed through the command of **show captive-portal configuration <1-10> status**.

Example: Under the CP instance, configure/delete the login-url of the web server.

ac(config)# captive-portal

ac(config-cp)#configuration 1

ac(config-cp-instance)#ext-web-server login-url http://192.168.105.200/loginfail.html

2.6.4 ext-web-server logout-url <word>

Command: ext-web-server logout-url <word>

no ext-web-server logout-url

Function: Configure the logout-url of the web server. The no command deletes it.

Parameters: <word>: it is the logout-url such as http://200.101.13.4/logout.html. 128 characters can be input at most.

Default: None.

Command Mode: Captive Portal Instance Mode.

Usage Guide: Configure the logout-url of the web server and save the configuration. Notice: The logout-url is the same url to the login-url. The result can be viewed through the command of **show captive-portal configuration <1-10> status**.

Example: Under the CP instance, configure/delete the logout-url of the web server.

ac(config)# captive-portal

ac(config-cp)#configuration 1

ac(config-cp-instance)#ext-web-server logout-url http://192.168.105.200/logout.html

2.6.5 ext-web-server logout-success -url <word>

Command: ext-web-server logout-success-url <word>

no ext-web-server logout-success-url

Function: Configure the logout-success-url of the web server. The no command deletes it.

Parameters: <word>: it is the logout-success-url such as http://200.101.13.4/logoutsuccess.html. 128 characters can be input at most.

Default: None.

Command Mode: Captive Portal Instance Mode.

Usage Guide: Configure the logout-success-url of the web server and save the configuration. Notice: The logout-url is the same url to the login-url. The result can be viewed through the command of **show captive-portal configuration <1-10> status**.

Example: Under the CP instance, configure/delete the logout-success-url of the web server.

ac(config)# captive-portal

ac(config-cp)#configuration 1

ac(config-cp-instance)#ext-web-server logout-success-url http://192.168.105.200/logoutsuccess.html

2.6.6 redirect url-head <word>

Command: redirect url-head <word>

no redirect url-head

Function: Configure the redirect url-head. The no command deletes it.

Parameters: <word>: it is the redirect url-head such as http://200.101.13.4/index.jsp or http://www.portal.com /index.jsp. 128 characters can be input at most.

Default: None.

Command Mode: Captive Portal Instance Mode.

Usage Guide: Configure the redirect url-head including the transmission protocol, host name, port and path. The no command deletes the configuration, it means to delete the login-url of web server. Save the configuration.

Example: Under the CP instance, configure the redirect url-head.

ac(config)# captive-portal

ac(config-cp)#configuration 1

ac(config-cp-instance)#redirect url-head http://www.portal.com /index.jsp

2.7 Commands for Automatic Page Pushing after Successful Authentication

2.7.1 redirect attribute url-after-login enable

Command: redirect attribute url-after-login enable

no redirect attribute url-after-login enable

Function: Enable the function that the redirect url carrys the pushed url after the successful authentication. The no command disables this function.

Parameters: None.

Command Mode: Captive Portal Instance Mode.

Default: Disable.

Usage Guide: This command is used to enable the function that the redirect url carrys the pushed url after the successful authentication. After enabled this command, the redirect url pushed by AC will carry the url which needs to be pushed after the successful authentication. At the same time, when the <url-value> of redirect attribute url-after-login

value is configured as empty, the carried url is the page url that the user access before the authentication. If it is not empty, the carried url is the page url configured by <url-value>.

Example: Enable the function that the redirect url carrys the pushed url after the successful authentication.

AC(config-cp-instance)#redirect attribute url-after-login enable

2.7.2 redirect attribute url-after-login name

Command: redirect attribute url-after-login name <name>

no redirect attribute url-after-login name

Function: Configure the attribute name of the pushed url after the successful authentication which is carried in the redirect url. The no command recovers it to be the default value.

Parameters: <name>, it is the attribute name including 32 characters at most.

Command Mode: Captive Portal Instance Mode.

Default: The default name is srcurl.

Usage Guide: This command is used to configure the attribute name of the pushed url after the successful authentication which is carried in the redirect url.

Example: Configure the attribute name of the pushed url after the successful authentication which is carried in the redirect url as redirect.

AC(config-cp-instance)#redirect attribute url-after-login name redirect

2.7.3 redirect attribute url-after-login encode

Command: redirect attribute url-after-login encode {plain-text|base64}

Function: Configure the encode of the pushed url after the successful authentication which is carried in the redirect url.

Parameters: plain-text, it is the plain-text;

base64, It is the base64 encode.

Command Mode: Captive Portal Instance Mode.

Default: The default encode is plain-text.

Usage Guide: This command is used to configure the encode of the pushed url after the successful authentication which is carried in the redirect url. It can be configured according to the encode supported by the portal server.

Example: Configure the encode of the pushed url after the successful authentication which is carried in the redirect url as base64.

AC(config-cp-instance)#redirect attribute url-after-login encode base64

2.7.4 redirect attribute url-after-login value

Command: redirect attribute url-after-login value <url-value>

no redirect attribute url-after-login value

Function: Configure the appointed url which is popped up after the success authentication. The no command deletes it.

Parameters: <url-value>, it is the configured appointed url including 512 characters at most.

Command Mode: Captive Portal Instance Mode.

Default: None.

Usage Guide: This command is used to configure the appointed url which is popped up after the success authentication. If enable the function that the redirect url carries the pushed url after the successful authentication, the redirect url will carry the url with the <url-value>.

Example: Configure the appointed url which is popped up after the success authentication as http://www.test.com.

AC(config-cp-instance)#redirect attribute url-after-login value http://www.test.com

2.8 Commands for Advertisement Page of Captive-portal

2.8.1 verification none

Command: verification none

Function: Configure the STA authentication method as none. It means no authentication.

Parameters: None.

Default: None.

Command Mode: captive-portal Instance Mode.

Usage Guide: After configured this command, the captive-portal instance will not certificate the STA and it considers that the accessed STA are all lawful.

Example: Configure the STA authentication method as none.

AC(config)#captive-portal

AC(config-cp)#configuration 1

AC(config-cp-instance)#verification none

AC(config-cp-instance)#

2.8.2 redirect attribute url-after-login enable

Command: redirect attribute url-after-login enable

no redirect attribute url-after-login enable

Function: Enable the function that the redirection url has the advertisement page url after the successful authentication.

Parameters: None.

Default: Disable.

Command Mode: Captive Portal Instance Mode.

Usage Guide: After configured the captive-portal redirection URL, AC will deal with the advertisement page URL information.

Example: Enable the function that the redirection url has the advertisement page url after the successful authentication. It means the automatic pushing function after the successful authentication.

AC(config-cp-instance)#redirect attribute url-after-login enable

AC(config-cp-instance)#

2.8.3 redirect attribute url-after-login value WORD

Command: redirect attribute url-after-login value *WORD*

no redirect attribute url-after-login value *WORD*

Function: Configure the advertisement page URL. The no command deletes the configured URL.

Parameters: *WORD*, it is the URL of the page after the successful captive portal authentication.

Default: The WORD is null.

Command Mode: Captive Portal Instance Mode.

Usage Guide: After configured this command, STA can associate with the network. It will be redirect to the configured URL when accesses the web page first time. In the later times of accessing, it will not be redirected.

Example: Configure the advertisement page URL as http://200.1.1.200/.

AC(config-cp-instance)#redirect attribute url-after-login value http://200.1.1.200/

AC(config-cp-instance)#

2.9 Commands for Huawei Portal 2.0 Supporting

2.9.1 portal version <1|2>

Command: portal version <1|2>

Function: Enable/disable the portal 2.0 supporting function of captive-portal, the default supporting is portal 1.0. Portal Ver2.0 is added the expansion of the field of version, and is added the field of Authenticator. It can verify the packets legally.

Parameters: None.

Default: Portal 1.0 supporting.

Command Mode: captive-portal Global Mode.

Usage Guide: After configured this command, captive-portal will use the portal 2.0 for all instances.

Example: Enable the portal 2.0 supporting function of captive-portal.

AC(config)#captive-portal

AC(config-cp)#portal version 2

AC(config-cp)#

2.9.2 external portal-server server-name WORD

Command: external portal-server server-name WORD <ipv4|ipv6> <A.B.C.D|X:X::X:X> port <0-65535> key WORD

Function: Appoint the parameters of the external portal-server, including IP address, port number, key, etc.

Parameters: server-name: it can be defined and can be used in the captive-portal instance; **port:** it is the port that BAS sends the active offline packet to notify the portal server, it should be consistent with the configuration on portal server; key: it is the key of portal server version 2.0 configured on iMC, it should be consistent with the configuration on iMC.

Default: None.

Command Mode: captive-portal Global Mode.

Usage Guide: For the portal 2.0, the parameter of key must be configured when enable this command.

Example: Configure the parameters of the external portal-server on AC.

AC(config)#captive-portal

AC(config-cp)# external portal-server server-name iMC ipv4 1.1.1.1 key test

AC(config-cp)#

2.10 Commands for URL Filter

2.10.1 url-filter permit (Global Mode)

Command: url-filter permit <rule-number><hostname>

no url-filter permit {rule-number|all}

Function: Configure the global url-filter white-list rule. The no command deletes the global url white-list rule.

Parameters: <rule-number>: the ID of the white-list rule;

<hostname>: the domain name that the white-list rule matches;

{rule-number|all}: rule-number means to delete the ID of the appointed white-list rule, all means to delete all the configured white-list rules.

Command Mode: Global Mode.

Default: None.

Usage Guide: This command can configure that the client can access the appointed domain name before the authentication in the portal authentication. Binding the white-list rule to the portal configuration can make the client access the appointed resource before the authentication.

