Content

Chapter 1 Wireless Client Access and Authentication

1.1 Introduction to Wireless Client Access and Authentication

Wireless local area network (WLAN) has the advantages that wired network cannot be compared of convenient installing, flexible using, thrift, easing to expand etc. So WLAN is usd more and more widely. But the attackers are easy to tap, modify and transmit maliciously because of the feature of opened channel. Security becomes the most important factor of obstructing WLAN to develop. For solving this problem, there is need to add some items as below:

1. User identity authentication, it can prevent someone to access network resource without authentication.

2. Data privating, it can protect data to keep integrity and transmission privacy.

1.1.1 Link Authentication

Link authentication is the necessary step of all access service. It supports two kinds of authentication ways: OSA authentication (Open System Authentication) and Shared-key authentication (Shared Key Authentication). 802.11 link authentication is achieved through authentication packets. Open system authentication or share key authentication can be selected in static WEP service; only open system authentication can be used in other types of service.

1. OSA authentication

OSA authentication conducts no configuration to user. It just makes sure if the client authentication successes according to if WLAN supports OSA authentication. When WLAN provides static WEP security service, OSA and share key can be selected for link authentication; when it is other security service, user must use OSA authentication and shared key authentication cannot be used.

2. Shared Key authentication

Shared key authentication needs client and AP configuration share the key; AP will produce a random string to send to client in link authentication; the client will copy the received string to the new message and encrypt it to send to AP; after AP received this message, it will compare the decrypted string and the original string of client and make sure if client passed the authentication. If the strings are matching, it means client has the

same shared key with device, it passed the shared key authentication; otherwise, shared key authentication fails.

As shown in the picture below, it is the OSA and shared key authentication process.

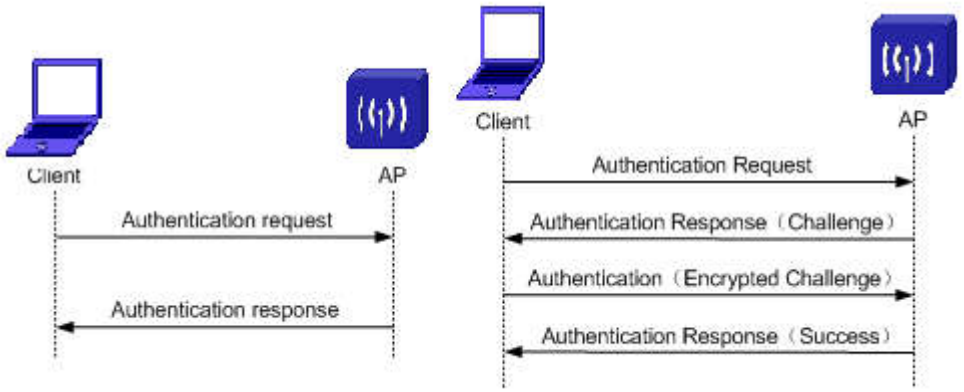


Fig 1-1 client link authentication process

1.1.2 Secure Access Authentication

The ways of achieving client security authentication in system include: static WEP, WEP 802.1x, WPA/WPA2 personal and WPA/WPA2 Enterprise. Static WEP only needs the client link authentication mentioned above and it does not need the secure access authentication in this section. Secure access authentication can be divided to some kinds as below according to the implementation mechanism:

1. 802.1x authentication

WEP 802.1x and WPA/WPA2 Enterprise use 802.1x authentication. 802.1x authentication is the port based network access control protocol. “port based network access control protocol” means in the level of WLAN access port, authenticate and control the user device accessed. If the user device connected to port can pass authentication, the resource in WLAN can be interviewed; if it does not pass the authentication, the resource cannot be interviewed.

For improving data security of WLAN service, 802.1x uses EAPOL-Key agreement, AP and client achieves automatic key agreement and management; at the same time, through 802.1x agreement, AP and client consult the same seed key of PMK and improve the security of key agreement.

2. PSK

PSK is the authentication method used by WPA/WPA2 personal, the same pre-shared key is needed to configure on client and AP in PSK authentication. If the keys are the same, PSK accesse authentication successes; if they are different, PSK accesse authentication fails. PSK authentication is completed in the process of EAPOL-Key agreement. Make sure if this side and the other side of configurations pre-share the same key and complete the authentication between device and client through if decrypting

message of agreement successfully.

3. MAC access authentication

In our system, AC configuration decides if conducting MAC access authentication and AC conducts MAC authentication for client in the process of client association, MAC address authentication will not be conducted anymore in other processes. WLAN does not adopt MAC authentication clearly. In WLAN application, MAC authentication and other authentication ways (802.1x, PSK etc) will be used together. For example, for the WLAN of WPA and WPA2, MAC access authentication can be used at the same time.

1.1.3 Key Agreement

For achieving security of WLAN data, IEEE802.11i defined EAPOL-Key agreement mechanism (4-Way Handshake); WLAN uses this mechanism to achieve the key agreement of WLAN device and WLAN client. The key of agreement will be as the encryption/decryption key in the process of 802.11 data transmission.

For WLAN which supports WPA service, EAPOL-Key agreement should be conducted. Key agreement can be regarded as a part of access authentication on logic. Only after EAPOL-Key agreement was successful, access authentication will enable the port to allow the packets of user passing by.

WLAN key agreement includes 4-way handshake and group key agreement. These two kinds of ways are both achieved through EAPOL-Key agreement. WLAN client and device use 4-way handshake to consult the key usd by unicast packets of this client, WLAN device can message the key used bybroadcast and multicast to all WLAN clients through group key agreement.

1.1.4 Data Encryption

After link authentication, access authentication and key agreement of client, it will enter network communication stage. In communication, the data should be encrypted. The main encryption ways are as below:

1. WEP encryption

WEP (Wired Equivalent Privacy) uses RC4 algorithm to achieve packets encryption and encrypts the key management through shared key.

2. TKIP encryption

TKIP and WEP both use RC4 algorithm, but TKIP improves the security of WEP encryption through increasing IV length of algorithm; second, TKIP supports automatic agreement of key and solves the limit that WEP encryption needs to configure key statically; last, TKIP also supports MIC authentication (Message Integrity Check) and Countermeasure function.

3. CCMP encryption

CCMP (Counter mode with CBC-MAC Protocol) is based on CCM (Counter-Mode/CBC-MAC) method of AES (Advanced Encryption Standard). It is used on RSNA client only. CCM combines with CTR (Counter mode) to conduct confidentiality check. At the same time, it combines with CBC-MAC to check the authentication and integrity.

1.1.5 Client Disassociation

Client disassociation is divided into several situations:

1. Automatic logoff of Client

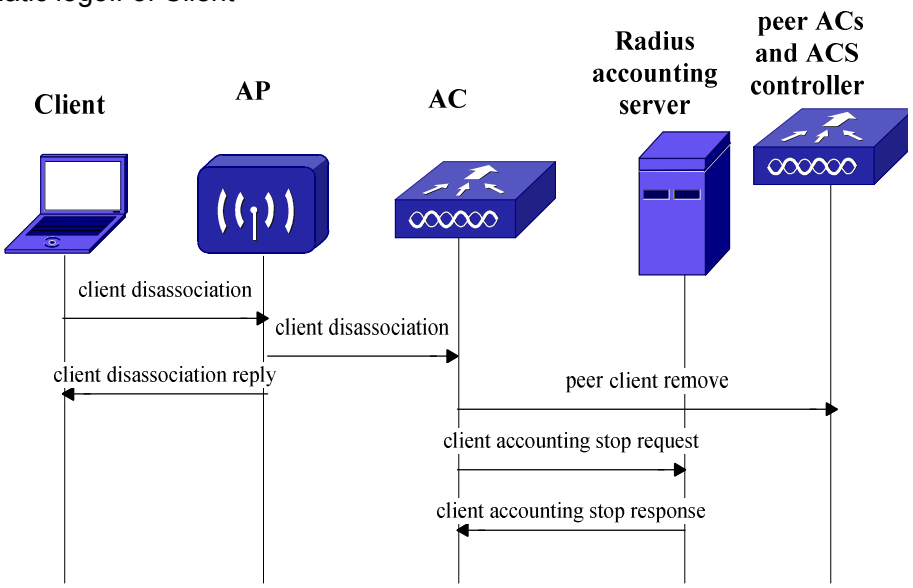


Fig 1-2 timing diagram of client disassociation

The picture above is the timing diagram of client disassociation, the whole process includes:

- ✧ Client send the disassociation frame to AP;
- ✧ AP disassociates client and send client disassociation message to AC;
- ✧ Within a certain time of 30s(it can be configured), AC discovers that client does not associate and authenticate other AP, it wll notice peer ACs (including AC controller) that there is client disassociation and synchronize client information to notice radius accounting server to stop accounting to client;
- ✧ Radius accounting server deals with accounting stop requisition;
- ✧ After those notification events above are completed, all ACs delete all relevant information of local client.

2. Administrator disassociates client forcibly

Administrator send client disassociation command to AC, AC send **Disassociate Client Command Message** to AP associated with client and request AP to disassociate client. Other process is the same as “1”.

3. Client has no reaction for a long time, AP disassociates client

After client authentication was successful, the network can be interviewed. When client does not communicate to AP for a long time, AP will disassociate client forcibly.

4. Forced disassociation when clients are excessive

Because system deals with client association requisition asynchronously, in local saving client information, it will appears the case of that associated client list is full although judging client number in client association. Then, the program will request to disassociate the excess client automatically.

5. Disassociate roaming client and the old AP forcibly

In the process of client roaming, when AC deals with peer-client-discover notification from other AC, if it discovers this client was associated with the AP managed by itself before, this AC will request the AP to disassociate this client.

1.1.6 Load-balance

AP and AC are responsible for radio load-balance of client connection and disconnection. AP supports two modes: conversation and flow. Conversation mode decides if allowing client association according to users' number of current association of radio interface. Flow mode decides if allowing client association according to maximum broadband utilization of radio interface.

AC decides if allowing client association according to the total number of clients in current system. At the same time, it monitors radio interface load of local AP. When exceeding the maximum load, send trap to network management. Except that AC can control client number according to the total number of current client of client association, AC can also disassociate the exceeded part of clients when it discovers clients' number exceeds the maximum which system can bear.

1.1.7 WLAN Access Service

1. Laws WLAN service

Laws WALN service is a kind of WLAN service without data security protection. The access authentication policy of wired user can be used, but the security policy of WLAN cannot be used.

2. Static WEP encryption WLAN service

WEP encryption WLAN service provides the security protection for packets. Use WEP encryption to protect the data of WLAN client and device. There are two link authentication ways of open system and share key protecting 802.11 link security.

3. WEP 802.1x encryption WLAN service

WEP 802.1x=WEP+802.1x/EAP. Radius server provides a wep key through 802.1x authentication, there is not the key agreement process.

4. WPA/WPA2 personal WLAN service

WPA personal = PSK + TKIP/CCMP

WPA2 personal = PSK + TKIP/CCMP+identity pre-authentication

WPA WLAN can support TKIP encryption and it is compatible with WEP encryption (multicast and broadcast can use WEP encryption for protection). Currently, WPA also supports CCMP encryption. WPA2 WALN supports CCMP encryption, but the TKIP or CCMP encryption must be appointed. This authentication way uses PSK to produce PTK through key agreement. PTK will be used for the encryption and decryption of network communication data.

5. WPA/WPA2 Enterprise WLAN service

WPA Enterprise = IEEE 802.1x/EAP + TKIP/CCMP

WPA2 Enterprise= IEEE 802.1x/EAP + TKIP/CCMP+ identity pre-authentication

WPA/WPA2 Enterprise authentication service produces PMK through 802.1x authentication. At last, it used PMK to produce PTK through key agreement.

6. Comparison among the access services

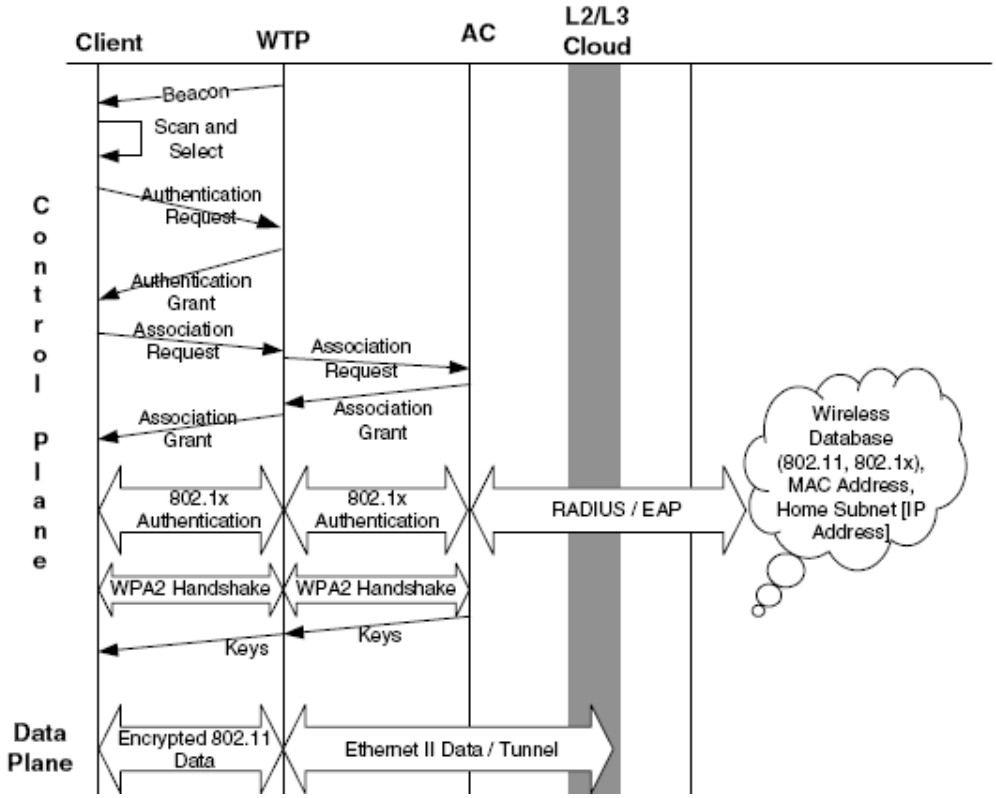


Fig 1-3 flow diagram of client association authentication

As shown in the picture above, it is the client association authentication process before network communication. It is divided into link authentication, association requisition, 802.1x authentication, key agreement etc. Compare the WLAN access services according to the diagram. Because laws service does not have relevant wireless security configuration, it does not include laws service.

1) Link authentication is the necessary step of all access services. The differences are that static WEP service can select open system authentication or share key authentication or both of them, other services just can use open system authentication.

2) Association requisition is the necessary step of all access services. And the action of AP and AC are the same. The difference is if system uses radius server to authenticate for MAC address of client. This is determined by mac authentication mode configuration of system and it is unrelated with access service selected.

3) 802.1x authentication is needed only when user chooses WEP 802.1x authentication or WPA/WPA2 enterprise access service.

4) The key agreement is needed when choosing WPA/WPA2 personal or WPA/WPA2 Enterprise service. Use PSK or PMK produced by 802.1x authentication to produce PTK. The key agreement is not needed in static wep and wep 802.1x authentication.

1.1.8 Conforming Operators Radius Interface Standard

Conforming operators Radius interface standard is in order to satisfy the requirement of different operators for the property fields which are used for marking different types of clients or switches in packets interaction between switch and radius. Because of client roaming, this function is produced. It is convenient for operators to identify the records of client positions and types and authentication property.

1.1.9 User Offline Based on Flow

The user offline function based on flow is usually used in the wireless environment of enabling accounting function. When the online user does not use the wireless network and the data flow is less, this function can force user offline for reducing the loss of flow and cost.

1.1.10 Reject the Client with Weak Signal Accessing

The client with weak signal is rejected accessing for ensuring the effectiveness of the network.

1.2 Wireless Client Access and Authentication Configuration

1.2.1 AC Configuration

1. Configure the keeping time of data in AC database/recover to be default.

Command	Explanation
Wireless Global Mode	
agetime {ad-hoc | ap-failure | rf-scan | detected-client} <0-168> **no agetime {ad-hoc | ap-failure | rf-scan | detected-client}**	Configure the keeping time of data in AC database. The no command recovers to be default.

2. Configure the longest time that AC will keep record related to client in associated client list after client disassociated/recover to be default.

Command	Explanation
Wireless Global Mode	
client roam-time <1-65535> **no client roam-time**	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.

3. Configure Radius server name used for client authentication or billing/recover to be default group.

Command	Explanation
Wireless Global Mode	
radius server-name {auth | acct} <*name*> **no radius server-name {auth | acct}**	Configure radius groups used for client authentication or billing. The no command recovers to be default group.

Notice: Please configure and use wireless global radius server under network.

4. Configure MAC authentication mode of AC. Use white-list or black-list when it is global/recover to be default of white-list.

Command	Explanation
Wireless Global Mode	
mac-authentication-mode {white-list | black-list} **no mac-authentication-mode**	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.

5. Add/delete the appointed client in Known client database.

Command	Explanation
Wireless Global Mode	
know-client <*macaddr*> [action {global-action | grant | deny}] [name <*name*>] **no know-client <*macaddr*>**	Configure client in Known client database. The no command deletes the appointed client.

Notice: action field appoints default to allow, refuse or use the global MAC authentication to judge if the client association is allowed. When MAC-Authentication-Action of client is configured as deny or grant, client will be refused or accepted accordingly wether the MAC-Authentication-Action is configured as white-list or black-list. Only when MAC-Authentication-Action is configured as global, MAC-Authentication-Action configuration is effective, it is refused in black-list and accepted in white-list.

1.2.2 Wireless Network Configuration

1. Add/delete a network configuration

Command	Explanation
Wireless Global Mode	
network <*1-64*> **no network <*1-64*>**	Add/delete a network configuration

Notice: If this network is used by VAP, it cannot be deleted; the first 16 network cannot be deleted forever as default.

2. Configure SSID of wireless network

Command	Explanation
Network Configuration Mode	

ssid <*name*>	Configure SSID of wireless network

3. Hide/do not hide SSID of network

Command	Explanation
Network Configuration Mode	
hide-ssid **no hide-ssid**	Hide/do not hide SSID of network

4. Configure authentication and encryption method supported by network/recover to be laws.

Command	Explanation
Network Configuration Mode	
security mode {none | static-wep | wep-dot1x | wpa-enterprise | wpa-personal} **no security mode**	Configure authentication and encryption method supported by network/recover to be laws.

Notice: The configuration is saved in AC; AC needs to send the configuration to AP to be effective.

5. Configure link authentication method/recover to be default.

Command	Explanation
Network Configuration Mode	
wep authentication {open-system | share-key} **no wep authentication**	Configure link authentication method/recover to be default.

Notice: Only when it is static wep authentication, this configuration will be effective.

6. Configure types of share keys of static wep authentication method/recover to be default.

Command	Explanation
Network Configuration Mode	
wep key type {ascii | hex} **no wep key type**	Configure the key encoding type of share key. The no command recovers to be default.

7. Configure share keys length of static wep authentication method/recover to be default.

Command	Explanation
Network Configuration Mode	
wep key length {64 | 128} **no wep key length**	Configure share keys length of data transmission encryption/recover to be default.

8. Configure/delete share keys of static wep authentication method.

Command	Explanation
Network Configuration Mode	
wep key <*1-4*> [encrypted] <*value*> **no wep key <*1-4*>**	Configure/delete share keys of static wep authentication method.

9. Configure serial number of share keys of static wep authentication method/recover to be default.

Command	Explanation
Network Configuration Mode	
wep tx-key <*1-4*> **no wep tx-key**	Configure which share-key will be used by encryption.

10. Enable/disable MAC authentication and configure local authentication or radius authentication.

Command	Explanation
Network Configuration Mode	
mac authentication {local | Radius} **no mac authentication**	Enable/disable MAC authentication and configure local authentication or radius authentication.

11. Configure radius server name used for client authentication or billing in network/recover to be default.

Command	Explanation

Network Configuration Mode	
radius server-name {auth | acct} <*name*> **no radius server-name {auth | acct}**	Configure radius groups used for client authentication or billing in network. The no command recovers to default of Default-RADIUS-Server.

12. Configure if using radius server configured against network/use radius server of wireless global configuration.

Command	Explanation
Network Configuration Mode	
radius use-network-configuration **no radius use-network-configuration**	Configure if using radius server configured against network. The no command configures network to use radius server of wireless global configuration.

13. Configure WPA version supported by network/recover to be default.

Command	Explanation
Network Configuration Mode	
wpa versions {wpa [wpa2] | wpa2} **no wpa versions**	Configure WPA version supported by network/recover to be default.

Notice: It supports that wpa and wpa2 coexist, it also supports one of them.

14. Configure WPA encryption algorithm supported by network/recover to be default.

Command	Explanation
Network Configuration Mode	
wpa ciphers {ccmp [tkip] | tkip} **no wpa ciphers**	Configure WPA encryption algorithm supported by network/recover to be default.

Notice: It can be ccmp or tkip, or both of them coexist. When they coexist, users who use TKIP or AES-CCMP can all relate to AP.

15. Configure WPA share key of network

Command	Explanation
Network Configuration Mode	
wpa key <*value*>	Configure WPA share key of network.

16. Enable/disable WPA2 pre-authentication function when client is roaming.

Command	Explanation
Network Configuration Mode	
wpa2 pre-authentication **no wpa2 pre-authentication**	Enable/disable WPA2 pre-authentication function when client is roaming.

17. Configure how many client most can be checked identity in advance with an AP network allows/recover to be default.

Command	Explanation
Network Configuration Mode	
wpa2 pre-authentication limit <*0-192*> **no wpa2 pre-authentication limit**	Configure how many client most can be checked identity in advance with an AP network allows.

Notice: 0 means do not limit the number.

18. Configure the re-authentication holdtime of AP to relevant client/recover to be default.

Command	Explanation
Network Configuration Mode	
wpa2 key-caching holdtime <*1-1440*> **no wpa2 key-caching holdtime**	Configure the maximum time of PMK that AP caches the client under WPA2/recover to be default.

19. Configure the update rate of broadcast key/recover to be default.

Command	Explanation
Network Configuration Mode	

dot1x bcast-key-refresh-rate <*0-86400*> **no dot1x bcast-key-refresh-rate**	Configure the update rate of broadcast key; the no command recovers to be default.

20. Configurethe interval of the re-authentication for client.

Command	Explanation
Network Configuration Mode	
dot1x session-key-refresh-rate <*0，30-86400*> **no dot1x session-key-refresh-rate**	Configurethe interval of the re-authentication for client; the no command recovers to be default.

21. Recover the network configuration to default.

Command	Explanation
Network Configuration Mode	
clear	Recover the network configuration to default.

1.2.3 VAP Configuration

1. Entering VAP configuration mode

Command	Explanation
Radio Configuration Mode	
vap <*0-15*>	Entering VAP configuration mode.

2. Enable VAP of radio.

Command	Explanation
VAP Configuration Mode	
enable **no enable**	Enable/disable VAP of radio.

Notice: The default is enabling of VAP0, and it is disabling for VAP 1-15. VAP0 cannot be disabled as default.

3. Configure network configuration applied to VAP.

Command	Explanation
VAP Configuration Mode	

network <*1-1024*>	Configure network configuration applied to VAP.

Notice: One VAP must be appointed which network it belongs. If VAP is applies to this network, this network cannot be deleted.

1.2.4 Load-balance Configuration

1. Enable/disable load-balance function of system

Command	Explanation
Radio Configuration Mode	
load-balance [utilization <*1-100*>] **no load-balance [utilization]**	Utilization is the optional parameter, if there is not utilization, it means enabling/disabling load-balance function of system; if there is utilization, it means radio load configuration can achieve the percentage of total radio load/recover to be default.

2. Configure the most number of clients which is allowed to associate with every radio interface at same time/recover to be default.

Command	Explanation
Radio Configuration Mode	
max-client <*0-200*> **no max-client**	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.

1.2.5 Client Disassociation Configuration

1. Disassociate client with appointed MAC address forcibly

Command	Explanation
Admin Mode	
wireless client disassociate [macaddr]	Disassociate client with appointed MAC address forcibly.

Notice: When MAC address is not appointed, disassociate all client managed in local. If local AC is controller, disassociate all clients in system.

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

Command	Explanation
Admin Mode	
wireless client disassociate ap <*macaddr*>	Disassociate all clien of managed AP which is appointed MAC address forcibly.

3. Disassociate all clien of network which is appointed ssid forcibly.

Command	Explanation
Admin Mode	
wireless client disassociate ssid <*name*>	Disassociate all clien of network which is appointed ssid forcibly.

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

Command	Explanation
Admin Mode	
wireless client disassociate vap <*macaddr*>	Disassociate all clien of VAP which is appointed MAC address forcibly.

1.2.6 Ad Hoc Client List Configuration

1. Delete all records in Ad Hoc client list

Command	Explanation
Admin Mode	

clear wireless client adhoc list	Delete all records in Ad Hoc client list.

1.2.7 Detected Client Database Configuration

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

Command	Explanation
Admin Mode	
clear wireless detected-client [<*macaddr*>] roam-history	Delete roaming history of all clients or the appointed clients from Detected Clients Roam History list.

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

Command	Explanation
Admin Mode	
clear wireless detected-client [<*macaddr*>] preauth-history	Delete the advance identity authentication history of all clients or the appointed client from Detected Clients Pre-Auth History list.

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

Command	Explanation
Admin Mode	
clear wireless detected-client [<*macaddr*>] non-auth	Delete all authentication failure records in detected client or client with appointed MAC address.

Notice； If the mac address is not appointed, delete all authentication failure records in detected client.

1.2.8 Related Configuration of Radius

1. Enable global aaa authentication function

Command	Explanation
Global Mode	
aaa enable **no aaa enable**	This command is used for configuring to enable global authentication function. The no command disables this function.

2. Enable global accounting function

Command	Explanation
Global Mode	
aaa-accounting enable **no aaa-accounting enable**	This command is used to configure to enable global accounting function; the no command disables this function.

3. Configure the vlan-id type issued by radius on AC

Command	Explanation
aaa radius server group configuration mode	
radius-attribute vlan-id format {integer|string}	Use this command to configure the vlan-id type issued by radius on AC.

4. Configure the global shared password of AC and RADIUS server communication

Command	Explanation
Global Mode	
radius-server key WORD **no radius-server key**	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.

5. Configure the appointed radius authentication server host

Command	Explanation
Global Mode	
radius-server authentication host <*A.B.C.D*> [port <*0-65535*>] [key WORD] [primary] **no radius-server authentication host <*A.B.C.D*>**	This command is used to configure the appointed radius authentication server host. The no command deletes the appointed radius authentication server host.

6. Configure the appointed radius accounting server host

Command	Explanation
Global Mode	
radius-server accounting host <*A.B.C.D*> [port <*0-65535*>] [key WORD] [primary] **no radius-server accounting host <*A.B.C.D*>**	This command is used to configure the appointed radius accounting server host. The no command deletes the appointed radius accounting server host.

7. Appoint source address of radius packets

Command	Explanation
Global Mode	
radius nas-ipv4 <*A.B.C.D*> **no radius nas-ipv4**	Appoint source address of radius packets, the no command deletes the appointed source address of radius packets.

8. Configure radius dead-time

Command	Explanation
Global Mode	

radius-server dead-time <*1-255*> **no radius-server dead-time**	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.

9. Configure the times of retransmitting packets before radius server does not have reaction

Command	Explanation
Global Mode	
radius-server retransmit <*0-100*> **no radius-server retransmit**	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.

10. Configure time of retransmission radius packets waiting for reaction of safety server

Command	Explanation
Global Mode	
radius-server timeout <*1-1000*> **no radius-server timeout**	Use this command to configure time of retransmission radius packets waiting for reaction of safety server. The no command recovers to be default.

11. Configure an aaa radius server group name

Command	Explanation
Global Mode	

aaa group server radius WORD **no aaa group server radius WORD**	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.

12. Add the server of aaa radius server group

Command	Explanation
aaa Radius Server Group Configuration Mode.	
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*>]**	Use this command to add the server of aaa radius server group. The no command deletes this server.

13. Configure deadtime of aaa radius server group

Command	Explanation
aaa Radius Server Group Configuration Mode.	
deadtime <*1-255*> **no deadtime**	Use this command to configure deadtime of aaa radius server group; the no command recovers to be default.

1.2.9 Conforming Operators Radius Interface

Standard Configuration

The task list is as below:

1. Configure authentication server group
2. Configure authentication property of authentication server

(1) Configure property of nas-identifier

(2) Configure property of nas-port-type

(3) Configure property of nas-port

1. Configure authentication server group

Command	Explanation

Global Mode	
aaa group server radius < *LINE* > **no aaa group server radius < *LINE* >**	Configure a switch as server group of authentication server. The no command deletes the server group.

2. Configure authentication property of authentication server

Command	Explanation
Radius Group Configuration Mode	
nas-identifier <*string*> **no nas-identifier**	Configure nas device to send nas-identifier property in packets to radius server. The no command recovers to be default.
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**	(4) Configure authentication type interface adopts of client. The no command recovers to be default.
nas-port <*int-value*> **no nas-port**	This command is used to mark the physical port connected between client and switch. The no command recovers to be default.

1.2.10 User Offline Based on Flow Configuration

The basic configuration of the user offline function based on flow is as below:

1. Enable/disable the user offline-detect function based on flow
2. Configure the idle-timeout and flow threshold in the user offline-detect function based on flow

1. Enable/disable the user offline-detect function based on flow

Command	Explanation
Network Config Mode	
offline-detect **no offline-detect**	Enable the offline-detect function based on flow on AC. The no command disables this function.

2. Configure the idle-timeout and flow threshold in the user offline-detect function based on flow

Command	Explanation
Network Config Mode	
offline-detect (idle-timeout [seconds]|) (threshold [bytes]|)	Configure the idle-timeout and flow threshold of the offline-detect function.

1.2.11 Debug Configuration

1. Relevant configuration of debug

Command	Explanation
Admin Mode	
debug wireless auth wdm <*macaddr*> **no debug wireless auth wdm <*macaddr*>**	Enable/disable client authentication in wireless module or the WDM debug information in AP authentication.
debug wireless client-association packet {all | send | receive | dump} <*macaddr*> **no debug wireless client-association packet {all | send | receive | dump} <*macaddr*>**	Enable/disable the receiving and sending packets debug information in all client association requesting of the appointed AP.
debug wireless client-association internal-info <*macaddr*> **no debug wireless client-association internal-info <*macaddr*>**	Enable/disable the internal debug information of all client association requesting under the appointed AP.
debug wireless client-auth error **no debug wireless client-auth error**	Enable/disable the error debug information in wireless module.
debug wireless client-auth radius-info <*macaddr*> **no debug wireless client-auth radius-info <*macaddr*>**	Enable/disable radius debug information of client authentication in wireless module.

debug wireless client-auth internal-info <*macaddr*> **no debug wireless client-auth internal-info <*macaddr*>**	Enable/disable the internal debug information of all client authentication requesting under the appointed AP.
debug wireless client-auth packet {all | receive | send | dump} <*macaddr*> **no debug wireless client-auth packet {all | receive | send | dump} <*macaddr*>**	Enable/disable the receiving and sending packets debug information of all client authentication requesting under the appointed AP.
debug wireless client-disasso packet {all | receive | send } <*macaddr*> **no debug wireless client-disasso packet {all | receive | send } <*macaddr*>**	Enable/disable the receiving and sending packets debug information of all client disassociation under the appointed AP.
debug wireless client-pmk <*macaddr*> **no debug wireless client-pmk <*macaddr*>**	Enable/disable debug information of the appointed client PMK auth.
debug wireless client-preauth <*macaddr*> **no debug wireless client-preauth <*macaddr*>**	Enable/disable debug information of advance identity authentication of the appointed client.

1.2.12 Reject the Client with Weak Signal Accessing

1. Enable/disable the function of rejecting the client with weak singal accessing

Command	Explanation
Radio Configuration Mode	
client-reject rssi-threshold <0-100> **no client-reject rssi-threshold**	Enable the function of rejecting the client with weak singal accessing. The no command disables it.

1.2.13 Universal Character Configuration

1. Enable/disable the universal character configuration function

Command	Explanation
Config Mode	
UCS enable **UCS disable**	Enable the UCS function, the no command d isables it.

