Content

Chapter 1 Automatic Discovery and Cluster Creating

1.1 Introduction to Automatic Discovery and Cluster Creating

Through automatic discovery function, more than one AP and AC can connect pairwisely to make up the cluster and provide wireless service. This function provides multiple kinds of modes of static configuration, DNS, DHCP etc. The automatic discovery function is based on IP, so it can discover the equipment which is not at the same network segment.

1.2 Automatic Discovery and Cluster Creating Configuration

Automatic discovery function task list is as below:

1. Add IP address to IP address list which is discovered automatically by UDP
2. Configure automatic discovery mode
3. Configure VLAN ID of layer2 broadcast discovery
4. Configure cluster mark of AC
5. Configure the time interval of sending keep-alive message
6. Configure the maximum times of sending keep-alive message

1. Add IP address to IP address list which is discovered automatically by UDP

Command	Explanation
Wireless Global Mode	
discovery ip-list <*ipaddr*> **no discovery ip-list [<*ipaddr*>]**	Add the new IP address to the IP address table that UDP found it automatically. The no command clears IP address in the table.
discovery ipv6-list <*ipv6addr*> **no discovery ipv6-list [<*ipv6addr*>]**	Add the new IPv6 address to the IPv6 address table that UDP found it automatically. The no command clears IPv6 address in the table.

2. Configure automatic discovery mode

Command	Explanation
Wireless Global Mode	
discovery method [ip-poll | l2-multicast] **no discovery method [ip-poll | l2-multicast]**	Appoint the automatic discovery mode. The no command disables the function of automatic discovery.

3. Configure VLAN ID of layer2 broadcast discovery

Command	Explanation
Wireless Global Mode	
discovery vlan-list <*1-4094*> **no discovery vlan-list [<*1-4094*>]**	Add a VLAN to the VLAN table discovered by layer 2 broadcast. The no command deletes the VLAN in the VLAN table discovered by layer 2 broadcast.

4. Configure cluster mark of AC

Command	Explanation
Wireless Global Mode	
peer-group <*1-255*> **no peer-group**	Configure the cluster mark-Group ID for AC. The no command deletes the Group ID of AC and recovers to be default of 1.

5. Configure the time interval of sending keep-alive message

Command	Explanation
Wireless Global Mode	
keep-alive-interval <5000-60000>	Configure the time interval of AC sending keep alive message.

6. Configure the maximum times of sending keep-alive message

Command	Explanation
Wireless Global Mode	
keep-alive-max-count<1-15>	Configure the maximum sending times of AC sending keep alive message.

1.3 Automatic Discovery Configuration Examples

1. Automatic discovery configuration example based on IP list.

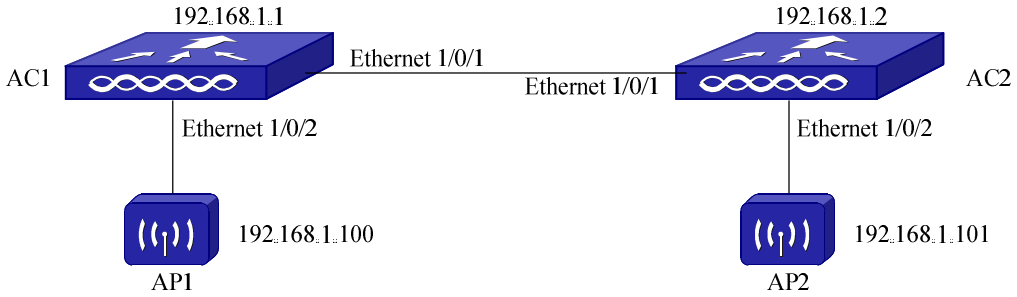


Fig 1-1 typical application environment of automatic discovery of IP

As shown in Fig 1-1, the wireless address of AC1 and the AC2 are 192.168.1.1, and 192.168.1.2 respectively. The address of AP1 is 192.168.1.100, and the address of AP2 is 192.168.1.101. There are ap database of both AP1 and AP2 on AC1 and AC2. Now AC1, AC2, AP1 and AP2 need to create the cluster. It can be achieved through the following automatic discovery configuration:

AC1 Configuration:

AC(config-wireless)#enable

AC(config-wireless)#discovery ip-list 192.168.1.2

AC(config-wireless)#discovery ip-list 192.168.1.100

AC(config-wireless)#discovery ip-list 192.168.1.101

AC(config-wireless)#discovery method ip-poll

AC2 Configuration:

AC(config-wireless)#enable

AC(config-wireless)#discovery ip-list 192.168.1.1

AC(config-wireless)#discovery ip-list 192.168.1.100

AC(config-wireless)#discovery ip-list 192.168.1.101

AC(config-wireless)#discovery method ip-poll

2. Automatic discovery configuration example based on IPv6 list.

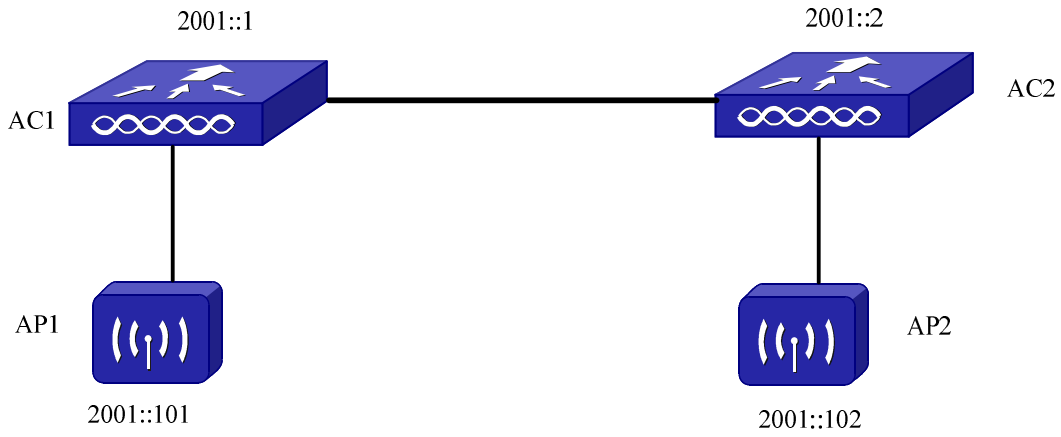


Fig 1-2 typical application environment of automatic discovery of IPv6

As shown in Fig 1-2, the wireless address of AC1 and the AC2 are 2001::1 and 2001::2 respectively. The address of AP1 is 2001::100, and the address of AP2 is 2001::101. There are ap database of both AP1 and AP2 on AC1 and AC2. Now AC1, AC2, AP1 and AP2 need to create the cluster. It can be achieved through the following automatic discovery configuration:

AC1 configuration：

AC (config-wireless)# no discovery ip-list 192.168.1.2

AC (config-wireless)#no auto-ip-assign

AC (config-wireless)#enable

AC (config-wireless)#static-ipv6 2001::1

AC (config-wireless)#enable

AC (config-wireless)#discovery ipv6-list 2001::2

AC(config-wireless)# discovery method ip-poll

AC (config-wireless)#sho wireless peer-switch

IP Address	Vendor ID	Disc. Reason	Age
2001::2	Digital China (Shan.	IP Poll	0d:00:00:08

AC (config-wireless)#

AC(config-wireless)# discovery ipv6-list 2001::101

AC(config-wireless)# discovery ipv6-list 2001::102

AC(config-wireless)#discovery method ip-poll

AC2 configuration：

AC (config-wireless)# no discovery ip-list 192.168.1.1

AC (config-wireless)#no auto-ip-assign

AC (config-wireless)#enable

AC (config-wireless)#static-ipv6 2001::2

AC (config-wireless)#enable

AC(config-wireless)# discovery method ip-poll

AC(config-wireless)# discovery ipv6-list 2001::101

AC(config-wireless)# discovery ipv6-list 2001::102

AC(config-wireless)# discovery method ip-poll

3. Automatic discovery configuration example based on layer2 broadcast.

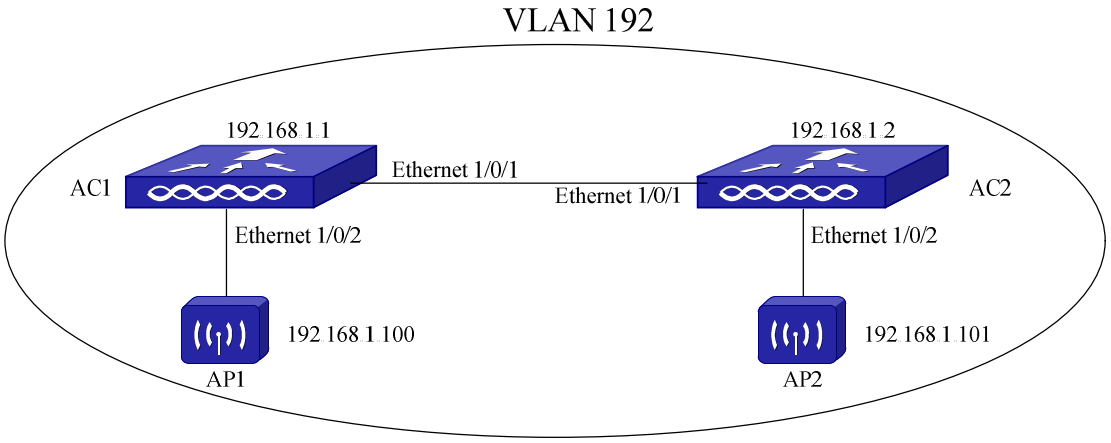


Fig 1-3 typical application environment of automatic discovery of layer2 broadcast

As shown in Fig 1-3, create the cluster on AC1, AC2 and AP1, AP2. All equipments are in VLAN192. The port Ethernet1/0/1 and Ethernet1/0/2 of AC1 and AC2 will be included in VLAN192. AC1 and AC2 adopt automatic discovery of layer2 broadcast, the configuration method is as bellow:

AC1 Configuration:

AC(config)#vlan 192

AC(config-vlan192)#switchport interface Ethernet 1/0/1;1/0/2

AC(config-vlan192)#exit

AC(config)#wireless

AC(config-wireless)#enable

AC(config-wireless)#discovery vlan-list 192

AC(config-wireless)#discovery method l2-multicast

AC2 Configuration:

AC(config)#vlan 192

AC(config-vlan192)#switchport interface Ethernet 1/0/1;1/0/2

AC(config-vlan192)#exit

AC(config)#wireless

AC(config-wireless)#enable

AC(config-wireless)#discovery vlan-list 192

AC(config-wireless)#discovery method l2-multicast

1.4 Automatic Discovery Configuration Troubleshooting

If the automatic discovery function cannot be used normally, please check if it is wrong with the following reasons:

- If the IP address of AC or AP which is discovered exists in IP automatic discovery list;
- If the VLAN that discovered AC or AP belongs to it exists in automatic discovery VLAN list of layer2 broadcast;
- When using controller as DHCP Server, if there is AP address got automatically which is conflict to static address of other equipments in network. If this case exists, enable ping detection function of conflict prevention on DHCP Server through **ip dhcp conflict ping-detection enable** command to avoid this case. This way can also avoid distributing IP address which is conflict to other equipments static address for client which related to AP.
- Examine if the relevant automatic discovery methods are enabled through **show wireless discovery** command.
- If the network is connected.

Chapter 2 Automatic Deployment and Duplex Authentication

2.1 Introduction to Automatic Deployment and Duplex Authentication

The network is an open space. For avoiding the unknown equipments to join to cluster to bring the potential risk, duplex authentication function can be enabled. This command allows equipments with certificate passing by authentication and joining the cluster through issuing X.509 certificate. This function includes producing, distributing, saving and using of certificate.

Creating connection between AC and AC or between AC and AP and making up the cluster are achieved through automatic discovery. The automatic discovery function is flexible and simple to configure but it is not safe enough. The cluster management function of wireless controller is added duplex authentication to increase security and prevent equipments without authority to access in the cluster. The practices are that every device produces the only private key and public key (certificate) through RC4+MD5 algorithm, and then authorize for the other side through certificate exchanging function or certificate requesting function to exchange certificate. For this cluster, the certificate transmission in ACs is achieved through certificate exchanging and certificate requesting function. The certificate transmission between AC and AP is achieved through automatic deployment of AP.

2.2 Introduction to Automatic Deployment

This cluster supports duplex authentication function to improve security. Duplex authentication requests both sides of detecting saving the certificate of other side, so certificate distribution and transmission become a problem. Cluster management supports the most basic and straightforward manual distribution function, it can copy contents that certificate considers to the relevant equipment. For improving the degree of automation and making easy of unity management of the whole cluster, the cluster provides automatic deployment function to distribute certificates.

Automatic deployment includes deployment for AP and for AC. Deployment for AC is through AC controller, it can deploy AP joined the cluster again and it also can deploy AP which does not join the cluster (redeployment of AP). As long as appointing AC for AP on

AC controller, the certificate they need when authenticating will transmit automatically in the cluster, then automatic discovery is the next. Deployment for AC means adding AC to the cluster. This AC needs to get certificates of all AC in the cluster, every AC in the cluster also needs to get the certificate of this AC, This process can be achieved by any AC in the cluster, it is responsible for transit of certificate between ACs.

2.3 Automatic Deployment and Duplex Authentication Configuration

Automatic deployment and duplex authentication configuration list:

1. Delete AP record in AP Provisioning table
2. Appoint effective Profile ID in automatic deployment for AP
3. Configure Primary AC and Backup AC for automatic deployment AP
4. Start automatic deployment
   （1）Start automatic deployment of AP on AC Controller
   （2）Start automatic deployment function of this machine on AC
   （3）Start automatic deployment with the appointed AC
   （4）Un-Managed AP redeployment
5. X.509 certificate configuration
   （1）Generate X.509 certificate on AC
   （2）Trigger AC to request X.509 certificate before automatic deployment
   （3）Initialize the trigger of X.509 certificate exchange
6. Configure agetime recorded in AP Provisioning table
7. Enable duplex authentication function of the cluster

1. Delete AP record in AP Provisioning table

Command	Explanation
Admin Mode	
clear wireless ap provisioning [<*macaddr*>]	Delete one or all record of AP in AP Provisioning table.

2. Appoint effective Profile ID in automatic deployment for AP

Command	Explanation
Admin Mode	
wireless ap provision <*macaddr*> profile <*1-1024*> **no wireless ap provision <*macaddr*>**	Appoint profile ID for AP and it becomes effective when disposing automatically. The no command cancels the appointed

profile	effective profile ID.

3. Configure Primary AC and Backup AC for automatic deployment AP

Command	Explanation
Admin Mode	
wireless ap provision <*macaddr*> switch {backup | primary} {<*ipaddr*>|<*ipv6addr*>}	Configure primary and backup AC for AP of automatic disposition. The default address of AC is 0.0.0.0.