Example: Configure the url-filter white-list rule whose domain name is www.white.com.

AC(config)#url-filter permit 1 www.white.com

2.10.2 url-filter deny (Global Mode)

Command: url-filter deny <rule-number><hostname>

no url-filter deny {rule-number|all}

Function: Configure the global url-filter black-list rule. The no command deletes the global url black-list rule.

Parameters: <rule-number>: the ID of the black-list rule;

<hostname>: the domain name that the black-list rule matches;

{rule-number|all}: rule-number means to delete the ID of the appointed black-list rule, all means to delete all the configured black-list rules.

Command Mode: Global Mode.

Default: None.

Usage Guide: This command can configure that the client cannot access the appointed domain name after the authentication in the portal authentication. Binding the black-list rule to the portal configuration can make the client cannot access the appointed resource before the authentication.

Example: Configure the url-filter black-list rule whose domain name is www.black.com.

AC(config)#url-filter deny 1 www.black.com

2.10.3 show url-filter status

Command: show url-filter status

Function: Show all the global configured url rules.

Parameters: None.

Command Mode: Admin Mode.

Default: None.

Usage Guide: This command can show the global configured url rules including url black-list rules and url white-list rules.

Example: View the global configured url rule.

AC#show url-filter status

Rule ID host action

-------- ---------- -----

1 www.test.com permit

1 www.baidu.* deny

2.10.4 url-filter permit (Portal Mode)

Command: url-filter permit <rule-number>

no url-filter permit {rule-number|all}

Function: Bind the url white-list rule to the portal configuration. The no command removes the binding of the appointed white-list rule or all the white-list rules.

Parameters: <rule-number>: the ID of the white-list rule;

{rule-number|all}: rule-number means to delete the binding of the appointed white-list rule, all means to delete the binding of all the configured white-list rules.

Command Mode: Portal Mode.

Default: None.

Usage Guide: This command can bind the white-list rule to the portal configuration. One portal configuration can bind multiple rules, and the one rule can be bound to multiple portal configurations.

Example: Bind the white-list rule 1 to the portal configuration.

AC(config-cp-instance)#url-filter permit 1

2.10.5 url-filter deny (Portal Mode)

Command: url-filter deny<rule-number>

no url-filter deny {rule-number|all}

Function: Bind the url black-list rule to the portal configuration. The no command removes the binding of the appointed black-list rule or all the black-list rules.

Parameters: <rule-number>: the ID of the white-list rule;

{rule-number|all}: rule-number means to delete the binding of the appointed black-list rule, all means to delete the binding of all the configured black-list rules.

Command Mode: Portal Mode.

Default: None.

Usage Guide: This command can bind the black-list rule to the portal configuration. One portal configuration can bind multiple rules, and the one rule can be bound to multiple portal configurations.

Example: Bind the black-list rule 1 to the portal configuration.

AC(config-cp-instance)#url-filter deny 1

2.11 Commands for No Perception of Portal

2.11.1 fast-mac-auth

Command: fast-mac-auth

Function: This command configures to enable the quick mac authentication function.

Parameters: None.

Command Mode: captive portal config mode.

Default: Disable.

Usage Guide: After enabled this command, there is no need to carry on the portal authentication if the mac authentication is successful.

Example: Enable the quick mac authentication function.

AC(config-cp-instance)#fast-mac-auth

2.11.2 no fast-mac-auth

Command: no fast-mac-auth

Function: This command disables the quick mac authentication function.

Parameters: None.

Command Mode: captive portal config mode.

Default: Disable.

Usage Guide: After disabled this function, all the users must carry on the portal authentication.

Example: Disable the quick mac authentication function.

AC(config-cp-instance)#no fast-mac-auth

2.12 Commands for Portal Escaping

2.12.1 portal-server-detect server-name <name>

Command: portal-server-detect server-name <name> [interval <interval>] [retry <retries>][action {log | permit-all | trap }]

no portal-server-detect server-name <name>

Function: Enable the Portal server escaping function and configure the related parameters and the server configuration of status changing.

Parameters: <name> is the Portal server name, it is the string including 1 to 32 characters and the upper and lower case letters should be distinguished. This portal server must exist. <interval>: it is the interval of probing attempt, the range is from 20 to 600 and the unit is second. The default value is 20. <retries>: it is the maximum number of the probing failures, the range is from 1 to 5 and the default value is 3. If the probing failures achieve this value, the server is considered unreachable. { log | permit-all | trap }: when the unreachable status of the Portal server changed, it can trigger the configuration including the following situations and multiple configurations can be selected at the same times.

- ☞ log: when the unreachable status of the Portal server changed, the log information can be sent. In the log, it records the portal server name and the status information before and after the change of the server status.
- ☞ trap: when the unreachable status of the Portal server changed, the trap information can be sent to the network management server. In the trap, it records the portal server name and the status information before and after the change of the server status.
- ☞ permit-all: it is also named as portal escaping. It means to cancel the portal authentication temporarily and allow all the portal users accessing the network when the portal server is in the unreachable status (down). If the server status changes to the reachable status (up), the portal authentication function will be recovered.

Default: Disable. The default values of interval, retries and action are 20, 3 and permit-all respectively.

Command Mode: Captive Portal Global Configuration Mode.

Usage Guide: This command can be used to enable the portal escaping function when the portal server has fault. After enabled this function, there is no effect for the user authentication if the connection between AC and Portal server is normal; only when the connection between the AC and Portal server is broken, the user can be allowed accessing the network without the authentication. The operations can enable this function too, but the triggered configuration must be selected as log or trap.

Example: Enable the escaping function of the portal server whose name is test. Configure the interval as 30s, configure the retries as 2 and configure the configuration of the server status change as log and permit-all.

AC(config-cp)# portal-server-detect server-name test interval 600 retry 2 action log permit-all trap

2.12.2 show captive-portal ext-portal-server server-name <name> status

Command: show captive-portal ext-portal-server server-name <name> status

Function: Show the portal server status including the server address and if the portal escaping function is enabled.

Parameters: <name> is the Portal server name, it is the string including 1 to 32 characters and the upper and lower case letters should be distinguished.

Default: None.

Command Mode: Admin Mode.

Usage Guide: Checking the server status is the important method to check the fault. When the portal escaping function is not effective, the configuration may be wrong; the command can be modified to help the administrator to remove the fault. If there is not the parameter of <name>, the status of all the servers will be shown. If there is the parameter of <name>, the detailed status information of the server will be shown.

Example: Show the status of all the ext-portal-server.

AC(config-cp)#show captive-portal ext-portal-server status

Server Name	Server IP Address	port	key
testserver	192.168.19.1	7749	
portalserver1	101.1.1.11	7749	
portalserver2	101.1.1.12	7749	
Portaltest	101.1.1.6	7749	

Show the detailed status information of the servers whose name is Portaltest.

AC(config-cp)#show captive-portal ext-portal-server server-name Portaltest status

Server Name..... portaltest
Server IP..... 101.1.1.6
Server Port..... 7749
Server Key.....
Detect Mode..... Enable
Detect Interval..... 20
Detect Retries..... 3
Detect Trap Mode..... Disable
Detect Log Mode..... Disable
Detect Permit-all Mode..... Enable
Detect Operational Mode..... Enable
Detect Operational Status..... Down
Detect Operational Fails..... 1
Detect Operational Time..... 0d:00:00:11

2.13 Commands for Two-dimension-code Authentication

2.13.1 two-dimension-code enable

Command: two-dimension-code enable

Function: This command is used to enable the two-dimension code authentication function.

Command Mode: Captive Portal Config Mode.

Default: Disable.

Usage Guide: After configured this command, the two-dimension-code scanning accessing of the client can be completed with the hot spot server.

Example: Enable the two-dimension-code authentication function.

AC (config-cp-instance)#two-dimension-code enable

2.13.2 two-dimension-code disable

Command: two-dimension-code disable

Function: This command is used to disable the two-dimension code authentication

function.

Command Mode: Captive Portal Config Mode.

Default: Disable.

Usage Guide: After disabled this function, user can only carry through the ordinary portal authentication, the two-dimension-code authentication cannot be used.

Example: Disable the two-dimension-code authentication function.

AC(config-cp-instance)# two-dimension-code disable

2.14 Wechat Authentication

2.14.1 thirdpart-auth discover url-head (Global)

Command: thirdpart-auth discover url-head

Function: Configure the URL head of the thirdpart authentication discovery packet.

Parameters: <word>, the URL head of the thirdpart authentication discovery packet such as http://www.dcme.net.cn/dreg/status

Command Mode: Global Mode.

Usage Guide: This command is used to configure the URL head of the thirdpart authentication discovery packet, including transmission protocol, domain name. it is configured according to the real domain name of the cloud platform.

Example: Configure the URL head of the thirdpart authentication discovery packet.

AC(config)# thirdpart-auth discover url-head http://www.dcme.net.cn/dreg/status

2.14.2 thirdpart-auth server-ipv4 (Global)

Command: thirdpart-auth server-ipv4

Function: Configure the IPv4 address of the thirdpart server.

Parameters: <ipv4>: the IPv4 address of the thirdpart server.

Command Mode: Global Mode.

Usage Guide: This command is used to configure the IPv4 address of the thirdpart server.

Example: Configure the IPv4 address of the thirdpart server.

AC(config)# thirdpart-auth server-ipv4 115.29.96.60

2.14.3 redirect url-mode thirdpart-auth (CP Instance Mode)

Command: redirect url-mode thirdpart-auth

Function: Configure the redirected URL mode of the thirdpart agency.

Parameters: standard: Configure the standard redirected URL mode;
thirdpart-auth: Configure the redirected URL mode of the thirdpart agency.