1.3 Wireless Client Access and Authentication Examples

Case 1:

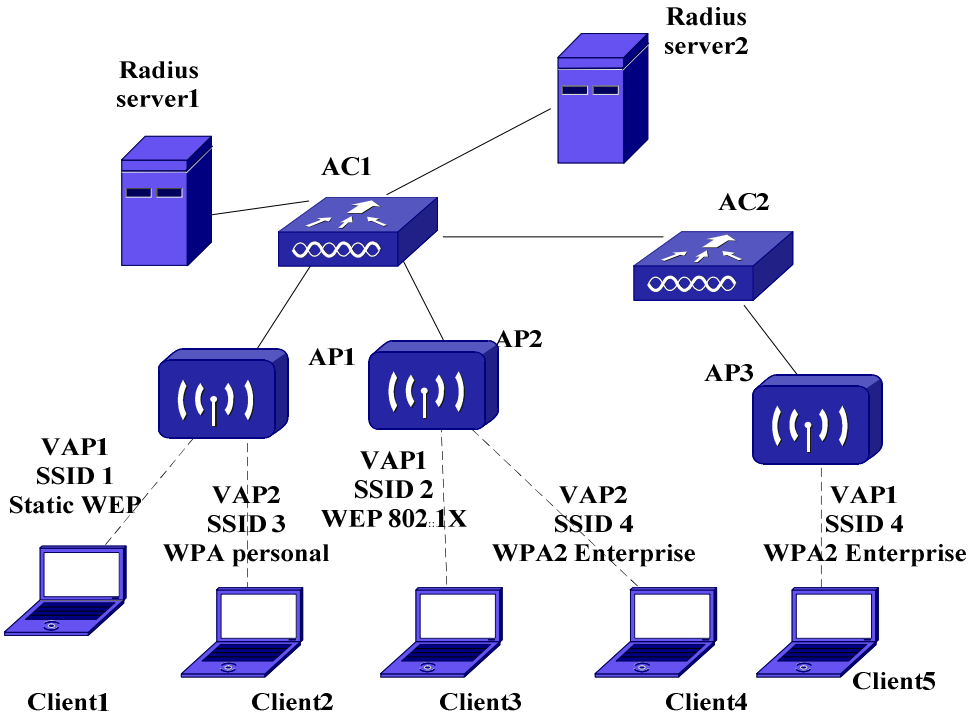


Fig 1-4 Wireless client access and authentication example

Introduction to Case:

As shown in the picture above, there are two AC make up the network system. Its feature is as below:

- Global authentication radius server is Radius server 1;
- Global accounting radius server is Radius server 2;
- Keeping time of data in AC database is 20 hours;
- After client is disassociated, the longest keeping time of AC keep client in associated client list is 120 seconds;

- MAC authentication: use local white-list authentication method;
- There are 4 network, their relevant authentication methods are: static WEP, WEP 802.1x, WPA personal and WPA2 Entrprise;
- Network 2 which adopts WEP 802.1x authentication uses MAC authentication;
- Network 3 which adopts WPA personal authentication uses radius server configured by this network to authenticate and account. And it uses radius server 1 to authenticate and account;
- Assume the relevant AP configuration files of AP1, AP2 and AP3 are AP Profile 1, AP Profile 2 and AP Profile 3;
- Network 4 uses WPA2 Enterprise authentication and keep WPA2 pre-authentication function enabling; client 4 can skip the whole 802.1x authentication when roaming to AP3 in 20 minutes.

Configuration Process:

For the network in the configuration picture, there is need to configure AC and 4 network respectively. The detailed configuration is as below:

1. Radius server configuration

AC>enable
AC#config
AC(config)#radius-server key 0 test
AC(config)#radius-server authentication host 100.1.1.100
AC(config)#radius-server authentication host 100.1.1.101
AC(config)#radius-server accounting host 100.1.1.100
AC(config)#radius-server accounting host 100.1.1.100
AC(config)#aaa group server radius radius_server_1
AC(config-sg-radius)#server 100.1.1.100
AC(config)#aaa enable
AC(config)#aaa-accounting enable
AC(config)#aaa group server radius radius_server_2
AC(config-sg-radius)#server 100.1.1.101

2. AC configuration

AC>enable
AC#config
AC(config)#wireless
AC(config-wireless)#agetime detected-clients 20
AC(config-wireless)#client roam-time 120
AC(config-wireless)#radius server-name auth radius_serve_1
AC(config-wireless)#radius server-name acct radius_serve_2

3. Configure network1: ssid 1, share-key link authentication, non-mac authentication, static WEP security authentication service, paying uses wireless global radius server. (Assume AP Profile 1 corresponds to AP1)

1) Network configuration

AC(config-wireless)#network 1
AC(config-network)#ssid ssid 1
AC(config-network)#security mode static-wep
AC(config-network)#wep authentication shared-key
AC(config-network)#wep key type ascii
AC(config-network)#wep key length 64
AC(config-network)#wep key 1 wepk1
AC(config-network)#wep key 2 wepk2
AC(config-network)#wep tx-key 1
AC(config-network)#no mac authentication
AC(config-network)#no Radius use-network-configuration
AC(config-network)#dot1x bcast-key-refresh-rate 400
AC(config-network)#dot1x session-key-refresh-rate 400

2) VAP configuration

AC(config-network)#exit
AC(config-wireless)#ap profile 1
AC(config-ap-profile)#radio 1
AC(config-ap-profile-radio)#vap 0
AC(config- ap-profile-vap)#network 1
AC(config-ap-profile-vap)#enable
AC(config- ap-profile-vap)#exit
AC(config-ap-profile-radio)#exit
AC(config-ap-profile)#exit
AC(config-wireless)#exit
AC(config)#exit
AC#wireless ap profile apply 1

4. Configure network2: ssid 2, open-system link authentication, mac authentication, WEP 802.1x security authentication service, authentication and paying use wireless global radius server. (Assume AP Profile 2 corresponds to AP2)

1) Network configuration

AC(config-wireless)#network 2
AC(config-network)#ssid ssid 2

AC(config-network)#security mode wep-dot1x
AC(config-network)#wep key type ascii
AC(config-network)#wep key length 64
AC(config-network)#wep key 1 wepk1
AC(config-network)#wep key 2 wepk2
AC(config-network)#wep tx-key 1
AC(config-network)#mac authentication radius
AC(config-network)#no Radius use-network-configuration
AC(config-network)#dot1x bcast-key-refresh-rate 400
AC(config-network)#dot1x session-key-refresh-rate 400

2) VAP configuration
AC(config-network)#exit
AC(config-wireless)#ap profile 2
AC(config-ap-profile)#radio 1
AC(config-ap-profile-radio)#vap 1
AC(config- ap-profile-vap)#network 2
AC(config-ap-profile-vap)#enable
AC(config- ap-profile-vap)#exit
AC(config-ap-profile-radio)#exit
AC(config-ap-profile)#exit
AC(config-wireless)#exit
AC(config)#exit
AC#wireless ap profile apply 2

5. Configure network3: ssid 3, open-system link authentication, non-mac authentication, wpa-personal security authentication service, paying uses radius server configured by this network. (Assume AP Profile 1 corresponds to AP1)
1) Network configuration
AC>enable
AC#config
AC(config)# wireless
AC(config-wireless)#network 3
AC(config-network)#ssid ssid 3
AC(config-network)#security mode wpa-personal
AC(config-network)#wpa version wpa.
AC(config-network)#wpa ciphers tkip
AC(config-network)#wpa key wpakey110
AC(config-network)#no mac authentication

AC(config-network)#radius accounting
AC(config-network)#radius server-name acct radius_server_2
AC(config-network)#radius use-network-configuration
AC(config-network)#dot1x bcast-key-refresh-rate 400
AC(config-network)#dot1x session-key-refresh-rate 400

2) VAP configuration
AC(config-network)#exit
AC(config-wireless)#ap profile 1
AC(config-ap-profile)#radio 1
AC(config-ap-profile-radio)#vap 2
AC(config- ap-profile-vap)#network 3
AC(config-ap-profile-vap)#enable
AC(config- ap-profile-vap)#exit
AC(config-ap-profile-radio)#exit
AC(config-ap-profile)#exit
AC(config-wireless)#exit
AC(config)#exit
AC#wireless ap profile apply 1

6. Configure network4: ssid 4, open-system link authentication, non-mac authentication, WPA2 enterprise security authentication service, paying uses wireless global radius server. (Assume AP Profile 2 corresponds to AP2 and AP Profile 3 corresponds to AP3)
1) Network configuration
AC>enable
AC#config
AC(config)# wireless
AC(config-wireless)#network 4
AC(config-network)#ssid ssid 4
AC(config-network)#security mode wpa-enterprise
AC(config-network)#wep authentication open-system
AC(config-network)#wpa version wpa2
AC(config-network)#wpa ciphers ccmp tkip
AC(config-network)#wpa2 pre-authentication
AC(config-network)#no wpa2 pre-authentication limit
AC(config-network)#no wpa2 key-caching holdtime
AC(config-network)#no mac authentication
AC(config-network)#no Radius use-network-configuration
AC(config-network)#dot1x bcast-key-refresh-rate 400

AC(config-network)#dot1x session-key-refresh-rate 400

2) VAP configuration

ap profile 2 configuration:

AC(config-wireless)#ap profile 2

AC(config-ap-profile)#radio 1

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

AC(config-ap-profile-radio)#load-balance

AC(config-ap-profile-radio)#vap 3

AC(config- ap-profile-vap)#network 4

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

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

AC(config-ap-profile-radio)#exit

AC(config-ap-profile)#exit

AC(config-wireless)#exit

AC(config)#exit

AC#wireless ap profile apply 2

ap profile 3 configuration:

AC(config-wireless)#ap profile 3

AC(config-ap-profile)#radio 1

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

AC(config-ap-profile-radio)#load-balance

AC(config-ap-profile-radio)#vap 3

AC(config- ap-profile-vap)#network 4

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

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

AC(config-ap-profile-radio)#exit

AC(config-ap-profile)#exit

AC(config-wireless)#exit

AC(config)#exit

AC#wireless ap profile apply 3

7. Configure the function of rejecting the client with weak singal accessing

AC(config-ap-profile)#radio 1

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

Case 2:

As shown in the following picture, AC1, AC2 and AC-controller make up a cluster. AC-Controller is the controller of the cluster. Configure AP1 to broadcast SSID1, client1

associates with SSID1 of AP1, client port associates with SSID1, configure this function property on AC1. When client 1 which associates with AC1 is authenticating, the authentication and accounting packets in interaction between AC1 and radius server will carry the configured property.

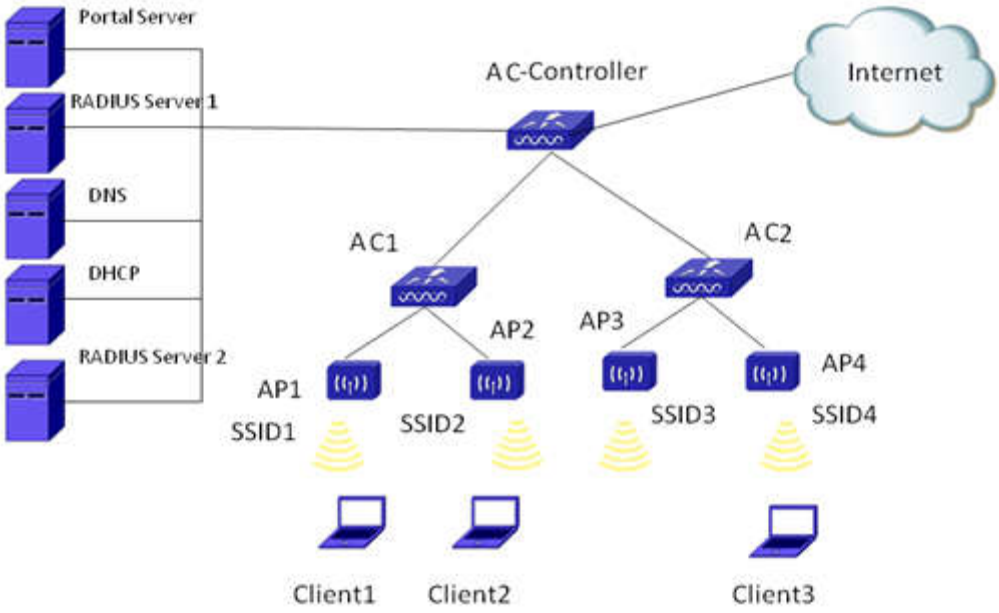


Fig 1-5 Conforming Operators Radius Interface Standard

Configuration steps:

1. Configure authentication server group

AC(config)#aaa group server radius DCSM-weiruan

AC((config-sg-radius)#

2. Configure authentication property

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

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

AC (config-sg-radius)#nas-port 17

Case 3:

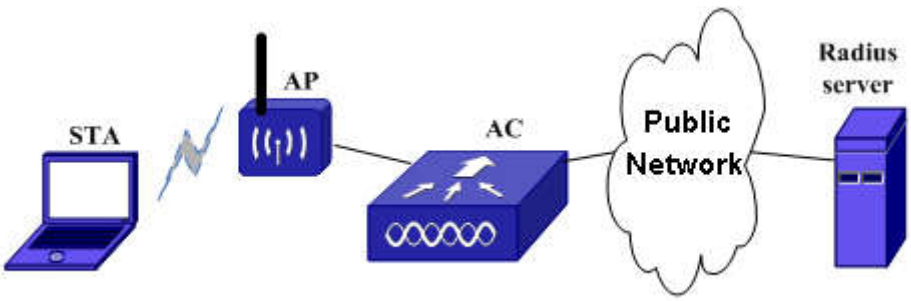


Fig 1-6 Typical Case of User Offline Function Based on Flow

The environment of user offline function based flow is as above. All the users' information is saved in the Radius server and the authentication and accounting function

are completed through the Radius server.

There are the following parts:

(1) AC, it is the access management device on the whole wireless network, it manages AP and it is the entrance that the wireless network access the wired network. Multiple ACs can be added according to the requirements in the whole topology.

(2) AP, it is the wireless access point and it is configured and managed by AC.

(3) STA, the wireless user can associate with AP and access the wireless network through the AP.

(4) Public network, this part can be empty and can also be the other switch devices.

(5) Radius Server, it is the AAA server and it completes the authentication and accounting for user.

When the wireless user STA accesses successfully and the network flow is lower then the flow threshold in a long time, AP will force this user offline and send the user offline notification to AC. AC deletes the user entry and send the accounting stopping packet to Radius Server. When the offline STA needs to access the network again, STA should request for authentication again.

Configuration:

AC#config

AC(config)#wireless

AC(config-wireless)#network 1

/* Only enable the on-off of the offline-detect function, the idle-timeout and flow threshold are both the default values. */

AC(config-network)#offline-detect

/* Enable the offline-detect function on-off and configure the idle-timeout and flow threshold. */

AC(config-network)#offline-detect idle-timeout 200 threshold 1024

/* Issue the parameters to profile 1*/

AC#wireless ap profile apply 1

/* Disable the offline-detect function on-off */

AC(config-network)#no offline-detect

1.4 Wireless Client Access and Authentication Troubleshooting

- ☞ Make sure the physical connection of network is correct.
- ☞ Use **show wireless ap profile <1-16>1 radio <1-2> vap** command to make sure the

related VAP is enabled or not.

- ☞ Use **show wireless client status** 和 **show wireless ap profile <1-16>1 radio <1-2>** command to examine the maximum client access number is achieved. **max-client <0-256>** command can be used to adjust the maximum client access number.
- ☞ Use **show wireless ap FF-FF-FF-FF-FF-FF radio 1 status** command to examine if the wlan utilization exceeds the system loading percentage. **load-balance [utilization <1-100>]** command can be used to adjust the loading percentage.
- ☞ Use **show wireless known-client** command to examine if the configuration white-list is correct.
- ☞ When there are problems of using the function of conforming operators Radius interface standard, check if configured authentication server group correctly.
- ☞ When there are problems of using the function of conforming operators Radius interface standard, check if associated authentication server group with network correctly.
- ☞ Please check the reasons if the offline-detect function is not effective in using:
  (1) Whether the user offline function based on flow is enabled.
  (2) If the on-off is enabled, please ensure whether it is issued to AP manually through the command of **wireless ap profile apply 1**.
  (3) Check if the offline-detect on-off, idle-timeout and flow threshold of the current VAP are consistent with AC through the command of **get vap vap<vap-id>**.
  (4) Check the client flow change and the idle-timeout issued by radius server through the command of **get association**.

Chapter 2 Captive Portal Authentication

2.1 Captive Portal Authentication Configuration

2.1.1 Introduction to Captive Portal Authentication

The authentication function is a way to manage and control the network resources for users. Authentication function memories the client authentication information in ~~authentication~~ the server according to a certain principles. When a user needs to use the network resources, the function of captive portal will redirect the network request of user to the authentication server, and then the user needs to provide allowed username, password and other information, the authentication server will judge the information of user and decide whether the user can be allowed to use the network resources. AC and AP in authentication function play a role of communicating the user and the authentication server. Through the AC configuration, it enables the user could connect and communicate with the authentication server, and the server will analyze the data and provide the corresponding feedback to the user. Authentication function based on the redirection function.

Redirection is a function of re-connecting the original request to a predetermined site and continous to operate. The function is when the AP receives a client request, then transfer the client request to a predetermined address, after the operation of the client and the redirected address, in order to complete certain functions and operations. This operation can achieve the aim to manage and monitor the user. Client redirected to portal authentication interface, requiring the user to fill in the username and password, only when the username and password pass the certification and they can use the network resources. Portal authentication can achieve different control strategies for different types of users.

Portal server is including external portal server and built-in portal server. The external portal server is integrated the function of the portal server in the radius server. And the built-in server is method of providing portal server service by AC’s built-in portal server. Both the built-in portal server and the external portal server, the purpose is to launch the authentication page to users who is not be authenticated yet. Different users can choose different types of portal server with respect to their needs. When configured external portal server, you should using the https protocol type, and when configured a built-in portal server using the http protocol type.

The portal server function is a way to configure different external portal server for different CP configuration. When network bind different CP configuration, has configured different portal server, it will launch the redirect page through their binding portal server. You can configure up to 10 external portal servers. Each CP configuration can bind one portal server.

Captive Portal Supporting pap&chap function is mainly used for configuring the encryption method used in authentication between client and authentication server. Use pap method or chap method.

2.1.2 Captive Portal Authentication Configuration

Authentication function task list is as below:

1. Enable/disable captive portal authentication function
2. Configure authentication types (internal portal server or external portal server)
3. Configure captive portal redirect function
   1) Configure protocol types of captive portal
   2) Configure redirect address
   3) Configure the AC to listen the portal server packet port
   4) Configure the redirect url-head
   5) Configure/delete radius server name
   6) Configure/delete portal server name
   7) Add/delete additional HTTP port
   8) Create/delete captive portal configuration
   9) Enable/disable a captive portal configuration
   10) Bind to network
   11) Configure url to carry the AP mac
   12) Configure url to carry the name of AP mac
   13) Configure url to carry the user mac
   14) Configure url to carry the name of user mac
   15) Configure url to carry the custom string
   16) Configure the url to carry the parameter of wlanacname
   17) Configure the url to carry the parameter of ssid
   18) Configure the url to carry the parameter of nas-ip
4. Configure AAA function
   1) Enable/stop AAA function
   2) Configure RADIUS authentication server group name
5. Configure RADIUS authentication server
   1) Configure RADIUS server key
   2) Configure RADIUS authentication server address

6. Configure captive portal supporting pap&chap

1. Enable/disable captive portal authentication function

Command	Explanation
Captive Portal Configuration Mode	
enable **disable**	Enable/disable captive portal function of AC globally. This function includes captive portal function on AC and AP.

2. Configure authentication types

Command	Explanation
Captive Portal Configuration Mode	
authentication-type {internal | external} **ip http server**	Configure portal server type as internal or external server. If adopt internal portal mode, enable http server function first.
authentication timeout <timeout> **no authentication timeout**	Configure timeout of portal server authentication. The no command recovers to be default.

3. Configure captive portal redirect function

Command	Explanation
Captive Portal Configuration Mode	
external portal-server server-name <*name*> {ipv4 | ipv6} <*ipaddr*> [port <*1-65535*>] **no external portal-server {ipv4 | ipv6}server-name <*name*>**	Configure/delete external portal server.
configuration <*cp-id*> **no configuration <*cp-id*>**	Configure/delete portal routine of different types of users. 10 kinds of routines can be configured.
Captive Portal Instance Configuration Mode	
protocol {http | https}	Configure a protocol mode captive portal supports. Adopt https mode when using external portal server and adopt http mode when using internal portal server.

http port <*port-num*> **no http port**	Add/delete additional http redirect port.
listen portal-server-port <1-65535> **no listen portal-server-port**	Configure the AC to listen the portal server packet port. The no command recovers it to be the default port.
redirect url-head <word> **no redirect url-head**	Configure the redirect url-head including transmission protocol, host name, port and path. The no command deletes the configuration.
radius-auth-server <*server-name*> **no radius-auth-server**	Configure/delete authentication server name.
portal-server {ipv4 | ipv6} <*name*> **no portal-server {ipv4 | ipv6}**	Bind/unbind portal server name.
enable **disable**	Enable/disable a portal routine.
interface ws-network <*1-1024*> **no interface ws-network <*1-1024*>**	Bind/delete a type of users to a type of network. User can associate with the network resource with different configuration used in different networks.
redirect attribute apmac enable **no redirect attribute apmac enable**	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.
redirect attribute apmac name<apmac-name> **no redirect attribute apmac name**	Configure the direct url address to carry the name of apmac. The no command recovers it to be the default value.
redirect attribute usermac enable **no redirect attribute usermac enable**	Enable the function that the parameter of usermac is carried in the redirect url address. The no command cancels it.

redirect attribute usermac name<usermac-name> **no redirect attribute usermac name**	Configure the direct url address to carry the name of usermac. The no command recovers it to be the default value.
redirect attribute custom-string name<custom-string> **no redirect attribute custom-string name**	Configure the direct url address to carry the custom string. The no command cancels it.
ac-name <word> **no ac-name**	Configure the url to carry the parameter of wlanacname. The no command deletes it.
redirect attribute ssid name <word> **no redirect attribute ssid name**	Configure the url to carry the parameter of ssid. The no command recovers the ssid to be the default value.
redirect attribute nas-ip enable **no redirect attribute nas-ip enable**	Configure the url to carry the parameter of nas-ip. The no command disables this function.
redirect attribute nas-ip name <word> **no redirect attribute nas-ip name**	Configure the name of the parameter of nas-ip carried in url. The no command recovers the name to be the default value.
Network Configuration Mode	
network <*1-1024*>	Create a network.
ssid <*name*>	Configure SSID for the configured network.

4. Configure AAA function

Command	Explanation
Global Mode	
aaa enable **no aaa enable**	Enable/stop the AAA function of a captive portal routine.
aaa group server radius <*word*> **no aaa group server radius <*word*>**	Configure/delete RADIUS name of AAA function.

5. Configure RADIUS authentication server

Command	Explanation
Global Mode	

radius-server key <*word*> **no radius-server key**	Configure/delete RADIUS server key.
radius-server authentication host <*A.B.C.D*> **no radius-server authentication host <*A.B.C.D*>**	Configure/delete RADIUS authentication server address.

6. Configure captive portal supporting pap&chap

Command	Explanation
captive portal Configuration Mode	
authentication-mode {pap|chap} **no authentication-mode**	Configure the encryption method used in authentication between client and authentication server. The no command recovers to be default mode.

2.1.3 Captive Portal Authentication Examples

Case 1：

Set up an environment as shown below. AC1, AC2 and the AC-Controller consisting of a cluster. Moreover, the AC-Controller controls the cluster. The configuration makes AP1 broadcast SSID1, Client1 connects to AP1 SSID1, and designing the RADIUS Server1 an authentication server. Configure the DHCP address pool (or use DHCP server) on AC-Controller. After the client related to SSID1, then redirected to the username and password, the authentication server judge the user information and notify AC1 client to release or prohibited to achieve the function of controlling the users authentication. Portal user roaming can be achieved through configure all AC portal to the same in the same cluster.

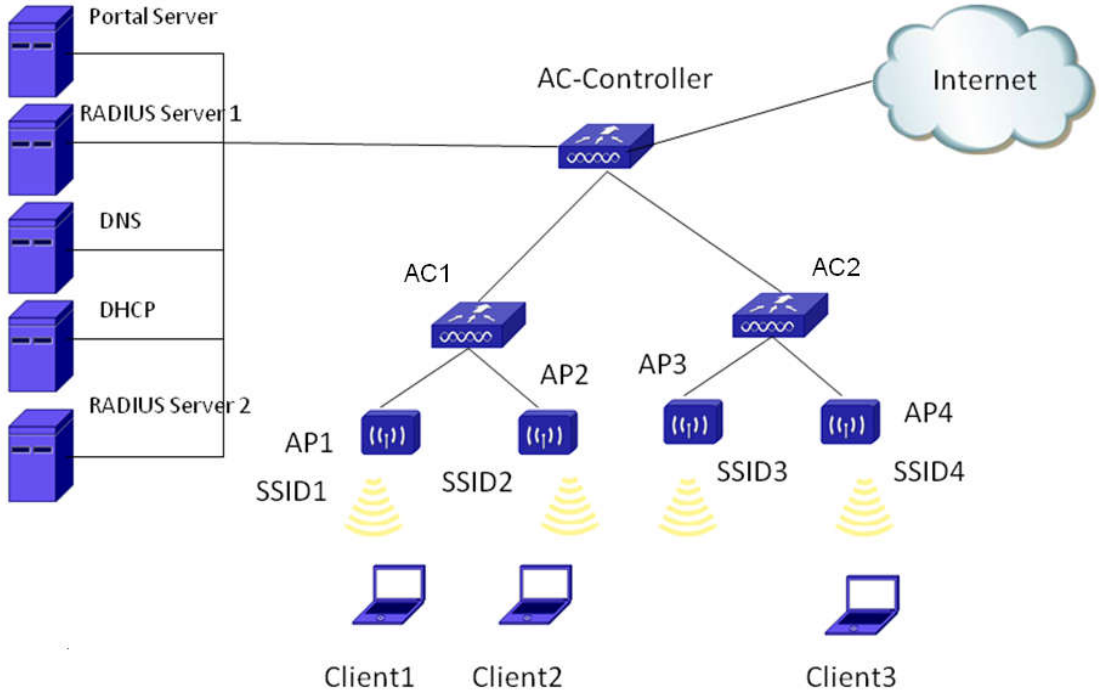


Fig 2-1 authentication function configuration

Configuration steps:

1. Configure the DHCP server.

Configuration of AC-Controller:

AC(config)#ip dhcp pool 123

2. Configure the authentication controller:

Configuration of AC1：

The configuration with the external portal server is as below:

AC(config)#radius-server key 0 test

AC(config)#radius-server authentication host 100.1.1.100

AC(config)#radius-server accounting host 100.1.1.100

AC(config)#aaa-accounting enable

AC(config)#aaa enable

!

AC(config)#aaa group server radius radius_server_1 server 100.1.1.100

AC(config-wireless)#network 1

AC(config-network)#ssid network1

AC(config-wireless)#network 2

AC(config-network)#ssid network 2

AC(config-cp)#enable

AC(config-cp)# authentication-type external

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

AC(config-cp)# external portal-server server-name x2 ipv4 1.0.0.2

AC(config-cp)# free-resource 1 destination ipv4 1.0.0.1/32 source any
AC(config-cp)# free-resource 2 destination ipv4 1.0.0.2/32 source any
AC(config-cp)#configuration 1
AC(config-cp-instance)#enable
AC(config-cp-instance)#protocol http
AC(config-cp-instance)# radius-auth-server radius_aaa_1
AC(config-cp-instance)# portal-server ipv4 x1
AC(config-cp-instance)# free-resource 1
AC(config-cp-instance)#ac-name 0100.0010.010.00
AC(config-cp-instance)#redirect url-head http://1.0.0.1/control
AC(config-cp-instance)#interface ws-network 1
AC(config-cp)#configuration 2
AC(config-cp-instance)#enable
AC(config-cp-instance)#protocol https
AC(config-cp-instance)# radius-auth-server radius_aaa_1
AC(config-cp-instance)# portal-server ipv4 x2
AC(config-cp-instance)# free-resource 2
AC(config-cp-instance)#ac-name 0100.0010.010.00
AC(config-cp-instance)#redirect url-head http://1.0.0.2/control
AC(config-cp-instance)#interface ws-network 2

The configuration with the internal portal server is as below:
AC(config)#radius-server key 0 test
AC(config)#radius-server authentication host 100.1.1.100
AC(config)#radius-server accounting host 100.1.1.100
AC(config)#aaa-accounting enable
AC(config)#aaa enable
!
AC(config)#aaa group server radius radius_server_1 server 100.1.1.100
AC(config-wireless)#network 1
AC(config-network)#ssid network1
AC(config-cp)#enable
AC(config-cp)# authentication-type internal
AC(config-cp)#configuration 1
AC(config-cp-instance)#enable
AC(config-cp-instance)#protocol http
AC(config-cp-instance)# radius-auth-server radius_aaa_1
AC(config-cp-instance)#interface ws-network 1

Case 2：

As shown in the following picture, AC1, AC2 and AC-controller make up a cluster. AC-Controller is the controller of the cluster. Configure AP1 to broadcast SSID1, client1 associates with SSID1 of AP1, client port associates with SSID1, configure this function property on AC1. When client 1 which associates with AC1 is authenticating, configure the authentication encryption method between AC1 and radius server as chap and client will conduct portal authentication.

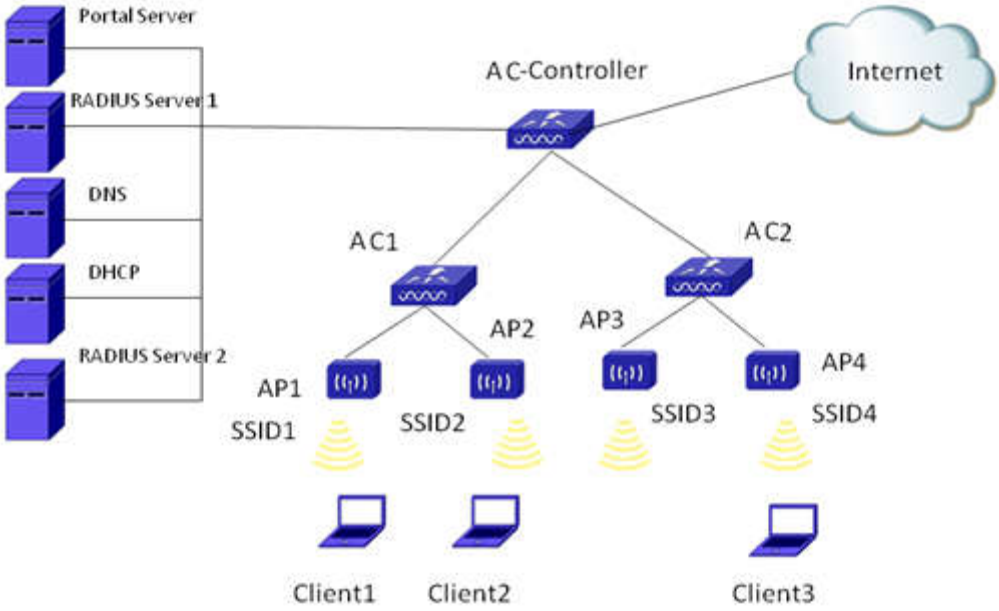


Fig 2-2 Captive Portal Supporting pap&chap

Configuration steps:

1. Configure Captive Portal Supporting pap&chap method

AC (config-cp)# authentication-mode chap

2.1.4 Captive Portal Authentication Troubleshooting

Encounter problems when using the redirection function, please check whether the reasons are as follows:

- ☞ Whether configured the AC correctly, launched the captive portal function and opened the portal configuration switch. Both the captive portal and the portal configuration should be open; otherwise, the captive portal function will not work, the client also cannot be redirect to the specified page.
- ☞ Whether the client is connected to the network correctly, the client needs to relate to AP successfully, and check whether configured DHCP service correctly. After related to AP, the client must obtain the IP so as to redirection and achieve the captive portal authentication function.

- ☞ Whether AC and AP correct connected. AC can manage AP, and can view the status of the AP through the command: show wireless ap status.
- ☞ The authentication server name of AAA module is same to the configured authentication name of captive portal.
- ☞ When the client with internal portal mode cannot pop out the redirection page, please check if enabled http server function.
- ☞ When there are problems of using Captive Portal Supporting pap&chap, check if configured pap&chap methods correctly.
- ☞ When there are problems of using Captive Portal Supporting pap&chap, check if configured client authentication methods on authentication server correctly.

2.2 Accounting Function Configuration

2.2.1 Introduction to Accounting Function

The accounting function is used to monitoring and accounting users who using the network resources. Client is unable to access the network resources before pass the captive portal authentication, only through the portal authentication to access network resources. However, on the competence and capability of different types of customers with network access is usually different. According to actual situation users on the network divided into different types, the different types of user settings for different network permissions and billing.

Accounting function can be achieved with client different uplink and downlink rate as well as input and output flow limit. Define user's session duration to control the use of network resources time and flow of information.

2.2.2 Accounting Function Configuration

Accounting function configuration task list is as below:

1. Configure RADIUS accounting server
   1) Configure/delete accounting server address
2. Configure AAA accounting function
   1) Enable/disable accounting service function
3. Configure captive portal accounting function
   1) Block/unblock portal function
   2) Configure/delete captive portal configuration name
   3) Enable/disable captive portal accounting function
   4) Configure/delete captive portal accounting server name
   5) Configure/delete captive portal session time

6) Configure/delete user uplink rate restriction

7) Configure/delete user downlink rate restriction

8) Configure/delete the maximum bytes that user sending is allowed.

