Content

Chapter 1 Device-finger Recognition

1.1 Introduction to Device-finger Recognition

DHCP protocol is one of necessary protocol that each network terminal device supported, and it can used to get a dynamic IP address. All part of DHCP is described by option way, each filed option has different meaning. Option numbers, sequence and combination may be different when different operation system send DHCP request, so it can identify operating system quickly by identify permutation and combination of DHCP parameters. For example, subparameters permutation and combination of option 55 may be different for different operation system, according to the parameters permutation of option; users can identify hundreds of terminal equipment and operation system types.

Common DHCP packets carried related information in option is as follows:

Option 12 usually carries equipment manufacturer information;

Option 55 Parameter Request List, different operation system request different parameter type or sequence of parameter list, user can identify different terminal operation system by different sequence parameter;

Vendor class identifier of option 60 usually carries software information that equipment used;

Option 61 carries mac address that has manufacturer information of hardware.

DCN wireless control system (AC&AP) authencate carried operation system attribute value when request IP address, it matched with predefined DHCP attributes in controller, users can get corresponding authority after pass match authencation. According to device-finger recognition, users can send different ACL rules to different terminal equipment and get different access rights to increase the security of Enterprise network and resources; users also can send different web access page for different terminal system, and improve the user experience.

DCN wireless control system device-finger recognition function is realized by AC and AP, the specific process is as follows:

(1) Configure device-finger information in AC wireless global mode;

(2) Configure device-finger recognition switch in AC network mode, and sending command “wireless ap profile apply <ap profile id>” to AP;

(3) AP receives the information that configures send, open corresponding device-finger recognition function in VAP, and start to listen client DHCP Request packets.

(4) AP listen to DHCP Request packs ,there have option 55 or option 60 attribute values in packets, and users use key client mac can check user table in AP wireless table,

AP create Device-Finger request messages to AC, request to recognize device type of client and according ACL rules.

(5) After AC receive Device-Finger request messages, parse DHCP option attribute type and value, and matched with DHCP attribute value that configured in AC. If matched, update device-description information of client table in association client tree; if matched and configured ACL rules in device-finger information mode, create Device-Finger response information to AP and sending ACL rules related information to AP; if not match with device-finger information or matched but ACL rules do not exist, return error and sending nothing information to AP.

(6) After AP received Device-Finger response messages, parse client mac, ACL type and name, ACL rules take effect on client.

1.2 Basic Device-finger Recognition Configuration

The basic configuration sequence of device-finger recognition is as follows:

1. Configure device-finger recognition information
2. Configure device type bind ACL rule
3. Configure device-finger recognition switch
4. Sending device-finger recognition configuration
5. Show user's device-finger recognition information
6. Show related configuration of device-finger recognition information
7. Device-finger recognition debug

1. Configure Device-finger Recognition Information

Command	Explanation
Wireless global configuration mode	
device-finger dhcp-option {55|60} {equals|starts-with} <option-number> device-description <description-info>	Configure device-finger recognition information and the most AC can configured device-finger information is 256.
no device-finger dhcp-option {55|60} {equals|starts-with} <option-number>	Delete device-finger recognition information, corresponding to delete configured all ACL rules; when the delete information does not exist, give an error messages.

2. Configure device type bind ACL rule

Command	Explanation
device-finger configuration mode	

access-control {down|up} {ip{<1-199>|<acl-name>}|ipv6<acl-name>|mac<acl-name>}
no access-control {down|up}
	Add one kind of input, output ACL rules information of terminal users. ACL supported types are as follows: L2 is MAC, L3 is IP, and L4 is port. When configure ACL rules, users must be sure that the ACL rule already exists. Add or delete ACL rules do not work for authenticated and online users, it only works for the terminal users which are new authenticated and online.

3. Configure device-finger recognition switch

Command	Explanation
Network configuration mode	
device-finger enable **no device-finger enable**	Open or close device-finger recognition function. Fingerprint recognition function aimed at some VAP of AP.

4. Sending device-finger recognition configuration

Command	Explanation
Admin configuration mode	
wireless ap profile apply <*1-1024*>	Sending specified profile configuration file to the AP that configured corresponding configuration file.

5. Show user's device-finger recognition information

Command	Explanation
Admin configuration mode	
Show wireless client device-type [<device-descrip>|]	Show all users' device-finger information or all users that a type of device-finger information corresponded.