Default: Standard mode.

Command Mode: Captive Portal Instance Mode.

Usage Guide: This command is used to configure the redirected URL mode of the thirdpart agency.

Example: Configure the redirected URL mode of the thirdpart agency.

AC(config-cp-instance)#redirect url-mode thirdpart-auth

2.14.4 redirect attribute url-after-login weixin (CP Instance Mode)

Command: redirect attribute url-after-login weixin

Function: Configure the URL of the page after the successful thirdpart authentication.

Parameters: <WORD>: http://www.dcme.net.cn/portal must be configured in the wechat authentication.

Command Mode: Captive Portal Instance Mode.

Usage Guide: Configure the URL of the page after the successful thirdpart authentication.

Example: Configure the URL of the page after the successful thirdpart authentication.

AC(config-cp-instance)# redirect attribute url-after-login weixin http://www.dcme.net.cn/portal

2.14.5 redirect attribute url-after-login name url (CP Instance Mode)

Command: redirect attribute url-after-login name url

Function: Configure the URL name in the redirected packet of captive portal.

Parameters: None.

Command Mode: Captive Portal Instance Mode.

Usage Guide: Configure the parameter name in the redirected packet of captive portal.

Example: Configure the parameter name in the redirected packet of captive portal. Only url is received, the srcurl is not received.

AC(config-cp-instance)# redirect attribute url-after-login name url

2.14.6 redirect attribute custom-string name devicetype=6028

Command: redirect attribute custom-string name devicetype=6028

Function: Configure the URL property of the captive portal redirected packet.

Parameters: For distinguishing from the switch device, the property of devicetype=6028 is added in the redirected URL for showing that it is the redirected user from AC, the cloud platform will deal with it according to the AC process.

Command Mode: Captive Portal Instance Mode.

Usage Guide: Configure the URL property of the captive portal redirected packet.

Example: Configure AC to carry through the wechat authentication.

AC(config-cp-instance)# redirect attribute custom-string name devicetype=6028

Chapter 3 Commands for WAPI Access and Authentication

3.1 Commands for Global Configuration

3.1.1 wapi enable

Command: wapi enable

no wapi enable

Function: Enable global wapi function. The no command disables this function.

Parameters: None.

Default: Disable.

Command Guide: Wireless Global Mode.

Usage Guide: Use this command to enable global wapi function. If the global wapi function is not enabled, other wapi commands cannot be configured. Use **show wireless wapi status** command to check whether the global wapi function is enabled.

Example: Disable the global wapi function and then enable it.

AC(config-wireless)#no wapi enable

AC(config-wireless)#wapi enable

3.1.2 wapi authentication-server

Command: wapi authentication-server <1-5> <ipAddr> [port <0-65535>]

no wapi authentication-server [<1-5>]

Function: Configure the IPv4 AS when wapi certificate authenticates. The no command deletes the IPv4 AS.

Parameters: <1-5>, server number, 5 AS servers can be configured by system.

<ipAddr>, IPv4 address of authentication server.

<0-65535>, the port of the authentication packets which is dealt by authentication server. Select 3810 port as default. The field of port is optional and if it is not configured, 3810 port is selected as default.

Default: None.

Command Guide: Wireless Global Mode.

Usage Guide: Use this command to configure the IPv4 AS when wapi certificate authenticates. The field of port is optional and if it is not configured, 3810 port is selected

as default. When delete it, it cannot be deleted if server is bond by network. Use **show wireless wapi authentication-server status** command to check the configured AS status.

Example: Configure the ip address of AS server 1 as 192.168.1.100, and the port is 65535.

AC(config-wireless)#wapi authentication-server 1 ip 192.168.1.100 port 65535

3.1.3 wapi authentication-server timeout

Command: wapi authentication-server timeout <1~1000>

no wapi authentication-server timeout

Function: Configure the timeout of AS server response. The no command recovers to be default of 3s.

Parameters: <1-1000>: unit is s and it is the timeout of AS server response.

Default: 3s.

Command Guide: Wireless Global Mode.

Usage Guide: This command is used to configure the timeout of AS server response. AC sends the certificate to AS server to distinguish the requisition information. If the AS server response is not received in this time, the requisition fails. If configured retransmission, AC will retransmit. If there is still not response after retransmission more than once, the authentication fails. Use **show wireless wapi status** command to view the configured timeout.

Example: Configure the timeout of AS server response as 1000s.

AC(config-wireless)#wapi authentication-server timeout 1000

3.1.4 wapi authentication-server retransmit

Command: wapi authentication-server retransmit<0~100>

no wapi authentication-server retransmit

Function: Configure the retransmission times of AC sending requisition to AS. When there is no response in the timeout, then retransmit. The no command recovers the times to default of 3.

Parameters: <*0-100*>, the retransmission times of AC sending requisition to AS.

Default: 3 times.

Command Guide: Wireless Global Mode.

Usage Guide: This command is used to configure the retransmission times of AC sending requisition to AS. AC sends the certificate to AS server to distinguish the requisition information. If the AS server response is not received in this time, the requisition fails. If

configured retransmission, AC will retransmit. If there is still not response after retransmission more than once, the authentication fails. Use **show wireless wapi status** command to view the configured retransmission times.

Example: Configure the retransmission times of AC sending requisition to AS as 100.

AC(config-wireless)#wapi authentication-server retransmit 100

3.1.5 wapi certificate format

Command: wapi certificate format *{gbw | x509}*

no wapi certificate format

Function: Configure the certificate format when using wapi certificate authentication method. The no command recovers to be default format of X509.

Parameters: {gbw | x509}, appoint the certificate format of wapi certificate; GBW: it is a management system of distinguishing the key based on public key system; X509: it is the digital certificate standard formulated by International Telecommunications Union (ITU-T). and it is a management system of distinguishing the key based on public key system.

Default: Use the certificate with X509 format.

Command Guide: Wireless Global Mode.

Usage Guide: Configure the certificate format when using wapi certificate authentication method. The no command recovers to be default format of X509. Use **show wireless wapi status** command to view the configured certificate format.

Example: Configure the certificate format as X509.

AC(config-wireless)#wapi certificate-format x509

3.1.6 wapi certificate-mode

Command: wapi certificate-mode *{2|3}*

no wapi certificate-mode

Function: Configure the certificate mode when using wapi authentication method. The no command recovers to be default mode of 2 certificate mode.

Parameters: {2|3}, it means 2 certificate mode or 3 certificate mode.

Default: 2 certificate mode.

Command Guide: Wireless Global Mode.

Usage Guide: Configure the certificate mode when using wapi authentication method. The no command recovers to be default mode of 2 certificate mode. Use **show wireless wapi status** command to view the configured certificate mode.

Example: Configure the certificate mode when using wapi authentication method as 3 certificate mode.

AC(config-wireless)#wapi certificate-mode 3

3.1.7 snmp-server enable traps wapi

Command: snmp-server enable traps wapi

no snmp-server enable traps wapi

Function: Enable wapi traps function globally. The no command disables all wapi traps function.

Parameters: None.

Default: Disable.

Command Guide: Global Mode.

Usage Guide: Use this command to enable wapi traps function. The no command disables all wapi traps function.

Example: Enable wapi traps function (enable snmp-server and global traps function firstly).

AC(config)#snmp-server enable

AC(config)#snmp-server enable traps

AC(config)#snmp-server enable traps wapi

3.2 Commands for Network Configuration

3.2.1 security mode

Command: security mode *{none | static-wep | wep-dot1x | wpa-enterprise | wpa-personal | wapi-certificate | wapi-psk}*

no security mode

Function: Configure the authentication and encryption method that network supports. The no command deletes the configured authentication and encryption method (recover to be lawful method).

Parameters: {none | static-wep | wep-dot1x | wpa-enterprise | wpa-personal | wapi-certificate | wapi-psk}, none means lawful method, there is no wireless authentication and encryption configuration. Others are wireless security access methods that 802.11 defines. wapi-certificate means to configure the access authentication method as wapi authentication; wapi-psk means to configure the access authentication method as wapi pre-shared key authentication.

Default: none (lawful method).

Command Guide: Network Configuration Mode.

Usage Guide: This command can configure all kinds of authentication and encryption methods for network. The no command deletes the authentication and encryption methods that network supports (recover to be lawful method). Use **show wireless network *<1-1024>*** command to view the configured authentication and encryption methods.

Example: Configure network 101 to use wapi pre-shared key authentication.

AC(config-wireless)#network 101

AC(config-network)#security mode wapi-psk

3.2.2 wapi authentication-server

Command: wapi authentication-server <1-5>

no wapi authentication-server

Function: Configure the ipv4 AS number value used by network when it uses wapi certificate authentication method. The no command deletes the ipv4 AS.

Parameters: <1-5>, wapi authentication server number.

Default: None.

Command Guide: Network Configuration Mode.

Usage Guide: Configure the ipv4 AS number value used by network when it uses wapi certificate authentication method. The no command deletes the ipv4 AS. One network only can configure one ipv4 AS. Use **show wireless network *<1-1024>* wapi status** command to view the AP number that network used.

Example: Configure the ipv4 AS number value used by network 101 when it uses wapi certificate authentication method as 5.

AC(config-wireless)#network 101

AC(config-network)#wapi authentication-server 5

3.2.3 wapi bk-refresh-rate

Command: wapi bk-refresh-rate *<0,30-43200>*

no wapi bk-refresh-rate

Function: Configure the BK updating frequency of network when it uses wapi authentication method. The no command recovers to be default.

Parameters: *<0,30-43200>*, the updating frequency of BK key, unit is second. 0 means to disable the BK key updating function.

Default: 43200s.

Command Guide: Network Configuration Mode.