9) Configure/delete the maximum bytes that user receiving is allowed

10) Configure/delete the maximum bytes that user transmission is allowed

1. Configure RADIUS accounting server

Command	Explanation
Global Mode	
radius-server accounting host <*A.B.C.D*> **no radius-server accounting host <*A.B.C.D*>**	Configure/delete accounting server address

2. Configure AAA accounting function

Command	Explanation
Global Mode	
aaa-accounting enable **no aaa-accounting**	Enable/disable accounting service function

3. Configure captive portal accounting function

Command	Explanation
Captive Portal Configuration Mode	
block **no block**	Block/unblock portal function
name <*word*> **no name**	Configure/delete captive portal configuration name
radius accounting **no aaa-accounting**	Enable/disable captive portal accounting function
radius-acct-server <*word*> **no radius-acct-server**	Configure/delete captive portal accounting server name
session-timeout <*0-86400*> **session-timeout**	Configure/delete captive portal session time
max-bandwidth-up <*0-536870911*> **no max-bandwidth-up**	Configure/delete user uplink rate restriction
max-bandwidth-down <*0-536870911*> **no max-bandwidth-down**	Configure/delete user downlink rate restriction

max-input-octets ***<0-4294967295>*** **no max-input-octets**	Configure/delete the maximum bytes that user sending is allowed.
max-output-octets ***<0-4294967295>*** **no max-output-octets**	Configure/delete the maximum bytes that user receiving is allowed.
max-total-octets ***<0-4294967295>*** **no max-total-octets**	Configure/delete the maximum bytes that user transmission is allowed.

2.2.3 Accounting Function Examples

Case：

Set up the environment as shown below. AC1, AC2 and the AC-Controller are consisting of a cluster. In addition, the AC-Controller controls the cluster. The configuration makes AP1 broadcast SSID1, Client1 connects to AP1 SSID1. And design the RADIUS Server1 as authentication server, the RADIUS Server2 as accounting server. And then configure the DHCP address pool (or use DHCP Server) on AC-Controller. After the Client port related to SSID1, then one can achieve the accounting function without through portal authentication.

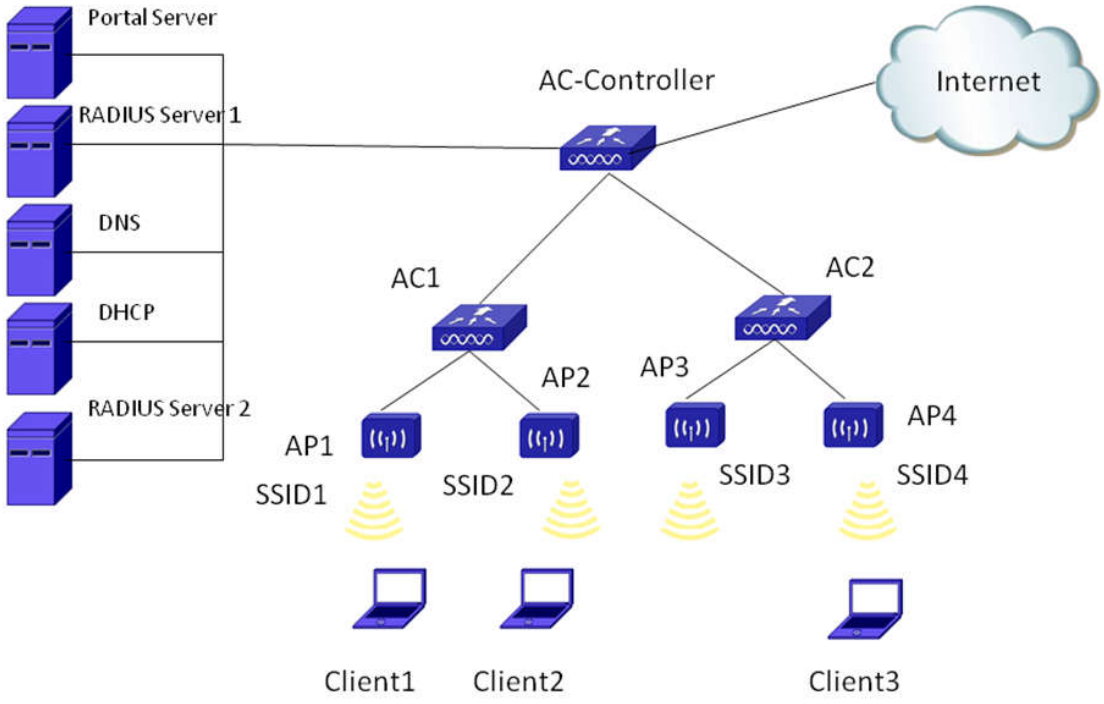


Fig 2-3 accounting function configuration

Configuration steps:

1. Configure RADIUS accounting server

RADIUS configuration of AC1:

AC(config)# radius-server accounting host 100.1.1.101

2. Configure AAA accounting function

AAA configuration of AC1:

AC(config)# aaa enable

AC(config)# aaa-accounting enable

AC(config)# radius-server accounting host 100.1.1.101

AC(config)#radius-server key test

AC(config)#aaa group server radius radius_aaa_1

AC(config-sg-radius)# server 100.1.1.101

3. Configure captive portal accounting function

AC(config-cp-instance)#name AC1_CP1

AC(config-cp-instance)#radius accounting

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

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

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

AC(config-cp-instance)# max-bandwidth-down 2048

AC(config-cp-instance)# max-input-octets 5000

AC(config-cp-instance)# max-output-octets 5000

AC(config-cp-instance)# max-total-octets 60000

2.2.4 Accounting Function Troubleshooting

Encounter problems when using the accounting function, please check whether the reasons are as follows:

- ☞ Whether configured the AC correctly, launched the captive portal function and opened the portal configuration switch. Both the captive portal and the portal configuration should be open. Otherwise the captive portal function will not work.
- ☞ Configure the nap ip of AC same as wireless IP of controller.

2.3 Free-resource Configuration

2.3.1 Introduction to Free-resource

Free-resource function is a method of captive portal module to achieve access the free resources rule. By configuring the free-resource rules, one can makes certain the client directly access the specific network resources without going through the portal authentication.

2.3.2 Free-resource Configuration

Free-resource function configuration task list is as below:

1. Enable/disable captive portal authentication function
2. Configure free-resource rule and bind it to CP configuration

1. Enable/disable captive portal authentication function

Command	Explanation
Captive Portal Configuration Mode	
enable **disable**	Enable/disable captive portal authentication function of AC globally. This function includes the captive portal function on AC and AP.

2. Configure free-resource rule and bind it to CP configuration

Command	Explanation
Captive Portal Configuration Mode	
free-resource <*rule-number*> {destination {any | { ipv4 | ipv6} <*ip-addr*> } | source {any | { ipv4 | ipv6} <*ip-addr*> }} **no portal free-resource {<*rule-number*> | all}**	Configure/delete free-resource rule.
Captive Portal Instance Configuration Mode	
free-resource <*rule-number*> **no free-resource <*rule-number*>**	Bind/unbind free-resource rule.

2.3.3 Free-resource Examples

Case：

Set up an environment as shown below. AC1, AC2 and the AC-Controller are consisting of a cluster. And the AC-Controller controls the cluster. The configuration makes AP1 broadcast SSID1, Client connects to AP1 SSID1 (SSID1 binding to CP Configuration1 below), the CP Congfiguration1 below also bind a free-resource rule (Source IP is the address segment for the Client1, and the Destination IP is the address segment for client who wants to access the resources).And design the RADIUS Server1 as authentication server. Then configure the DHCP address pool (or use DHCP Server) on AC-Controller. Once the Client1 related to SSID1, it can access the free-resource and

will not be redirected to the authentication server.

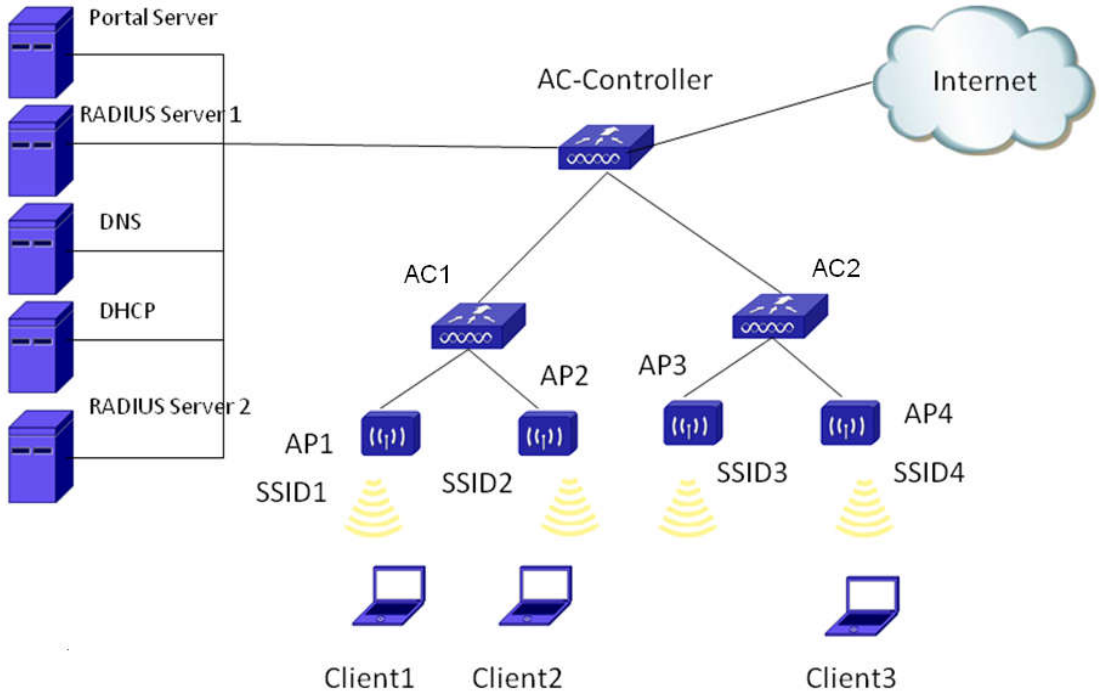


Fig 2-4 multi-portal servers function configuration

Configuration steps:

Configure portal server information for AC1:

AC(config-cp)#enable

AC(config-cp)# free-resource 1 destination ipv4 1.0.0.1/8 source ipv4 10.0.0.2/8

AC(config-cp)#configuration 1

AC(config-cp-instance)#enable

AC(config-cp-instance)# free-resource 1

2.3.4 Free-resource Troubleshooting

Encounter problems when using the redirection function, please check whether the reasons are as follows:

- ☞ Whether configured the AC correctly, launched the captive portal function and opened the portal configuration switch. Both the captive portal and the portal configuration should be open; otherwise, the captive portal function will not work, the client also cannot be redirect to the specified page.
- ☞ Whether the client is connected to the network correctly, the client needs to relate to AP successfully, and check whether configured DHCP service correctly. After related to AP, the client must obtain the IP so as to redirection and achieve the captive portal authentication function.
- ☞ Whether AC and AP correct connected. AC can manage AP, and can view the status

of the AP through the command: show wireless ap status.

☞ The authentication server name of AAA module is same to the configured authentication name of captive portal.

2.4 MAC Portal Configuration

2.4.1 Introduction to MAC Portal

Mac portal is used for some special users in the network. The administrator can set permission to allow the users to connect to the network to use network resources without authentication, but the administrator needs to get the user's mac address. At the same time the user who has the permission to use network resources do not need to billing. So the user belongs to the advanced user.

2.4.2 MAC Portal Configuration

Mac portal function configuration task list is as below:

1. Configure user mac with mac portal function purview
2. Enable mac portal function on-off
3. Issue mac portal function

1. Configure user mac with mac portal function purview

Command	Explanation
Captive Portal Configuration Mode	
mac-portal known-client <*macAddr*> **no mac-portal known-client <*macAddr*>**	Configure/delete user mac with mac portal function purview

2. Enable mac portal function on-off

Command	Explanation
Captive Portal Routine Configuration Mode	
mac-portal authentication **no mac-portal authentication**	Enable mac portal function on-off under the mode of Captive portal routine.

3. Issue mac portal function

Command	Explanation
Admin Mode	

wireless ap profile apply *<1-16>*	Issue mac portal function on-off.

2.4.3 MAC Portal Examples

Case:

Set up an environment as shown below. AC1, AC2 and the AC-Controller are consisting of a cluster. And the AC-Controller controls the cluster. The configuration makes AP1 broadcast SSID1, Client connects to AP1 SSID1, Client port related to SSID1. In portal global mode, the client mac address is added to mac portal function, and opens the mac portal switch in the SSID1 of the associated portal routines. The client can achieve access the resources without authentication.

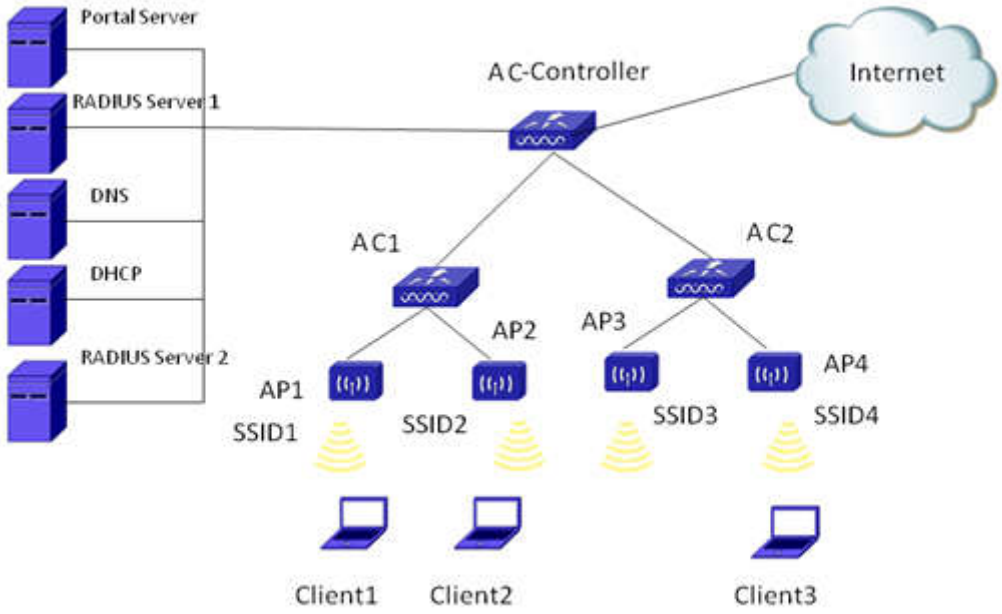


Fig 2-5 mac portal function configuration

Configuration steps:

1. Configure MAC portal function

mac portal function configuration of AC1:

AC(config-cp)# mac-portal known-client 68-74-7f-29-76-04

2. Enable mac portal function on-off

mac portal function on-off of AC1:

AC(config-cp-instance)# mac-portal authentication

3. Issue mac portal function

Issue mac portal function on AC1:

AC#wireless ap profile apply 1

2.4.4 MAC Portal Function Troubleshooting

When encountered problems in the process of using the mac portal function, please check whether the reasons are as follows:

- ☞ If not entered into force after completed configuration mac portal, then check whether the AP made a configuration. After configured the completion of the mac function, if the client is currently online, mac portal function will not work unless the user reconnect to the internet..
- ☞ If issued configuration has not entered into force, please check whether you add a mac address of the client not to open Mac portal switch function in the routine.

2.5 User Verification of Internal Portal

2.5.1 Introduction to User Verification of Internal Portal

In portal authentication, there are two important servers. One is portal server which is used to pop up the verification page; another one is the authentication server which is used for the authentication.

For the portal authentication framework, the portal server can be divided into external and internal portal server. The external portal server is a standalone dedicated device which is used to complete the verification page popping up, verification launching; the internal portal server is a function module on AC which can provide the function of portal server.

Similarly, the authentication server can be also divided into external and internal server. The external authentication server is general; it adopts the dedicated RADIUS authentication server for the user authentication. For the internal authentication server, the user authentication is completed by AC; this function can create the local user authentication database on AC.

The internal portal user is very important for saving user resources and simplifying network structure. In the specific application, the external RADIUS server does not need to be set as the authentication server; the local authentication user can be configured on AC and enables the local authentication. The user name and password can be checked on AC to complete the portal authentication.

The two applications of internal portal user are as below:

In the first application as shown in Fig 2-6, there is an external portal server which is used to pop up the verification page and launch the user authentication. But the external

RADIUS authentication server is not needed; AC is as the authentication server.

In the second application as shown in Fig 2-7, there is not the external portal server and external RADIUS authentication server. AC can pop up the portal verification page and carry out the user authentication.

Fig 2-6external portal server, internal user verification

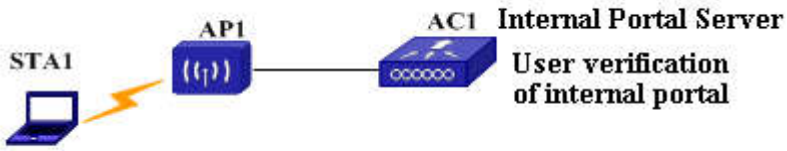


Fig 2-7 internal portal server, internal user verification

2.5.2 User Verification of Internal Portal Configuration

The basic configuration task list of User Verification of Internal Portal is as below:

1. Create the local user database; configure the user password, group and other parameters.
2. Choose the verification method under the Captive Portal Instance mode as local and configure the associated group of instance.
3. Show if the database and configuration is correct.
4. Configure network and apply it.

1. Configure the verification method of captive portal instance

Command	Explanation
Captive Portal Instance Mode	
verification {local | radius|ladp|none}	Configure the verification method of captive portal instance, which including local, radius, ladp and none. The default method is radius.

2. Configure a user group for the captive portal instance

Command	Explanation

Captive Portal Instance Mode	
group <group-name> **no group**	Configure a user group for the captive portal instance. The no command cancels this configuration.

3. Create/delete a local user or enter into the captive portal user mode

Command	Explanation
Captive Portal Global Mode	
user <user-name> **no user <user-name>**	Create a local user or enter into the captive portal user mode. The no command deletes the local user.

(Notice: If a user-name has been created, user can enter into the captive portal user mode when enable the command of user <user-name>.)

4. Configure/delete the password of the local user

Command	Explanation
Captive Portal User Mode	
password <user-password> **no password**	Configure the password for the local user. The no command deletes the password.

5. Configure the encrypted password for the local user

Command	Explanation
Captive Portal User Mode	
password-encrypted < encrypted -pwd>	Configure the encrypted password for the local user.

6. Associate a user group with the local user/delete the association

Command	Explanation
Captive Portal User Mode	
group< group-name > **no group**	Associate a user group with the local user. The no command deletes the association.

7. Configure the timeout of session for the local user

Command	Explanation

Captive Portal User Mode	
session-timeout< timeout > **no session-timeout**	Configure the timeout of session for the local user. The no command recovers it to be the default value.

8. Configure the maximum uplink bandwidth of the local user

Command	Explanation
Captive Portal User Mode	
max-bandwidth-up <rate> **no max-bandwidth-up**	Configure the maximum uplink bandwidth of the local user. The no command cancels the uplink bandwidth limit.

9. Configure the maximum downlink bandwidth of the local user

Command	Explanation
Captive Portal User Mode	
max-bandwidth-down <rate> **no max-bandwidth-down**	Configure the maximum downlink bandwidth of the local user. The no command cancels the downlink bandwidth limit.

10. Configure the total number of bytes which are allowed to be sent

Command	Explanation
Captive Portal User Mode	
max-input-octets <bytes> **no max-input-octets**	Configure the total number of bytes which are allowed to be sent. The no command cancels the limit.

11. Configure the total number of bytes which are allowed to be received

Command	Explanation
Captive Portal User Mode	
max-output-octets <bytes> **no max-output-octets**	Configure the total number of bytes which are allowed to be received. The no command cancels the limit.

12. Configure the total number of bytes which are allowed to be transmitted

Command	Explanation
Captive Portal User Mode	
max-total-octets <bytes> **no max-total-octets**	Configure the total number of bytes which are allowed to be transmitted. The no command cancels the limit.

13. Show the configured local user information of captive portal.

Command	Explanation
Admin Mode	
show captive-portal user [<user-name>]	Show the configured local user information of captive portal.

(Notice: 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.)

14. Delete all the users of the local verification database

Command	Explanation
Admin Mode	
clear captive-portal users	Delete all the users of the local verification database.

2.5.3 User Verification of Internal Portal Examples

Case:

As shown below, configure the captive-portal as local verification, create the local user database, create a user whose name is wlantest, configure the password as 123456, and associate with a group of abc. Under the captive portal instance mode, choose the verification method as local. Configure the group that the instance is associated with and bind the corresponding network. Configure the network and apply it at last.

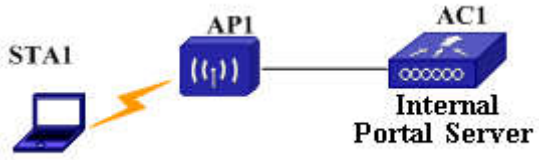


Fig 2-8 application of the local verification of internal portal

Configuration steps:

Under the captive-portal mode, configure the local verification, create the user id, user name and password, the configuration is as below:

AC(config)#captive-portal
AC(config-cp)#enable
AC(config-cp)#user wlantest
AC(config-cp-local-user)# password 123456
AC(config-cp-local-user))#session-timeout 86400
AC(config-cp-local-user)#max-bandwidth-up 10485760
AC(config-cp-local-user)#max-bandwidth-down 10485760
AC(config-cp-local-user)#max-total-octets 42940000
AC(config-cp-local-user)# group abc

Under the captive-portal mode, create the cp instance and the configuration is as below:

AC(config)#captive-portal
AC(config-cp)#enable
AC(config-cp)#authentication-type internal
AC(config-cp)#configuration 1
AC(config-cp-instance)#enable
AC(config-cp-instance)# verification local
AC(config-cp-instance)# group abc
AC(config-cp-instance)#protocol http
AC(config-cp-instance)#interface ws-network 1

Configure network1 and apply it.
AC(config-wireless)#network 1
AC(config-network)#ssid portal-test
AC(config-network)#security mode none
AC(config-wireless)#ap profile 1
AC(config-ap-profile)#radio 1
AC(config-ap-profile-radio)#vap 0
AC(config-ap-profile-vap)#enable
AC(config-ap-profile-vap)#network 1
AC#wireless ap profile apply 1

2.5.4 User Verification of Internal Portal Troubleshooting

When there is problem in using the user verification of internal portal, please check the following reasons:

- ☞ After configured the internal portal, if user cannot pop up the redirection page, please check whether the authentication type is internal, whether the verification method is local, and whether the protocol is http under the captive portal instance mode.
- ☞ After the redirection page is popped up, if the verification cannot be successful after input the user name and password, please check whether the user name and password are correct by. The command is **show captive-portal user user1**.
- ☞ If the user name and password are correct, please check whether the same group is bound under the captive portal user mode and captive portal instance mode. If not, the user will be treated as the illegal user; the verification cannot be carried out.

2.6 Internal Portal Page Customization Configuration

2.6.1 Introduction to Internal Portal Page Customization

After using the browser to input the website, the internal portal authentication user will be redirected to a unified authentication page. After inputting the user name and password to pass the authentication, user can use the Internet resources. To meet the individual needs of different users, this function achieves the internal portal page customization. The pages that the user can define according to their needs are as below: the authentication page before Internet, the welcome page and the logout page after the successful authentication, and the prompt page after the successful logout.

2.6.2 Internal Portal Page Customization Configuration

The internal portal page customization task list as below:

1. Create the web locale page
2. Configure the global parameters

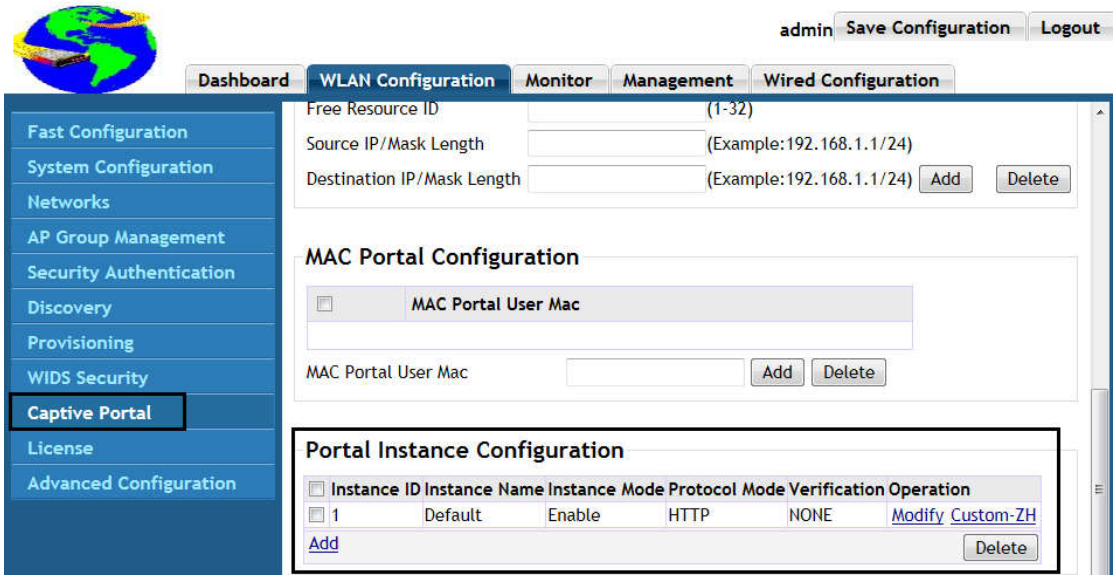
3. Configure the authentication page parameters
4. Configure the welcome page parameters
5. Configure the logout page parameters
6. Configure the successful logout page parameters

2.6.2.1 Create Web Locale Page

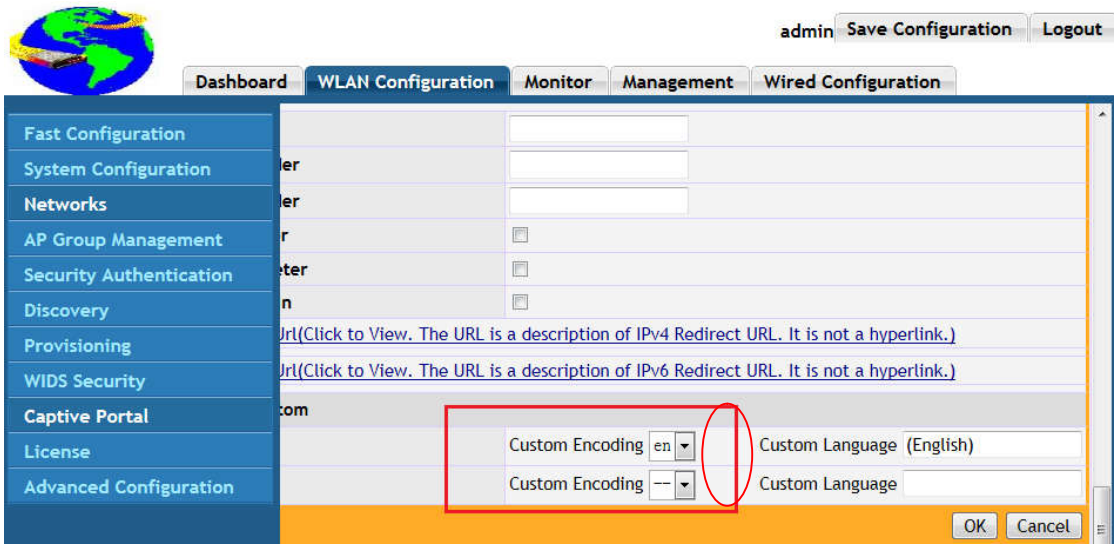
Before custom made the internal portal page, the web portal authentication functionshould be configured first, the detailed configuration can be seen in the part of Captive Portal.

Under the Captive Portal mode, one web locale will be created as default when creating the configuration 1, and the textual encoding of this web locale is consistent with the switch web language. The following example is for the English page.

Log in the web management system of AC through the browser (take http://192.1.1.1 for example), and open the CP configuration page:



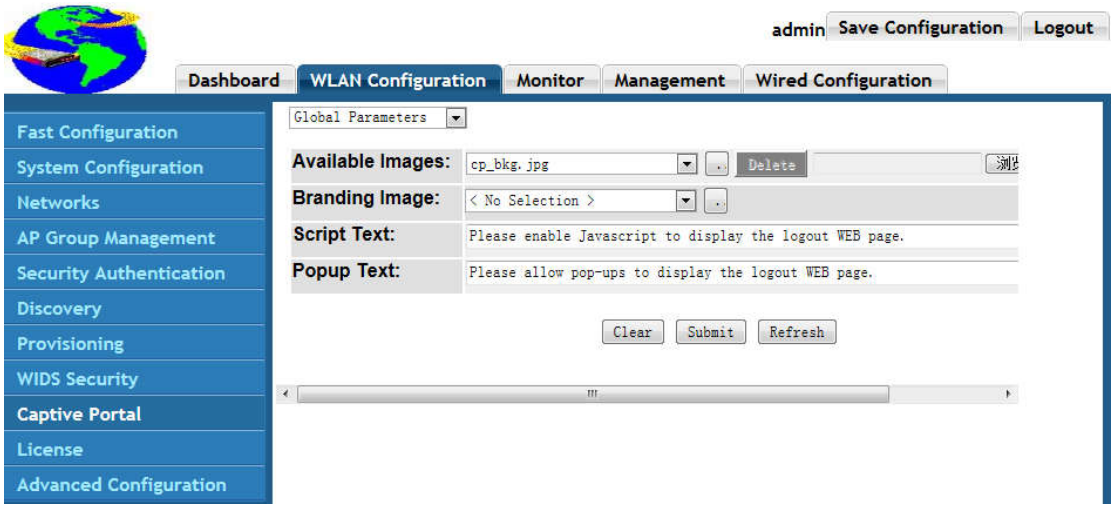
Choose the “Add”. Because the web language has been configured as English, there has existed an English page:



Click  can add the language that means to create a web locale, and submit to become effective.

2.6.2.2 Global Parameters Configuration

Choose captive portal and the Custom-ZH is the global parameters configuration.



The main functions of the global parameters configuration page are as below:

(1) Upload the self-defined pictures

Choose the local pictures through the browse button and click the upload button, then there will be the prompt if uploaded successfully.

The pictures which can be uploaded include the flowing kinds:

Background picture, the suggested size is 1366*768

Trademark picture, the suggested size is 283*85

Description picture, the suggested size is 499*93

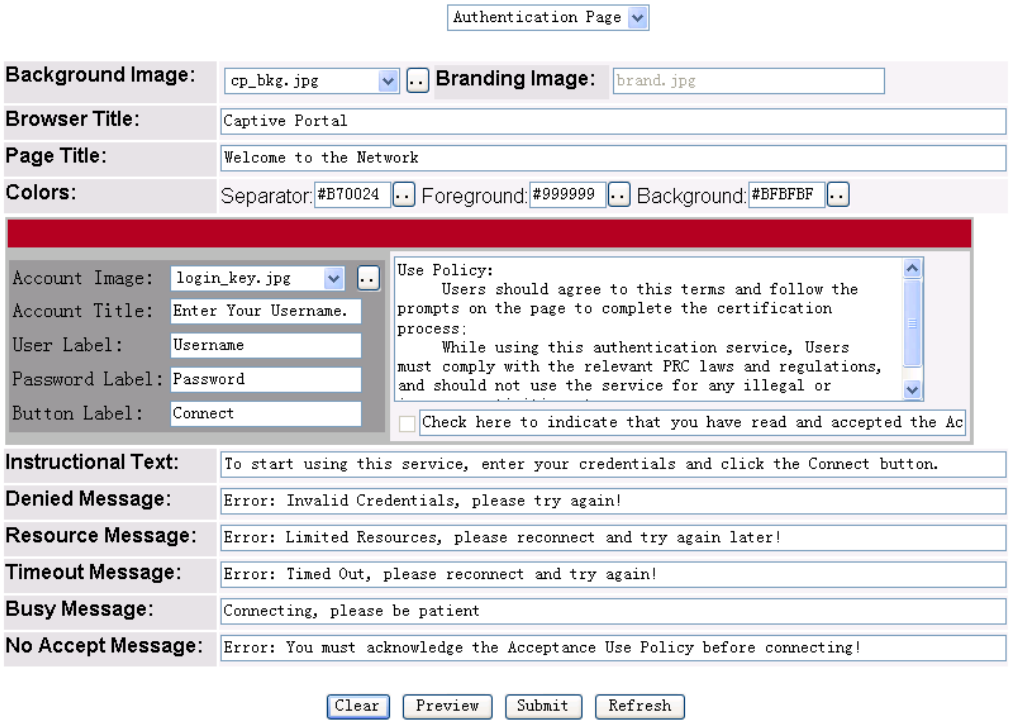
(2) Configure the global used trademark picture

Choose the pictures through the browse or drop-down list, and submit to become effective.