4. Start automatic deployment

Command	Explanation
Admin Mode	
wireless ap provision start	Begin the automatic disposition of AP on AC Controller.
Wireless Global Mode	
switch-provisioning **no switch-provisioning**	Enable the function of automatic disposition of this switch. The no command disables the function of automatic disposition.
Admin Mode	
wireless switch provision <*ip address*>	Notice local AC and the appointed AC to start automatic deployment.

5. X.509 certificate configuration

Command	Explanation
Admin Mode	
wireless certificate-generate	Generate X.509 certificate on AC.
wireless switch certificate-request {<*ipaddr*>|<*ipv6addr*>}	Trigger AC to request X.509 certificate before automatic deployment.
wireless cluster exchange-certificate	Initialize the trigger of X.509 certificate exchange.

6. Configure agetime recorded in AP Provisioning table

Command	Explanation
Wireless Global Mode	
agetime ap-provisioning-db <*0-240*> **no agetime ap-provisioning-db**	Configure the ageing time for the record of AP Provisioning table. The no command recovers the ageing time to be

	default of 72 hours.

7. Enable duplex authentication function of the cluster

Command	Explanation
Wireless Global Mode	
mutual-authentication-mode **no mutual-authentication-mode**	Enable the mutual authentication function in the whole cluster. The no command disables the mutual authentication function in the whole cluster.

2.4 Automatic Deployment Configuration Examples

1. Automatic deployment configuration example of managed AP

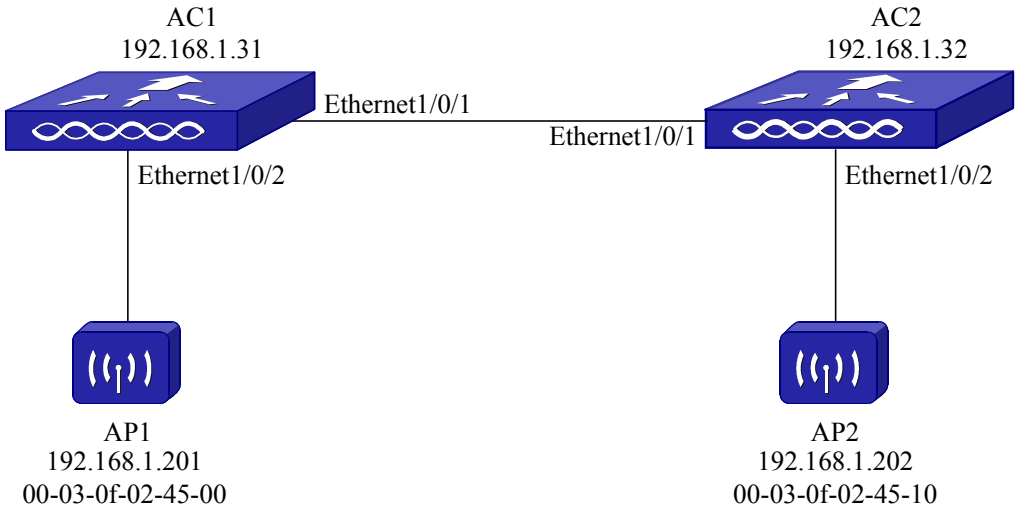


Fig 2-1 Typical application environment of automatic deployment of managed-AP

As shown in Fig 2-1, AC1 is controller. AP1 is managed by AC1 and AP2 is managed by AC2. Deploy automatically for AP1 and AP2 on AC1, primary AC is AC2, backup AC is AC1. The configuration method is as below:

AC1 configuration:

AC#wireless ap provision 00-03-0f-02-45-00 switch primary 192.168.1.32

AC#wireless ap provision 00-03-0f-02-45-00 switch backup 192.168.1.31

AC#wireless ap provision 00-03-0f-02-45-10 switch primary 192.168.1.32

AC#wireless ap provision 00-03-0f-02-45-10 switch backup 192.168.1.31

AC#wireless ap provision start

AC# wireless ap reset /*AP1 and AP2 are both managed by AC2 after restarted.*/

2. Automatic deployment configuration example of unmanaged AP

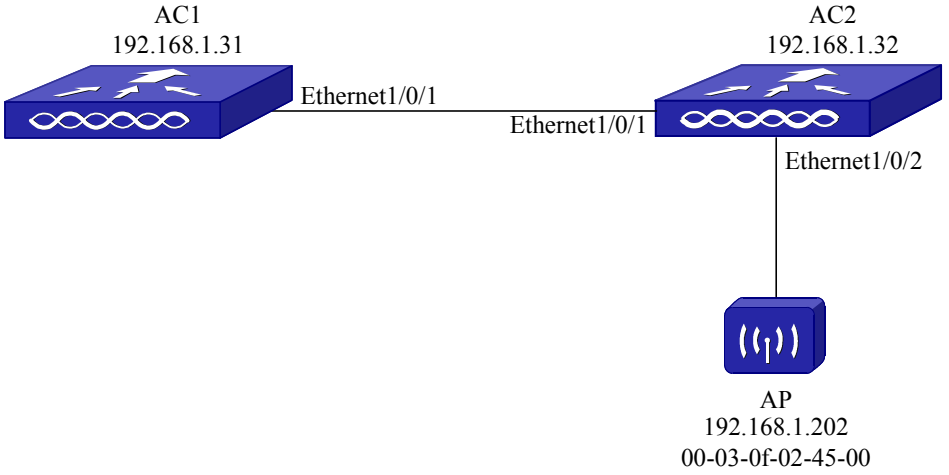


Fig 2-2 Typical application environment of automatic deployment of unmanaged-AP

As shown in Fig 2-2, create the cluster between AC1 and AC2 and AC1 is controller. AP is unmanaged. Deploy automatically for AP on AC1 to make it be managed by AC2.