Usage Guide: Configure the BK updating frequency of network when it uses wapi

authentication method. The no command recovers to be default. Use **show wireless network <*1-1024*> wapi status** command to view the BK updating frequency of network when it uses wapi authentication method.

Example: Configure the BK updating frequency of network when it uses wapi authentication method as 3000s.

AC(config-network)#wapi bk-refresh-rate 30000

3.2.4 wapi msk-refresh client-offline

Command: wapi msk-refresh client-offline

no wapi msk-refresh client-offline

Function: Enable the function that the downline user triggers MSK updating when network uses wapi authentication method. The no command disables this function.

Parameters: None.

Default: Disable.

Command Guide: Network Configuration Mode.

Usage Guide: Enable the function that the downline user triggers MSK updating when network uses wapi authentication method. The no command disables this function. Use **show wireless network <*1-1024*> wapi status** command to check if this function is enabled.

Example: Enable the function that the downline user triggers MSK updating when network uses wapi authentication method.

AC(config-network)#wapi msk-refresh client-offline

3.2.5 wapi msk-refresh-rate

Command: wapi msk-refresh-rate *{packet-based <30-86400>|} { time-based <30-86400>|}*

no wapi msk-refresh-rate

Function: Configure the MSK updating frequency when network uses wapi authentication method. The no command recovers to be default updating method that the time interval triggers MSK updating and the time interval is 86400s.

Parameters: *packet-based <0,30-86400>*: configure that MSK updating based on the number of packets. 0 means not to trigger the MSK updating.

time-based <0,30-86400>: configure that MSK updating based on the time interval. Unit is second. 0 means time does not trigger the MSK updating.

Default: Time interval triggers the multicast key updating and the time interval is 86400s.

Command Guide: Network Configuration Mode.

Usage Guide: Configure the MSK updating frequency when network uses wapi authentication method. The no command recovers to be default updating method that the time interval triggers MSK updating and the time interval is 86400s. When the parameters of packet-based and time-based both exist and they are not 0, it means that both of them trigger the MSK updating. When both of them are 0, disable MSK updating function. Notice: The configurations of packet-based and time-based are independent. Configuring the packet-based only will not cover the parameter of time-based configured before. Use **show wireless network <*1-1024*> wapi status** command to view the MSK updating frequency.

Example: Configure the MSK updating frequency when network uses wapi authentication method: trigger the updating every 40000 packets and every 50000s.

AC(config-network)#wapi msk-refresh-rate packet-based 40000 time-based 50000

3.2.6 wapi psk

Command: wapi psk *{ciper | pass-phrase}* <*value*>

no wapi psk

Function: Configure the pre-shared key of network when it uses wapi psk authentication method. The no command deletes this pre-shared key.

Parameters: *{ciper* | *pass-phrase}*, ciper means to select the PSK value of AKM kit of WAPI for PSK mode, BK will be produced by this object. Pass-phrase means a kind of method which can be replaced, use command-key algorithm to configure the PSK, this variable provides a kind of method of inputting command, when this variable is written, WAPI substance will use command-key algorithm to export a pre-shared key.

<*value*>, key value.

Default: None.

Command Guide: Network Configuration Mode.

Usage Guide: Configure the pre-shared key of network when it uses wapi psk authentication method. The no command deletes this pre-shared key. Use **show wireless network <*1-1024*> wapi status** command to view the configured Wapi PSK.

Example: Configure the pre-shared key of network when it uses wapi psk authentication method as 12345678.

AC(config-network)#wapi psk cipher 12345678

3.2.7 wapi psk length

Command: wapi psk length <*8-64*>

no wapi psk length

Function: Configure the key length when the network uses wapi psk authentication method. The no command recovers to be default of 8.

Parameters: <*8-64*>, length of wapi psk.

Default: 8.

Command Guide: Network Configuration Mode.

Usage Guide: Configure the key length when the network uses wapi psk authentication method. The no command recovers to be default of 8. Use **show wireless network *<1-1024>* wapi status** command to view the configured length of pre-shared key.

Example: Configure the key length when the network uses wapi psk authentication method as 64.

AC(config-network)#wapi psk length 64

3.2.8 wapi psk type

Command: wapi psk type *{ascii | hex}*

no wepkey type

Function: Configure the key type when the network uses wapi psk authentication method. The no command recovers to be default of Hex.

Parameters: *{ascii* | *hex}*, type of wapi psk, they are represented with ASCII and hexadecimal respectively.

Default: Hex.

Command Guide: Network Configuration Mode.

Usage Guide: Configure the key type when the network uses wapi psk authentication method. The no command recovers to be default of Hex. Use **show wireless network *<1-1024>* wapi status** command to view the configured type of pre-shared key.

Example: Configure the key type when the network uses wapi psk authentication method as ASCII.

AC(config-network)#wapi psk type ascii

3.2.9 wapi usk-refresh-rate

Command: wapi usk-refresh-rate *{packet-based <30-86400>|} { time-based <30-86400>|}*

no wapi usk-refresh-rate

Function: Configure the USK updating frequency when the network uses wapi psk authentication method. The no command recovers to be default value. Time interval triggers unicast key updating and the time interval is 86400s.

Parameters: *packet-based <0,30-86400>*: configure USK updating based on the number

of packets. 0 means not to trigger USK updating.

time-based <0,30-86400>: configure that USK updating based on the time interval. Unit is second. 0 means time does not trigger the MSK updating.

Default: Time interval triggers the unicast key updating and the time interval is 86400s.

Command Guide: Network Configuration Mode.

Usage Guide: Configure the USK updating frequency when the network uses wapi psk authentication method. The no command recovers to be default value. When the parameters of packet-based and time-based both exist and they are not 0, it means that both of them trigger the USK updating. When both of them are 0, disable USK updating function. Notice: The configurations of packet-based and time-based are independent. Configuring the packet-based only will not cover the parameter of time-based configured before. Use **show wireless network *<1-1024>* wapi status** command to view the USK updating frequency.

Example: Configure the USK updating frequency when the network uses wapi psk authentication method: trigger the updating every 40000 packets and every 50000s.

AC(config-network)#wapi usk-refresh-rate packet-based 40000 time-based 50000

3.3 Commands for AP database

3.3.1 wapi certificate ap

Command: wapi certificate ap *<name>*

no wapi certificate ap

Function: Configure the certificate file name of AP itself in ap database. This certificate is used for AP to conduct wapi authentication to user. The command deletes the configured authentication file.

Parameters: <name>, it is the authentication file name represented with string, length is 1 to 128 characters, including all the characters which can be printed. When select x509 certificate format, the file name must be end with .cer; when select GBW certificate format, the file name must be end with .wcr.

Default: None.

Command Guide: Ap Database Global Mode.

Usage Guide: Configure the certificate file name of AP itself in ap database. This certificate is used for AP to conduct wapi authentication to user. The command deletes the configured authentication file. This command just modifys or configures the file name and it will not issue certificate to AP, use **wapi certificate- distribute** command to issue certificate to AP for effective.

Example: Configure the AP certificate file name of the AP with MAC address of

00-03-0f-01-0b-80 as AP101.cer.

AC(config-wireless)#ap database 00-03-0f-01-0b-80

AC(config-ap)#wapi certificate ap AP101.cer

3.3.2 wapi certificate as

Command: wapi certificate as *<name>*

no wapi certificate as

Function: Configurethe certificate file name of AS server related to AP in ap database. This certificate is used for AP to conduct signature checking to AS message in wapi authentication. The no command deletes the certificate file name.

Parameters: <name>, it is the authentication file name represented with string, length is 1 to 128 characters, including all the characters which can be printed. When select x509 certificate format, the file name must be end with .cer; when select GBW certificate format, the file name must be end with .wcr.

Default: None.

Command Guide: Ap Database Global Mode.

Usage Guide: Configurethe certificate file name of AS server related to AP in ap database. This certificate is used for AP to conduct signature checking to AS message in wapi authentication. The no command deletes the certificate file name. This command just modifys or configures the file name and it will not issue certificate to AP, use **wapi certificate- distribute** command to issue certificate to AP for effective.

Example: Configure the AS certificate file name of the AP with MAC address of 00-03-0f-01-0b-80 as AS101.cer.

AC(config-wireless)#ap database 00-03-0f-01-0b-80

AC(config-ap)#wapi certificate as AS101.cer

3.3.3 wapi certificate ca

Command: wapi certificate ca *<name>*

no wapi certificate ca

Function: Configure the CA root certificate file related to AP in ap database. This certificate is used for AP to conduct certificate checking to AP certificate and AS server certificate. The no command deletes the CA root certificate file name.

Parameters: <name>>, it is the authentication file name represented with string, length is 1 to 128 characters, including all the characters which can be printed. When select x509 certificate format, the file name must be end with .cer; when select GBW certificate format, the file name must be end with .wcr.

Default: None.

Command Guide: Ap Database Global Mode.

Usage Guide: Configure the CA root certificate file related to AP in ap database. This certificate is used for AP to conduct certificate checking to AP certificate and AS server certificate. The no command deletes the CA root certificate file name. This command just modifys or configures the file name and it will not issue certificate to AP, use **wapi certificate- distribute** command to issue certificate to AP for effective.

Example: Configure the CA root certificate file name of the AP with MAC address of 00-03-0f-01-0b-80 as CA101.cer.

AC(config-wireless)#ap database 00-03-0f-01-0b-80

AC(config-ap)#wapi certificate ca CA101.cer

3.4 Commands for Admin

3.4.1 clear wireless wapi ap statistics

Command: clear wireless wapi ap *[<macaddr>]* statistics

Function: Clear wapi statistic information of the appointed AP or all APs.