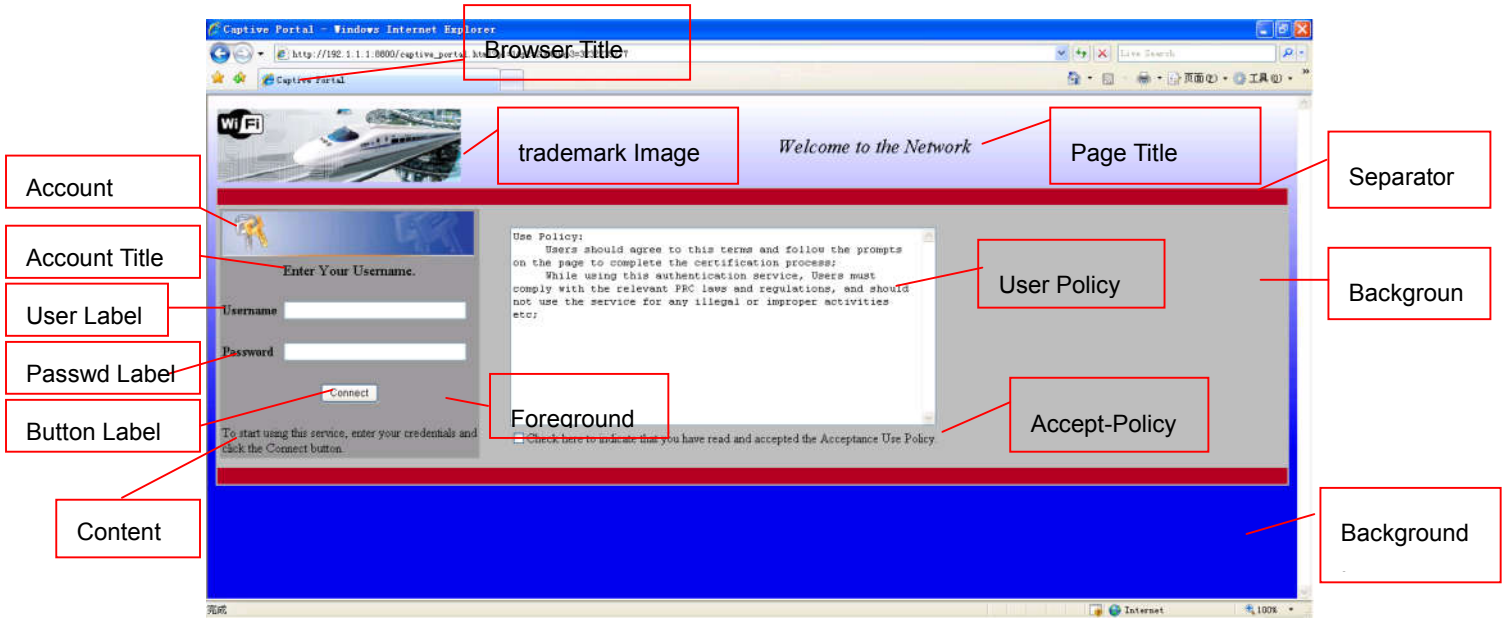
2.6.2.3 Authentication Page Parameters Configuration

The authentication page is the one that user is redirected to when access Internet through the browser first time. After inputting the user name and password to pass the authentication, user can use the Internet resources.

User can define the background picture, color, title, prompt message and content of the authentication page according to their needs.



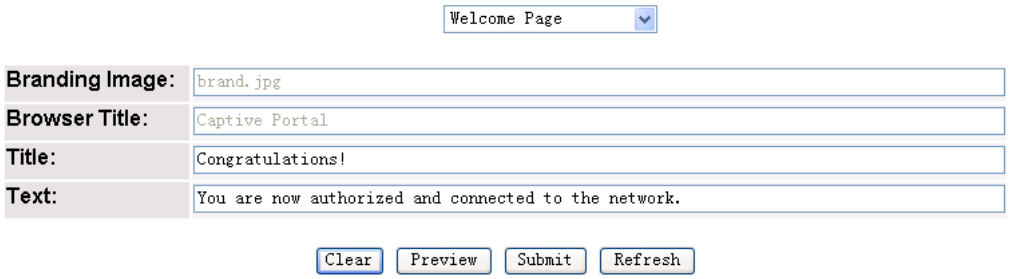
The correspondence between the authentication page and parameters is as below:



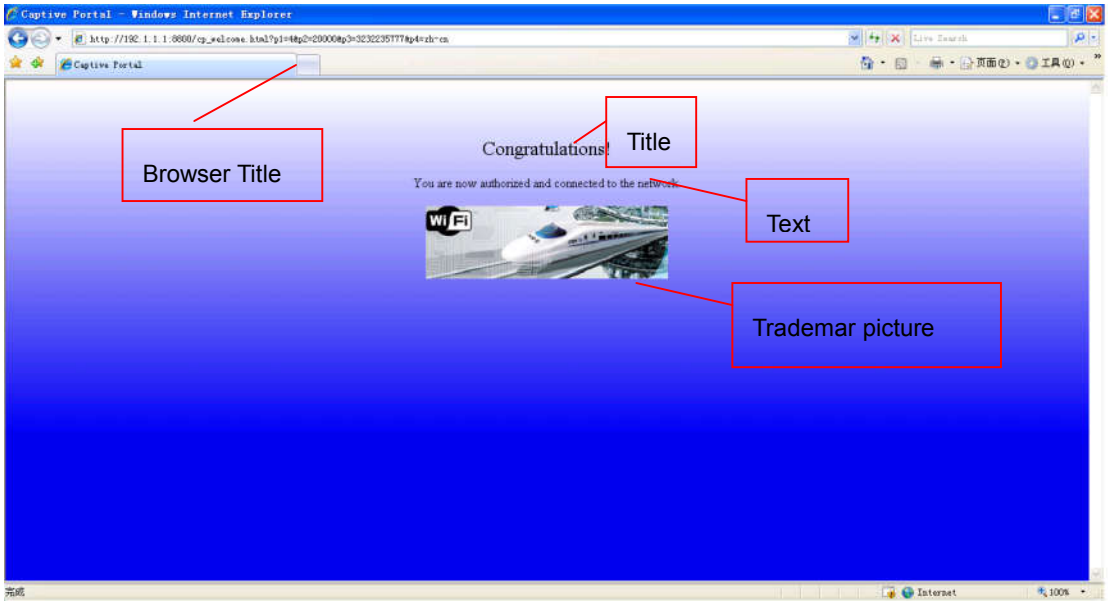
The above parameters will be effective after modified and submitted; if use the clear button, all the parameters will be reset to be default except the trademark picture.

2.6.2.4 Welcome Page Parameters Configuration

After user passed the authentication, it will go to the welcome page. If user has passed the authentication, the Internet service can be used.

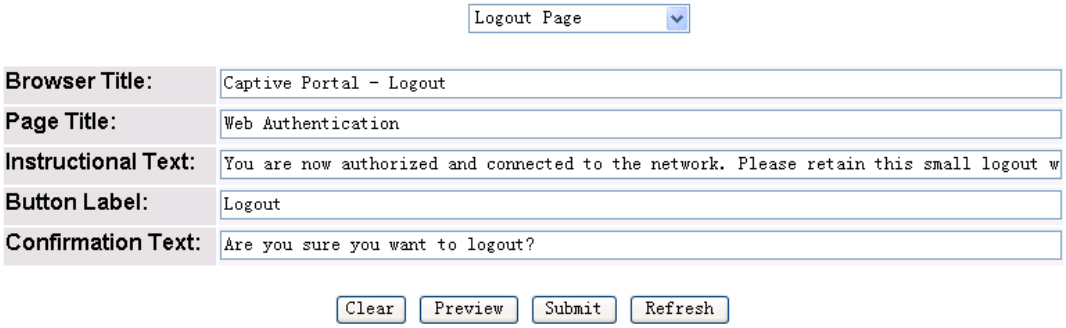


The correspondence between the welcome page and parameters is as below:

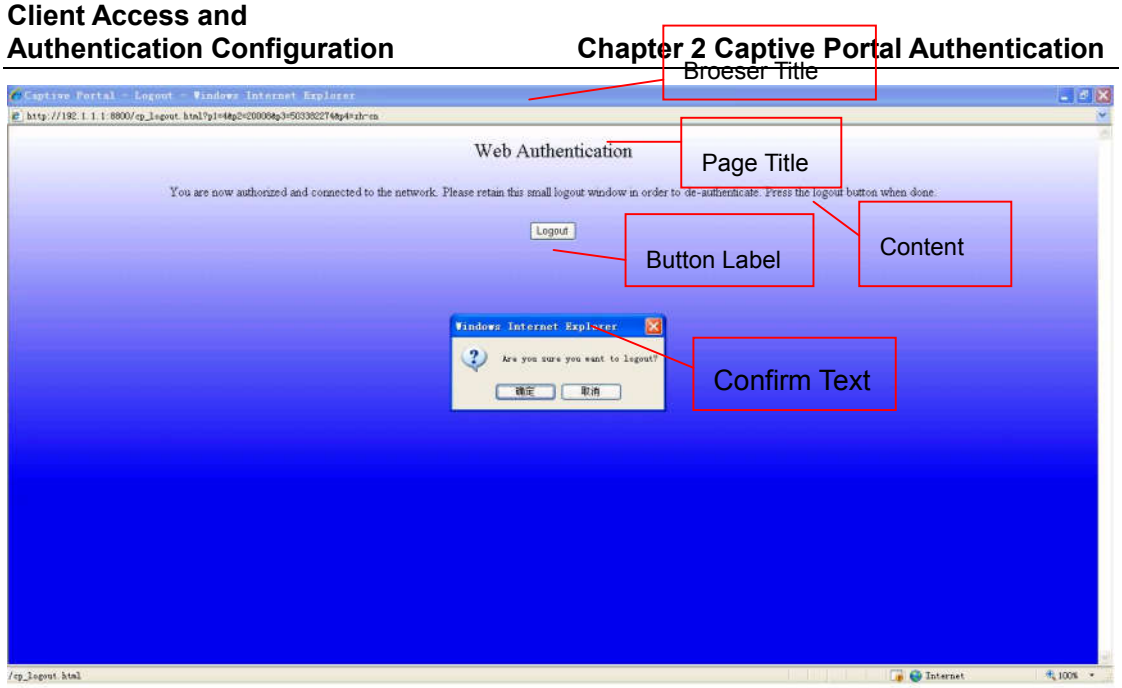


2.6.2.5 Logout Page Parameters Configuration

The logout page means that there will pop up a new window after the user authenticated successfully. It is mainly used for user to be off line. After user finish working on the Internet, click the logout button to stop the Internet service and charging.

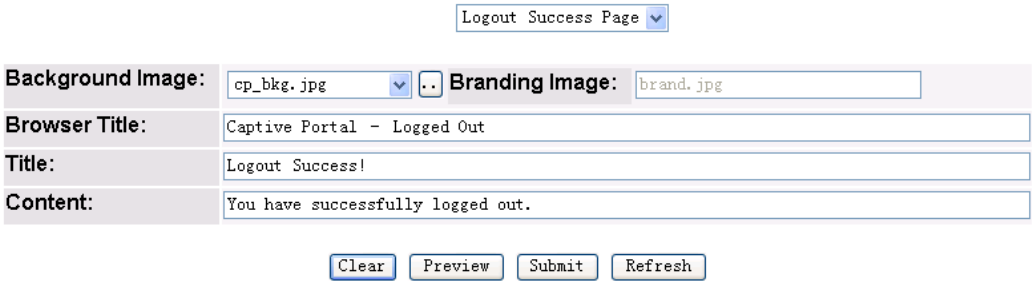


The correspondence between the logout page and parameters is as below:



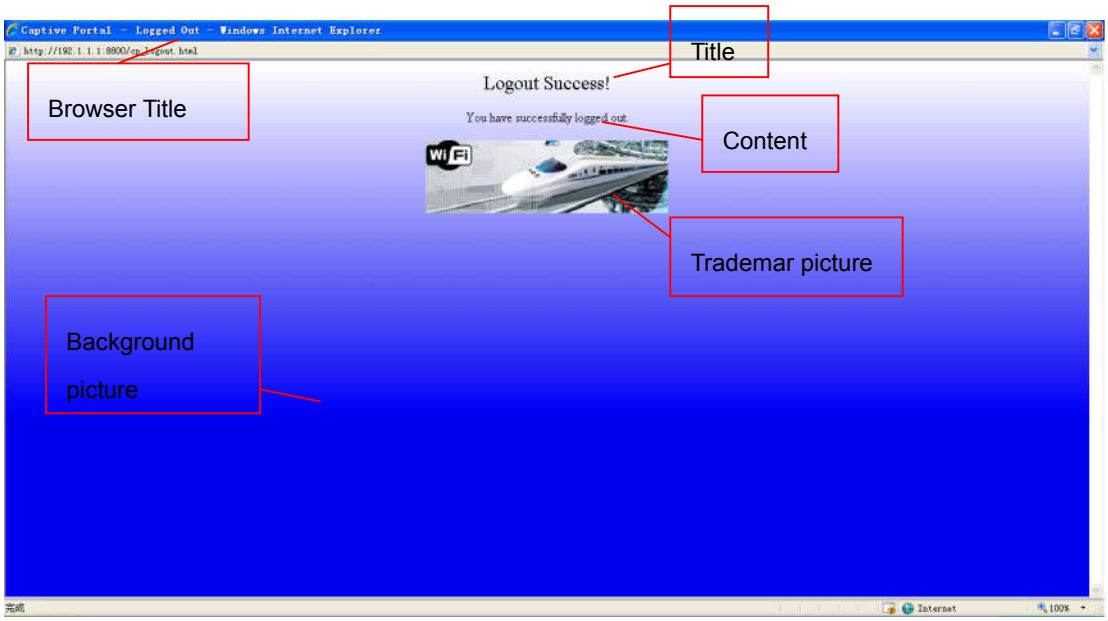
2.6.2.6 Successful Logout Page Parameters Configuration

The successful logout page is the prompt page which can show user the logout result.



Notice: The background picture of this configuration page will affect all the welcome, logout and successful logout page.

The correspondence between the successful logout page and parameters is as below:



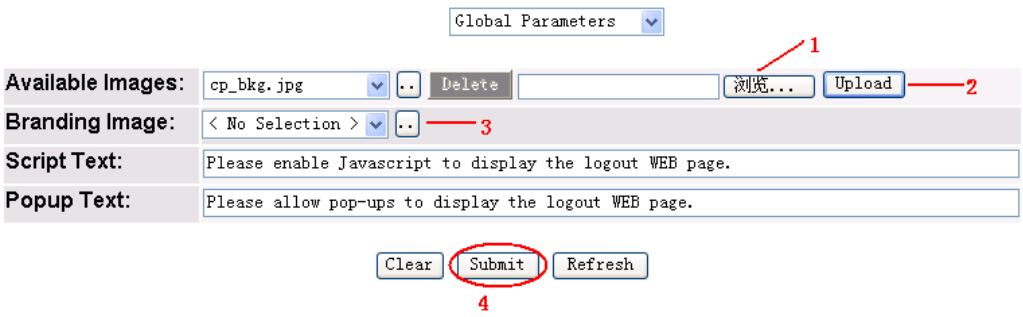
2.6.3 Internal Portal Page Customization Examples

User has the following needs:

1. Upload two self-defined pictures of green.jpg and ka.jpg as the background of different pages through the CP configuration page, choose the system picture as the trademark picture;
2. Choose the self-defined picture of green.jpg as the background picture of the authentication and welcome pages, choose the colors of #FFFFCC, #CCFFCC and #CCFFFF as the separator bar, foreground and background color respectively;
3. Configure the title of the welcome page as: congratulations! Configure the text content as: You are now authorized and connected to the network. Please click the logout button when you ending using the network, or it will cause extra cost;
4. Choose the self-defined picture of ka.jpg as the background of the welcome, logout and successful logout pages.

Configuration methods:

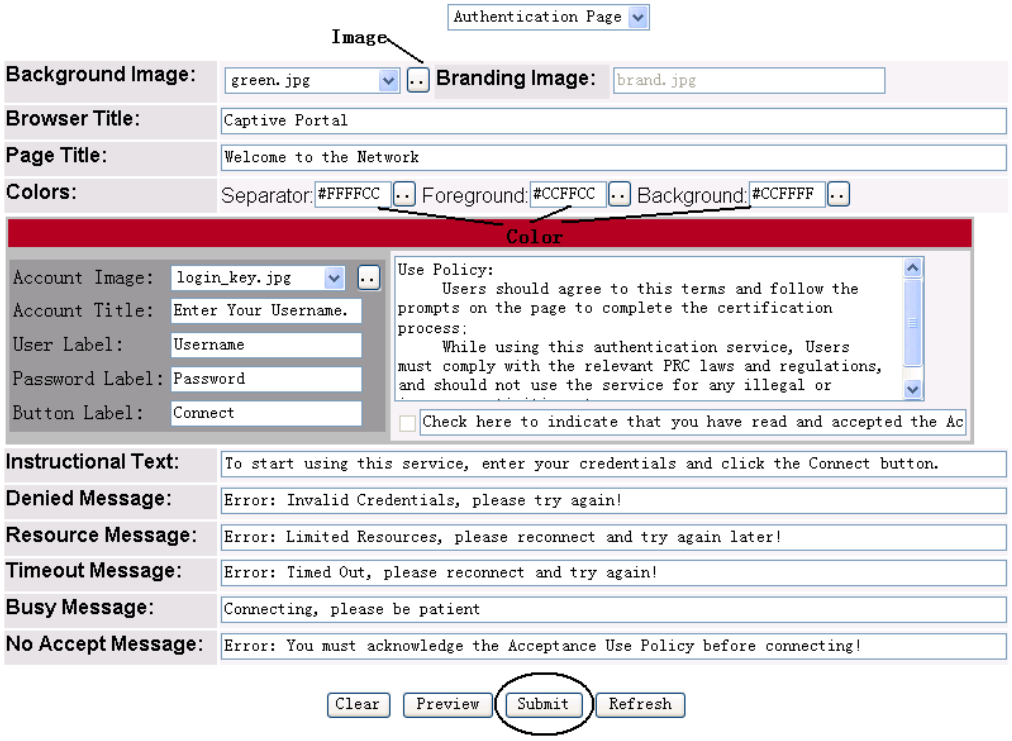
1. Global parameters page:



Enter into the global parameters page, click the browse button to choose the picture of green.jpg, and then click the upload button to wait the page to refresh for uploading successfully. Upload the picture of ka.jpg as the same way;

Click the browse button of the trademark picture to choose the system picture and submit.

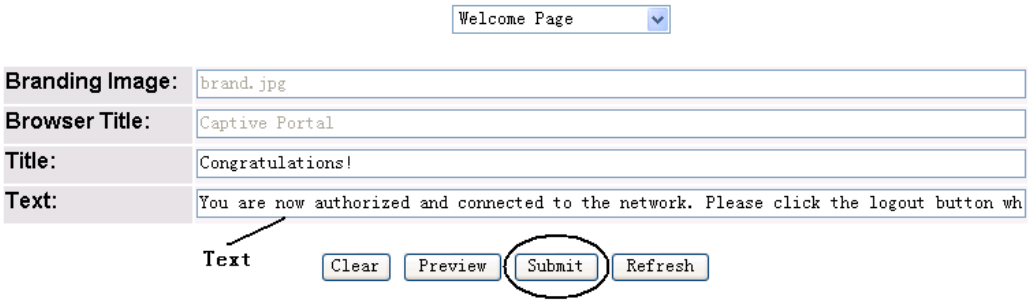
2. Authentication page:



Enter into the authentication page and choose the background picture of green.jpg;

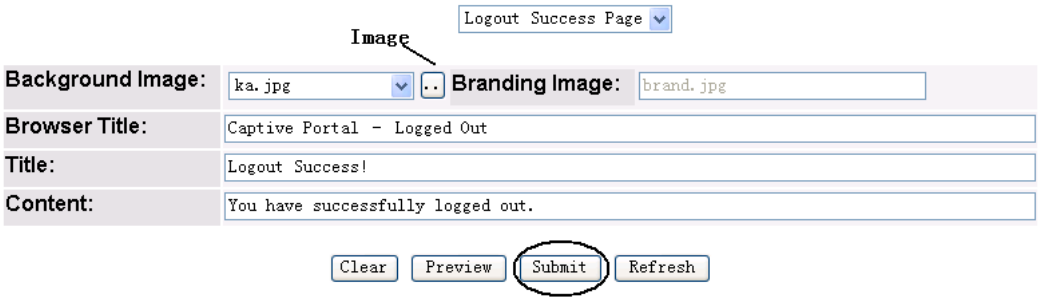
Choose the color through the browse selection or manually and then submit.

3. Welcome page:



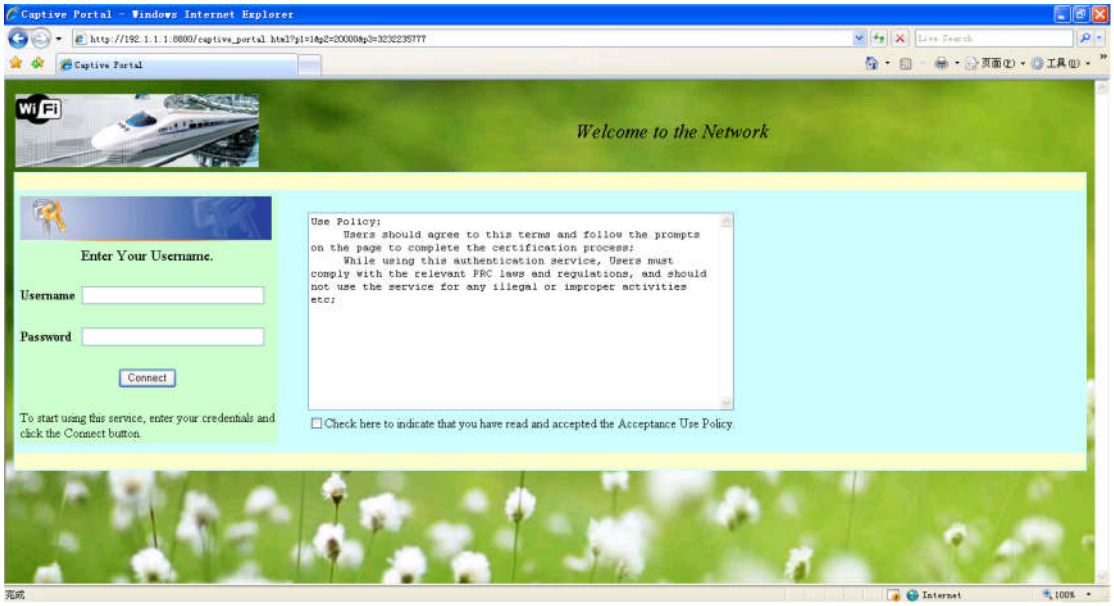
Modify the text as: You are now authorized and connected to the network. Please click the logout button when you ending using the network, or it will cause extra cost. And then submit.

4. Successful logout page:

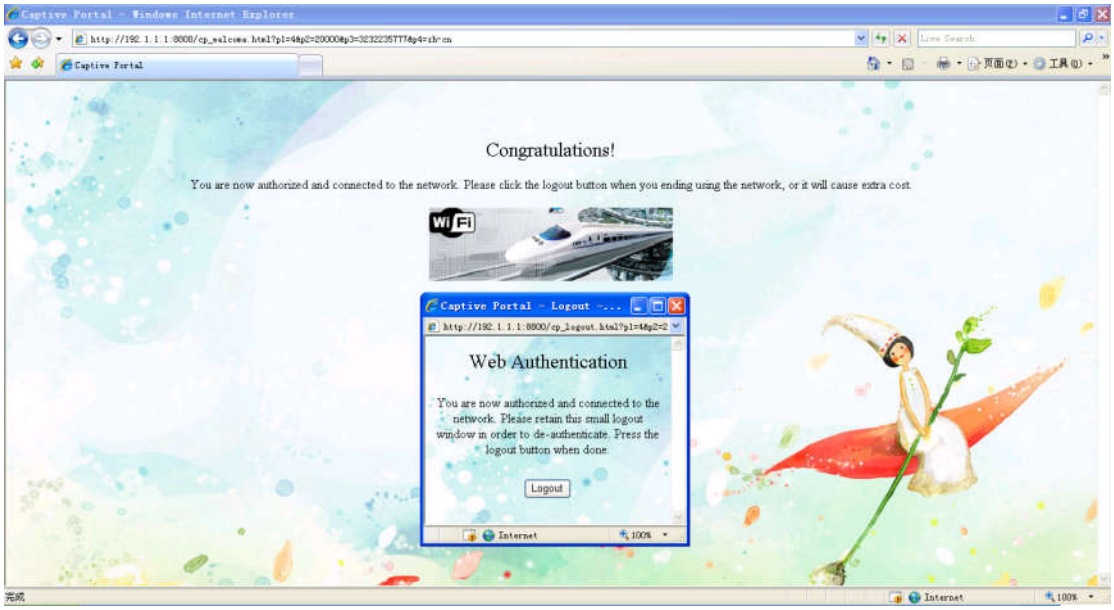


Choose the background picture of ka.jpg through the browse selection;

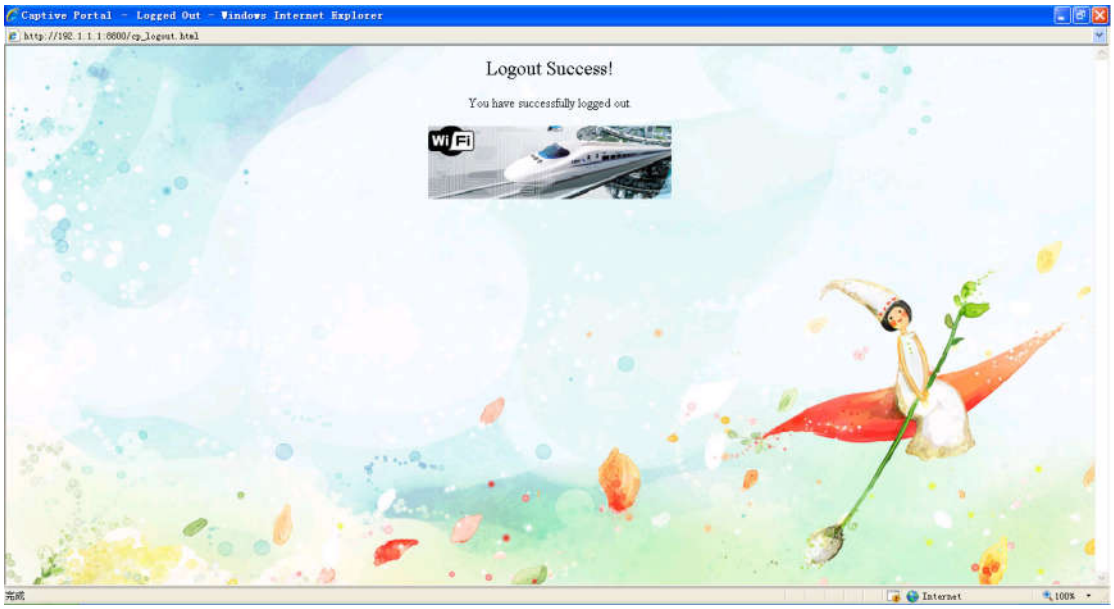
After configuration as the above steps, log in through the client to check the situation. Input a website in the browser website bar, such as http://3.3.3.3, enter it and it will be redirected to the authentication page:



Select the acception and input the user name and password, and then connect it to enter into the welcome and logout page:



Click the logout button and enter into the successful logout page:



2.6.4 Internal Portal Page Customization Troubleshooting

- If the picture failed to uploade, please check if the size exceeds the left space of Flash; check if the picture name includes the special characters except '_' and '-'; check if the picture name exceeds 32 characters. Moreover, it needs some time to upload the file, please do not configure anything before there is the uploading result.
- When uploaded a self-defined file which has existed in AC to cover the original file and configure it as the background picture, then user discovers it is still the

original picture. At this time, please pay attention that user should clear the IE cache manually after uploaded the file with the same name; otherwise, the preview picture will be still the original file that has been uploaded in IE cache.

- ☞ If the background picture does not become effective after submitted, please check if configured the background picture in the global parameters page incorrectly. The global page shows all the pictures which can be used, but the background picture just can be configured on the authentication and the successful logout pages respectively.
- ☞ If all the configurations disappeared after restart the AC, please pay attention that it only becomes effective immediately after configured the web pages, but user should save the configuration through the write command, otherwise it will invalid after restart the AC.

2.7 Portal Page of Web Server

2.7.1 Introduction to Portal Page of Web Server

Internal portal, it means the AC can conduct the portal authentication as the portal server. In this process, the communication between AC and the external portal server is not needed. For the current internal portal, the authentication url, logout url, etc. are all the internal urls of AC, and they are compiled in the system img. The format cannot be modified. Even though the AC provides the internal portal page customizing function, the pages are not flexible enough and different requirements from users are difficult to meet. So the method to put the authentication url on the external web server appeared.

This method is named portal page of web server. Users can manage the web server according to their need through creating this external web server.

The application of the portal page of web server is as below:

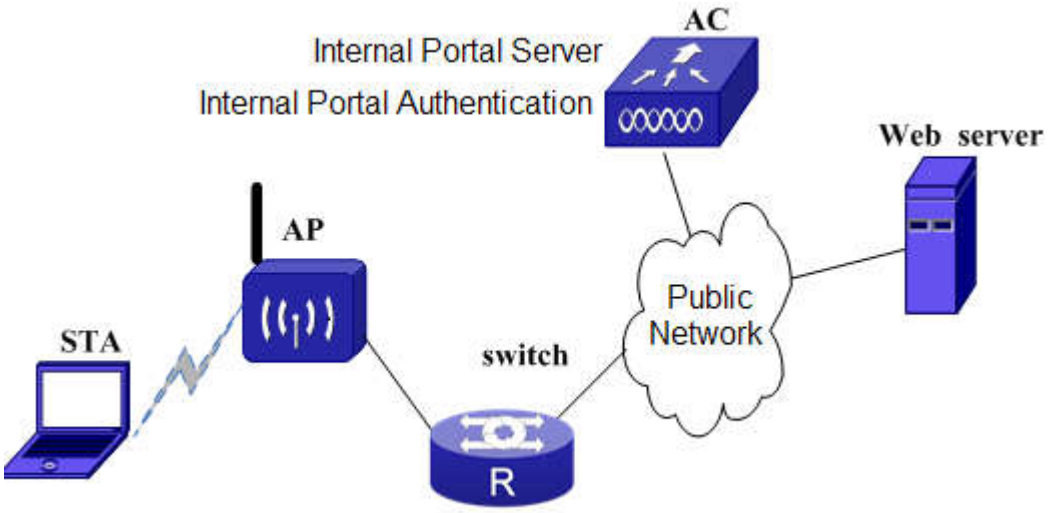


Fig 2-9 portal page of web server

2.7.2 Portal Page of Web Server Configuration

The configuration task list of Portal Page of Web Server is shown as below:

1. Enable/disable the portal page of web server on AC for the CP instance
2. Configure/delete the login-url of the web server
3. Configure/delete the login-failure-url of the web server
4. Configure/delete the logout-url of the web server
5. Configure/delete the logout-success-url of the web server
6. Configure/delete the redirect url-head

1.Enable/disable the portal page of web server on AC for the CP instance

Command	Explanation
Captive Portal Instance Mode	
ext-web-server enable **no ext-web-server enable**	Enable/disable the portal page of web server on AC for the CP instance.

2.Configure/delete the login-url of the web server

Command	Explanation
Captive Portal Instance Mode	
ext-web-server login-url<word> **no ext-web-server login-url<word>**	Configure the login-url of the web server. The no command cancels this configuration.

3.Configure/delete the login-failure-url of the web server

Command	Explanation
Captive Portal Instance Mode	
ext-web-server login-failure-url <word> **no ext-web-server login-failure-url <word>**	Configure the login-failure-url of the web server. The no command cancels this configuration.

4.Configure/delete the logout-url of the web server

Command	Explanation
Captive Portal Instance Mode	

ext-web-server logout-url <*word*> **no ext-web-server logout-url**	Configure the logout-url of the web server. The no command deletes it.

5.Configure/delete the logout-success-url of the web server

Command	Explanation
Captive Portal Instance Mode	
ext-web-server logout-success-url <*word*> **no ext-web-server logout-success-url**	Configure the logout-success-url of the web server. The no command deletes it.

6.Configure/delete the redirect url-head

Command	Explanation
Captive Portal Instance Mode	
redirect url-head <*word*> **no redirect url-head <*word*>**	Configure the redirect url-head. The no command deletes it.

2.7.3 Portal Page of Web Server Example

Case:

as shown below, configure the captive-portal as the local authentication, create the local database, create the user name of wlantest and the password of 123456, associate with the group of abc, choose the authentication method of local under the captive portal instance mode, configure the group that the instance associated with user, bind the corresponding network, configure the network and apply it. The portal page of web server function can be configured.