AC1 configuration:

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

This configuration will be sent to all switches in the cluster.

Are you sure you want to continue? (y/n) y

Unmanaged AP Re-provisioning Mode set.

AC(config-wireless)#exit

AC(config)#exit

AC#wireless ap provision 00-03-0f-02-45-00 switch primary 192.168.1.32

AC#wireless ap provision start 00-03-0f-02-45-00

And then restart the AP, it will be managed by AC2 after restarted. Configure the command of show wi ap status on AC2 and the status of AP is shown as managed, the configuration status is shown as success.

3. Automatic deployment configuration example of AC

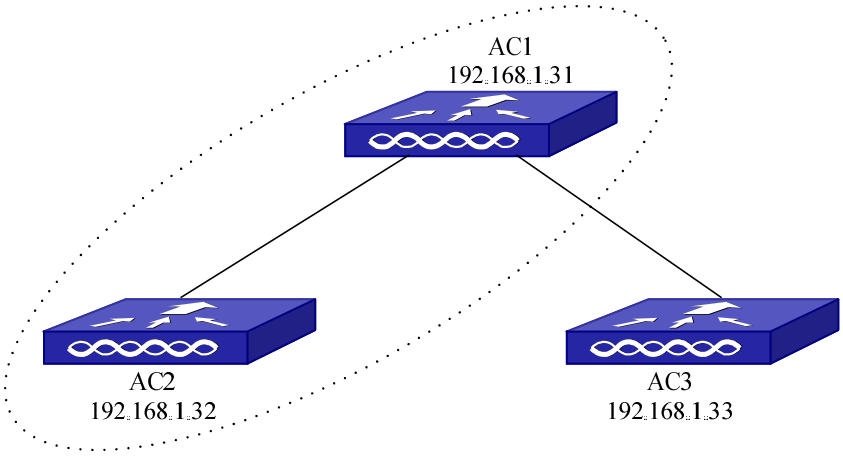


Fig 2-3 AC Typical application environment of automatic deployment

As shown in Fig 2-3, AC1 and AC2 make up the cluster and AC1 is AC controller. AC3 is out of the cluster. Now if user wants to make AC3 join to the cluster of AC1 and AC2, make AC3 create TLS connection with any AC (it is AC1 in this example) in the cluster through automatic deployment of AC. Then make AC3 join to the cluster and connect to other AC in the cluster.

Configuration method:

First, enable duplex authentication function on AC1 and AC3:

AC1 configuration:

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

Changing Mutual Authentication Mode might result in network traffic disruption. Are you sure you want to continue? [Y/N]y

Network Mutual Authentication Mode set.

AC3 configuration:

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

Changing Mutual Authentication Mode might result in network traffic disruption. Are you sure you want to continue? [Y/N]y

Network Mutual Authentication Mode set.

Then, request X.509 certificate of AC3 no AC1 and request X.509 certificate of AC1 on AC3:

AC1 configuration:

AC#wireless switch ceritificate-request 192.168.1.33

AC3 configuration:

AC#wireless switch ceritificate-request 192.168.1.31

Last, deploy automatically on AC3 and AC1:

AC3 configuration:

AC#wireless switch provision 192.168.1.31

At this time, connection can be created between AC3 and AC1. Then create connection with AC2.

2.5 Automatic Deployment and Duplex Authentication Troubleshooting

The switch as the wired and wireless intelligent integration controller has the phenomenon of that first starting load-time is too long. The reason is the switch needs to produce X.509 certificate of duplex authentication when it is enabled first time, it is about 20 to 30 minutes. Now the terminal equipment has no reaction, it does not show neither input. After 20 to 30 minutes, the terminal equipment will prompt port UP/DOWN information. This is a normal phenomenon of switch. Then user can input relevant command to manage.

When enabling duplex authentication or automatic deployment of AP/AC, if there is something wrong, please check if it is wrong with the reasons below:

- ☞ When deploying automatically for AP, the correct IP address of primary/backup AC is appointed or not.
- ☞ when duplex authenticating, the certificate saved on AC and AP is correct or not.