Parameters: <*macaddr*>: MAC address of AP, this parameter is optional.

Default: None.

Command Guide: Previlidged EXEC Mode.

Usage Guide: If this command is with MAC address, clear wapi statistic information of the appointed AP. If it is without parameter, clear wapi statistic information of all APs.

Example: Clear wapi statistic information of the appointed AP with MAC address of 00-03-0f-01-0b-80.

AC#clear wireless wapi ap 00-03-0f-01-0b-80 statistics

The AP wapi statistics will be cleared. Are you sure you want to clear the statistics on the switch? [Y/N] y

The ap wapi statistics has been cleared.

3.4.2 copy wapi-certificate

Command: copy wapi-certificate *<source-url> <destination-url>*

Function: Import the certificates of AP, AS and CA to AC manually.

Parameters: <source-url>: source path of the certificate file, for example: tftp://server_ip/path/filename;

<destination-url>, the destination path copied by certificate file.

Default: None.

Command Guide: Previlidged EXEC Mode.

Usage Guide: Import the certificates of AP, AS and CA to AC manually. After applying the certificate in certificate version agency, it needs to be imported to AC manually and AC will issue it to AP.

Example: Import the AP certificates of AP20120625.cer to AC manually.

AC#copy wapi-certificate tftp://194.168.1.203/AP20120625.cer AP20120625.cer

3.4.3 show wireless network wapi status

Command: show wireless network <*1-1024*> wapi status

Function: Show the information of network wapi configuration.

Parameters: <*1-1024*>, network number.

Default: None.

Command Guide: Previlidged EXEC Mode.

Usage Guide: Use this command to inquiry network configuration and show the wapi configuration parameters.

Example: View the wapi configuration parameters of network 101.

AC#show wireless network 101 wapi status

Network ID..... 101
Wapi Authentication-Server-Index..... 0
Wapi Psk Configuration Method..... cipher
Wapi Psk Type..... ASCII
Wapi Psk Length..... 9
Wapi Psk..... 123456789
Wapi Bk-Refresh-Rate..... 10000
Wapi Usk-Refresh-Method..... timePacket-based
Wapi Usk-Refresh-Time-Rate..... 30000
Wapi Usk-Refresh-Packet-Rate..... 20000
Wapi Msk-Refresh-Method..... timePacket-based
Wapi Msk-Refresh-Time-Rate..... 50000
Wapi Msk-Refresh-Packet-Rate..... 40000
Wapi Msk-Refresh Client-Offline..... Enable

3.4.4 show wireless wapi ap statistics

Command: show wireless wapi ap <*macaddr*> statistics

Function: Show the wapi statistic information of ap.

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

Default: None.

Command Guide: Previlidged EXEC Mode.

Usage Guide: Show the wapi statistic information of ap with the appointed MAC address.

Example: Show the wapi statistic information of the AP with MAC address of 00-03-0f-01-0b-80.

AC#show wireless wapi ap 00-03-0f-01-0b-80 statistics

MAC address..... 00-03-0f-01-0b-80
WPI Replay Counters..... 0
WPI Decryptable Errors..... 0
WPI MIC Errors..... 0
WAI Sign Errors..... 0
WAI HMAC Errors..... 0
WAI Authentication Result Failures..... 0
WAI Discard Counters..... 0
WAI Timeout Counters..... 0
WAI Format Errors..... 0
WAI Certificate Handshake Failures..... 0
WAI Unicast Handshake Failures..... 0
WAI Multicast Handshake Failures..... 0

3.4.5 show wireless wapi ap-certificate status

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

Function: Show the status of AP installing certificate.

Parameters: *[<macaddr>]*: MAC address of AP.

Default: None.

Command Guide: Previlidged EXEC Mode.

Usage Guide: When it is with MAC address, show the certificate installation status of the appointed AP. If there is no MAC address, show the certificate installation status of all APs.

Example: After showing the certificate installation status of all APs, show the certificate installation status of the AP with MAC address of 00-03-0f-01-0b-80.

AC#show wireless wapi ap-certificate status

Certificate Status..... Success

Certificate Total AP count..... 1

Certificate Success AP count..... 1

Certificate Failure AP count..... 0

AC#show wireless wapi ap-certificate 00-03-0f-01-0b-80 status

MAC address..... 00-03-0f-01-0b-80

AP Certificate Name..... AP20120625.cer

AS Certificate Name..... as20120625.cer

CA Certificate Name.....

Certificate Status..... Success

3.4.6 show wireless wapi authentication-server status

Command: show wireless wapi authentication-server status

Function: Show AS information of global wapi configuration.

Parameters: None.

Default: None.

Command Guide: Previlidged EXEC Mode.

Usage Guide: Use this command to show AS information of global wapi configuration.

Example: Show AS information of global wapi configuration.

AC#show wireless wapi authentication-server status

Server Index	IP Address	port	SocketNo
1	194.168.1.200	3810	0
2	194.168.1.202	3810	0
3	194.168.1.203	3810	0
4	194.168.1.204	3810	0
5	194.168.1.205	3810	0

3.4.7 show wireless wapi status

Command: show wireless wapi status

Function: Show global wapi information.

Parameters: None.

Default: None.

Command Guide: Previlidged EXEC Mode

Usage Guide: Use this command to show global wapi information.

Example: Show global wapi information.

AC#show wireless wapi status

Wapi Mode..... Enable

Wapi Certificate Format..... x509

Wapi Certificate Mode..... 2 certificate

Wapi Authentication-Server Timeout(Second)..... 1000

Wapi Authentication-Server Retransmit..... 100

Max-client Allowed..... 200

Mix Radio Support..... Enable

3.4.8 wapi certificate- distribute

Command: wapi certificate- distribute *[<macaddr>]*

Function: Issue the certificate file to the AP with appointed MAC address or all managed APs.

Parameters: *[<macaddr>]*: MAC address of AP. It is optional field. When not to input this parameter, it means to issue certificate to all managed APs.

Default: None.

Command Guide: Previlidged EXEC Mode.

Usage Guide: Use this command to issue the certificate file to the AP with appointed MAC address or all managed APs, including AP certificate and AS certificate; there is also CA certificate if select 3 certificate mode.

Example: Issue the certificate file to all managed APs.

AC#wapi certificate-distribute

3.5 Commands for Debug

3.5.1 debug wireless wapi error

Command: debug wireless wapi error

no debug wireless wapi error

Function: Enable the error debug on-off in client wapi authentication. The no command disables this on-off.

Parameters: None.

Default: Disable.

Command Guide: Previlidged EXEC Mode.

Usage Guide: Use this command to enable the error debug on-off in client wapi authentication. User can examine the error debug information in client wapi authentication on AC controller platform. The no command disables this on-off.

Example: Enable the error debug on-off in client wapi authentication.

AC#debug wireless wapi error

error WD_LEVEL_WAPI_ERROR debug is on

3.5.2 debug wireless wapi internal

Command: debug wireless wapi internal *<macaddr>*

no debug wireless wapi internal *<macaddr>*

Function: Enable the internal detailed debug on-off in client wapi authentication. The no command disables this on-off.

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

Default: Disable.

Command Guide: Previlidged EXEC Mode.

Usage Guide: Use this command to enable the internal detailed debug on-off in client wapi authentication. User can examine the internal detailed debug information in client wapi authentication on AC controller platform. The no command disables this on-off.

Example: Enable the internal detailed debug on-off in client wapi authentication for the AP with MAC address of 00-03-0f-01-0b-80.

AC#debug wireless wapi internal 00-03-0f-01-0b-80

MAC:00-03-0f-01-0b-80 internal WD_LEVEL_WAPI_INTERNAL, debug is on

3.5.3 debug wireless wapi packet

Command: debug wireless wapi packet*{all | receive | send | dump}* *<macaddr>*

no debug wireless wapi packet*{all | receive | send | dump}* *<macaddr>*

Function: Enable the debug information in client wapi authentication. The no command disables it.

Parameters: *send*: Enable the debug information of sending packets to AP and AS in client wapi authentication;

Receive: Enable the debug information of receiving packets from AP and AS in client wapi authentication;

dump: Enable the printing information of sending and receiving packets from AP and AS in client wapi authentication;

All: Enable the printing debug information of sending, receiving packets and packets in dealing with STA association;

<*macaddr*>: Launch the MAC address of AP in authentication.

Default: Disable.

Command Guide: Previlidged EXEC Mode.

Usage Guide: Use this command to enable the debug information in client wapi authentication. User can examine the packets debug information in client wapi authentication on AC controller platform. The no command disables the debug information.

Example: For the AP with MAC address of 00-03-0f-01-0b-80 AP, enable the printing debug information of sending, receiving packets and packets in dealing with STA association.

AC#debug wireless wapi packet all 00-03-0f-01-0b-80

MAC:00-03-0f-01-0b-80 packet WD_LEVEL_WAPI_PKT_RX debug is on

MAC:00-03-0f-01-0b-80 packet WD_LEVEL_WAPI_PKT_TX debug is on

MAC:00-03-0f-01-0b-80 packet WD_LEVEL_WAPI_PKT_DUMP debug is on

3.5.4 debug wireless wapi trace

Command: debug wireless wapi trace <*macaddr*>

no debug wireless wapi trace <*macaddr*>

Function: Enable the track debug on-off in client wapi authentication. The no command disables this on-off.

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

Default: Disable.

Command Guide: Previlidged EXEC Mode.

Usage Guide: Use this command to enable the track debug on-off in client wapi authentication. User can examine the track debug information in client wapi authentication on AC controller platform. The no command disables this on-off.

Example: For the AP with MAC address of 00-03-0f-01-0b-80 AP, enable the track debug on-off in client wapi authentication.