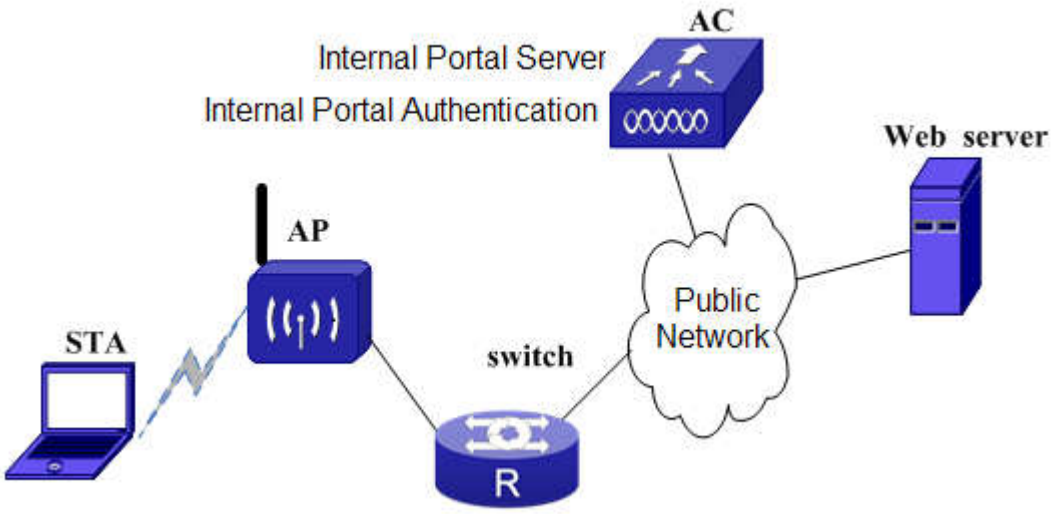


Fig 2-10 portal page of web server

Configuration steps:

1. Under the captive-portal mode, configure the local authentication, create the user id, user name and password, the configuration is as below:

   AC(config)#captive-portal

   AC(config-cp)#enable

   AC(config-cp)#user wlantest

   AC(config-cp-local-user)# password 123456

   AC(config-cp-local-user))#session-timeout 86400

   AC(config-cp-local-user)#max-bandwidth-up 10485760

   AC(config-cp-local-user)#max-bandwidth-down 10485760

   AC(config-cp-local-user)#max-total-octets 42940000

   AC(config-cp-local-user)# group abc
2. Under the captive-portal mode, create the cp instance, the configuration is as below:

   AC(config)#captive-portal

   AC(config-cp)#enable

   AC(config-cp)#authentication-type internal

   AC(config-cp)#configuration 1

   AC(config-cp-instance)#enable

   AC(config-cp-instance)# verification local

   AC(config-cp-instance)# group abc

   AC(config-cp-instance)#protocol http

   AC(config-cp-instance)#interface ws-network 1
3. Configure the network1 and apply it.

   AC(config-wireless)#network 1

   AC(config-network)#ssid portal-test

   AC(config-network)#security mode none

   AC(config-wireless)#ap profile 1

   AC(config-ap-profile)#radio 1

   AC(config-ap-profile-radio)#vap 0

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

   AC(config-ap-profile-vap)#network 1

   AC#wireless ap profile apply 1
4. Configure the portal page of web server function:

   AC(config)#captive-portal

   AC(config-cp)# authentication-type internal

   AC(config-cp)#free-resource 1 destination ipv4 172.16.1.200/32 source any

AC(config-cp)#configuration 1

AC(config-cp-instance)#free-resource 1

AC(config-cp-instance)#ext-web-server enable

AC(config-cp-instance)#ext-web-server login-url http://172.16.1.200/login.html

AC(config-cp-instance)#ext-web-server login-failure-url http://172.16.1.200/login_fail.html

AC(config-cp-instance)#ext-web-server logout-url http://172.16.1.200/logout.html

AC(config-cp-instance)#ext-web-server logout-success-url http://172.16.1.200/logout_success.html

AC(config-cp-instance)#interface ws-network 1

2.7.4 Portal Page of Web Server Troubleshooting

When there is problem in using the function of portal page of web server, please check the following reasons:

- If the wireless client cannot access the authentication url of web server, please check whether the web server is configured as free-resource.
- After configured the web server as free-resource, if the wireless client cannot access the authentication url of web server, please check whether the portal page of web server function is enabled: ext-web-server enable.
- If the wireless client cannot access the authentication url of web server, please check whether link between AC and web server is well.

2.8 Automatic Page Pushing after Successful Authentication

2.8.1 Introduction to Automatic Page Pushing after Successful Authentication

The automatic page pushing function after the successful authentication means that the web page which user needs to access can be re-opened after the authentication. According to the actual situation, the welcome page before the automatic pushing authentication or the appointed web page by the automatic pushing function can be configured.

2.8.2 Automatic Page Pushing after Successful Authentication Configuration

Automatic Page Pushing after Successful Authentication Configuration is as below:

1. Enable/disable the captive portal authentication function
2. Configure the automatic page pushing after successful authentication

1. Enable/disable the captive portal authentication function

Command	Explanation
Captive Portal Mode	
enable **disable**	Enable/disable the captive portal authentication function. This global function contains the captive portal function on AC and AP.

2. Configure the automatic page pushing after successful authentication

Command	Explanation
Captive Portal Instance Mode	
redirect attribute url-after-login enable **no redirect attribute url-after-login enable**	Enable the function that the redirect url carries the pushed url after the successful authentication. The no command disables it.
redirect attribute url-after-login name <name> **no redirect attribute url-after-login name**	Configure the attribute name of the pushed url after the successful authentication which is carried in the redirect url. The no command recovers the name to be the default value.
redirect attribute url-after-login encode {plain-text|base64}	Configure the encode of the pushed url after the successful authentication which is carried in the redirect url.
redirect attribute url-after-login value <url-value> **no redirect attribute url-after-login value**	Configure the appointed url which is popped up after the successful authentication. The no command deletes it.

2.8.3 Automatic Page Pushing after Successful Authentication Example

Case:

Create the topology as below: AC1, AC2 and AC-Controller make up a cluster. The AC-Controller is the controller of this cluster. Configure AP1 to broadcast SSID1, configure the client1 to associate with SSID1 of AP1 (SSID1 is bound to CP configuration1), appoint the RADIUS server 1 as the authentication server, configure the DHCP address pool on AC-Controller (or use the DHCP server). Configure the automatic page pushing function after the successful authentication on configuration 1. The automatic pushed page is http://www.test.com.

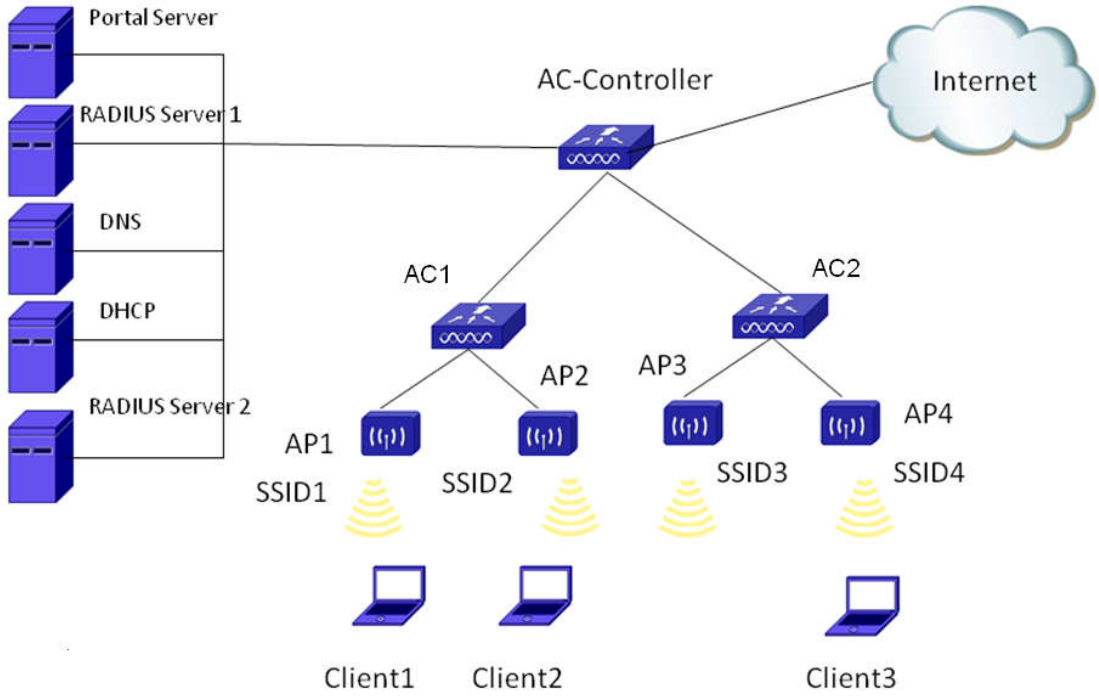


Fig 1 Automatic Page Pushing after Successful Authentication Configuration

Configuration steps:

Configure the portal server information for AC1.

AC(config-cp)#enable

AC(config-cp)#configuration 1

AC(config-cp-instance)#enable

AC(config-cp-instance)# redirect attribute url-after-login enable

AC(config-cp-instance)# redirect attribute url-after-login encode plain-text

AC(config-cp-instance)# redirect attribute url-after-login name ad

AC(config-cp-instance)# redirect attribute url-after-login value http://www.test.com

2.8.4 Automatic Page Pushing after Successful Authentication Troubleshooting

When there is problem in using the automatic page pushing function after the successful authentication, please check the following reasons:

- ☞ Check if the captive portal authentication function is configured correctly. The automatic page pushing function after the successful authentication can be effect when the captive portal function is normal.
- ☞ If the command of **redirect attribute url-after-login value** is configured, the configured page url can be pushed automatically after the authentication; if that command is not configured, the page that the user access before the authentication can be pushed.
- ☞ Check if the page before the authentication or the pushed page appointed by command exists, if not, the page cannot be accessed after pushing.

2.9 Advertisement Page of Captive-portal

2.9.1 Introduction to Advertisement Page of Captive-portal

The scene of the advertisement page of captive-portal function is: STA associates with the wireless network. When it accesses any website first time, AC can redirect the page to the advertisement WEB page. When STA accesses any website again, it will not be limited any more.

2.9.2 Advertisement Page of Captive-portal Configuration

1. Enable the captive-portal function
2. Add a captive-portal instance
3. Enable a captive-portal instance
4. Configure the authentication method of captive-portal instance as none
5. Configure the advertisement page's URL of captive-portal instance
6. Configure the associated ws-network of the captive-portal instance

1. Enable the captive-portal function

Command	Explanation

Captive-portal Global Mode	
enable **disable**	Enable the captive-portal function globally. After configured this command, AC can apply the captive-portal function to the client. The no command disables this function, AC cannot apply the captive-portal function to the client any more.

2. Add a captive-portal instance

Command	Explanation
Captive-portal Global Mode	
configuration <1-10> **no configuration <1-10>**	Configure the captive-portal instance for different users. 10 instances can be configured at most. The no command deletes the captive-portal instance.

3. Enable a captive-portal instance

Command	Explanation
Captive-portal Instance Mode	
enable **disable**	Enable a captive-portal instance. After configured this command, AC can apply the captive-portal function to the client which is associated with the instance. The no command disables the captive-portal instance.

4. Configure the authentication method of captive-portal instance as none

Command	Explanation
Captive-portal Instance Mode	
verification none	Configure that the client of the instance can pass through the portal authentication without certification.

5. Configure the advertisement page's URL of captive-portal instance

Command	Explanation
Captive-portal Instance Mode	
redirect attribute url-after-login enable **redirect attribute url-after-login value *WORD***	Configure the advertisement page's URL of captive-portal instance. The parameter of WORD is the URL.

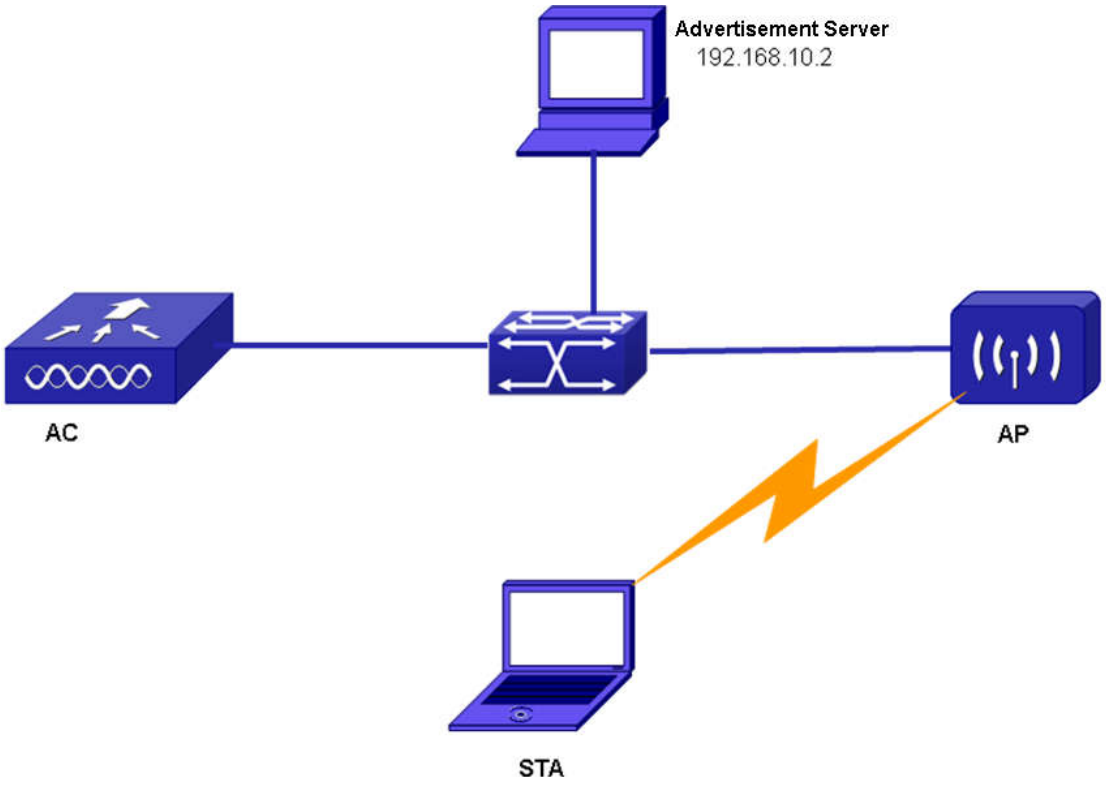
6. Configure the associated ws-network of the captive-portal instance

Command	Explanation
Captive-portal Instance Mode	
interface ws-network <1-1024> **no interface ws-network <1-1024>**	Configure the associated ws-network of the captive-portal instance. The no command cancels it.

2.9.3 Advertisement Page of Captive-portal Example

Case:

As shown below, after STA associated with AP, it should be redirected to the advertisement server when accesses the web page.



The configuration on AC is as below:

```
captive-portal
    enable
    configuration 1
        enable
        verification none
        redirect attribute url-after-login enable
        redirect attribute url-after-login value http://192.168.10.2/  #advertisement URL
        redirect url-head http://17.16.1.26  #any URL of non-STA network segment
```

interface ws-network 1

the configuration is completed.

2.9.4 Advertisement Page of Captive-portal Troubleshooting

If the advertisement page cannot pop out, please check the following reasons:

- ☞ Please ensure that the network router between STA and advertisement server is opened.
- ☞ Please ensure that the associated interface ws-network of captive-portal instance is correct.
- ☞ Please check whether the configured redirect url-head is in the same network segment to STA. If they are in the same network segment, please modify it to be other URL.

2.10 Huawei Portal 2.0 Supporting

2.10.1 Introduction to Huawei Portal 2.0 Supporting

Enable the Huawei portal 2.0 supporting function. The BAS device can work together with the portal server, radius server (iMC) of Huawei. The BAS means the achieved BAS function on wireless AC. BAS is Broad Access Server.

This function is the modification for the external portal, so please do not make any configuration when using the internal portal.

2.10.2 Portal 2.0 Configuration

1. Configure portal version 2.0
2. Configure the external portal server
3. Other parameters can be configured according to the normal external portal command

1. Configure portal version 2.0

Command	Explanation
Captive-portal Global Mode	
portal version 1|2 **no portal version**	Enable the Huawei portal 2.0 supporting function. The default supported protocol is portal 1.0. The no command recovers to be the

	default protocol.

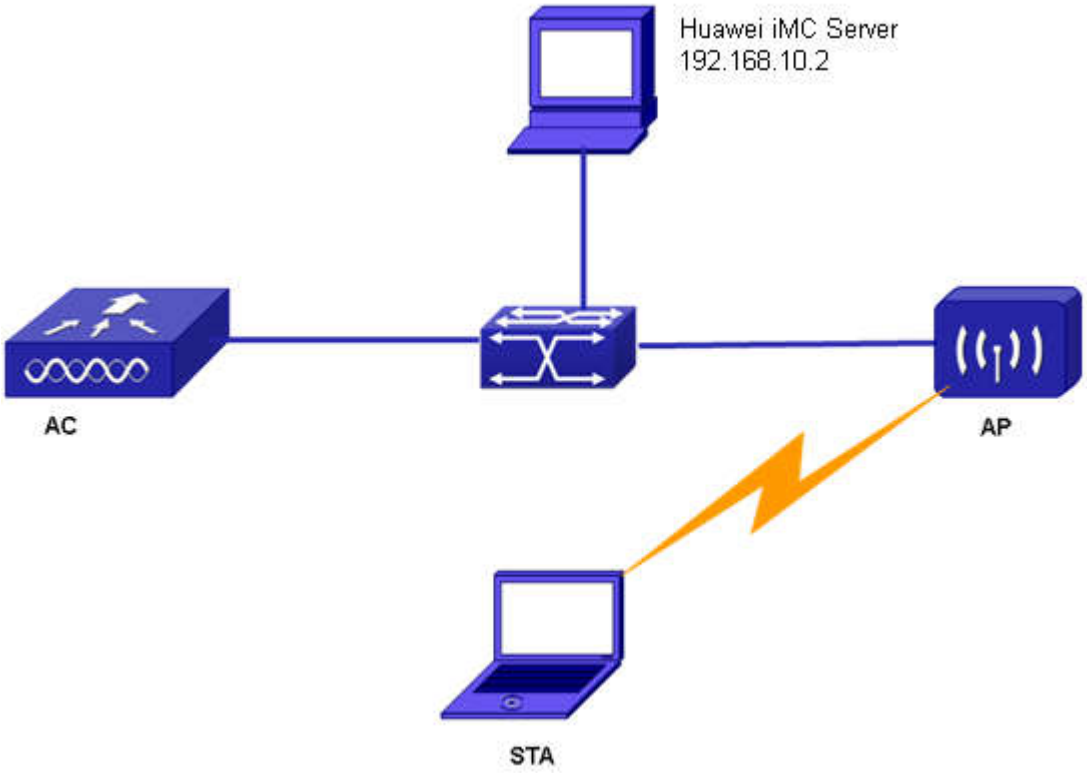
2. Configure the external portal server

Command	Explanation
Captive-portal Global Mode	
external portal-server server-name *WORD* ipv4|ipv6 A.B.C.D|X:X::X:X port <0-65535> key *WORD* **no external portal-server ipv4|ipv6 server-name *WORD***	Configure the IP and other parameters of the external portal server. The parameter of server-name can be defined, it can be used in the captive-portal instance; the parameter of port is the one that the BAS sends the active offline packet to notice the portal server, it should be consistent to the configured port on portal server; the parameter of key is the one of the configured portal server version 2.0 on iMC, it should be consistent to the configured key of iMC. The no command deletes the configured external portal-server.

2.10.3 Portal 2.0 Examples

Case:

As show below: AC can work with the Huawei iMC server as the portal BAS. The iMC configuration is not introduced; there is only the configuration of AC as BAS. We assume that the shared key of radius authentication in iMC is test; the shared key of portal server is version2-key. The configuration on iMC is completed.



The configuration on AC is as below:

```
radius-server authentication host 192.168.10.2 key 0 test
radius-server accounting host 192.168.10.2 key 0 test
aaa-accounting enable
aaa enable
aaa group server radius imc
 server 192.168.10.2

captive-portal
 enable
 portal version 2
 external portal-server server-name h3c ipv4 192.168.10.2 port 50100 key
version2-key
 free-resource 1 destination ipv4 192.168.10.2/32 source any
 configuration 1
  enable
  radius accounting
  radius-acct-server imc
  radius-auth-server imc
```

redirect attribute ssid enable

redirect attribute nas-ip enable

ac-name 0001.0002.003.04

redirect url-head http://192.168.10.2:8080/portal

portal-server ipv4 h3c

free-resource 1

interface ws-network 1

!

The configuration is completed.

2.11 URL Filter Configuration

2.11.1 Introduction to URL Filter Configuration

URL (Uniform Resource Locator) is a kind of network page filtration function. It supports to filter the request packets for the HTTP based on IP address, domain name and regex. The url filter depends on a url filter rule database, user can customize the url filter rule.

URL rule includes two kinds: white-list and black-list. The white-list is the websites that the user can access directly without authentication; the black-list is the websites which are forbidden accessing for user even though the user has passed the authentication.

This function can be used together with Captive Portal. It means to achieve the website filtration for user When the captive portal authentication is enabled.

2.11.2 URL Filter Configuration

The url filter configuration task list is as below:

1. Configure the url filter rule
2. Configure to bind the url filter rule to cp instance

1. Configure the url filter rule

Command	Explanation
Global Mode	
url-filter permit <rule-number><hostname> **no url-filter permit {rule-number|all}**	Configure the global url-filter white-list rule. The no command deletes the global url white-list rule.

url-filter deny <rule-number><hostname> **no url-filter deny {rule-number|all}**	Configure the global url-filter black-list rule. The no command deletes the global url black-list rule.
show url-filter status	Show all the global configured url rules.

2. Configure to bind the url filter rule to cp instance

Command	Explanation
Portal Mode	
url-filter permit <rule-number> **no url-filter permit {rule-number|all}**	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.
url-filter deny<rule-number> **no url-filter deny {rule-number|all}**	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.

2.11.3 URL Filter Configuration Example

Typical case:

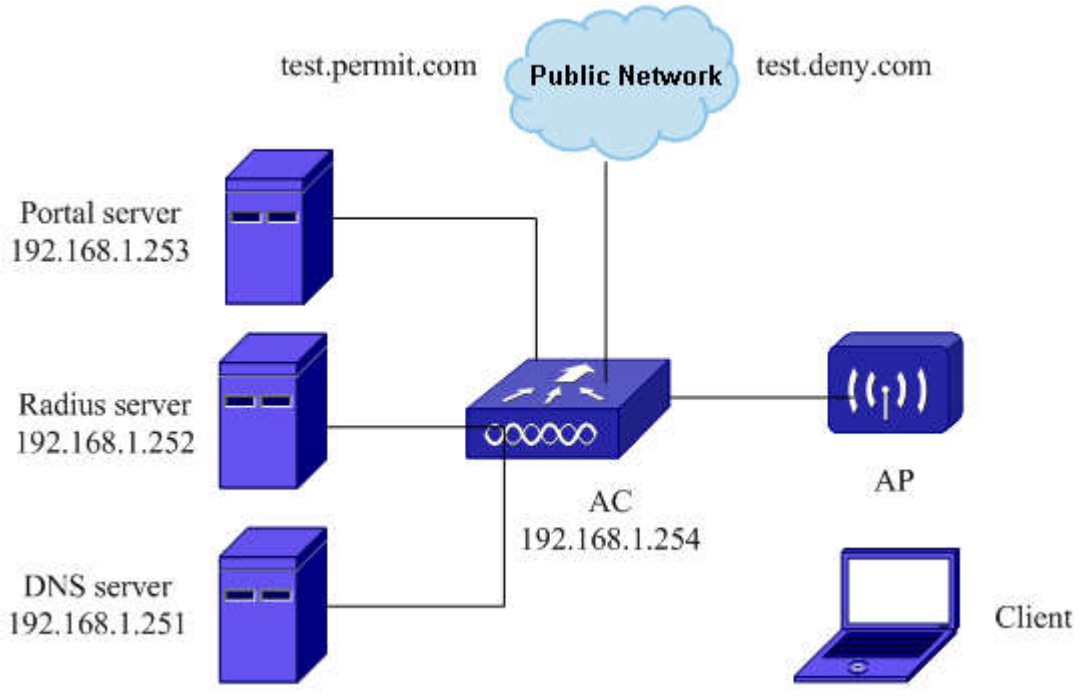


Fig 2-11 typical case of url filter function

As show in the above figure, the client wants to access the public network of “test.permit.com” before the portal authentication; the url white-list should be configured. The client needs to forbid accessing the public network of “test.deny.com” after the authentication; the url black-list should be configured.

The configuration is as below:

1. Under the global mode, configure the authentication key, authentication server, accounting server and aaa mode of the radius server:

AC(config)#radius-server key 0 test

AC(config)#radius-server authentication host 192.168.1.252

AC(config)#radius-server accounting host 192.168.1.252

AC(config)#aaa-accounting enable

AC(config)#aaa enable

AC(config)#radius nas-ipv4 192.168.1.254

AC(config)#radius source-ipv4 192.168.1.254

AC(config)#aaa group server radius wlan

AC(config-sg-radius)#server 192.168.1.252

2. Under the captive portal mode, create the cp instance:

AC(config)#captive-portal

AC(config-cp)#enable

AC(config-cp)#external portal-server server-name nat ipv4 192.168.1.253 port 2000

AC(config-cp)#free-resource 1 destination ipv4 192.168.1.253/32 source any

AC(config-cp)#configuration 1

AC(config-cp-instance)#enable

AC(config-cp-instance)#radius accounting

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

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

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

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

AC(config-cp-instance)#redirect url-head http://192.168.1.253/index.jsp

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

AC(config-cp-instance)#interface ws-network 1

3. Configure the network and apply it:

AC(config-wireless)#network 1

AC(config-network)#ssid portal-nat

AC(config-network)#security mode none

AC(config-network)#exit

AC(config-wireless)#ap profile 1

AC(config-ap-profile)#radio 1

AC(config-ap-profile-radio)#vap 0

AC(config-ap-profile-vap)#network 1

AC#wireless ap profile apply 1

4. Configure the url filter rule:

AC(config)#url-filter permit 1 test.permit.com

AC(config)#url-filter deny 1 test.deny.com

AC(config)#captive-portal

AC(config-cp)#configuration 1

AC(config-cp-instance)#url-filter permit 1

AC(config-cp-instance)#url-filter deny 1

Through configuring the url filter white-list, the client can access “test.permit.com” before the authentication. Through configuring the url filter black-list, the client can forbid accessing “test.deny.com” after the authentication.

2.11.4 URL Filter Configuration Troubleshooting

If there is problem in using the url filter configuration, please check the following reasons:

- ☞ Check if the matching black-list and white-list rules are configured under the cp instance of the ssid that the client associates with. Use the command of **show running-config current-mode** to view under the portal mode.
- ☞ Check if the rule content of the cp instance is matching the domain name. Use the command of **show url-filter status** to view.
- ☞ When conducts the fuzzy matching, for the domain with “www.” as the start, “www.” should be ignored. If the domain of “www.test.com” needs to be allowed before the authentication, the rule should be configured as “url-filter permit 1 test.com”, it cannot be configured as “url-filter permit 1 *.test.com”.

2.12 Portal Non-perception

2.12.1 Introduction to Portal Non-perception

Because of the wide variety of handheld terminals, in order to ensure the compatibility, the earliest Wi-Fi access uses the Portal authentication. Through the built-in browser, to solve the access problem of the handheld terminal that it is not easy to install authentication client software. However the browser is needed to be opened in Portal authentication and enter your user name and password to access the network, resulting in lower efficiency. According to statistics, the average time of user authentication using Portal takes 2 minutes to access the network.

With the development of technology, handheld terminals are more intelligent, and installing the client software has become a very simple thing .Handheld terminal client

solves the problem of low efficiency of the Portal authentication. Just enter a user name and password, and click on the icon next time to complete the authentication without repeated input, greatly improving the efficiency of the Portal authentication.

However, this approach requires users to install the client, combined with existing networks and the use of technology as well as for the Chinese consumer behavior, the current proposed fast authentication of MAC binding technical ideas.

The fast authentication of MAC features are as follows:

(1) The user experience is improved; first-time users need the manual Portal authentication, the non-perception of authentication can be used in subsequent configuration;

(2) The terminal adaptation is good, adapting most of the WLAN terminals, without the need for adaptation client;

(3) Authentication has better compatibility, compatibility with existing Portal authentication mode.

MAC authentication has the user experience that is "a authentication, multiple use". If you opened the fast authentication of MAC, the user successfully authenticates the first landing Portal page, subsequent long associated WLAN Internet access you can use any application.

Currently known client mac authentication, the use of AC local table entries for MAC matching and require manual configuration, so the number of users that can be supported is limited, and the local mac-portal billing authentication is not required.

In order to achieve a large number of user's fast authentication of MAC, user must use an external server to save the MAC binding information, and add it dynamically but not manually. This new realization of the program is called fast authentication of MAC scheme, since the user does not need to manually enter the user name and password for authentication when access network again, also known as Portal non-perception of authentication scheme.

The specific design and implementation is shown as below:

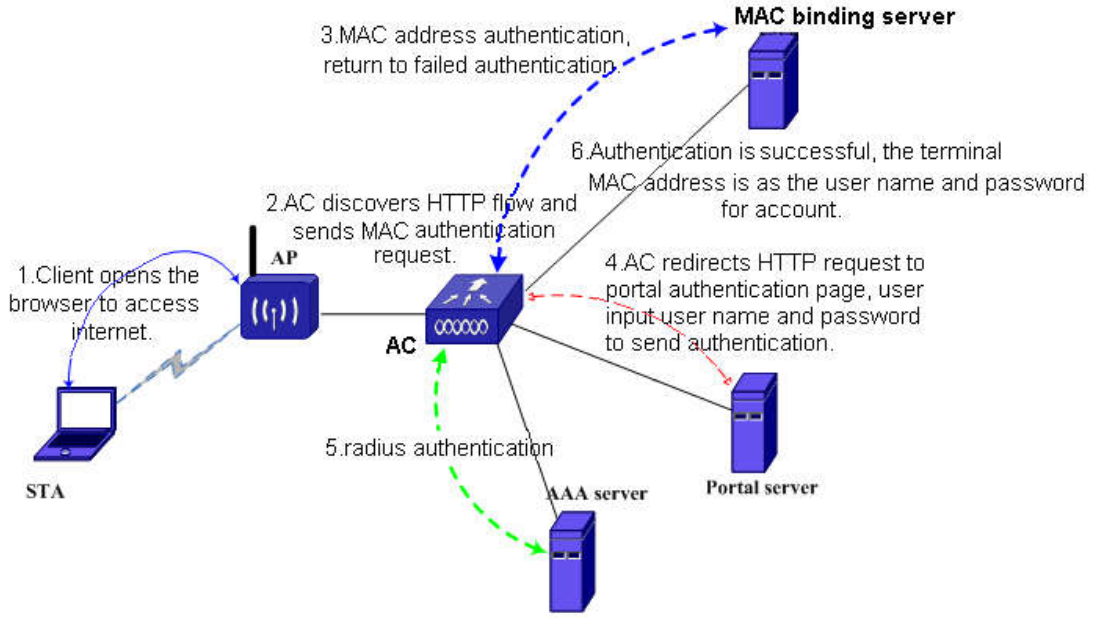


Fig 2-12 schematic diagram of the first authentication

In the Portal non-perception authentication scheme, the client for the first time to access to the WLAN authentication process, as described below:

(1) In wireless access association phase, users access the network SSID via an AP, the wireless on-line users obtain the IP address information through the DHCP server, the users access to the network, AP forwards the HTTP request to the AC.

(2) AC sends the MAC authentication request to the MAC binding server.

(3) MAC Binding server carry on the user authentication according to the packets sent by terminal, and the authentication result is returned to the AC. As terminal users for the first time connect to WLAN networks, MAC binding server has no this terminal's MAC address information, authentication fails.

(4) AC Redirects the HTTP requests to the Portal authentication page, enter your user name and password before launching Portal authentication.

(5) Complete the Portal authentication between AC and Portal server, AC and AAA server.

(6) After the user authentication is successful, the MAC Binding server will save the terminal MAC, AC sends the billing to the billing server and informs the AP to release flow; user can access the network normally.

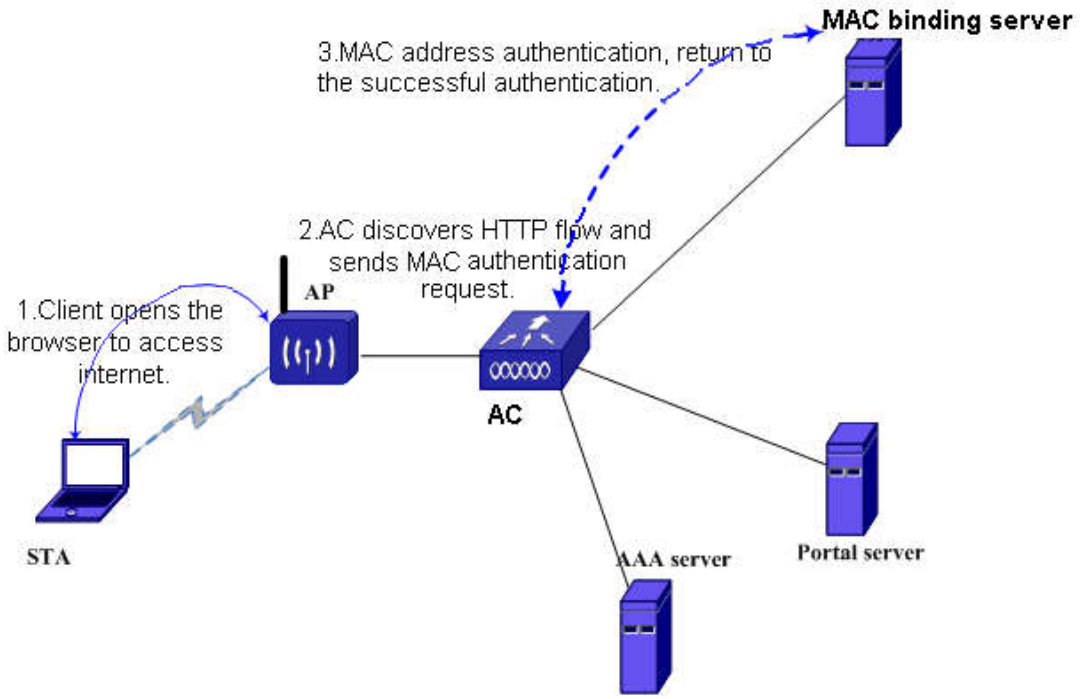


Fig 2-13 schematic diagram of the on-line authentication again

In the Portal non-perception authentication scheme, the client re-accesses WLAN network authentication process is described below:

(1) In wireless access association phase, users access the network SSID via an AP, the wireless on-line users obtain the IP address information through the DHCP server, the users access to the network, AP forwards the HTTP request to the AC;

(2) AC sends the MAC authentication request to the MAC binding server;;

(3) MAC Binding server carry on the user MAC authentication according to the packets sent by terminal, and the successful authentication result is returned to the AC. As terminal users have completed the first login, MAC binding server has this terminal's MAC address information, authentication is successful.