Chapter 3 Automatic Cluster Election

3.1 Introduction to Automatic Cluster Election

In order to make the whole cluster look like overall, user needs a unified interface to manage and configure. The cluster management module elects an AC as this role through automatic election function. It is responsible for collecting all information of all equipments in cluster, user can make configuration according to this information and then this configuration will be issued to the relevant equipment to be effective. This AC is called AC Controller. Automatic election is according to priority and IP address configured before, the AC whose priority is the highest and IP is the smallest will be elected to be AC Controller. If this AC breaks down, members of cluster will elect another AC as this role according to the rule. So the automatic election function also includes backup function, it means that there is always backup AC Controller. Even if there is only one AC in cluster, it will be AC Controller by itself. On AC which is selected to be AC Controller, the information of all AC, AP and clients in cluster can be examined; the situation of all equipments which are not discovered but not belong to this cluster also can be examined. AC Controller is generated automatically; the same logic determines the uniqueness of election result of all AC in cluster.

3.2 Automatical Cluster Election Configuration

Automatic cluster election function configuration list is as below:

1. Configure the priority of AC in automatic election.

1. Configure the priority of AC in automatic election.

Command	Explanation
Wireless Global Mode	
cluster-priority <*0-255*> **no cluster-priority**	Configure/recover the priority of AC in automatic election.

3.3 Automatical Cluster Election Configuration Examples

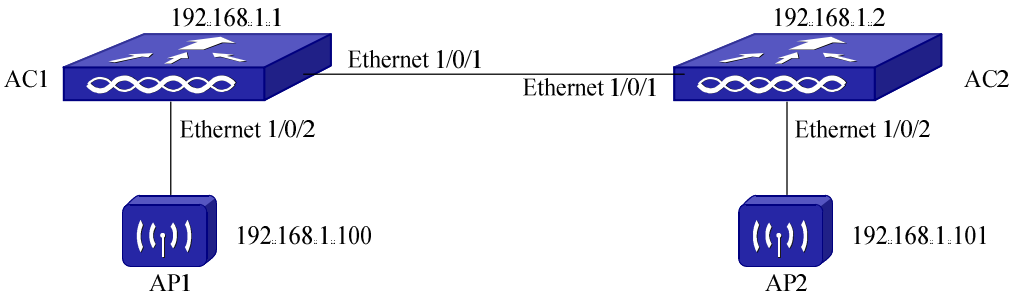


Fig 3-1 automatic cluster election configuration environment

As shown in Fig 3-1, create cluster between AC1 and AC2. The addresses of AC1 and AC2 are 192.168.1.1 and 192.168.1.2 respectively, the preset priority is 1 for each of them. Because the wireless ip address of AC1 is smaller, AC1 is AC controller of cluster. If user wants to make AC2 become AC controller of cluster, configure priority of AC2 larger than 1.

AC2 Configuration:

AC#config

AC(config)#wireless

AC(config-wireless)#cluster-priority 10

AC(config-wireless)#

After modifying priority of AC2, it will trigger the new election of AC controller. After election, AC2 can become the new AC controller of cluster.

3.4 Automatical Cluster Election Troubleshooting

If the appointed AC cannot be elected to be the new AC Controller in cluster, please check out if it is wrong with reasons below:

- If the wireless address of this AC is configured as the minimum wireless ip address in cluster;
- If this AC has the highest election priority in cluster;
- If the election priority of this AC is configured as 0. If it is configured as 0, it will not participate election of AC Controller;
- Check if the keepalive information sending and receiving between AC is normal through **debug wireless cluster packet all** command.

Chapter 4 Pushing Configuration

4.1 Introduction to Pushing Configuration

At many cases, the configuration of some or all AC in cluster is requested to be consistent. The functions supported by this wireless cluster are flexible and sundry, but configure all these functions are time consumeing. Pushing configuration function allows user to configure AC to be automatic transmission and apply it to any appointed ACs in cluster after configuring one AC. Only IP address, priority and port number are not in the range of pushing.

The sender AC of pushing configuration will save all configurations before pushing local configuration, and then it pushes these configurations. If the configuration of sender is changed by administrator during pushing, the configuration changed will not be transmitted to receiver in local pushing.

Currently, the functions which can be pushed supported by AC include: AP Database, AP Profile, Channel Powe, Discovery, Global, Known Client, Captive Portal, RADIUS Client, QoS ACL and QoS DiffServ. Undergo the pushing configuration discovery function is not pushed as default, others are pushed as default.

4.2 Pushing Configuration

Pushing configuration function of AC task list is as below:

1. Appoint configuration needed when pushing configuration for AC.
2. Enable AC pushing configuration

1. Appoint configuration needed when pushing configuration for AC

Command	Explanation
Wireless Global Mode	
peer-switch configuration [ap-database | ap-profile | captive-portal | channel-power | discovery | global | known-client | radius-client] **no peer-switch configuration [ap-database | ap-profile | captive-portal | channel-power | discovery | global | known-client | radius-client]**	Configure the pushing transmission for AC. The no command configures the pushing no transmission.

2. Enable AC pushing configuration

Command	Explanation
Admin Mode	
wireless peer-switch configure [<*ipaddr*> | <*ipv6addr*>]	Configure pushing for AC in the cluster.