AC#debug wireless wapi trace 00-03-0f-01-0b-80

MAC:00-03-0f-01-0b-80 internal WD_LEVEL_WAPI_TRACE debug is on

Chapter 4 Commands for Access Authentication Based on Domain

4.1 delimiter<string>

Command: delimiter<string>

no delimiter<string>

Function: Configure the delimiter that the domain adopts. The no command deletes the configuration.

Parameters: < string > is the delimiter. The string can be @/.

Default: @.

Command Mode: Domain Config Mode.

Usage Guide: The delimiter is used to separate the user name and domain. In using, the delimiter and user name (including pure user name and domain name) are compared. After matched, the front part will be distinguished as the user name, and the back part will be distinguished as domain. When the user name (including pure user name and domain name) has multiple delimiters, only the first delimiter can be compared, the back part will be as a part of domain. When the delimiter is configured as string, it means this domain uses multiple delimiters, and every character in the string all can be the delimiter. After configured the no command, the default delimiter of @ will be used.

Example: Configure the delimiter of domain1 as @ or /.

AC(config-wireless)# domain 3

AC(config-domain)# delimiter @/

4.2 domain<1-5> (Network Configuration Mode)

Command: domain<1-5>

no domain<1-5>

Function: Bind the appointed domain to network. The no command deletes the binding relationship between domain and network.

Parameters: <1-5> is the domain number and the range is 1~5.

Default: None.

Command Mode: Network Configuration Mode.

Usage Guide: After the domain is configured, it must be bound to the network to be effective, and then it can extract the domain name from the user name. if the extracted

domain name from the user name and the one configured by domain are the same, the radius server configured by domain will be adopted for the authentication and accounting. If they are different, the radius server configured under the network will still be used. The domain must be configured first, and then it can be bound to the network, otherwise, there will be error. The newest configuration of this command can cover the previous configuration. If the appointed domain has been bound to this network, the configuration will not be changed and there will not be the prompt. One domain can be bound to multiple networks.

Example: Bind domain3 to the network.

AC(config-wireless)# network 3

AC (config-network)# domain 3

4.3 domain<1-5> (Wireless Global Mode)

Command: domain<1-5>

no domain<1-5>

Function: Add a domain configuration or enter into the domain configuration mode. The no command deletes the domain configuration.

Parameters: <1-5> is the domain number and the range is 1~5.

Default: None.

Command Mode: Wireless Global Mode.

Usage Guide: The domain must be added first, and then the delimiter, domain name and the corresponding radius server of the domain can be configured and this domain can be bound to the network. The domain number is the only mark; it must be used when binding the domain to the wireless network. 5 domains can be configured at most on AC. The no command deletes the configured domain. When the domain is deleted, the corresponding delimiter, domain name and radius server will be deleted at the same time.

Example: Add domain 3.

AC(config-wireless)# domain 3

4.4 Radius server-name {auth|acct}<name>

Command: radius server-name *{auth|acct}<name>*

no radius server-name *{auth|acct}<name>*

Function: Configure the radius server name that the domain adopts. The no command deletes the configured server name.

Parameters: {*auth*|*acct*} is the server type. Auth means the authentication server, acct

means the accounting server. <*name*> is the server name.

Default: None.

Command Mode: Domain Config Mode.

Usage Guide: After configured this server, the authentication request and accounting packet will be sent to the server if the domain name of the user name and the one of domain are matching. If they are not matching, the authentication request and accounting packet will be sent to the network or the server under the wireless global mode. Notice: The server name must exist, because this command cannot do the effective check.

Example: Configure the authentication server name of domain1 as wlantest. (we assume the server of wlantest has existed.)

AC(config-wireless)# domain 3

AC(config-domain)# radius server-name auth wlantest

4.5 realm<string>

Command: realm<string>

no realm

Function: Configure the domain name of the domain. The no command deletes it.

Parameters: < string > is the domain name. it is the string with 1 to 32 characters. The characters can be letters, numbers and special characters of -_@./

Default: None.

Command Mode: Domain Config Mode.

Usage Guide: One domain must be configured a domain name with more than one character, otherwise, this domain has no practical value. The domain names cannot be same. If the configured domain name has been used by other domain, there will be the prompt of error and the configuration will fail. The domain name can be effective after being modified.

Example: Configure the domain name of domain 1 as com.cn.

AC(config-wireless)# domain 3

AC(config-domain)#realm com.cn

Chapter 5 Commands for LDAP

5.1 authentication line

Command: authentication line {console | vty | web} login {local | radius | tacacs | ldap}

no authentication line {console | vty | web} login

Function: This command is used to configure the verification methods and selection priority of VTY (Telnet and ssh login methods), Web and Console methods to login user. Console, VTY and Web login can configure the corresponding login verification methods respectively. Their verification methods can be selected with the any combination of Local, RADIU, tacacs and ldap. The no command recovers the configuration.

Parameters: The parameters of console, vty and web respectively mean that login the AC through console, telnet, ssh and web. Vty includes telnet and ssh; local, radius, tacacs and ladp mean the use verification methods in login.

Default: No verification for Console and the local verification for VTY and Web as default.

Command Mode: Global Mode.

Usage Guide: When adopting combination verification method, the priority of the first method is the highest and they are in descending order. If the method with higher priority passed, allow the user to login and ignore the following methods. Notice: As long as one verification method received the clear response from the corresponding protocol, it will not try the next verification method no matter refusing or receiving (Exception: when local verification method failed, the next method will be tried for sure.).if the clear response is not received, try the next method. When using LDAP authentication, LDAP server must be configured. **authentication line console login** command is repulsed to **login** command. **authentication line console login** command configures the verification method of Console login but **login** command enables the Console login verification which is configured by **password** command. Even if configured local options, Console method can be used to login AC directly if the local users are not configured.

Example: Configure to adopt LDAP method to authenticate when using VTY login method.

ac(config)# authentication line vty login ldap

5.2 debug ldap error

Command: debug ldap error

no debug ldap error

Function: In LDAP module, print error information in the wrong code, including the error position and relevant parameters.

Parameters: None.

Default: Do not print.

Command Mode: Admin Mode.

Usage Guide: In LDAP module, if there is anomalies in codes conducting, the program will print the position of error code and the relevant information.

Example: Enable LDAP printing error.

ac# debug ldap error

5.3 debug ldap packet {send|receive|all}

Command: debug ldap packet {send|receive|all}

no debug ldap packet {send|receive|all}

Function: Enable debug on-off of receiving and sending packets of LDAP module; print the received, sent packets and interact two-way packets in AC and LDAP interaction. The no command disables the debug on-off.

Parameters: None.

Default: Disable.

Command Mode: Admin Mode.

Usage Guide: Enable **debug ldap packet send** on-off, AC will print the data packets from AC to LDAP server; enable **debug ldap packet receive** on-off, AC will print the data packets of LDAP server received; enable **debug ldap packet all** on-off, AC will print the two-way data packets in interaction with LDAP server.

Example: Enable d**ebug ldap packet all** on-off.

ac# debug ldap packet all

5.4 debug ldap trace

Command: debug ldap trace

no debug ldap trace

Function: Enable code trace debug on-off of ldap module. This debug mainly prints the code conducting process of LDAP module, such as process branch, current position.

Parameters: None.

Default: Do not print.

Command Mode: Admin Mode.

Usage Guide: Print the trace of code and examine the entire process.

Example: Enable code trace debug on-off of ldap module.

ac# debug ldap trace

5.5 ldap-server <server-index>

Command: ldap-server <*server-index*>

no ldap-server <*server-index*>

Function: Configure the LDAP server instance when authentication portal user adopts LDAP authentication. The no command deletes this configuration. Then the authentication requisition of portal user will be sent to all configured ldap servers successively until ldap server returns the clear authentication result (received or refused).

Parameters: < *server-index* > is the index of server instance, range is 1 to 64.

Default: Adopt all configured LDAP servers to authenticate.

Command Mode: Captive Portal Instance Mode.

Usage Guide: When portal user adopts LDAP authentication user name, adopt this server instance. Each instance of portal only can bind to one LDAP server. Before conducting this command, if portal instance has bond to LDAP authentication server, enabling this command will modify the LDAP server bond to portal instance.

Example: Configure LDAP authentication server of captive portal instance 1 as ldap server 1.

ac (config)#captive-portal

ac (config-cp)#configuration 1

ac (config-cp-instance)#ldap server 1

5.6 ldap server <server-index> authentication-methed {anonymous | authenticated username <username> password <password>}

Command: ldap server <*server-index*> authentication-methed {*anonymous* | *authenticated* username <*username*> password <*password*>}

Function: This command is used to configure the authentication method when inquire binding.

Parameters: <*server-index*> is LDAP server instance index, range is 1 to 64. System supports 64 LDAP server instances at most. *Anonymous* means anonymous authentication; *authenticated* means simple authentication. <*username*> is administrator DN of LDAP server and the length is no more than 64; <*password*> is administrator password, the length is no more than 32; these two parameters are used to create simple

binding relationship between AC and LDAP server to achieve the inquiry permission of Base DN.

Default: Anonymous authentication.

Command Mode: Global Mode.

Usage Guide: This command is used to configure the authentication method of LDAP server instance. If the current server is not existing, it will show the error prompt; otherwise, configure the authentication method of this server instance. If the server instance is in dead state, modifying the authentication method of the server instance will change the state of this instance from dead to not dead.