2.12.2 Portal Non-perception Configuration

Portal non-perception configuration task list:

1. Enable/disable the quick mac authentication function

1. Enable/disable the quick mac authentication function

Command	Explanation
Captive Portal Config Mode	
fast-mac-auth **no fast-mac-auth**	Enable/disable the quick mac authentication function.

2.12.3 Portal Non-perception Examples

The created environment is as the following figure including the parts as below:

1. AC, the unified wireless switch. It is the access management device of the entire wireless network and it manages the AP. It is the access from wireless to wired network. Multiple ACs can be added according to the requirement in the topology.

2. AP1 and AP2, wireless access point. They are managed and configured by AC.

3. STA1, the wireless user. It can access the wireless network through the AP.

4. Public network, this part can be free or other switch devices.

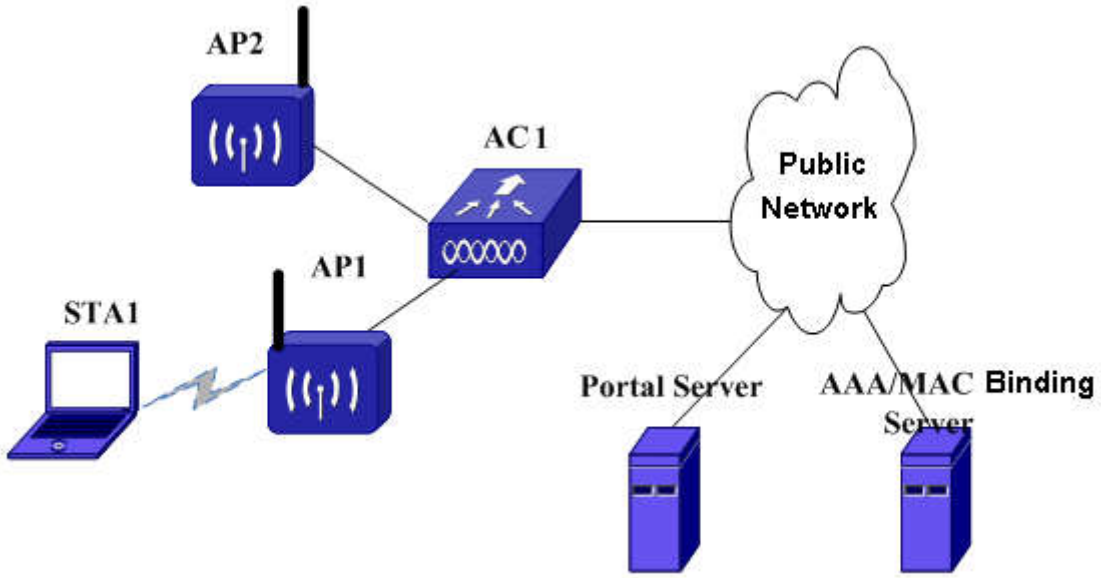
5. Server, it includes:

MAC binding server, it is used to save the authenticated terminal mac address;

Radius server, it is used for the 802.1x authentication and accounting;

Portal server, it is used for the portal authentication;

MAC binding server, Radius server and portal server can be the same one device. The mac binding server is the spread on the radius server.



Configure as the following steps:

1. Configure the related authentication key, authentication server, accounting server and aaa mode of the radius server under the global mode:

AC(config)#radius-server key 0 test

AC(config)#radius-server authentication host 100.1.1.1

AC(config)#radius-server accounting host 100.1.1.1

AC(config)#aaa-accounting ena

AC(config)#aaa enable

AC(config)#radius nas-ipv4 192.1.1.1

AC(config)#radius source-ipv4 192.1.1.1

AC(config)#aaa group server radius wlan-ac

AC(config-sg-radius)#server 100.1.1.1

2. Configure under the captive-portal mode and create the cp instance as below:

AC(config)#captive-portal

AC(config-cp)#enable

AC(config-cp)# external portal-server server-name wlan-portal ipv4 101.1.1.6 port 2000

AC(config-cp)# free-resource 1 destination ipv4 101.1.1.6/32 source any

AC(config-cp)# configuration 1

AC(config-cp-instance)# enable

AC(config-cp-instance)# radius accounting

AC(config-cp-instance)# protocol http

AC(config-cp-instance)# radius-acct-server wlan-ac

AC(config-cp-instance)# radius-auth-server wlan-ac

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

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

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

AC(config-cp-instance)# redirect url-head http://101.1.1.6/control

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

AC(config-cp-instance)# free-resource 1

AC(config-cp-instance)# interface ws-network 1

3. Configure the network1 and apply.

AC(config-wireless)#network 1

AC(config-network)#ssid mac-auth-test

AC(config-network)#security mode none

AC(config-network)#exit

AC(config-wireless)#ap profile 1

AC(config-ap-profile)#radio 1

AC(config-ap-profile-radio)#vap 0

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

AC(config-ap-profile-vap)#network 1

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

AC#wireless ap profile apply 1

4. Configure the quick mac authentication function.

AC(config)#captive-portal

AC(config-cp)#configuration 1

AC(config-cp-instance)#fast-mac-auth

After the wireless terminal is associated with the AP through SSID mac-auth-test, the normal portal authentication is needed in the first access. After the first time, user can use

the non-perception authentication of portal.

2.12.4 Portal Non-perception Troubleshooting

Please check if the reasons are the following situations when there are problems in using the function of portal non-perception:

- ☞ Check whether the captive-portal function is enabled.
- ☞ Check whether the quick mac authentication function is enabled.
- ☞ Check whether issued the configuration to AP if the quick mac authentication is not effective after configured.

2.13 Portal Escaping

2.13.1 Introduction to Portal Escaping

There is a risk in the current portal application. When the communication between the access device and portal server is broken, the new user cannot get on-line and the on-line user cannot get down; and the information of the access device and portal server is inconsistent. This will bring the accounting error. These phenomenons can bring the inconvenience to the operations and users.

The portal escaping function provides a good method to solve the above problems. It can make the user on-line and use the network normally when the portal server cannot working normally, and the new user can still access the network. It reports the fault through the log and trap.

The principle of portal escaping function is that: AC probes the portal server periodically. If the probing is successful, the server status will be configured as UP; if the probing failed N times (N can be configured), it will change the status of unreachable to be DOWN (escaping status), cancel the network authentication limit, allow the portal user accessing the network without authentication and send the trap and log information of the status changing. When it probes the server is reachable, it will recover the server status to be UP (authentication status), restart the network authentication limit, reject the user without authentication accessing the network and send the log and trap information of the status recovering.

The method that AC probes the portal server status is probing the TCP connection: AC launches the TCP connection to the portal server port of the portal server (the default is 2000, it can be configured) regularly. If the connection is successful, it means that this portal server is enabled, we consider that the probing is successful and the server is reachable (the status is UP); if the connection failed, we consider the probing failed.

Probing interval and maximum number of probing failures: the interval of the probing

can be configured through the command. The maximum number of probing failures means that the probing failures before that the server is reachable. One probing failure does not mean that the server is unreachable; user should view if the number of the probing failures achieves the configured maximum value. If the number achieves the configured value, the server can be considered as unreachable; otherwise, the number is just cumulative. After that the probing is successful, this number will be cleared to be 0. The probing interval and maximum number of probing failures can be configured through the command.

The server triggers the following three configurations when the status changes from reachable to unreachable, the administrator can select through the configuration:

- Send trap: send the trap information 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.
- Send log: send the log information to the log server. In the log, 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).

The server triggers the following three configurations when the status changes from unreachable to reachable. “Send trap” and “send log” can be selected through the configuration; “Disable portal escaping” is enforced to carry on:

- Send trap: send the trap information 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.
- Send log: send the log information to the log server. In the log, it records the portal server name and the status information before and after the change of the server status.
- Disable portal escaping: If the portal server status changes to the reachable status (up), the portal authentication function of VAP will be recovered. The new user must pass the portal authentication for accessing the network.

Notice: The portal escaping function can only achieve that the new and old users are not affected when accessing the network currently. For the situation that user cannot get down the line normally, there are other methods such as user flow monitoring function. When the user flow is monitored less than the threshold, the access device will enforce the user to get down the line. The wireless part of AP also provides the silent terminal

detection, these can ensure that user can get down the line normally.

2.13.2 Portal Escaping Configuration

Portal escaping function configuration task list:

1. Enable the Portal escaping function and configure the probing interval and maximum number of failures.
2. Show the current connection status of the Portal server.

1. Enable the Portal escaping function and configure the probing interval and maximum number of failures

Command	Explanation
Captive Portal Global Configuration Mode	
portal-server-detect server-name <name> [interval <interval>] [retry <retries>][action {log | permit-all | trap }] **no portal-server-detect server-name <name>**	Enable the Portal server escaping function and configure the related parameters (selectable) and the server configuration of status changing.

2. Show the current connection status of the Portal server

Command	Explanation
Admin Mode	
show captive-portal ext-portal-server server-name <name> status	Show the portal server status including the server address and if the portal escaping function is enabled.

2.13.3 Portal Escaping Examples

Typical case:

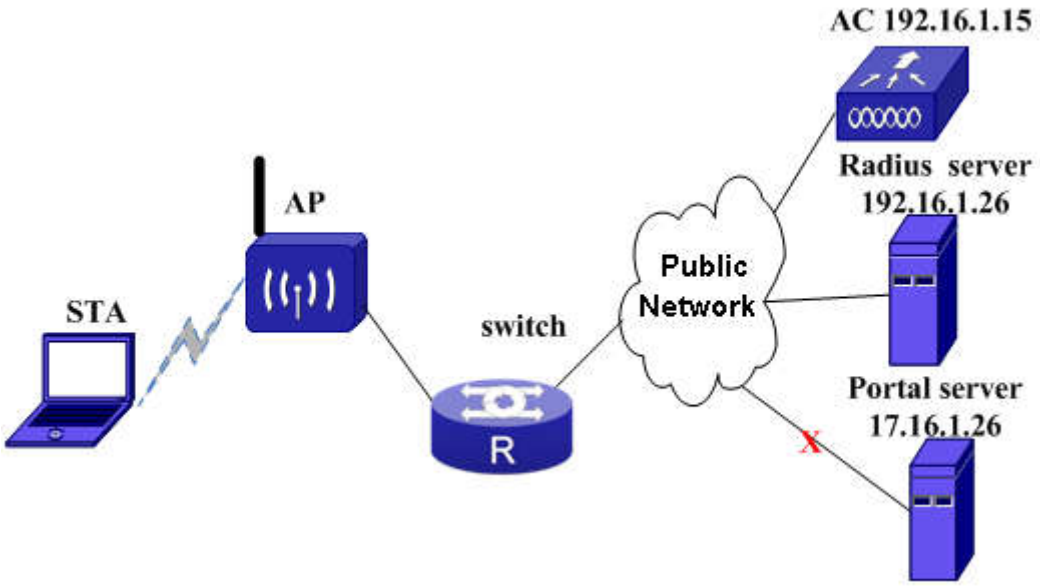


Fig 2-14 Portal escaping function case

As shown above, in the situation of the normal working of portal server, the portal authentication can be normal for the network accessing when STA is on-line. When the portal server is down or the connection between it and AC is broken, STA cannot authenticate to on-line if the portal escaping function is not enabled on AC. If the portal escaping function is enabled on AC, AC can probe that the portal server is unavailable and start the portal escaping function. And the STA can access the network without authentication. If STA has passed the authentication before the portal server is broken, it will not be affected and it can still access the network.

The configuration is as below:

1. Configure the related authentication key, authentication server, accounting server and aaa mode of the RADIUS server in global mode.
   AC(config)#radius-server key 0 test
   AC(config)#radius-server authentication host 192.16.1.26
   AC(config)#radius-server accounting host 192.16.1.26
   AC(config)#aaa-accounting enable
   AC(config)#aaa enable
   AC(config)#radius nas-ipv4 192.16.1.15
   AC(config)#radius source-ipv4 192.16.1.15
   AC(config)#aaa group server radius cmcc
   AC(config-sg-radius)# server 192.16.1.26
2. The configuration under the captive-portal mode is as below, create the cp instance.
   AC(config)#captive-portal
   AC(config-cp)#enable
   AC(config-cp)#external portal-server server-name cmcc ipv4 17.16.1.26 port 2000

AC(config-cp)#free-resource 1 destination ipv4 17.16.1.26/32 source any

AC(config-cp)#configuration 1

AC(config-cp-instance)#enable

AC(config-cp-instance)#radius accounting

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

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

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

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

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

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

AC(config-cp-instance)#interface ws-network 1

3. Configure the network1 and apply.
   AC (config-wireless)#network 1

   AC (config-network)#ssid portal-detect-test

   AC (config-network)#security mode none

   AC (config-wireless)#ap profile 1

   AC (config-ap-profile)#radio 1

   AC (config-ap-profile-radio)#vap 0

   AC (config-ap-profile-vap)#network 1

   AC#wireless ap profile apply 1

4. Configure the portal escaping.
   AC (config)#

   AC(config-cp)#enable

   AC(config-cp)# portal-server-detect server-name cmcc interval 600 retry 2 action log permit-all trap

As shown above, the portal server of cmcc is bound to CP instance and the probing function is configured; the probing interval is 600s. If the probing failed twice, send the trap information and log of the unreachable server and the enable the portal escaping function to allow the user without authentication accessing the network.

2.13.4 Portal Escaping Troubleshooting

In using, please adopt the following methods if the portal escaping function cannot be effective.

- Find the corresponding network according to the SSID connected by user and find the corresponding captive portal instance of the network; and then find the portal server that this instance used. Use the command of **show captive-portal ext-portal-server server-name <name> status** to check if the detect mode of the portal server is “enable”. If it is not “enable”, it means that the portal server

escaping function is not enabled, please enable it.

- ☞ If the portal escaping function is enabled, check if the Detect Operational Status is down. Only when the server status is down, the portal escaping function can be enabled.
- ☞ If the portal server status is down, there may be the problem in the synchronization between AC and AP, use **wireless ap reset** to restart the AP remotely.
- ☞ If the AP reconnection failed, and the escaping function cannot be effective, the device may have the problem. Please contact to the sales engineers.

2.14 Two-dimension-code Authentication

2.14.1 Introduction to Two-dimension-code Authentication

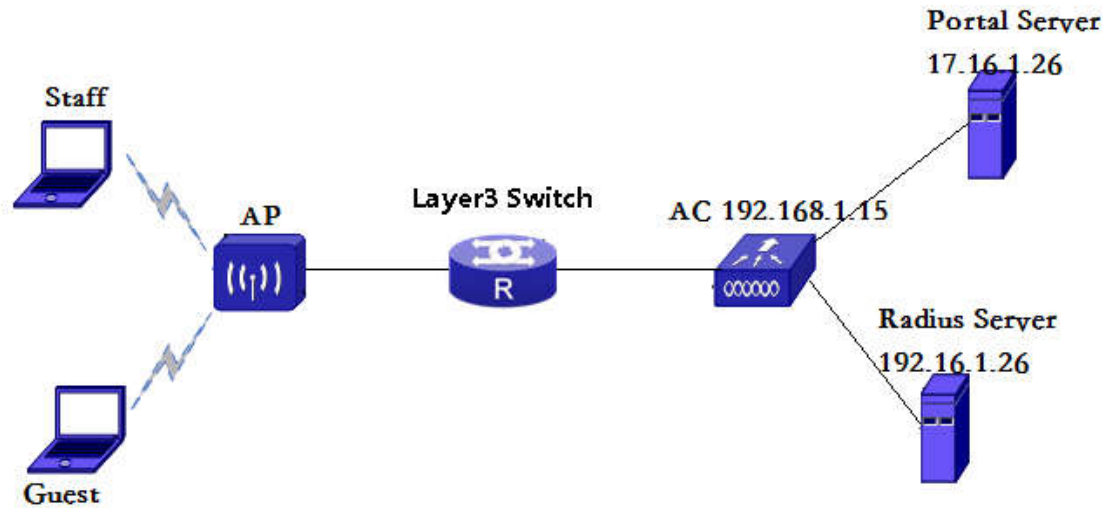
The Two-dimension-code is mainly used in school, restaurant, enterprise and otherplaces where is frequented by visitors, it is a kind of secure wireless accessing authentication method. When there is someone visits the network or the specified network, the ssid which is different to the staffs or teachers will be used for accessing. Guest can input the target network address and a two-dimension-code will be disappeared. The staff or teacher who has been authenticated can scan the two-dimension-code and an URL will be disappeared. Clicking the URL can allow the guest accessing.

2.14.2 Two-dimension-code Authentication Configuration

1. Enable/Disable the two-dimension-code authentication function.

Command	Explanation
Captive Portal Config Mode	
two-dimension-code enable **two-dimension-code disable**	Enable the two-dimension-code authentication function, the disable command disables it.

2.14.3 Two-dimension-code Authentication Example



As shown in the picture, there is a staff and a guest accessing respectively, Portal Server is used for authentication, Radius Server is used for accounting. For distinguishing the portal page of the guest and staff, two different SSID are configured on AC which are portal-staff and portal-guest. They make the different users use the different VLAN to connect to the Internet. When the staff or guest connects to the Internet, the portal server can recommend different portal pages according to the different VLAN in client network card. It can ensure that the staff can take the standard portal authentication and the guest can take the two-dimension-code authentication. The two-dimension-code of guest needs the authorization by the authenticated staff.

The configuration is as below:

1. Configure the authentication key, authentication server, accounting server, aaa mode, etc of the RADIUS server under the global mode:
   AC(config)#radius-server key 0 test
   AC(config)#radius-server authentication host 192.16.1.26
   AC(config)#radius-server accounting host 192.16.1.26
   AC(config)#aaa-accounting enable
   AC(config)#aaa enable
   AC(config)#radius nas-ipv4 192.16.1.15
   AC(config)#radius source-ipv4 192.16.1.15
   AC(config)#aaa group server radius cmcc
   AC(config-sg-radius)# server 192.16.1.26
2. Create the cp instance under the captive-portal mode:
   AC(config)#captive-portal
   AC(config-cp)#enable
   AC(config-cp)#external portal-server server-name cmcc ipv4 17.16.1.26 port 2000
   AC(config-cp)#free-resource 1 destination ipv4 17.16.1.26/32 source any

AC(config-cp)#configuration 1

AC(config-cp-instance)#enable

AC(config-cp-instance)#two-dimension-code enable

AC(config-cp-instance)#radius accounting

AC(config-cp-instance)# protocol http

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

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

AC(config-cp-instance)# redirect attribute url-after-login enable

AC(config-cp-instance)# redirect attribute url-after-login encode base64

AC(config-cp-instance)# redirect attribute url-after-login name redirect

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

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

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

AC(config-cp-instance)# redirect attribute ssid value vlan

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

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

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

AC(config-cp-instance)#interface ws-network 112

AC(config-cp-instance)#interface ws-network 113

AC(config-cp-instance)# free-resource 1

3. Configure the staff network 112 and the guest network 113, and apply them.
   AC (config-wireless)#network 112

   AC (config-network)#ssid portal-staff

   AC (config-network)#security mode none

   AC (config-network)#quit

   AC (config-wireless)# network 113

   AC (config-network)#ssid portal-guest

   AC (config-network)#security mode none

   AC (config-network)#quit

   AC (config-wireless)#ap profile 1

   AC (config-ap-profile)#radio 1

   AC (config-ap-profile-radio)#vap 0

   AC (config-ap-profile-vap)#network 112

   AC (config-ap-profile-vap)#vap 1

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

   AC (config-ap-profile-vap)#network 113

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

   AC#wireless ap profile apply 1

4. Connect the staff and guest to the portal-staff and portal-guest respectively. The user

state can be viewed on AC.

AC#show captive-portal client status

The portal server cmcc is bound to CP instance. The matched hot spot server versions (portal server and radius server) are need for completing the two-dimension-code authentication. The root of RS server must be upgraded to the new version which supports the two-dimension-code authentication function.

2.14.4 Two-dimension-code Authentication Troubleshooting

If the two-dimension-code authentication function is not effective in using, please adopt the following steps to check it, but the premise is that the external portal authentication function is effective.

- ☞ Whether the address and port of the DCSM-BW are correct in the E-portal server management system.
- ☞ Whether the AC information is added in the advanced configuration in the Portal server management system.
- ☞ Whether the matching method is configured as VLAN in the template of Portal authentication scheme. The VLAN in configuration 1 should be the one of Guest.
- ☞ Whether the user and password are created in the DCSM authentication and accounting management system.

2.15 Wechat Authentication

2.15.1 Introduction to Wechat Authentication

The wechat is used widely, so the client suggests providing the wechat authentication for network in the third authentication. After connected SSID, the traffic is limited, only some of the white lists are allowed, including the wechat traffic. User can pay attention to the specific official account, choose the way for accessing the network and visit the network. For the external portal authentication, the wechat authentication is very flexible.

2.15.2 Wechat Authentication Configuration

1. Configure the URL head of the thirdpart authentication discovery packet under the global mode.
2. Configure the IPv4 address of the thirdpart server under the global mode.
3. Configure the redirected URL mode of the thirdpart agency under the Captive-portal mode.

4. Configure the URL of the page after the successful thirdpart authentication under the Captive-portal mode.

5. Configure the URL name in the redirected packet of captive portal under the Captive-portal mode.

6. Configure AC to carry through the wechat authentication under the Captive-portal mode. (Distinguish it from the switch device)

1. Configure the URL head of the thirdpart authentication discovery packet under the global mode

Command	Explanation
Global Mode	
thirdpart-auth discover url-head	Configure the URL head of the thirdpart authentication discovery packet. The no command deletes it.

2. Configure the IPv4 address of the thirdpart server under the global mode

Command	Explanation
Global Mode	
thirdpart-auth server-ipv4	Configure the IPv4 address of the thirdpart server. The no command deletes it.

3. Configure the redirected URL mode of the thirdpart agency

Command	Explanation
Captive-portal instance mode	
redirect url-mode thirdpart-auth	Configure the redirected URL mode of the thirdpart agency. The no command deletes it.

4. Configure the URL of the page after the successful thirdpart authentication

Command	Explanation
Captive-portal instance mode	
redirect attribute url-after-login weixin	Configure the URL of the page after the successful thirdpart authentication. http://www.dcme.net.cn/portal must be configured in the wechat authentication. The no command deletes it.

5. Configure the URL name in the redirected packet of captive portal

Command	Explanation
Captive-portal instance mode	
redirect attribute url-after-login name url	Configure the parameter name in the redirected packet of captive portal. Only url is received, the srcurl is received in the no command.

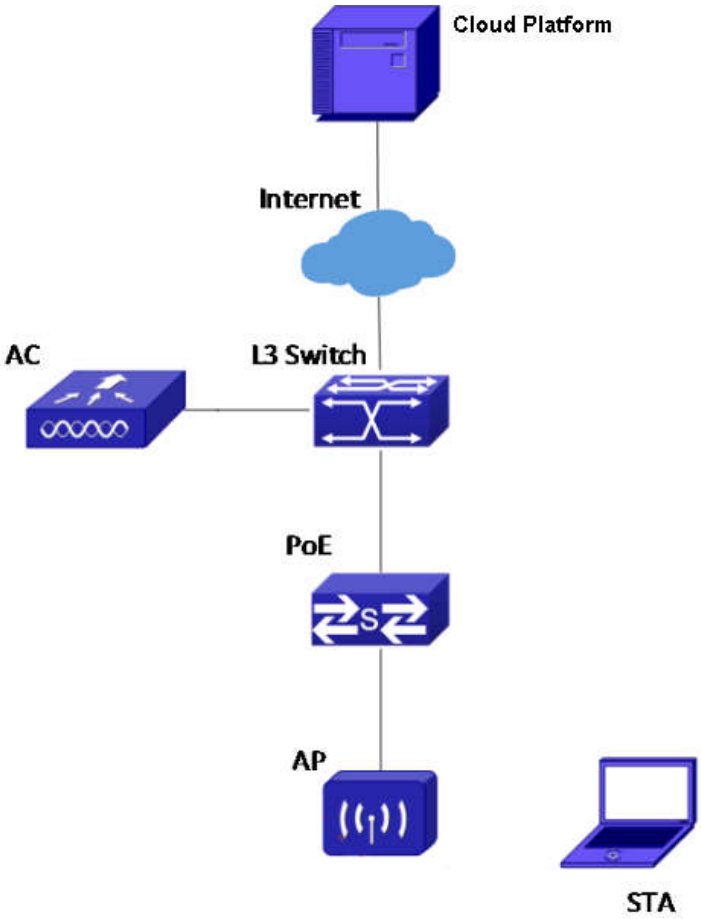
6. Configure AC to carry through the wechat authentication

Command	Explanation
Captive-portal instance mode	
redirect attribute custom-string name devicetype=6028	Configure the URL property of the captive portal redirected packet. 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.

2.15.3 Wechat Authentication Examples

Case:

As shown below, after AC logins on the cloud platform successfully, connect SSID with the phone, open the official account, and click “mobile Internet”, the browser will show the successful authentication page, and then this mobile can search the Internet. If connects SSID with notebook PC, the pushed page will reminder user to input the auth code. We can open the official account with the mobile, click “PC Internet” and get the auth code, and then provide this auth code to the PC user, the user can input it for successful authentication.



Configuration under the global mode:

thirdpart-auth discover url-head http://www.dcme.net.cn/dreg/status

thirdpart-auth server-ipv4 115.29.96.60

url-filter permit 1 *weixin.qq.com

url-filter permit 2 *apple.com

url-filter permit 3 *qq.com

Configuration under the captive-portal mode:

captive-portal

enable

nas-ipv4 172.30.0.252

free-resource 1 destination ipv4 115.29.96.60/32 source any

configuration 1

enable

redirect url-mode thirdpart-auth

redirect attribute url-after-login weixin http://www.dcme.net.cn/portal

redirect attribute url-after-login enable

redirect attribute url-after-login name url

redirect attribute nas-ip enable

redirect attribute usermac enable
redirect attribute nas-ip name gw
redirect attribute usermac name mac
redirect attribute custom-string name devicetype=6028
redirect url-head http://www.dcme.net.cn/auth
free-resource 1
url-filter permit 1
url-filter permit 2
url-filter permit 3
interface ws-network 1

2.15.4 Wechat Authentication Troubleshooting

- When AC cannot login successfully on the cloud platform, please check if the added MAC address is the CPU MAC of AC.
- After AC logins successfully, if the IP address is always 0.0.0.0, please use the command of **debug thirdpart-auth trace** and **debug thirdpart-auth packet all** to check if the keep-alive packet between the cloud platform and AC is normal.

Chapter 3 WAPI Access and Authentication

3.1 Introduction to WAPI

3.1.1 WAPI Overall Description

WAPI is the short form of WLAN Authentication and Privacy Infrastructure. It is using the 802.11wireless protocol, which bring forward by China, as the foundation of wireless safety standard. WAPI protocol is composing by 2 different parts:

WAI is the short form of WLAN Authentication Infrastructure. It is using for the authentication on the wireless network and safety scheme for the secret key management.WAI uses the open secret key and password system, and using the certificate to undergo the STA and AP authentication in the WLAN system. WAI has defined an ASU（Authentication Service Unit）entity, which is using for managing and information exchange for obtaining certificate (including issue, award, revoke and renew). Certificate including the ASU's and holder key and signature (using the WAPI signature method) which is the internet number warrant. WPI is the short form of WLAN Privacy Infrastructure, which is using for the security scheme of data transmission on the wireless network, including data encrypt , data distinguish and playback protection function.

3.1.2 WAPI System Composition

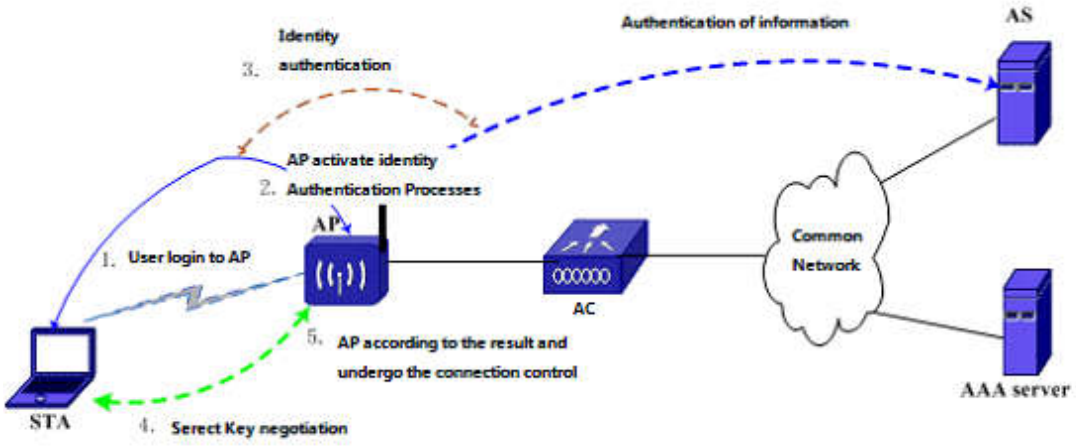


Fig 3-1 WAPI Authentication system

As show in the above figure, the whole authentication including certificate and secret key negotiation two parts:

1. When STA visit to LAN, first need to login to AP and build up the linkage;
2. After AP login to STA, AP sends the authentication frame to STA, and startup the whole authentication processes.
3. STA will send the acceptation of authentication request to AP, and send the user certificate to AP; AP will then send the STA and AP certificates with the AP signature to AS. AS will authenticate the AP signature and then validity of AP and STA certificates, and send the signature to AP. AP will send the AS authentication result to STA，AP and STA will authenticate the signature separately, and obtain the certificate result, if the certificate authentication is success, AP and STA need to authenticate others secret key, to ensure they are the legal holder of certificates. At the same time, they will undergo the conversational secret key negotiation.
4. AP and STA negotiation is using as the secret key of data communication.
5. AP and STA will accord the authentication result to control the network visiting. If the authentication is success, STA can visit the network.

3.1.3 WAPI Certificate Authentication

WAPI supports two authentication methods: certificate authentication mode and pre-sharing secret key authentication mode.

Numeric certificate is a type of certificate that through PKI（Public Key Infrastructure）for signing in the authorization center, including public key and the user related information, which is a numeric identity of the internet user. The user certificate that is

Using in the WAPI system is the numeric certificate. Through the AS to undergo the authentication of the user certificate, can only ensure the WAPI user identity and legality. Certificate authentication is base on both STA and AP certificates for authentication. Before the authentication, STA and AP need to obtain their own certificate, and throughout the identity authentication on AS and produce temporary public key and BK of temporary private key. And then get the perpetration for the signal broadcast and group broadcast secret key notices. The certificate authentication processes as shown on the following fig.

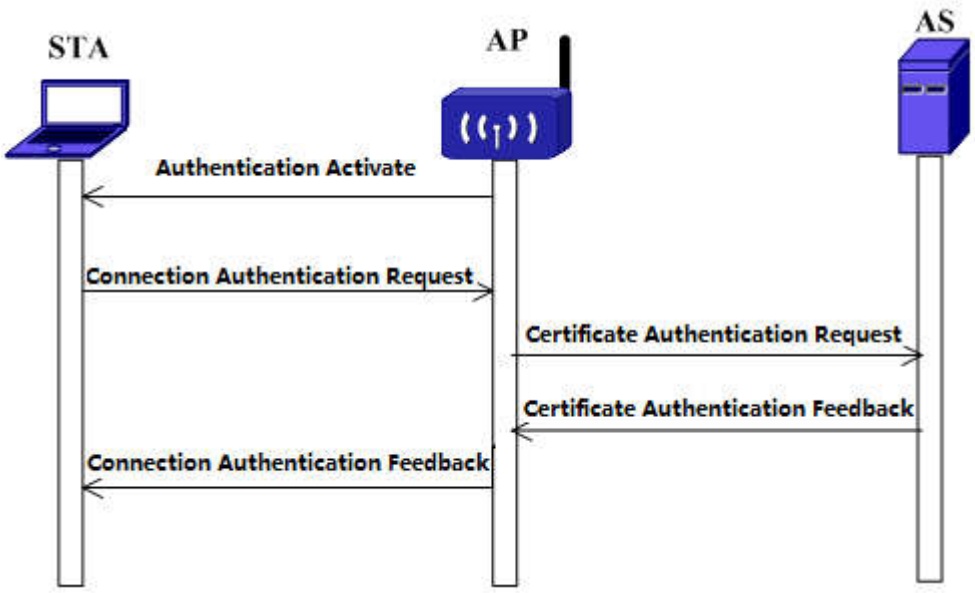


Fig 3-2 Certificate Authentication processes

The figure show as above is the certificate distinguish authentication processes, after the certificate distinguish processes is finished, AP and STA will undergo the signal broadcast and group broadcast secret key notices processes.