4.3 Pushing Configuration Examples

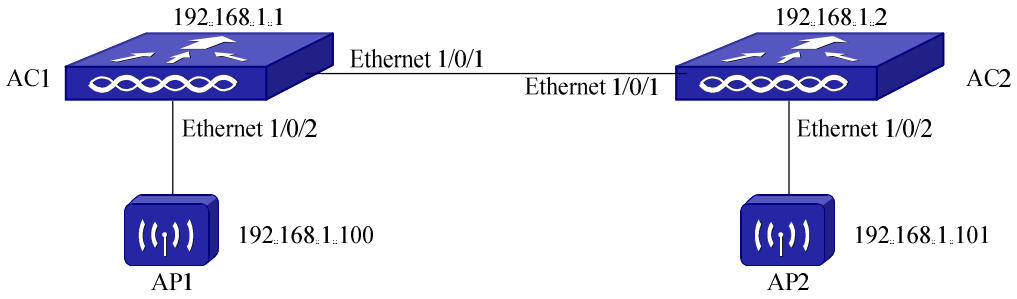


Fig 4-1 typical application environment of AC pushing configuration function

As shown in Fig 4-1, create cluster in AC1, AC2, AP1 and AP2. Now push wireless configuration of AC1 to AC2. Functions needed to transmit include: AP Database, AP Profile, Channel Power, Discovery, Global, Known Client, QoS ACL and QoS DiffServ.

AC1 configuration is as below:

AC(config)#wireless

AC(config-wireless)#peer-switch configuration discovery

AC(config-wireless)#no peer-switch configuration captive-portal

AC(config-wireless)#no peer-switch configuration radius-client

AC(config-wireless)#exit

AC(config)#exit

AC#wireless peer-switch configure 192.168.1.2

AC#

4.4 Pushing Configuration Troubleshooting

If pushing configuration is not successful, please check out if it is wrong with reasons below:

- Examine if the functions pushed is selected (the status is Enable) through **show wireless peer-switch configuration** command;
- If IP address of peer-switch when pushing configuration is correct;
- When pushing configuration, if pushing to peer-switch (do not appoint IP address of

peer-switch), please check out if the TLS connection between this machine and peer-switch is normal;

- ☞ If there is wrong configuration content or the configuration which is not supported by pushing configuration in the configuration needed pushing;
- ☞ If the country codes of sender and receiver of pushing configuration are different, it will cause pushing failure because ap database cannot be pushed.

Chapter 5 AP FLOOD Anti-attack

5.1 Introduction to AP FLOOD Anti-attack

After AP and AC discovered each other and created the TLS security connection, AP will be managed by AC successfully only if passed the authentication. If AP does not pass the authentication, it will carry out the discovery process with AC every 30 seconds. When there are many AP that did not pass the authentication, there will be many TCP connections and it will consume a large number of CPU resources. The CPU utilization will be 100% when it is serious. If enabled AP FLOOD anti-attack function, when the AP reconnection times exceeds the limited times within a certain time, the TCP connection with AC will be forbided temporarily and it can prevent the higher CPU utilization. Until the end of the aging time, or the administrator configures, it will be recovered the connection.

5.2 AP FLOOD Anti-attack Configuration

AP FLOOD anti-attack function configuration list is as below:

1. Enable/disable the AP FLOOD anti-attack function
2. Configure the detection time of AP FLOOD anti-attack function
3. Configure the maximum times of the allowed connection by AP FLOOD anti-attack function
4. Configure the aging time of the AP FLOOD anti-attack table
5. Showing configuration
6. Clear the AP from the AP FLOOD anti-attack table

1. Enable/disable the AP FLOOD anti-attack function

Command	Explanation
Wireless Global Mode	
wireless ap anti-flood **no wireless ap anti-flood**	Enable/disable the AP FLOOD anti-attack function.

2. Configure the detection time of AP FLOOD anti-attack function

Command	Explanation
Wireless Global Mode	
wireless ap anti-flood interval <1-15> **no wireless ap anti-flood interval**	Configure the detection time of AP FLOOD anti-attack function; no command recovers it to the

	default (5 minutes).

3. Configure the maximum times of the allowed connection by AP FLOOD anti-attack function

Command	Explanation
Wireless Global Mode	
wireless ap anti-flood max-conn-count <1-30> **no wireless ap anti-flood max-conn-count**	Configure the maximum times of the allowed connection by AP FLOOD anti-attack function; no command recovers it to be the default (4 times).

4. Configure the aging time of the AP FLOOD anti-attack table

Command	Explanation
Wireless Global Mode	
wireless ap anti-flood agetime <0-1440> **no wireless ap anti-flood agetime**	Configure the aging time of the AP FLOOD anti-attack table; no command recovers it to be the default (30 minutes).