Example: Configure the authentication method of LDAP server 1 as simple authentication, user name is root, password is 123456.

ac(config)# ldap server 1 authentication-methed *authenticated* username root password *123456*

5.7 ldap server <server-index> ipv4-address <ipv4-address> {port <port-num>|} user-base-dn <base-dn> user-attr <user-attr> {user-type <user-type>|}

Command: ldap server <*server-index*> ipv4-address <*ipv4-address*> {port <*port-num*>|} user-base-dn <*base-dn*> user-attr <*user-attr*> {user-type <*user-type*>|}

no ldap server <*server-index*>

Function: This command is used to create an LDAP server instance. The no command deletes it.

Parameters: *server-index* is server instance index, range is 1 to 64, system supports 64 LDAP server instances at most; *ipv4-address* is an effective server ip address and it is a string made up with points; <*port-num*> is server port number, range is 0 to 65535, it should be configured according to LDAP service port on server, the default configuration is 389; ip address and port can together make AC and LDAP create connection.

<*base-dn*> is used in inquiry process and it is used to appoint the start position of inquiry, we can inquire in all sub-tittles under base-dn, the length of <*base-dn*> is no more than 64 characters; <*user-attr*> is used to appoint the property type that authentication user belongs to; <*user-type*> is used to appoint the type that authentication user belongs to; these three parameters make up an inquiry factor, the authentication user DN can be inquired according to authentication user name. <*user-attr*> and <*user-type*> are both no more than 32 characters.

Default: None.

Command Mode: Global Mode.

Usage Guide: If this server instance is not existing, this command is used to create an LDAP server instance. Using this command can configure or modify the parameters of LDAP server instance, such as server address, port, Base DN, user property and type. If this server instance has existed, the configuration of current server instance will be modified. Modifying the ip address or port of a server instance which has been dead will change the state from dead to not dead. After modifying server instance successfully, all authentication requisitions after will adopt the new configuration.

Example: Create LDAP server instance, index is 1, IP address is 1.1.1.1, port is 389, user-base-dn is dc=internet dc=com, user-attr=uid and user-type class.

ac(config)# ldap server 1 ipv4-address 1.1.1.1 port 389 user-base-dn dc=internet dc=com user-attr uid user-type class

5.8 ldap server <server-index> search-filter <search-filter>

Command: ldap server <*server-index*> search-filter <*search-filter*>

no ldap server <*server-index*> search-filter

Function: This command is used to configure the additional filtration condition in inquiring for an LDAP server instance. The no command deletes the condition of the appointed LDAP server instance.

Parameters: *server-index* is LDAP server instance index, range is 1 to 64, system supports 64 LDAP server instances at most; *search-filter* is the filtration condition, it supports 64 characters at most, this filtration condition and the existed filtration condition in current inquiry configuration are the relationship of '&'. This filtration condition includes the logic condition of &, | and ！, as shown below:

inetUserStatus=Active: only one condition

!(inetUserStatus=Active): include the condition of “non”

&(inetUserStatus=Active)(qq=123456): include two conditions and they are the relationship of "&".

|(inetUserStatus=Active)(qq=123456): include two conditions and they are the relationship of "|".

&(&(property=value)(property=value))(|(property=value)(property=value)): include "&", "|" and "!".

Default: None.

Command Mode: Global Mode.

Usage Guide: Configure the filtration condition through this command. When ldap client sends inquiry requisition to ldap server, it will carry the filtration condition. If the range of server-index is not in 1 to 64 and the server instance has not been created or the length of

search-filter has exceeded the maximum length of 64, this configuration fails.

Example: Configure user filtration condition for LDAP server 1: inetUserStatus=Active) and (qq=123456).

ac(config)# ldap server 1 &(inetUserStatus=Active)(qq=123456)

5.9 ldap server timeout <1~1000>

Command: ldap server timeout *<1~1000>*

no ldap server timeout

Function: Configure the timeout of LDAP server response.

Parameters: *<1-1000>* (unit: s), timeout of LDAP server response.

Default: 3s.

Command Mode: Global Mode.

Usage Guide: This command is used to configure the timeout of LDAP server response. When AC sends message requisition to LDAP server, if the response is not received in this time, consider user authentication fails.

Example: Configure the timeout of LDAP server response as 10s.

ac(config)# ldap server timeout 10

5.10 no debug ldap all

Command: no debug ldap all

Function: Disable all debug of ldap module.

Parameters: None.

Default: None.

Command Mode: Admin Mode.

Usage Guide: None.

Example:

ac# no debug ldap all

5.11 show ldap server status

Command: show ldap server status

Function: Show the relevant overview information of current configured LDAP server.

Parameters: None.

Default: None.

Command Mode: Admin Mode.

Usage Guide: Show the items as below:

Items	Explanation
index	LDAP server instance index (1~64)
ipv4-address	LDAP server IP address
Port	LDAP server port
authentication-method	Authentication method of LDAP server

It will show the total number of configured servers and the timeout except the above information.

Example: Show the relevant overview information of current configured LDAP server.

ac# show ldap server status

index	ipv4-address	port	authentication-method
1	192.168.1.20	389	anonymous
2	200.1.1.20	389	authenticated
3	192.168.1.40	389	anonymous
4	200.1.1.40	389	authenticated

config *n* ldap server

server timeout is *m* second

5.12 show ldap server <server-index> status

Command: show ldap server <*server-index*> status

Function: Output the relevant detailed information of current configured LDAP server.

Parameters: None.

Default: None.

Command Mode: Admin Mode.

Usage Guide: Show the items as below:

Items	Explanation
index	LDAP server instance index (1~64)
ipv4-address	LDAP server IP address
port	LDAP server port
user-base-dn	Users' base DN fond by LDAP server
user-attr	The property that users on LDAP server belong to
user-type	The type that users on LDAP server belong to (objectclass)
authentication-method	Binding method of LDAP server
username	Show administrator DN of simple binding. Do not show this field for the anonymous binding.
password	Show administrator password of simple binding. Do not

	show this field for the anonymous binding.
search-filter	Show the additional filtration condition of configured user inquiry.

Example:

The showing format of ldap server instance of simple binding:

ac# show ldap server 1 status

index ---------- 1

ipv4-address ---------- 192.168.1.10

port ---------- 389

user-base-dn ---------- dc=dcn;dc=com

user-attr ---------- cn

user-type ---------- organizationalPerson

authentication-method ---------- authenticated

username ---------- ricky

password ---------- 123456

search-fileter ---------- inetUserStatus=Active

The showing format of ldap server instance of anonymous binding:

ac# show ldap server 2 status

index ---------- 2

ipv4-address ---------- 192.168.1.20

port ---------- 389

user-base-dn ---------- dc=dcn;dc=com

user-attr ---------- cn

user-type ---------- organizationalPerson

authentication-method ---------- anonymous

search-fileter ---------- inetUserStatus=Active

5.13 verification {ldap|none|radius}

Command: verification {*ldap*|*none*|*radius*}

Function: Configure the user authentication method of portal user appointing to adopt, it can be LDAP or RADIUS, it also can be the free authentication method.

Parameters: *ldap*: the user verification method of portal user is ldap; *none*: the user verification method of portal user is free authentication; *radius*: the user verification method of portal user is radius.

Default: radius.

Command Mode: Captive Portal Instance Mode.

Usage Guide: Appoint user verification method for portal user. If it is radius, the user name and password will be authenticated on radius server; if it is LDAP, the user password will be authenticated on LDAP server; if it is none, the user do not authenticate.

Example: Configure captive portal instance 1 to user ldap authentication.

ac (config)#captive-portal

ac (config-cp)#configuration 1

ac(config-)# verification ldap

Chapter 6 Commands for PPPoE Server

6.1 debug pppoe-server (discovery |lcp |auth| ipcp |receive |send | error)

Command: debug pppoe-server (discovery|lcp|auth|ipcp|receive|send| error)
no debug pppoe-server (discovery|lcp|auth|ipcp|receive|send| error)

Function: Enable pppoe-server debug information on-off.

Parameters: discovery: DISCOVERY stage debug; lcp: LCP consulting stage debug; auth: authentication stage debug; ipcp: IPCP consulting stage debug; receive: receiving packet information debug; error: error information debug.

Command Mode: Admin Mode.

Default: Disable.

Usage Guide: Enable the debug information on-off of the appointed stage. This command fits the persons who known the PPPoE function well. The key of Crtl+O can disable this debug.

Example: Enable the error debug information of PPPoE server.

AC#debug pppoe-server error

6.2 interface virtual-template

Command: interface virtual-template <1-255>
no pppoe-server enable <1-255>

Function: Create/cancel a virtual template.

Parameters: Template ID, range is 1 to 255.

Command Mode: Global Mode.

Default: No templates.

Usage Guide: Each virtual template can be applied on a specific VLAN. Through enabling PPPOE server on VLAN to bind the virtual template to provide PPPOE access service for client.

Example: Create a virtual template 1 on AC.

AC(config)# interface virtual-template 1

6.3 ip address

Command: ip address <A.B.C.D> <A.B.C.D>

no ip address <A.B.C.D> <A.B.C.D>

Function: Configure/cancel the virtual template IP address as PPPOE server address.

Parameters: <A.B.C.D>: IP address; **<A.B.C.D>**: address mask.

Command Mode: Virtual Template Configuration Mode.

Default: No IP address configuration as default.

Usage Guide: Configure/cancel the virtual template IP address and write in the IPCP configuration requisition packets.

Example: Configure PPPOE server address as 1.1.1.2 and the mask is 255.255.255.0.

AC(config-if-VT1)# ip address 1.1.1.2 255.255.255.0

6.4 ip pppoe pool pool-name

Command: ip pppoe pool <WORD> <A.B.C.D> <A.B.C.D>

no ip pppoe pool <WORD>

Function: Create/cancel IP address pool function. It is used to distribute IP address for client.

Parameters: <WORD> is the appointed name of this address pool; **<A.B.C.D>** is the prefix of the address; **<A.B.C.D>** is the mask of the address.