3.1.4 WAPI Pre-sharing Key Authentication

Pre-sharing secret key authentication is no need to follow the processes that show on the figure above. Pre-sharing secret key authentication is based on secret key of STA and AP both side for authentication. Before the authentication, STA and AP need to pre-set the same secret key, which is sharing secret key. Under this authentication, once STA through the link to connect with AP, AP will initiate the secret key negotiation request. AP and STA will undergo the signal broadcast and group broadcast secret key notices processes.

3.1.5 WAPI Working Processes

On the WLAN that has adopted the WAPI security related system, once STA need to visit that WLAN, will through the passive interception AP Beacon frame or active quizzical frame (the process as following Fig.) to recognize the security strategy that adopt by AP:

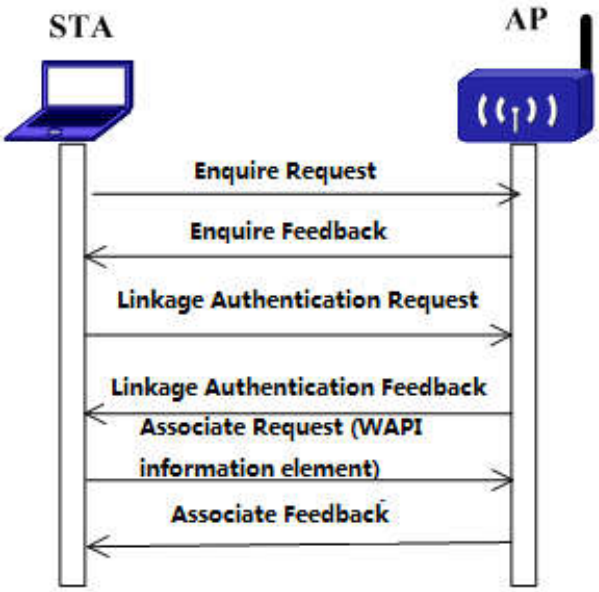


Fig 3-3 Active quizzical process

If AP adopt the certificate authentication method, AP will send the authentication activate to initiate the certificate authentication processes by group. After the certificate authentication finished, AP and STA will undergo the one way broadcast for secret key negotiation and group broadcast secret key notification.

If AP adopts the pre-sharing secret key authentication, AP will undergo the secret key negotiation and group broadcast secret key notification to STA directly.

Following is the WAPI working processes under the certificate authentication:

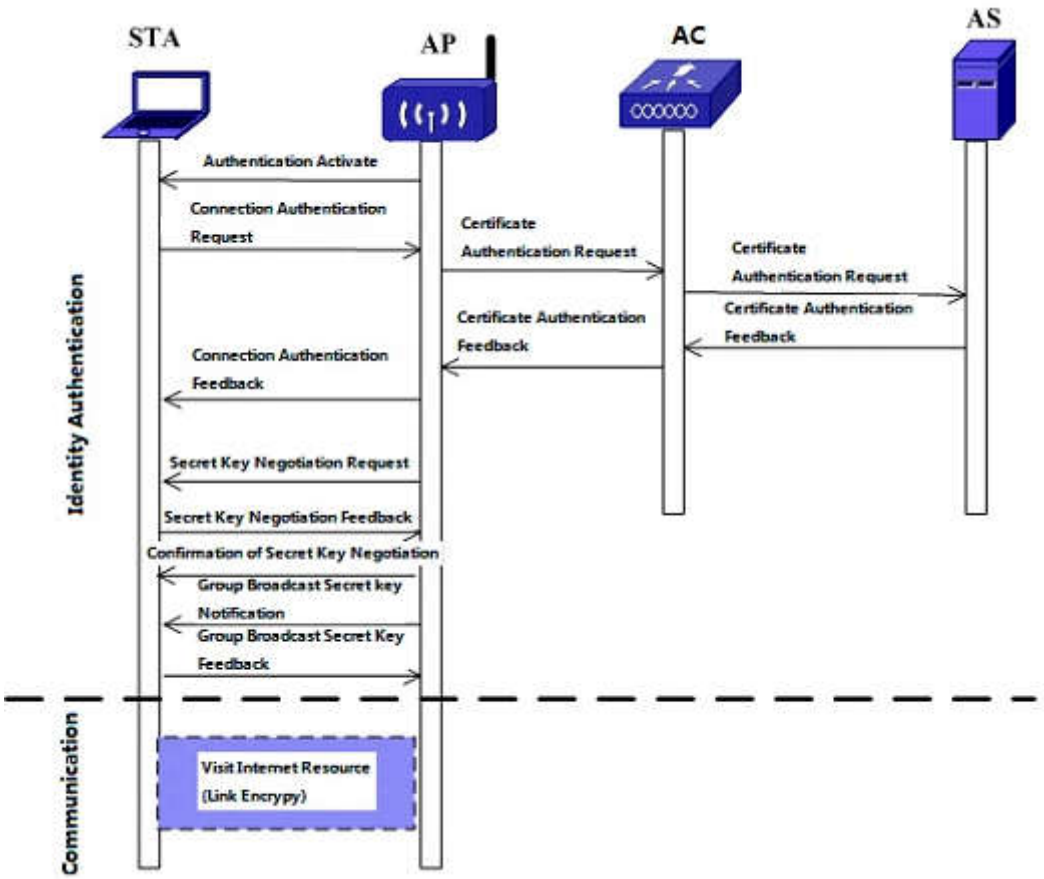


Fig 3-4 WAPI Authentication Processes

1. Authentication Activate. Once STA associate with AP, AP will send Authentication activate to STA in order to initiate the entire authentication processes.
2. Receive the authentication. STA will send connection authentication to AP; it means STA certificate will send to AP at STA system time. The system time calls connection authentication request time.
3. Certificate authentication request. Once AP receive STA connection authentication, it will send the certificate authentication request to AS (AP will send this request to AC and then forward to AS), that is STA certificate, connection authentication request time, AP certificate and AP secret key Authentication request message to AS.
4. Certificate authentication feedback. AS receives AP certificate authentication request, first it will authenticate AP signature. If it is not correct, the authentication is fail. Otherwise, it will continuous authenticate the validity of AP and STA. After the authentication is finished, AS will send the STA certificate authentication result (including STA certificate, authentication result, AS signature), AP certificate authentication result information (including AP certificate, authentication result, connection authentication request time and AS signature) to form certificate authentication feedback message to AC, and it send to AP.
5. Connection authentication feedback. AP will accord to AS certificate feedback to undergo the signature authentication and obtain the STA certificate

authentication result. AP will send the feedback information to STA. STA authenticate the AS signature, and then obtain the AP certificate authentication result. STA will accord to the result to decide whether connect AP or not.

6. Secret key Negotiation Request. If the STA certificate authentication is success, AP will send the secret key negotiation request; including the STA public key encrypt data and AP signature information and calculation method.
7. Secret key negotiation feedback. Once STA receive the secret key negotiation feedback, it will authenticate the AP signature. After it is passed, it will generate the secret key data and using AP public key to encrypt and send back to AP. Both parties using secret key negotiation data to generate the one way broadcast secret key.
8. Group Broadcast Secret key notification. One way broadcast negotiation successes, AP will send group broadcast notification to STA, and inform AP to send group broadcast data information encrypt secret key.
9. Group Broadcast feedback. STA authenticate the validity of the notification that is sending by AP, it will provide feedback to AP.

STA and AP will finish the identity authentication processes. If the authentication is success, AP will allow STA connect with it, otherwise, it will delete the association.

3.2 WAPI Configuration

3.2.1 Commands for Global Configuration

1、Enable/disable global wapi function

Command	Explanation
Wireless Global Mode	
wapi enable **no wapi enable**	Enable global wapi function. The no command disables this function. Use **show wireless wapi status** command to check whether the global wapi function is enabled.

2、Configure/delete wapi certificate authentication server

Command	Explanation
Wireless Global Mode	

wapi authentication-server <1-5> <ipAddr> [port <0-65535>] **no wapi authentication-server [<1-5>]**	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.

3、Configure timeout of AS server response

Command	Explanation
Wireless Global Mode	
wapi authentication-server timeout <1~1000> **no wapi authentication-server timeout**	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.

4、Configure the retransmission times of AC sending requisition to AS

Command	Explanation
Wireless Global Mode	
wapi authentication-server retransmit<0~100> **no wapi authentication-server retransmit**	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.

5、Configure the certificate format when using wapi certificate authentication method

Command	Explanation
Wireless Global Mode	
wapi certificate format *{gbw | x509}* **no wapi certificate format**	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.

6、Configure the certificate mode when using wapi authentication method

Command	Explanation
Wireless Global Mode	
wapi certificate-mode *{2|3}* **no wapi certificate-mode**	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.

7、Enable/disable wapi traps function globally

Command	Explanation
Global Mode	
snmp-server enable traps wapi **no snmp-server enable traps wapi**	Use this command to enable wapi traps function. (Enable snmp-server and global traps function firstly.) The no command disables all wapi traps function.

3.2.2 Commands for Network Configuration

1、Configure the authentication and encryption method that network supports

Command	Explanation
Network Configuration Mode	

security mode {none | static-wep | wep-dot1x | wpa-enterprise | wpa-personal|wapi-certificate|wapi-psk} **no security mode**	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.

2、Configure the ipv4 AS number value used by network when it uses wapi certificate authentication method

Command	Explanation
Network Configuration Mode	
wapi authentication-server <1-5> **no wapi authentication-server**	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.

3、Configure the BK updating frequency of network when it uses wapi authentication method

Command	Explanation
Network Configuration Mode	
wapi bk-refresh-rate *<0,30-43200>* **no wapi bk-refresh-rate**	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.

4、Enable/disable the function that the downline user triggers MSK updating

Command	Explanation
Network Configuration Mode	

wapi msk-refresh client-offline **no wapi msk-refresh client-offline**	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.

5、Configure the MSK updating frequency when network uses wapi authentication method

Command	Explanation
Network Configuration Mode	
wapi msk-refresh-rate {packet-based <30-86400>|} { time-based <30-86400>|} **no wapi msk-refresh-rate**	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.

6、Configure the pre-shared key of network when it uses wapi psk authentication method

Command	Explanation
Network Configuration Mode	
wapi psk *{ciper | pass-phrase}* *<value>* **no wapi psk**	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.

7、Configure the key length when the network uses wapi psk authentication method

Command	Explanation
Network Configuration Mode	
wapi psk length <*8-64*> **no wapi psk length**	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.

8、Configure the key type when the network uses wapi psk authentication method

Command	Explanation
Network Configuration Mode	
**wapi psk type *{ascii*	*hex}*** **no wepkey type**	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.

9、Configure the USK updating frequency when the network uses wapi psk authentication method

Command	Explanation
Network Configuration Mode	
wapi usk-refresh-rate {packet-based <30-86400>|} { time-based <30-86400>|} **no wapi usk-refresh-rate**	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.

3.2.3 Commands for AP database

1、Configure the certificate file name of AP itself in ap database

Command	Explanation
Ap Database Configuration Mode	
wapi certificate ap <*name*> **no wapi certificate ap**	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.

2、Configurethe certificate file name of AS server related to AP in ap database

Command	Explanation
Ap Database Configuration Mode	
wapi certificate as <*name*> **no wapi certificate as**	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.

3、Configure the CA root certificate file related to AP in ap database

Command	Explanation
Ap Database Configuration Mode	

wapi certificate ca <*name*> **no wapi certificate ca**	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.

3.2.4 Commands for Admin

1、Clear wapi statistic information of the appointed AP or all APs

Command	Explanation
Previlidged EXEC Mode	
clear wireless wapi ap [<macaddr>] statistics	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.

2、Import the certificates of AP, AS and CA to AC manually

Command	Explanation
Previlidged EXEC Mode	
copy wapi-certificate <*source-url*> <*destination-url*>	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.

3、Show the information of network wapi configuration

Command	Explanation
Previlidged EXEC Mode	
show wireless network <*1-1024*> wapi status	Use this command to inquiry network configuration and show the wapi configuration parameters.

4、Show the wapi statistic information of ap

Command	Explanation
Previlidged EXEC Mode	

show wireless wapi ap <*macaddr*> statistics	Show the wapi statistic information of ap with the appointed MAC address.

5、Show the status of AP installing certificate

Command	Explanation
Previlidged EXEC Mode	
show wireless wapi ap-certificate [<macaddr>] status	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.

6、Show AS information of global wapi configuration

Command	Explanation
Previlidged EXEC Mode	
show wireless wapi authentication-server status	Use this command to show AS information of global wapi configuration.

7、Show global wapi information

Command	Explanation
Previlidged EXEC Mode	
show wireless wapi *status*	Show global wapi information.

8、Issue the certificate file to the AP with appointed MAC address or all managed APs

Command	Explanation
Previlidged EXEC Mode	
wapi certificate- distribute [<macaddr>]	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.

3.2.5 Commands for Debug

1、Enable/disable the error debug on-off in client wapi authentication

Command	Explanation
Previlidged EXEC Mode	

debug wireless wapi error **no debug wireless wapi error**	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.

2、Enable/disable the internal detailed debug on-off in client wapi authentication

Command	Explanation
Previlidged EXEC Mode	
debug wireless wapi internal *<macaddr>* **no debug wireless wapi internal *<macaddr>***	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.

3、Enable/disable the debug information in client wapi authentication

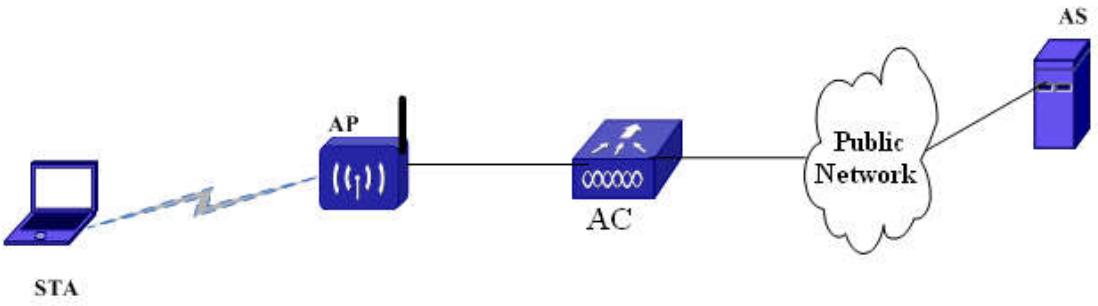
Command	Explanation
Previlidged EXEC Mode	
debug wireless wapi packet*{all* | *receive* | *send* | *dump}* *<macaddr>* **no debug wireless wapi packet *{all* | *receive* | *send* | *dump}* *<macaddr>***	Use this command to enable the debug information in client wapi authentication. User can examine the packets debug information in client wapi authentication on AC controller platform. The no command disables the debug information.

4、Enable/disable the track debug on-off in client wapi authentication

Command	Explanation
Previlidged EXEC Mode	
debug wireless wapi trace *<macaddr>* **no debug wireless wapi trace *<macaddr>***	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.

3.3 WAPI Configuration Example

3.3.1 WAPI Configuration Example Topology



1. AC is unifying wireless switch. It is the whole wireless network connection management facility. The system can add more than one AC as needed.
2. AP, wireless connection point, configures and manages by AC.
3. STA, wireless user, throughout AP to connect with wireless network.
4. Common network, this part can be omitted, is the other switch facility.
5. AS server, using for undergo the WAPI certificate authentication to the user (if it uses the pre-sharing secret key mode, AS does not need to participate).

3.3.2 WAPI Two Certificate Mode Example

3.3.2.1 Introduction to Example

Configure SSSDI as “WAPI_102_2certificate”, second layer using WAPI certificate configuration method and the certificate adopt the two certificate mode. After the set up, the wireless user can connect to “WAPI_102_2certificate” to visit the internet.

3.3.2.2 Configuration Processes

1、 Open the global wapi function, configure the two certificate mode, configure the wapi authentication server ip address as 194.168.1.200.

AC(config-wireless)#wapi enable
AC(config-wireless)#wapi certificate-mode 2
AC(config-wireless)#wapi authentication-server 1 ip 194.168.1.200

2、 Login the AS server, download the AS certificate: as20120625.cer. Apply AP certificate: AP20120625.cer and STA certificate: STA20120625.cer.

3、 Export the AS and AP certificates to AC

AC#copy wapi-certificate tftp://194.168.1.203/as20120625.cer as20120625.cer
AC#copy wapi-certificate tftp://194.168.1.203/AP20120625.cer AP20120625.cer

4、 Configure certificate document to managed AP

AC(config-wireless)#ap database 00-03-0f-01-0b-80

AC(config-ap)#wapi certificate ap AP20120625.cer
AC(config-ap)#wapi certificate as as20120625.cer

5、Sending certificate document to managed AP
AC#wapi certificate-distribute

6、Configure SSID：WAPI_102_2certificate
AC#config
AC(config)#wireless
AC(config-wireless)#network 102
AC(config-network)#security mode wapi-certificate
AC(config-network)# ssid WAPI_102_2certificate
AC(config-network)# wapi authentication-server 1
AC(config-network)#exit
AC(config-wireless)#ap profile 1
AC(config-ap-profile)#radio 1
AC(config-ap-profile-radio)#vap 0
AC(config-ap-profile-vap)#network 102
AC(config-ap-profile-vap)#enable
AC(config-ap-profile-vap)#end
AC#wireless ap profile apply 1

7、After the wireless user installed the AS certificate: as20120625.cer, STA certificate: STA20120625.cer. Select “wapi certificate authentication mode” and then it can connect to the “WAPI_102_2certificate”.

3.3.3 WAPI Three Certificate Mode Example

3.3.3.1 Introduction to Example

Configure SSSDI as “WAPI_103_3certificate”, second layer using WAPI certificate configuration method and the certificate adopt the three certificate mode. After the set up, the wireless user can connect to “WAPI_103_3certificate” to visit the internet.

3.3.3.2 Configuration Processes

1、Open the global wapi function, configure the three certificate mode, configure the wapi authentication server ip address as 194.168.1.200.
AC(config-wireless)#wapi enable
AC(config-wireless)#wapi certificate-mode 3
AC(config-wireless)#wapi authentication-server 1 ip 194.168.1.200

2、Login the AS server, download the CA certificate: ca20120625.cer and AS certificate: as20120625@ASU.cer. Apply AP certificate: AP20120625.cer and STA certificate: STA20120625.cer.

3、Export the CA, AS and AP certificates to AC
AC#copy wapi-certificate tftp://194.168.1.203/ca20120625.cer ca20120625.cer
AC#copy wapi-certificate tftp://194.168.1.203/ as20120625@ASU.cer

as20120625@ASU.cer

AC#copy wapi-certificate tftp://194.168.1.203/AP20120625.cer AP20120625.cer

4、Configure the certificate document to managed AP

AC(config-wireless)#ap database 00-03-0f-01-0b-80

AC(config-ap)#wapi certificate ap AP20120625.cer

AC(config-ap)#wapi certificate as asu20120625@ASU.cer

AC(config-ap)#wapi certificate ca ca20120625.cer

5、Sending the certificate document to managed AP

AC#wapi certificate-distribute

6、Configure SSID：WAPI_103_3certificate

AC#config

AC(config)#wireless

AC(config-wireless)#network 103

AC(config-network)#security mode wapi-certificate

AC(config-network)# ssid WAPI_103_3certificate

AC(config-network)# wapi authentication-server 1

AC(config-network)#exit

AC(config-wireless)#ap profile 1

AC(config-ap-profile)#radio 1

AC(config-ap-profile-radio)#vap 0

AC(config-ap-profile-vap)#network 103

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

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

AC#wireless ap profile apply 1

7、After the wireless user installed the CA certificate: ca20120625.cer, STA certificate: STA20120625.cer. Select “wapi certificate authentication mode” and then it can connect to the “WAPI_103_3certificate”

3.3.4 WAPI Pre-sharing Key Example

3.3.4.1 Introduction to Example

Configured SSID as “WAPI_101_PSK”, second layer uses the pre-sharing secret key configuration method. After the set up, the wireless user can connect to “WAPI_101_PSK” to visit the internet.

3.3.4.2 Configuration Processes

1、Open the global wapi function

AC(config-wireless)#wapi enable

2、Configure SSID：WAPI_101_PSK

AC#config

AC(config)#wireless

AC(config-wireless)#network 101

AC(config-network)#security mode wapi-psk
AC(config-network)# ssid WAPI_101_PSK
AC(config-network)# wapi psk length 9
AC(config-network)# wapi psk type ascii
AC(config-network)# wapi psk cipher 123456789
AC(config-network)#exit
AC(config-wireless)#ap profile 1
AC(config-ap-profile)#radio 1
AC(config-ap-profile-radio)#vap 0
AC(config-ap-profile-vap)#network 101
AC(config-ap-profile-vap)#enable
AC(config-ap-profile-vap)#end
AC#wireless ap profile apply 1

3、Wireless user selects the “wapi pre-sharing secret key authentication mode”, using the password as “123456789” can connect to “WAPI_101_PSK”.

3.4 WAPI Troubleshooting

☞ Ensure that the network is physically connecting correctly. AS server can be reached.

☞ Ensure the Global wapihas opened. (If Global wapi function is closed, other wapi releated command cannot configure)

☞ In the Wapi certificate authentication, need to configure the certificate mode and then sending the certificate, otherwise, it will have the error. Wapi

☞ STA uses the wapicertificate authentication, and it fail, you can check whether the following are correct:

✧ Whether the AS certificate installed on STA is correct, expire or revoke (if it is at 3 certificate mode, need to affirm the CA certificate).

✧ Whether the STA certificate installed on STA is correct, expire or revoke.

✧ Whether the AS certificate installed on AP is correct, expire or revoke (if it is at 3 certificate mode, need to affirm the CA certificate).

✧ Whether the AP certificate installed on AP is correct, expire or revoke.

☞ Ensure the renew ferequency of BK，USK，MSKis not too low, update the password toofrequently will affect the network access experience.

Chapter 4 Access Authentication Based on Domain

4.1 Introduction to Access Authentication Based on Domain

For many hotels and banks, they own some branches in many cities. Each branch has its wireless network, but the authentication and accounting servers may be only deployed in the headquarters. So there is the requirement that users in different areas authenticate to different servers.

The access authentication based on domain can meet this requirement. This function requests that the user name of the authentication user includes the pure user name and domain name. There is a delimiter between them such as mm@oa, mm is the pure user name, @ is the delimiter, and oa is the domain name. After AC received the authentication request from user, it can extract the domain name from the user name and then choose the authentication and accounting servers according to the domain name.

The principle of this function is as below:

The administrator creates a domain list on AC, the delimiter, domain name and radius server name of the domain are recorded in each entry. Under the network configuration mode, a network and a domain entry can be associated (bound) through the index number of the domain entry.

When the wireless user accesses, AC can find the network that the user accesses according to the SSID and find the domain according to the network. And then it extracts the domain name according to the delimiter, and compares the extracted domain name and the configured domain name in domain. If they are same, the radius server configured in domain can be used for authentication and accounting; otherwise, the radius server configured under the network will be used.

Multiple domains can be bound to a network. When associating with the wireless user with the same SSID, different domains can be matched according to the different domain names in the user name. And different radius servers can be adopted for authentication.

If configures under the network as: AC(config-network)#no radius use-network-configuration, any user associated with this network will use the radius server of the wireless global configuration for authentication no matter what user name they use.

If the user name includes multiple delimiters, AC will only regard the first delimiter as the delimiter, the back delimiters will be as a part of the domain name. For example, the

delimiter is @, the user name is test@abc@.com, so the pure user name is test, the domain name is abc@.com.

This function should be used together with radius server. The radius server must do: (1) divide the user to different domains; (2) after received the radius packet with the user name including domain name, it can distinguish the pure user name and domain name for completing the authentication.

4.2 Access Authentication Based on Domain Configuration

The configuration task list of access authentication based on domain is as below:

1. Configure the domain, domain name, delimiter and radius server name.
2. Bind the domain to network.

1. Configure the domain, domain name, delimiter and radius server name

Command	Explanation
Wireless Global Configuration Mode	
domain<1-5> **no domain<1-5>**	Add a domain configuration or enter into the domain config mode. The no command deletes the domain configuration.
Domain Config Mode	
delimiter<string> **no delimiter<string>**	Configure the delimiter that the domain adopts. The no command deletes the configuration.
realm<string> **no realm**	Configure the domain name of the domain. The no command deletes it.
radius server-name *{auth|acct}<name>* **no radius server-name *{auth|acct}<name>***	Configure the radius server name that the domain adopts. The no command deletes the configured server name.

2. Bind the domain to network

Command	Explanation
Network Configuration Mode	
domain<1-5> **no domain<1-5>**	Bind the appointed domain to network. The no command deletes the binding relationship between domain and network.

4.3 Access Authentication Based on Domain Examples

Typical case:

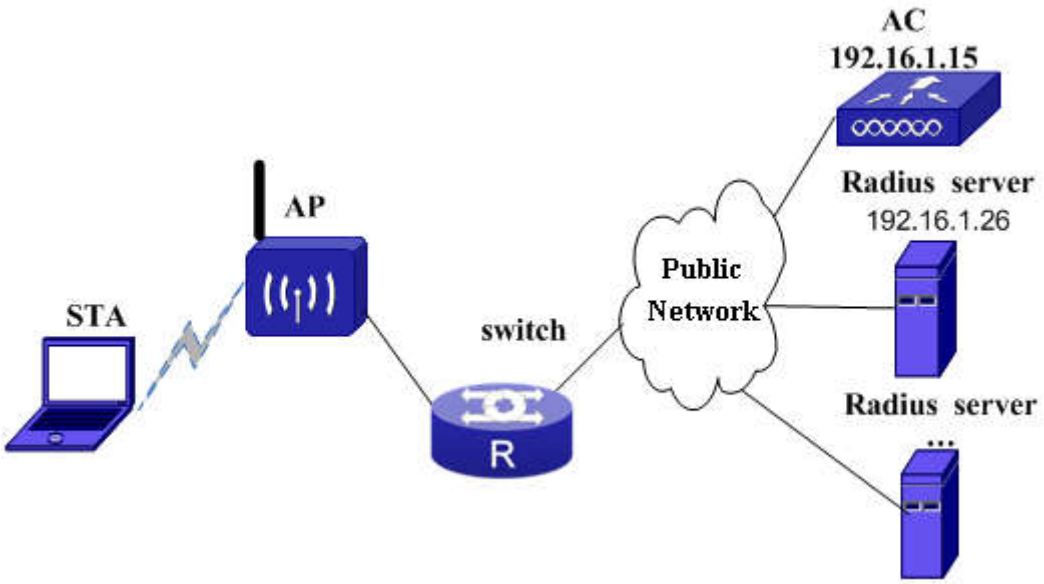


Fig 4-1 typical case of the access authentication based on domain

As the above figure shown, it including the following parts:

1. AC: It is the access management device of the whole wireless network; it manages AP and is the entrance of the wireless network accesses the wired network. The address is 192.16.1.15.
2. AP: It is the wireless access point and configured and managed by AC.
3. STA: It is the wireless user and accesses the wireless network through AP, there can be multiple STA.
4. Switch: It is the ordinary switch.
5. Pulic Network: It provides the public data transmission.
6. RADIUS server: It is used for the 802.1x authentication and according of user. There are multiple radius servers in system, they conduct the authentication and according to the users of different domains. In the case, there are 4 servers and their addresses are 192.16.1.26, 192.16.1.20, 192.16.1.25 and 192.16.1.24 respectively, their names are aaa, bbb, ccc and ddd respectively.

In the following example, 2 domains are created: domain1 and domain2. The domain name of domain1 is oa, the delimiter is the default value of @, the radius authentication and accounting server is aaa; the domain name of domain2 is ob, the delimiter is /, the radius authentication and accounting server is bbb.

There are 2 networks are configured: network1 and network2. Network1 is bound to domain1 and domain2, the configured radius server is ccc, SSID is oa-test and it is

applied to VAP 0. Network2 is bound to domain2, the configured radius is ccc, SSID is ob-test and it is applied to VAP 1.

The configured radius server under the wireless global mode is ddd.

After the configuration, there will be the following results.

- ☞ STA1 is associated with SSID of oa-test, input the user name of mm@oa for authentication. AC can divide it into the pure user name mm and domain name oa according to the delimiter @ of domain1 configured under the network1, and match it to the domain name oa of domain1. If match, the radius server aaa configured under the domain1 can be used for authentication.

- ☞ STA1 is associated with SSID of oa-test, input the user name of nn/ob. AC can divide it according to the delimiter @ of domain1 configured under the network1, bu there is no @ in nn/ob, it will divide it into the pure user name nn and the domain name ob according to the delimiter / of domain2, and match it to the domain name ob of domain2. If match, the radius server bbb configured under the domain2 can be used for authentication.

- ☞ STA1 and STA2 are associated with SSID of oa-test and ob-test respectively. STA1 uses the user name mm@oa for authentication; STA2 uses the user name nn/ob for authentication. After AC divided the user names, STA1 can conduct authentication and accounting through the aaa server, STA2 can conduct authentication and accounting through the bbb server.

- ☞ STA1 is associated with SSID of oa-test, input the user name of nn/oc. AC can divide it according to the delimiter @ of domain1 configured under the network1, bu there is no @ in nn/oc, it fails to divide. AC will divide it into the pure user name nn and the domain name oc according to the delimiter / of domain2, and match it to the domain name ob of domain2. If no match, the radius server ccc configured under the network1 can be used for authentication.

- ☞ If conducts the following configuration under network1: AC (config-network)#no radius use-network-configuration. It configures to use the radius server configured under the wireless mode, and then any user associated with network1 will use the radius server of the wireless global configuration for authentication no matter what user name they use.

The configuration is as below:

1. Configure the authentication key, authentication server, accounting server of radius server under the global mode. And enable the authentication service.
   AC(config)#radius-server key 0 test
   AC(config)#radius-server authentication host 192.16.1.26

AC(config)#radius-server accounting host 192.16.1.26

AC(config)#radius-server authentication host 192.16.1.20

AC(config)#radius-server accounting host 192.16.1.20

AC(config)#radius-server authentication host 192.16.1.25

AC(config)#radius-server accounting host 192.16.1.25

AC(config)#radius-server authentication host 192.16.1.24

AC(config)#radius-server accounting host 192.16.1.24

AC(config)#aaa-accounting enable

AC(config)#aaa enable

AC(config)#radius nas-ipv4 192.16.1.15

AC(config)#aaa group server radius aaa

AC(config-sg-radius)# server 192.16.1.26

AC(config)#aaa group server radius bbb

AC(config-sg-radius)# server 192.16.1.20

AC(config)#aaa group server radius ccc

AC(config-sg-radius)# server 192.16.1.25

AC(config)#aaa group server radius ddd

AC(config-sg-radius)# server 192.16.1.24

2. Under the wireless mode, create 2 domains. The domain name of domain1 is oa, the delimiter is the default value of @, the radius authentication and accounting server is aaa; the domain name of domain2 is ob, the delimiter is /, the radius authentication and accounting server is bbb. The steps are as below:
   AC(config-wireless)#domain 1

   AC (config-domain)#realm oa

   AC (config-domain)#radius server-name auth aaa

   AC(config-wireless)#domain 2

   AC (config-domain)#realm ob

   AC (config-domain)# delimiter /

   AC (config-domain)#radius server-name auth bbb

3. The configuration of radius server under the wireless global mode is as below:
   AC(config-wireless)# radius server-name auth ddd

   AC(config-wireless)# radius server-name acct ddd

4. Configure network1 and network2. Network1 is bound to domain1 and domain2, the configured radius server is ccc, and it is applied to VAP 0. Network2 is bound to domain2, the configured radius is ccc, and it is applied to VAP 1. The steps are as below:
   AC (config-wireless)#network 1

   AC (config-network)#ssid oa-test

   AC (config-network)# radius accounting

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

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

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

AC (config-network)#domain 1

AC (config-network)#domain 2

AC (config-wireless)#network 2

AC (config-network)#ssid ob-test

AC (config-network)# radius accounting

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

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

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

AC (config-network)#domain 2

AC (config-wireless)#ap profile 1

AC (config-ap-profile)#radio 1

AC (config-ap-profile-radio)#vap 0

AC (config-ap-profile-vap)#network 1

AC (config-ap-profile-radio)#vap 1

AC (config-ap-profile-vap)#network 2

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

AC#wireless ap profile apply 1

4.4 Access Authentication Based on Domain Troubleshooting

If the access authentication based on domain cannot be effective in using, please check the following reasons:

- ☞ Check if the user name for authentication is correct. The delimiter and domain name should be both same as the domain configuration.
- ☞ Check if the user password is correct. The user password must be same as the password on radius server.
- ☞ Check if the server name configured under domain and its IP address is correct, and check if the server can be achieved.
- ☞ Check if the domain is associated with the correct network.
- ☞ Check if the command of **no radius use-network-configuration** is configured under the network. If configured, any user will adopt the radius server under the wireless global mode for authentication.
- ☞ Check if the user name and password are configured for the server correctly, if not, please add them.