6. Show related configuration of device-finger recognition information

Command	Explanation
Admin configuration mode	
show wireless network <network-id>	Show device-finger recognition switch status in current network.
Show wireless client <client-mac>	Show device types description information

status	of current users.
show wireless client <client-mac>client-qos[radius|device|] status	Show device types description information of current users or all online users.
show wireless device-finger status	Check all device-finger switch status in current network.
show wireless device-finger configuration	Show all device-finger configuration.

7. Device-finger recognition debug

Command	Explanation
Admin configuration mode	
debug wireless device-finger detail event <client-mac> **no debug wireless device-finger detail event**	Open/Close debug wireless device-finger detail events switch.
debug wireless device-finger trace **no debug wireless device-finger trace**	Open/Close debug wireless device-finger trace switch.
debug wireless device-finger error **no debug wireless device-finger error**	Open/Close debug wireless device-finger error switch.
debug wireless device-finger packet all|send|receive|dump **no debug wireless device-finger packet all|send|receive|dump**	Open/Close debug wireless device-finger packet switch.
no debug all	Close debug wireless device-finger recognition information at the same time.
Show debugging other	Display all the debug switches that wireless device-finger opened at the same time.

1.3 Device-finger Recognition Configuration Example

Typical case 1:

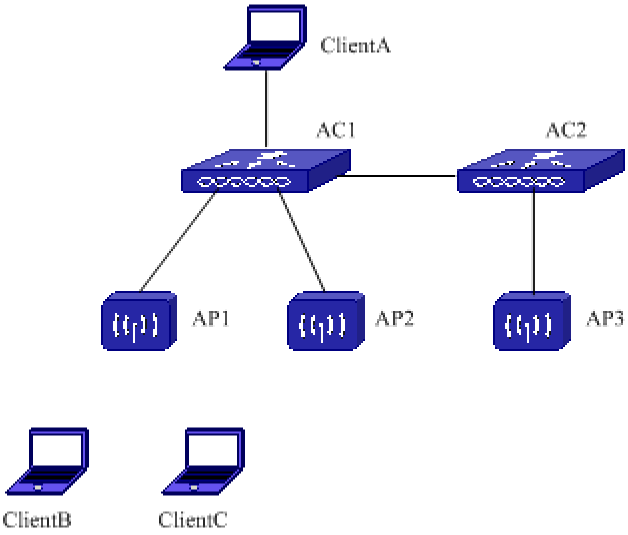

Fig 1-1 Typical device-finger recognition example

Topology description: as show in the Fig 1-2, AC connects AP by layer-2 network, client B and client C associated to VAPO. Bind VAPO to network 20. Client A linked to AC1 by wired, the IP address of client A is 80.1.1.5. Client B, client C and client A can communicate with each other in layer-2.

Configuration description: client B and client C are different terminal type, configure a device-finger information x201 mapped client B and a device-finger information apple mapped client C in AC. Bind an ACL list abc in client B device-finger information, and forbid client B communicate with client A, the device-finger information of client C do not bind any ACL lists.

Result: after client B and client C associated VAPO and get address, their device-finger information can be recognized correctly in AC, client B can not transmit data with client A, client C can transmit data with client A.

Specific configuration is as follows:

The configuration of AC1:

1. Configure ACL lists

```
AC1#config
AC1(config)#ip access-list standard abc
AC1 (config-ip-std-nacl-abc)#deny host-source 80.1.1.5
AC1 (config-ip-std-nacl-abc)#permit any-source
```

2. Configure device-finger recognition information

```
AC1(config)#wireless
AC1(config-wireless)#device-finger dhcp-option 55 starts-with 010f03062c device-description x201
AC1(config-wireless)#device-finger dhcp-option 55 starts-with 0103060f device-description apple
```

3. Configure bind ACL rule that device-finger is x201

```
AC1(config-wireless)#device-finger dhcp-option 55 starts-with 010f03062c device-description x201
AC1 (config-device-finger)#access-control down ip abc
```

4. Open device-finger recognition switch

```
AC1 (config)#wireless
AC1 (config-wireless)#network 20
AC1 (config-network)#device-finger enable
```

5. Open client qos switch in wireless global mode and network mode

```
AC1 (config-network)#client-qos enable
AC1 (config-network)#exit
AC1 (config-wireless)#ap client-qos
```

6. Sending device-finger recognition configuration to AP

```
AC1#wireless ap profile apply 20
```

1.4 Device-finger Recognition Troubleshooting

When using device-finger recognition function, ACL list may be failure, device-finger failed and so on, there problems may be cause by the following reasons:

- When band ACL failed, users can check whether open ap client-qos in wireless global mode or client qos in network mode.
- When device-finger recognition failed, users can check whether device-finger recognition information configured correctly in AC or device-finger recognition switch whether open in associated network.