Command Mode: Global Mode.

Default: No address pools.

Usage Guide: Only the configured address pool can be applied to the virtual template to distribute address for PPPoE client of a VLAN.

Example: Create pppoe address pool A on AC, the address prefix is 192.168.1.0 and the mask is 255.255.255.0.

AC(config)# ip pppoe pool A 192.168.1.0 255.255.255.0

6.5 max-terminate-request

Command: max-terminate-request <mtr-limit>

no max-terminate-request

Function: Configure/recover the times of sending the termination requisition packets.

Parameters: <mtr-limit>: maximum times of sending the termination requisition, range is 1 to 3.

Command Mode: Virtual Template Configuration Mode.

Default: 2 times.

Usage Guide: Configure/recover the times of sending the termination requisition packets. Before disconnecting a session, if received client affirmance, disconnect the session; if the response of client is not received, send mtr-limit times PPPOE termination requisition

packet at most and then disconnect the session.

Example: Configure max-terminate-request as 3 times.

AC(config-if-VT1)# max-terminate-request 3

6.6 no pppoe-session

Command: no pppoe-session (peer-ip|session-id)

Function: Disconnect the session connection.

Parameters: peer-ip: IP address of session client; session-id: session ID.

Command Mode: Global Mode/Virtual Template Configuration Mode.

Default: None.

Usage Guide: Disconnect the session connection and release the resource that the session occupied.

Example: Release the session connection with client 1.1.1.1.

AC(config)# no pppoe-session 1.1.1.1

6.7 ppp account-statistics enable

Command: ppp account-statistics enable

no ppp account-statistics enable

Function: Enable/disable PPP accounting statistic function. The statistic contents include the number of packets and bytes which flow through this link on two directions of ingress and egress. AAA application module can get the flow statistic information to use it for accounting.

Parameters: None.

Command Mode: Virtual Template Configuration Mode.

Default: Do not count.

Usage Guide: When enabled, all sessions send accounting starting packets to accounting server and send the updating packets regularly. When disabled, all sessions send accounting ending packets to accounting server.

Example: Enable PPP accounting statistic function.

AC(config-if-VT1)# ppp account-statistics enable

6.8 ppp authentication-mode

Command: ppp authentication-mode (pap| chap)

Function: Configure the default authentication mode of PPP protocol, including PAP and CHAP authentication. Use CHAP authentication as default.

Parameters: pap: PAP authentication; chap: CHAP authentication.

Command Mode: Virtual Template Configuration Mode.

Default: CHAP authentication.

Usage Guide: PAP (Password Authentication Protocol) is the twice handshake verification, the password is lawful. CHAP (Challenge-Handshake Authentication Protocol) is three-way handshake verification, the password is ciphertext (key).

Example: Configure the authentication mode of PPP protocol as CHAP.

AC(config-if-VT1)# ppp authentication-mode chap

6.9 ppp ipcp dns

Command: ppp ipcp dns <A.B.C.D> <A.B.C.D>

no ppp ipcp dns

Function: Configure DNS host server and aide server for the virtual template and issue it to client.

Parameters: <A.B.C.D>: the host server; **<A.B.C.D>**: the aide server.

Command Mode: Virtual Template Configuration Mode.

Default: There is no DNS server configuration.

Usage Guide: Configure to save in the virtual template configuration and issue to client in IPCP consulting.

Example: Configure the host dns of ppp ipcp as 2.2.2.2 and the aide dns is 3.3.3.3.

AC(config-if-VT1)# ppp ipcp dns 2.2.2.2 3.3.3.3

6.10 ppp lcp max-echo-interval

Command: ppp lcp max-echo-interval <interval>

no ppp lcp max-echo-interval

Function: Configure/recover the waiting time of client response after sending the LCP keep-alive requisition packet.

Parameters: <interval>: response interval, range is 1 to 10s.

Command Mode: Virtual Template Configuration Mode.

Default: 3s.

Usage Guide: Configure/recover the waiting time of client response after sending the LCP keep-alive requisition packet. If client does not give the response in this time, trigger the next requisition; after the set requisition times, disconnect this session if there is still not the response.

Example: Configure max-echo-interval as 5s.

AC (config-if-VT1)# ppp lcp max-echo-interval 5

6.11 ppp lcp max-echo-request

Command: ppp lcp max-echo-request < reqnum >

no ppp lcp max-echo-request

Function: Configure/recover the times of sending the LCP keep-alive requisition packets.

Parameters: < reqnum >: sending times, range is 1 to 10.

Command Mode: Virtual Template Configuration Mode.

Default: 5.

Usage Guide: Configure/recover the times of sending the keep-alive requisition packets. Every a certain time interval, send the requisition once to wait the client response. After the set requisition times, if there is still not response, disconnect this session.

Example: Configure max-echo-request as 10 times.

AC (config-if-VT1)# ppp lcp max-echo-request 10

6.12 ppp lcp mru

Command: ppp lcp mru <mru>

no ppp lcp mru

Function: Configure/recover the maximum receiving unit of lcp consulting to notice the client server how many data bytes of packet it can receive.

Parameters: <mru>: maximum received unit, range is 1 to 1-1492 bytes.

Command Mode: Virtual Template Configuration Mode.

Default: 1492.

Usage Guide: Configure/recover the maximum receiving unit of lcp consulting to notice the client server how many data bytes of packet it can receive.

Example: Configure mru as 1000.

AC(config-if-VT1)# ppp lcp mru 1000

6.13 ppp negotiate-timeout

Command: ppp negotiate-timeout <time-out>

no ppp negotiate-timeout

Function: Configure/recover the consulting timeout of PPP.

Parameters: <time-out>: timeout, range is 1 to 10s.

Command Mode: Virtual Template Configuration Mode.

Default: 3s.

Usage Guide: In this time, if the response of client cannot be received, re-issue the

consulting configuration requisition; if the response is still not received in the set number of requisition, disconnect this connection.

Example: Configure the consulting timeout of PPP as 10s.

AC (config-if-VT1)# ppp negotiate-timeout 10

6.14 pppoe-server bind radius-group

Command: pppoe-server bind radius-group WORD

no pppoe-server bind radius-group WORD

Function: Configure the associated RADIUS server groups.

Parameters: WORD: radius server name.

Command Mode: Global Mode.

Default: No configuration.

Usage Guide: Save the configured server group name globally. It is used to fill in when AAA requests.

Example: Configure the associated RADIUS server group as aaa1.

AC (config)# pppoe-server bind radius-group aaa1

6.15 pppoe-server bind virtual-template

Command: pppoe-server bind virtual-template <vtid>

no pppoe-server bind virtual-template <vtid>

Function: Enable/disable server binding the virtual template.

Parameters: <vtid>: virtual template ID, range is 1 to 255.

Command Mode: Virtual Template Configuration Mode.

Default: Server does not bind the virtual template.

Usage Guide: When enabled, PPPOE server is bond to this VLAN and uses this virtual template configuration to deal with the requisition that VLAN received. When disabled, this VLAN does not provide PPPOE service any more and releases all sessions.

Example: Bind the virtual template 1 to vlan 1.

AC(config-if-vlan1)# pppoe-server bind virtual-template 1

6.16 pppoe-server enable

Command: pppoe-server enable

no pppoe-server enable

Function: Enable/disable pppoe server function globally.

Parameters: None.

Command Mode: Global Mode.

Default: Disable.

Usage Guide: Only after enabled pppoe server function, PPPOE packets can be intercepted. After disabled this function, other configurations will not be deleted, but the port cannot receive PPPOE packets any more.

Example: Enable pppoe server function on AC.

AC(config)#pppoe-server enable

6.17 pppoe-server max-sessions

Command: pppoe-server max-sessions <limit>

no pppoe-server max-sessions

Function: Configure/recover the maximum number of sessions. If the number exceeded this restriction, the session connection will not be created any more.

Parameters: <limit>: maximum number restriction of sessions, range is 1 to 2048.

Command Mode: Global Mode.

Default: 2048 sessions can be created as default.

Usage Guide: Only this command is used to limit the number of sessions. If the number exceeded this restriction, the session connection will not be created any more. The no command recovers to be default.

Example: Limit the number of pppoe sessions as 100.

AC(config)# pppoe-server max-sessions 100

6.18 remote address pppoe-pool WORD

Command: remote address pppoe-pool WORD

no remote address pppoe-pool WORD

Function: The virtual template enables/abandons the IP address pool.

Parameters: WORD: address pool name.

Command Mode: Virtual Template Configuration Mode.

Default: Do not enable address pool as default.

Usage Guide: The virtual template enables the IP address pool and distributes address for client from this pool; when it abandoned the pool, delete all sessions under the virtual template and withdraw the address.

Example: Enable pppoe address pool A on virtual template 1.

AC(config-if-VT1)# remote address pppoe-pool A

6.19 show interface virtual-template

Command: show interface virtual-template vtid

Function: Show the appointed virtual template information.

Parameters: vtid: number of virtual template.

Command Mode: Any Mode.

Default: None.

Usage Guide: When the configurations shown in **show run** are too much, use this command to view the configuration information of virtual-template quickly.

Example: View the configuration information of virtual-template 1.

AC (config)# show interface virtual-template 1

6.20 show pppoe-server session

Command: show pppoe-server session ((interface virtual-template WORD)|all)

Function: Show the session information of the appointed template or all sessions' information.

Parameters: interface virtual-template: the virtual template; WORD: the virtual template number; All: all sessions.

Command Mode: Any Mode.

Default: None.

Usage Guide: Print session information of the appointed template or all sessions' information.

Example: View the session information of virtual-template 1.

AC (config)# show pppoe-server session interface virtual-template 1