Chapter 5 LDAP Authentication

5.1 Introduction to LDAP Authentication

LDAP (Lightweight Directory Access Protocol) is based on the directory access protocol. The function of directory service on LDAP is built up on the foundation of Client/Server, and all the directory messages are stored on the LDAP server. LDAP clients can through the interchange of messages to manipulate the data on the server.

The messages in the LDAP directory is organized in the tree diagram structure. The idiographic messages will store in the entries of directory and each of the entry is formulated by an attribute. Each of the attributes can contain of more than one attribute value and it is indicated by the unique DN (Distinguished Name). In the other words, the directory entry is similar to the record in the relation database. And DN is the index of entry.

Since LDAP as an authentication service protocol, it can unify the authentication and authorization of the user. In a large internet system, it usually contains of many sub-system. Take digital campus system as example, it contains of Portal authentication, finance system and Library leading information system etc; in the IT management system, the sub-system may including login system, payment enquire system and roll book system. The user needs to be authorized and authenticated to login each of the sub-systems. If each of the sub-system has their own user name and password, the administer need to pay more effort to manage it. From the user perspective, they need to remember different login name is quite annoying. If the system can perform the authentication and authorization function in one, it will be more convenient. It is because all of the sub-system needs to manage one user password only and the user needs to use the same password throughout all system as well. LDAP server can be the third party server for authentication.

LDAP protocol usually adopts the C/S mode. The user can send a command to the server and once LDAP receive the command; it will execute some necessary process on the directory and provide feedback to the user. In the feedback, it will contain of some data.

The basic procedure of using LDAP protocol for authentication as following:

(1) LDAP user need to use the directory which contains of enough resource to the purview user DN (generally, using the LDAP service administer DN) to connect with the LDAP server and obtain enquire purview.

(2) LDAP user use the user name in the authentication message as enquire condition, and check the user name in the particular directory for searching and obtain the DN.

(3) last but not least，LDAP user can use the DN and user password to connect with the LDAP server and check whether the password is correct.

And our company has already be the user of LDAP and apply this technology to the Captive Portal and manage the authentication.

5.2 LDAP Authentication Configuration

The steps of Authentication function Configuration as following:

1. The case of LDAP server application authentication configuration
2. The case of LDAP server application authentication and time out configuration
3. The filter conditions through the enquire of the LDAP service configuration
4. The configuration of LDPA mode authentication by using VTY (Telnet and ssh method), Web and Console login method
5. The configuration of Portal user using the LDAP authentication and LDAP server

1. The case of LDAP server application authentication configuration

Command	Explanation
Global Mode	
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*>**	The case of LDAP server application authentication configuration including index number ,IP address, service port number, user's DN, user attribute and classification. No command is used to delete the corresponding case of sever application

2. The case of LDAP server application authentication and time out configuration

Command	Explanation
Global Mode	

ldap server <server-index> authentication-methed {anonymous | authenticated username <username> password <password>}	The LDAP sever authentication method, including anonymity authentication and simple authentication. Simple authentication. Need to use user name and password.
ldap server timeout <1~1000> **no ldap server timeout**	LDAP server timeout configuration, the unit of time is second. NO command will reset.

3. The filter conditions through the enquire of the LDAP service configuration

Command	Explanation
Global Mode	
ldap server <server-index> search-filter <search-filter> **no ldap server <server-index> search-filter**	Configured on the particular server for filtering searching. NO command will reset.

4. The configuration of LDPA mode authentication by using VTY (Telnet and ssh method), Web and Console login method

Command	Explanation
Global Mode	
authentication line {console | vty | web} login {local | radius | tacacs | ldap} **no authentication line {console | vty | web} login**	Configured on the login authentication management. No command will reset the validate mode. Console login does not have any login validation, while VTY and Web is default as local validation.

5. The configuration of Portal user using the LDAP authentication and LDAP server

Command	Explanation
Captive Portal Instance mode	
verification {ldap|none|radius}	Is the Captive portal authentication mode. Can choose LDAP, none or RADIUS, RADIUS is set as default.

ldap-server <server-index> **no ldap-server <*server-index*>**	Configured on the Captive portal with LDAP server. Under default, will use LDAP server for authentication until it return to fail or success result. NO command set as reset.

5.3 LDAP Authentication Examples

Case：

Set up the environment as show below: the wireless user on AC1 is using Captive Portal to undergo the Authentication and the Authentication service server uses the LDAP server. Administer PC can telnet to AC1 and AC2 to perform the administrative work. Administer need to login to AC for Authenticating and the Authentication mode as LDAP.

LDAP serve IP address as 192.168.1.1 and the port number is 389.

The administer DN and password of the directory of LDAP server as following:

rootdn "cn=root,dc=internet,dc=com"

rootpw ricky

LDAP server has contained of the following portal user authentication:

dn:uid=portaluser,dc=internet,dc=com

objectClass:person

uid: portaluser

cn: ricky

sn: ren

userPassword: 123456

telephoneNumber:13811180180

description:a portal user from internet

telexNumber:tex-8888888

street:Shangdi 9th Street

postOfficeBox:postofficebox

displayName:portaluser

homePhone:home1111111

mobile:mobile99999

LDAP server has contained of the following exchange login authentication:

dn:uid=loginuser,dc=internet,dc=com

objectClass:management

objectClass:operator

uid: loginuser

cn: ricky

sn: ren

userPassword: 654321

telephoneNumber:13811180180

description: a switch user from internet

telexNumber:tex-8888888

street: Shangdi 9th Street

postOfficeBox:postofficebox

displayName:switchuser

homePhone:home1111111

mobile:mobile99999

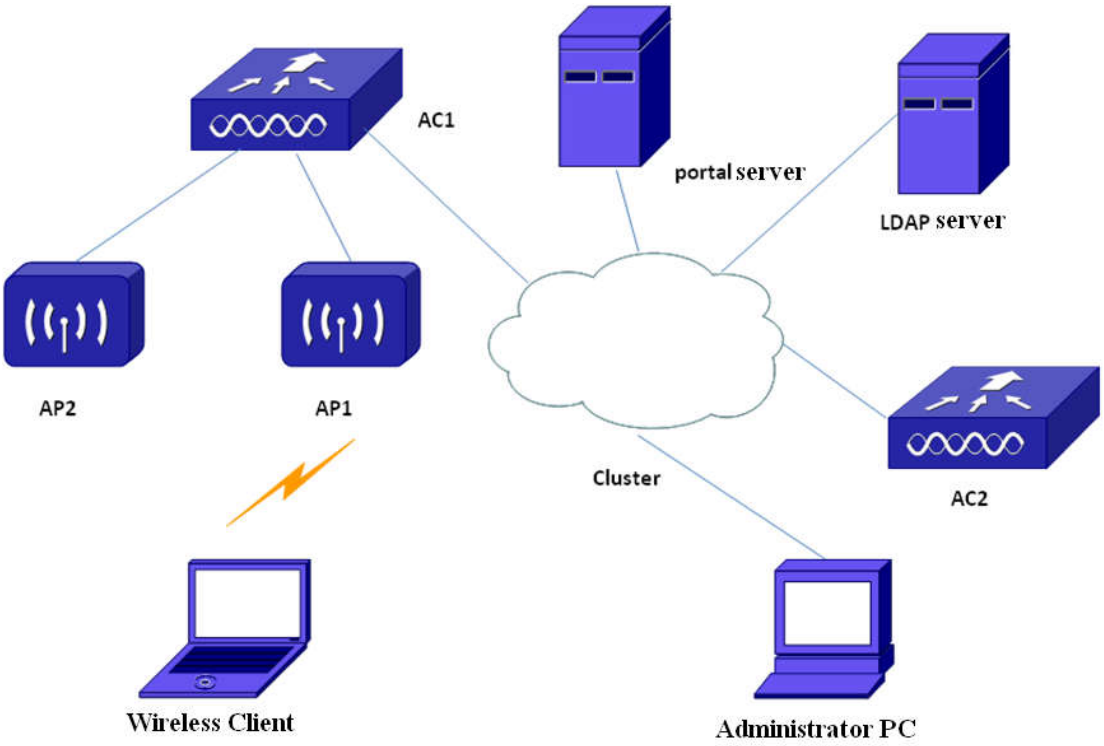


Fig 5-1 LDAP authentication function configuration

After the Portal user link to the ssid, and then enter to internet resource and redirect it to the longin page. Enter the user name as portaluser and the password as 123456 to obtain the portal authentication. (ssid，network，vap configuration can refer to the chapter of wireless authentication and connection)

The administer user can telnt to ac, and press in loginuser as the user name and the password as 654321. Then it can login to the administration interface. Only the user objectClass as management and operator can access.

Configuration steps：

AC1 portal user undergo LDAP authentication configuration：

1 configured ldap server IP address and authentication mode

AC(config)# ldap server 1 ipv4-address 192.168.1.1 port 389 user-base-dn dc=internetdc=com user-attr uid user-type person

AC(config)#ldap server 1 authenticated username cn=root,dc=internet,dc=com password ricky

2 configured the captive portal which adopt LDAP authentication

(here is assume that the user connection vap refer to network 1)

AC (config)#captive-portal

AC (config)#enable

AC (config-cp)#configuration 1

AC (config-cp)#enable

AC (config-cp-instance)#verification ldap

AC (config-cp-instance)#ldap server 1

AC (config-cp-instance)# interface ws-network 1

AC1 and AC2 administer login to LDAP for authentication configuration：

1 configured ldap server IP address and authentication mode

AC(config)# ldap server 2 ipv4-address 192.168.1.1 port 389 user-base-dn dc=internetdc=com user-attr uid

AC(config)#ldap server 2 authenticated username cn=root,dc=internet,dc=com password ricky

2 condition filtration configuration

AC(config)#ldap server 2 search-filter &(objectClass=management)(objectClass=operator)

3 Administer user login to LDAP authentication configuration

AC(config)#authentication line vty login ldap

5.4 LDAP Authentication Troubleshooting

When encountered problems in the process of using the redirection function, please check whether the reasons as follows:

- ☞ LDAP server can only support the IPv4 address.
- ☞ LDAP can only perform the Authentication function and not support the accounting function
- ☞ Only the administer login and captive portal（pap）Authentication can support the LDAP Authentication mode, other methods such as WPA should use the radius mode.
- ☞ The expression of user-base-dn in different LDAP server will have difference. User should notice of it before the configuration. If it cannot match, user can check the LDAP message from the server and base on the user-base-dn to configure.

Chapter 6 PPPoE Server Configuration

6.1 Introduction to PPP Protocol

PPP (Point to Point Protocol) is a type of point to point linkage to carry the network layer data package protocol. Because it can provide user authentication, easy to expand and support the synchronized/ asynchronized communication, thus it is widely used in our daily life.

PPP define an entire protocol, including Link Control Protocal (LCP), Network Control Protocol (NCP) and Authentication (PAP and CHAP).

- Link Control Protocol (LCP): Mainly use to build up, backout and inspect the data linkage.
- Network Control Protocol (NCP): Mainly use to treat with the data package format and type on the data linkage transmittion.
- PAP and CHAP is used for the network security authentication.

1. PAP authentication

PAP (Password Authentication Protocol) authentication is the two ways authentication.The password is law password. The following is the process of PAP authentication:

(1) Authenticatee will send the user name and password to authenticater.

(2) Authenticater will see whether the user is existed and whether the password is corrected according to the user list and then provide different feedback (Acknowledge or Not Acknowledge).

However, PAP is not a safe authentication method. During the authentication, command will use the law method to send in the linkage. Once PPP linkage is built up, the authenticatee will send the user name and command continuously, until the identification authentication is completed, so it cannot prevent attack.

2. CHAP authentication

CHAP (Challenge-Handshake Authentication Protocol) authentication is the three ways authentication. The password is cryptograph.

CHAP means that unilateral authentication. Other party regards as authenticatee. Dynamic authentication is double the one way authentication. In the other words, both parties not only are the authenticater but also the authenticatee. One way authentication

is commonly used in the daily application.

CHAP authentication as following:

(1) Authenticater initiates the authentication, and sending some random message (Challenge) to the authenticatee. Also, it will send the user name for authentication.

(2) Authenticatee once receive the request, it will check whether the port is configured default CHAP password. If it is set, the authenticatee will using the message ID, default password and MD5 calculate method to encrypt, and sending the cryptograph and user name（Response）to authenticater.

(3) If the default CHAP password does not exist during the authentication, then authenticater will accord to the receiving user name for checking corresponding password. If the user name is found, then using message ID, default password and MD5 calculate method to encrypt, and sending the cryptograph and user name（Response）to authenticater.

(4) Authenticater using its own authenticateepassword and MD5 calculationn method for encrypting, and comparing both cryptograph, and provide different feedback（Acknowledge or Not Acknowledge）.

PPP process as following:

(1) To build up the PPP linkage, need to enter the Establish stage.

(2) During the Establish stage, PPP linkage undergoes LCP negotiation. Negotiation content includes working method, authentication method and the maximium transmitted unit. Once LCP negotiation enters into Openedstage, it means that the bottom linkage layer had already built up.

(3) If the configuration is authenticated, then it enters into Authenticate stage. It will start the CHAP or PAP authentication.

(4) If the authentication is fail to enter into the Terminatestage, it will break down the linkage and LCP status will change to down. If the authentication enters into the Network negotiation（NCP）successfully, but the status of LCP ststus as Opened, then IPCP status will change from Initial to Request.

(5) NCP negotiation support the IPCP negotiation, IPCP negotiation mainly includes both of the IP addresses. Through the NCP negotiation to selecting and configure one network layer negotiation. Only the corresponding network layer negotiation success, that layer can through this PPP linkage to sending message.

(6) PPP linkage will continous communication, until having LCP or NCP frame to close this link, or some other thing has happened.

PPP process chart as following:

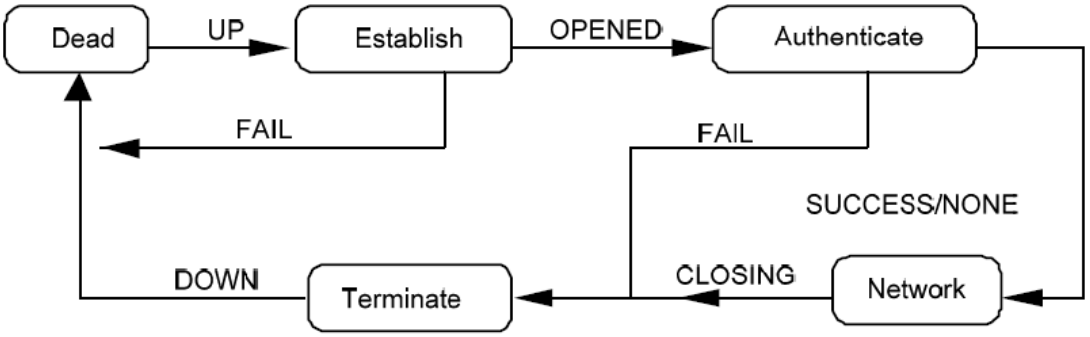


Fig 6-1 PPP process chart

6.2 Introduction to PPPoE

PPPoE is the short form of Point-to-Point Protocol over Ethernet. It is the application of PPP protocol on the internet. It using the internet to link up large amount of computer to form a network and using a port to connect into the internet. It will control to each f the compute that has already connected. The function of accounting, high performance make pppoe widely adopt in the build up the network in small group.

PPPoE using C/S working mode，which is Client/Serverworking mode.

PPPoE protocol working process has two stages: Discovery and Conversation stages.

- Discovery Stage：

During discovery stage, the user's server will use the broadcast method to search the switch and obtain the internet MAC address. And then select the server that would like to connect; confirm the PPP conversation marker number that needs to build up.

Discovery stage is the process of client searching the server，and build up the connection with server.

- Conversation stage：

After enter the conversation stage, the user's server and the switch will according to PPP conversation parameter that negotiate during the discovery stage and undergo the conversation. Once PPPoE conversation start, PPP data can using other PPP encapsulated method for sending. The entire internet frame is singular boardcast. SESSION-ID of the PPPoE conversation must not be changed; also the distributed value must be match with discovery stage.

PPPoE also has other PADT sub-group, it can be sending at any time as the conversation is built up. If ending the PPPoE conversation, it can be sent by the server or the switch. Once other receiving a PADT sub-group, then it will not allow to use this conversation to sending the PPP operation.

Wireless AC will be the PPPoE-Server, including providing RADIUS long-distance authentication, dynamic distributing IP, dynamic configuration DNS server function etc.

6.3 PPPoE-Server Configuration

1. Configure the relevant parameters of radius-server
   1) Authentication host
   2) accounting host
   3) key
2. Configure the relevant parameters of AAA
   1) Enable AAA
   2) Enable aaa-accounting
   3) Configure AAA group
3. Enable PPPoE-server function
4. Configure pppoe-server binding aaa group
5. Configure the maximum number of sessions of pppoe-server
6. Configure the automatic distributing address pool of pppoe-server
7. Add virtual-template of pppoe-server
8. The virtual-template configuration of pppoe-server
   1) Configure authentication-mode of PPP
   2) Configure the DNS distributed by PPP
   3) Configure PPPoE address pool used by virtual-template
   4) Enable PPP accounting statistic function
   5) Configure the waiting time of client response after sending the LCP keep-alive requisition packet
   6) Configure the times of sending the LCP keep-alive requisition packets
   7) Configure the times of sending the termination requisition packets
   8) Configure the maximum receiving unit of lcp consulting
   9) Configure IP address of the virtual template
   10) Configure PPP consulting timeout
9. Bind virtual-template on layer 3 interface

1. Configure the relevant parameters of radius-server

Command	Explanation
Global Mode	

radius-server authentication host <A.B.C.D| X:X::X:X> [port <0-65535>] [key WORD] [primary] **no radius-server authentication host <A.B.C.D>**	This command is used to configure the appointed radius authentication server host. The no command deletes the appointed radius authentication server host.
radius-server accounting host <A.B.C.D | X:X::X:X> [port <0-65535>] [key WORD] [primary] **no radius-server accounting host <A.B.C.D>**	This command is used to configure the appointed radius accounting server host. The no command deletes the appointed radius accounting server host.
radius-server key [0|7] WORD **no radius-server key**	Configure the key of radius-server, the no command deletes the radius-server key.

2. Configure the relevant parameters of AAA

Command	Explanation
Global Mode	
aaa enable **no aaa enable**	This command is used for configuring to enable AAA authentication function. The no command disables this function.
aaa-accounting enable **no aaa-accounting enable**	This command is used for configuring to enable AAA accounting function. The no command disables this function.
aaa group server radius LINE **no aaa group server radius LINE**	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.

3. Enable PPPoE-server function

Command	Explanation
Global Mode	

pppoe-server enable **no pppoe-server enable**	Enable/disable pppoe server function globally. 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.

4. Configure pppoe-server binding aaa group

Command	Explanation
Global Mode	
pppoe-server bind radius-group WORD **no pppoe-server bind radius-group WORD**	Configure the associated RADIUS server groups.

5. Configure the maximum number of sessions of pppoe-server

Command	Explanation
Global Mode	
pppoe-server max-sessions <limit> **no pppoe-server max-sessions**	Configure/recover the maximum number of sessions. If the number exceeded this restriction, the session connection will not be created any more. 2048 is default.

6. Configure the automatic distributing address pool of pppoe-server

Command	Explanation
Global Mode	
ip pppoe pool <WORD> <A.B.C.D> <A.B.C.D> **no ip pppoe pool <WORD>**	Create/cancel IP address pool function. It is used to distribute IP address for client.

7. Add virtual-template of pppoe-server

Command	Explanation
Global Mode	
interface virtual-template <1-255> **no interface virtual-template <1-255>**	Create/cancel a virtual template.

8. The virtual-template configuration of pppoe-server

Command	Explanation
Virtual-template Configuration Mode	

ppp authentication-mode (pap| chap)	Configure the default authentication mode of PPP protocol, including PAP and CHAP authentication. Use CHAP authentication as default.
ppp ipcp dns <A.B.C.D> <A.B.C.D> **no ppp ipcp dns**	Configure DNS host server and aide server for the virtual template and issue it to client.
remote address pppoe-pool WORD **no remote address pppoe-pool WORD**	The virtual template enables/abandons the IP address pool.
ppp account-statistics enable **no ppp account-statistics enable**	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.
ppp lcp max-echo-interval <1-10> **no ppp lcp max-echo-interval**	Configure/recover the waiting time of client response after sending the LCP keep-alive requisition packet. 3s is default.
ppp lcp max-echo-request < 1-10 > **no ppp lcp max-echo-request**	Configure/recover the times of sending the LCP keep-alive requisition packets. 5s is default.
max-terminate-request <1-3> **no max-terminate-request**	Configure/recover the times of sending the termination requisition packets.
ppp lcp mru <1-1492> **no ppp lcp mru**	Configure/recover the maximum receiving unit of lcp consulting to notice the client server how many data bytes of packet it can receive. 1492 is default.
ip address <A.B.C.D> <A.B.C.D> **no ip address <A.B.C.D> <A.B.C.D>**	Configure/cancel the virtual template IP address as PPPOE server address.
ppp negotiate-timeout <1-10> **no ppp negotiate-timeout**	Configure/recover the consulting timeout of PPP. 3s is default.

9. Bind virtual-template on layer 3 interface

Command	Explanation
Layer 3 Interface Configuration Mode	
pppoe-server bind virtual-template <1-255> **no pppoe-server bind virtual-template <1-255>**	Enable/disable server binding the virtual template. Server does not bind the virtual template as default.

6.4 Wireless PPPoE-server Authentication Examples

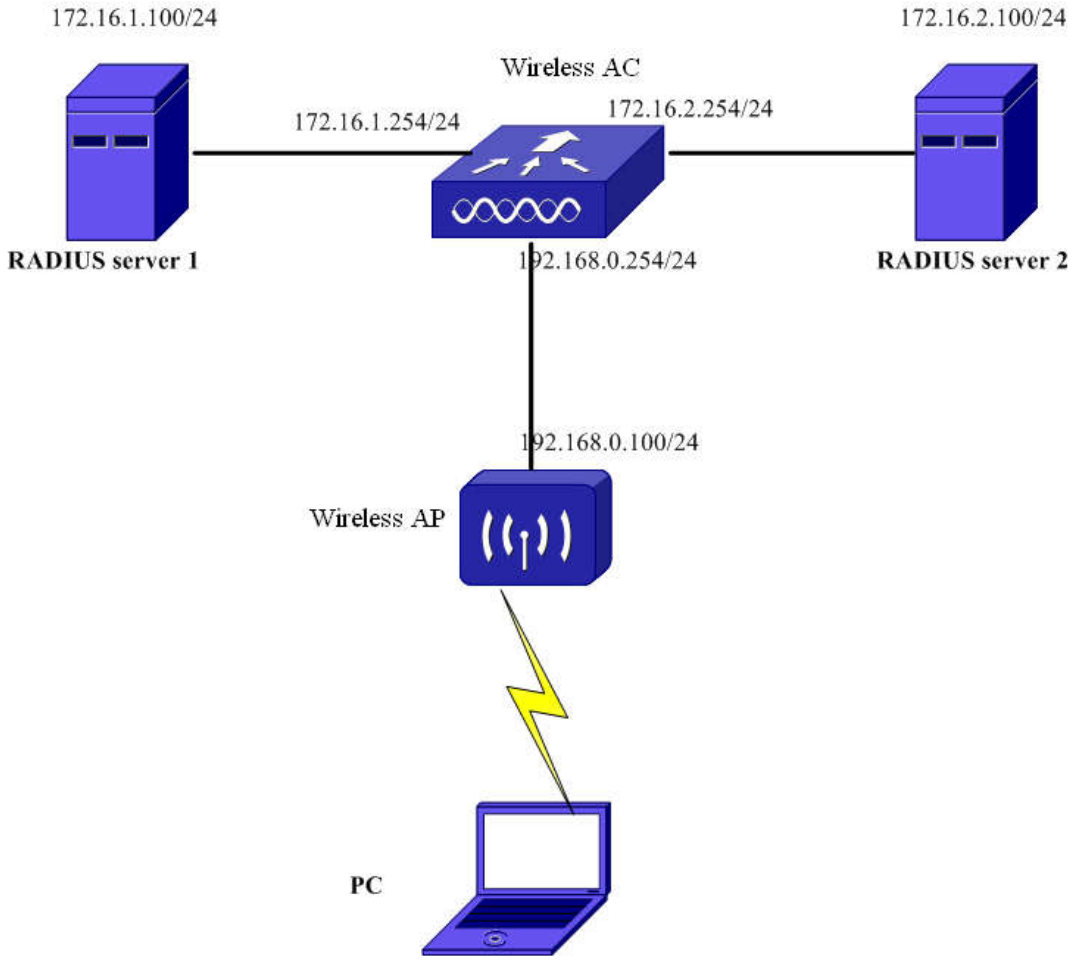


Fig 6-2 Wireless PPPoE-server Authentication Example topology

Once PC connects to the wieless network, it can send the PPPoE authentication request.

Wireless AC be the PPPoE server, will provide the PPPoE authentication to the user. Both of the RADIUS servers are the tools of PPPoE server to provide authentication for the user. The entire authentication is completed on the RADIS server.

PPPoE servercan also provide the PPPoE user with the IP, DSN configuration etc.

We start the configuration once both of the PC1、PC2 had connected to the wireless nectwork. Suppose the wireless address of AC is 1.1.1.1, the client gets the address of vlan4090 (192.168.0.x). Also, the RADIUS servers 1/2 need to be configured.

In order to complete the PPPoE authentication, need to peform the following task:

1. Configure RADIUS server:

```
AC(config)#radius source-ipv4 1.1.1.1
AC(config)#radius nas-ipv4 1.1.1.1
AC(config)#radius-server key 0 test
AC(config)#radius-server authentication host 172.16.1.100
AC(config)#radius-server authentication host 172.16.2.100
AC(config)#radius-server accounting host 172.16.1.100
AC(config)#radius-server accounting host 172.16.2.100
AC(config)#aaa enable
AC(config)#aaa-accounting enable
AC(config)# aaa group server radius RADIUS_GROUP_1_2
AC(config-sg-radius)#server 172.16.1.100
AC(config-sg-radius)#server 172.16.2.100
AC(config-sg-radius)#exit
AC(config)#
```

2. Configure PPPoE server:

Configure the pppoe function of AC and the authentication mode is chap. Configure the no command to cancel the address pool of the client.

```
AC(config)#pppoe-server enable
AC(config)#pppoe-server bind radius-group RADIUS_GROUP_1_2
AC(config)#ip pppoe pool public_ip_pool 192.168.0.0 255.255.255.0
AC(config)#interface virtual-template 1
AC(config-if-vt1)#ip address 192.168.0.254 255.255.255.0
AC(config-if-vt1)# ppp account-statistics enable
AC(config-if-vt1)#ppp authentication-mode chap
AC(config-if-vt1)#ppp ipcp dns 10.1.120.141 10.1.121.145
AC(config-if-vt1)#ppp lcp mru 1492
AC(config-if-vt1)#remote address pppoe-pool public_ip_pool
AC(config)#vlan 4090
AC(config-vlan4090)#interface vlan 4090
AC(config-if-vlan4090)#pppoe-server bind virtual-template 1
```

6.5 Wireless PPPoE server Troubleshooting

If the wireless PPPoE contains errors throughout the authentication, please check whether the following configuration is correct:

- ☞ radius server is correct, including Key, AAA is opened, has appointed the particular radius sever address in the aaa group.
- ☞ PPPoE-server colligate RADIUS group correctly.
- ☞ Open the PPPoE-server
- ☞ Configure the PPPoE pool
- ☞ Ensure that the configuration of authentication-mode in virtual-template is same with the encrypt method that chose by the user.
- ☞ In virtual-template, pppoe-pool is related correctly. The configuration command is pppoe-pool. This command is necessary.
- ☞ Send the correct IP address to virtual-template, this IP address need to be same with the IP address configuration that colligate with third layer VLAN port.
- ☞ Apply the corresponding virtual-template to third layers correctly. This command is need to be configured necessary.

Chapter 7 Local Forwarding

7.1 Introduction to Local Forwarding

Local forwarding is a forwarding mode of completing data interaction of clients on AP. It is also the forwarding mode of independent AP.

Local forwarding means authenticate in advance in wireless client (station). AC is needed to participate when station authentication, association and configuration. But in data forwarding, AC is not needed; data forwarding is in the main of AP completely.

The advantages of local forwarding: AP forwards client data directly; it can mitigate the flow pressure on AC.

The disadvantages of local forwarding: because AP forwards client data directly, the flow may not pass by AC, it will not achieve that monitor the data flow in centralized

Local forwarding can support the layer 2 roaming of client better. When the client conducts the layer 3 roaming, the distributed forwarding function should be enabled. (Shown in chapter 8)

7.2 Local Forwarding Configuration

1、Configure VLAN of network on AC

Command	Explanation
Network Configuration Mode	
vlan <*1-4094*>	Configure VLAN related to network on AC; the default configuration is VLAN 1.

7.3 Local Forwarding Configuration Examples

Configuration Topology:

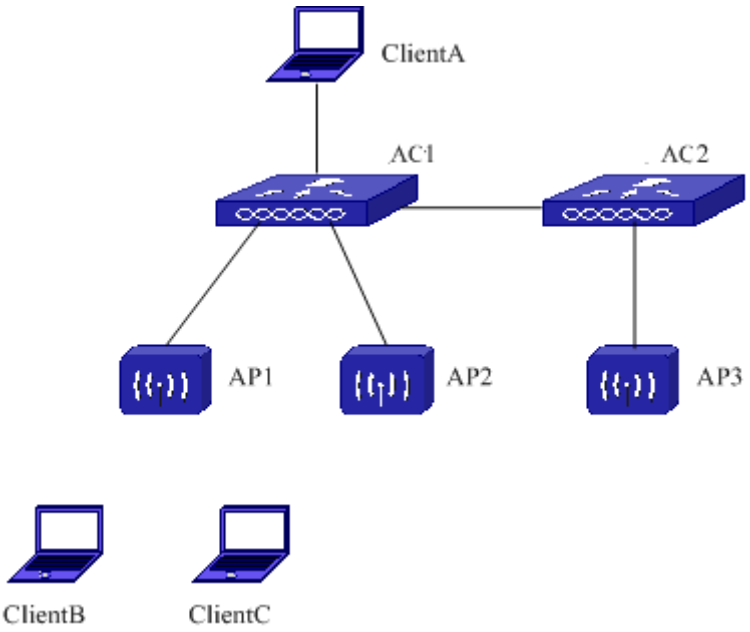


Fig 7-1 Local forwarding configuration topology

Introduction to Case:

1. AC1 and AC2 make up the cluster.
2. AP1 and AP2 are associated with AC1, AP 3 is associated with AC2.
3. Data forwarding uses local forwarding mode.

Configuration Process:

1. Configure network and ssid:ssidap1 on AC1, apply profile 1 on AP1.

AC> enable
AC# config
AC(config)# wireless
AC(config-wireless)# network 1
AC(config-network)# ssid ssidap1
AC(config-network)#vlan 11
AC(config-network)# exit
AC(config-wireless)#ap profile 1
AC(config-ap-profile)#radio 1
AC(config-ap-profile-radio)# enable
AC(config-ap-profile-radio)# vap 1
AC(config- ap-profile-vap)# network 1
AC(config-ap-profile-vap)# enable
AC(config- ap-profile-vap)# end
AC# wireless ap profile apply 1

2. Configure network and ssid:ssidap2 on AC1, apply profile 2 on AP2.

AC(config-wireless)# network 2

AC(config-network)# ssid ssidap2
AC(config-network)#vlan 12
AC(config-network)# exit
AC(config-wireless)#ap profile 2
AC(config-ap-profile)#radio 1
AC(config-ap-profile-radio)# enable
AC(config-ap-profile-radio)# vap 2
AC(config- ap-profile-vap)# network 2
AC(config-ap-profile-vap)# enable
AC(config- ap-profile-vap)# end
AC# wireless ap profile apply 2

3. Configure network and ssid:ssidap3 on AC2, apply profile 1 on AP3.
AC> enable
AC# config
AC(config)# wireless
AC(config-wireless)# network 1
AC(config-network)# ssid ssidap3
AC(config-network)#vlan 13
AC(config-network)# exit
AC(config-wireless)#ap profile 1
AC(config-ap-profile)#radio 1
AC(config-ap-profile-radio)# enable
AC(config-ap-profile-radio)# vap 1
AC(config- ap-profile-vap)# network 1
AC(config-ap-profile-vap)# enable
AC(config- ap-profile-vap)# end
AC# wireless ap profile apply 1

7.4 Local Forwarding Troubleshooting

- Make sure the physical connection of the whole network is correct.
- Make sure network cluster configuration is correct.
- Make sure wireless access authentication configuration is correct.