5. Showing configuration

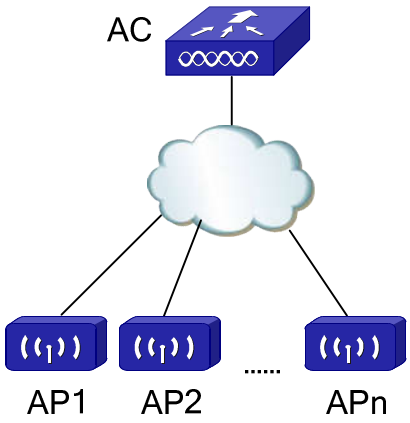
Command	Explanation
Admin Mode	
show wireless ap anti-flood	Show the current configuration parameters of the AP FLOOD anti-attack function.
show wireless ap anti-flood status	Show all the records of the AP FLOOD anti-attack table.

6. Clear the AP from the AP FLOOD anti-attack table

Command	Explanation
Admin Mode	
clear wireless ap anti-flood	Clear all the records from the AP FLOOD anti-attack table.

5.3 AP FLOOD Anti-attack Examples

Case:



There are many AP that did not pass the authentication, send the connection request to AC constantly. If user wants to detect the times of the connection between AP and AC are more than 5 in 10 minutes, make the AP join in the AP FLOOD anti-attack table and configure it not to connect in 60 minutes. The configuration of AC is as below:

First, enable the AP FLOOD anti-attack function and configure the parameters.

AC#config

AC(config)#wireless

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

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

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

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

Show the AP FLOOD anti-attack parameters configuration:

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

Show all the records in AP FLOOD table:

AC(config-wireless)#show wireless ap anti-flood status

Delete the AP from the anti-attack table and make it connect again; disable the AP FLOOD anti-attack function:

AC#clear wireless ap anti-flood

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

All AP flood entries cleared.

AC#config

AC(config)#wireless

AC(config-wireless)#no wireless ap anti-flood

5.4 AP FLOOD Anti-attack Troubleshooting

When configuring and using AP FLOOD anti-attack function, there may be something unusual or error because of the physical connection or configuration default. Please check out if it is wrong with reasons below:

- ☞ Ensure the physical connection is correct;
- ☞ Ensure the AP FLOOD anti-attack function has been enabled;
- ☞ Confirm if the AP has completed the limited connection times in the detection time through **show logging buffered** command under the admin mode, it will be joined in AP FLOOD table after the maximum times connections.

Chapter 6 Cluster Maintaining and Debugging

6.1 Introduction to Cluster Maintaining and Debugging

Maintaining and debugging cluster can be done through debug or SNMP network management software. When managing cluster through SNMP management, analyze and locate the bug in cluster according to trap information sent by AC.

6.2 Cluster Maintaining and Debugging Configuration

Cluster maintaining and debugging function task list is as below:

1. Configure flags of trap information
2. Configure information flag of syslogs
3. Enable SNMP TRAP function of whole cluster
4. Enable/disable debug information of cluster
5. Enable/disable debug information of SSL

1. Configure flags of trap information

Command	Explanation
Wireless Global Mode	
trapflags [{ap-failure | ap-state | client-failure | client-state | peer-ws | rf-scan | rogue-ap | wids-status | ws-status| attack-event}] **no trapflags [{ap-failure | ap-state | client-failure | client-state | peer-ws | rf-scan | rogue-ap | wids-status | ws-status| attack-event }]**	Enable SNMP Trap function against some events on AC. The no command disables the SNMP Trap function.

2. Configure information flag of syslogs

Command	Explanation
Wireless Global Mode	
syslogflags [{ap-failure | ap-state |	Enable wireless syslog function. The no

client-failure | client-state | peer-ws | rogue-ap | wids-status | ws-status| attack-event}] **no syslogflags [{ap-failure | ap-state | client-failure | client-state | peer-ws | rogue-ap | wids-status | ws-status| attack-event }]**	command disables this function.
Admin Mode	
show wireless syslogsflags	Show whether the syslogflags on-off of AC is enabled.

3. Enable SNMP TRAP function of whole cluster

Command	Explanation
Global Mode	
snmp-server enable traps wireless **no snmp-server enable traps wireless**	Enable the wireless SNMP Trap function of AC in the whole cluster. The no command disables the SNMP Trap function.

4. Enable/disable debug information of cluster

Command	Explanation
Global Mode	
debug wireless cluster packet {all | receive | send | dump} **no debug wireless cluster packet {all | receive | send | dump}**	Enable the packets printing debugging information of information collection and cluster controlling. The no command disables the information.
debug wireless cluster internal **no debug wireless cluster internal**	Enable the general debugging information of information collection and cluster controlling. The no command disables the general debugging information.

5. Enable/disable debug information of SSL

Command	Explanation
Global Mode	
debug wireless ssl packet {all | receive | send} **no debug wireless ssl packet {all | receive | send}**	Enable the packets printing debugging information of SSL. The no command disables the information.
debug wireless ssl timer	Enable the timer debugging information of

no debug wireless ssl timer	SSL. The no command disables the information.
debug wireless ssl error **no debug wireless ssl error**	Enable the anomalous debugging information of SSL. The no command disables the information.
debug wireless ssl detail **no debug wireless ssl detail**	Enable the detailed debugging information of SSL. The no command disables the information.
debug wireless ssl internal **no debug wireless ssl internal**	Enable the normal debugging information of SSL. The no command disables the information.