

目录

第 1 章 终端指纹识别	1-1
1.1 终端指纹识别介绍	1-1
1.2 终端指纹识别基本配置	1-1
1.3 终端指纹识别配置举例	1-3
1.4 终端指纹识别排错帮助	1-4

第1章 终端指纹识别

1.1 终端指纹识别介绍

DHCP 协议本身是各个网络终端设别都能够支持的必备协议之一，用来申请获得动态 IP 地址。DHCP 的所有部分都是以 Option 的方式描述，每类 Option 字段都有不同的含义。不同的操作系统在发送 DHCP 请求的时候的 Option 数量、顺序和组合都可能完全不同，因此仅仅先区分 DHCP 的参数排列组合就可以进行快捷的操作系统识别。例如类型 55 的 Option 里的子参数排列组合会根据不同的操作系统而不同，根据该 Option 的参数排列，可以区分数百种终端设备类型及操作系统类型。

常见的 DHCP 报文中 option 会携带的相关信息如下：

option 12 的 host name 中一般会携带设备生产厂家信息；

option 55 Parameter Request List，一般不同的操作系统请求参数列表的参数种类或者顺序不一样，可以通过不同的参数序列值来区分不同的终端操作系统；

option 60 的 vendor class identifier 字段一般会携带设备使用软件的信息；

option 61 携带的 mac 地址携带硬件的厂家信息。

DCN 无线控制系统（AC&AP）验证客户端申请 IP 地址时所携带的操作系统属性值，与控制器（AC）内预先定义 DHCP 属性相匹配，匹配验证通过后即可获得相应权限。通过终端指纹识别技术，可以给不同的终端设备下发不同的 ACL 规则，对不同类型的设备具有不同的访问权限，较大的提高了企业网络和资源的安全性；也可以针对不同的终端系统发送不同的 web 访问页面，能较好的增加用户体验。

DCN 无线控制系统终端指纹识别功能由 AC 和 AP 协作实现，具体流程如下所示：

- (1) AC 无线全局模式下配置终端指纹信息；
- (2) AC network 模式下配置终端指纹识别功能开关，执行 wireless ap profile apply <ap profile id>命令下发给 AP；
- (3) AP 接收到配置下发消息，在对应的 VAP 上开启终端指纹识别功能，开始侦听 client DHCP Request 报文；
- (4) AP 侦听到 DHCP Request 报文且报文中有 option 55 或 60 属性值，且以 client mac 为 key 在 AP 无线表项中能查到用户表项，则 AP 组建 Device-Finger request 消息给 AC，请求识别 client 的终端类型及其对应的 ACL 规则；
- (5) AC 收到 Device-Finger request 消息后，解析 DHCP option 属性类型和属性值与 AC 上预先配置好的 DHCP 属性值进行匹配。若匹配，则更新 association client tree 中 client 表项的 device-description 信息；若匹配且该终端指纹信息模式下有配置 ACL 规则，则组建 Device-Finger response 消息给 AP，将 ACL 规则相关信息下发给 AP；若终端指纹信息不匹配、或者已匹配但是 ACL 规则不存在，则返回错误，不给 AP 发送任

何消息；

- (6) AP 收到 Device-Finger response 消息后，解析出 client mac、ACL 类型及其名称，对该 client 生效该 ACL 规则。

1.2 终端指纹识别基本配置

终端指纹识别的基本配置序列：

1. 配置终端指纹识别信息
2. 配置终端类型绑定 ACL 规则
3. 配置终端指纹识别开关
4. 终端指纹识别配置下发
5. 查看用户的终端指纹信息
6. 查看终端指纹信息的相关配置
7. 终端指纹识别 Debug

1. 配置终端指纹识别信息

命令	解释
无线全局配置模式	
device-finger dhcp-option {55 60} {equals starts-with} <option-number> device-description <description-info> no device-finger dhcp-option {55 60} {equals starts-with} <option-number>	配置一条终端指纹识别信息，AC 上支持最多配置 256 条终端指纹信息。 no 命令删除一条终端指纹识别信息，且对应删除其配置的所有 ACL 规则，当 no 命令删除的信息不存在时，给出错误提示。

2. 配置终端类型绑定 ACL 规则

命令	解释
device-finger 配置模式	
access-control {down up} {ip{<1-199> <acl-name>}} ipv6<acl-name> mac<acl-name>} no access-control {down up}	配置添加/删除某一类型终端用户的出口、入口方向 ACL 规则信息。ACL 支持类型为：L2 为 MAC, L3 为 IP, L4 为端口。配置 ACL 规则时，需要保证该 ACL 规则已存在。添加、删除的 ACL 规则对已认证在线的用户不起作用，只对以后新认证上线的该类终端用户起作用。

3. 配置终端指纹识别开关

命令	解释
Network 配置模式	

device-finger enable	开启或关闭终端指纹识别功能。指纹识别功能针对于 AP 的某个 VAP 生效。
no device-finger enable	

4. 终端指纹识别配置下发

命令	解释
特权配置模式	
wireless ap profile apply <1-1024>	下发指定 profile 配置文件给配置了相应配置文件的 AP。

5. 查看用户的终端指纹信息

命令	解释
特权配置模式	
Show wireless client device-type [<device-descrip>]	显示所有在线用户的终端指纹信息或者某一类型终端指纹信息所对应的所有用户。

6. 查看终端指纹信息的相关配置

命令	解释
特权配置模式	
show wireless network <network-id>	查看当前 network 下终端指纹识别开关状态。
Show wireless client <client-mac> status	显示当前用户的终端类型描述信息。
show wireless client <client-mac>client-qos[radius device[]] status	查看当前用户或者所有在线用户的终端类型描述信息。
show wireless device-finger status	查看当前所有 network 下的 device-finger 开关状态。
show wireless device-finger configuration	查看当前所有终端指纹配置信息。

7. 终端指纹识别 Debug

命令	解释
特权配置模式	
debug wireless device-finger detail event <client-mac> no debug wireless device-finger detail event	打开/关闭无线终端指纹识别功能的详细事件调试开关。

debug wireless device-finger trace no debug wireless device-finger trace	打开/关闭无线终端指纹识别功能的跟踪调试开关。
debug wireless device-finger error no debug wireless device-finger error	打开/关闭无线终端指纹识别功能的错误调试开关。
debug wireless device-finger packet all send receive dump no debug wireless device-finger packet all send receive dump	打开无线终端指纹识别功能的报文调试开关。
no debug all	同时关闭无线终端指纹识别功能的 debug 信息。
Show debugging other	同时显示无线终端指纹识别已打开的调试开关。

1.3 终端指纹识别配置举例

典型案例 1:

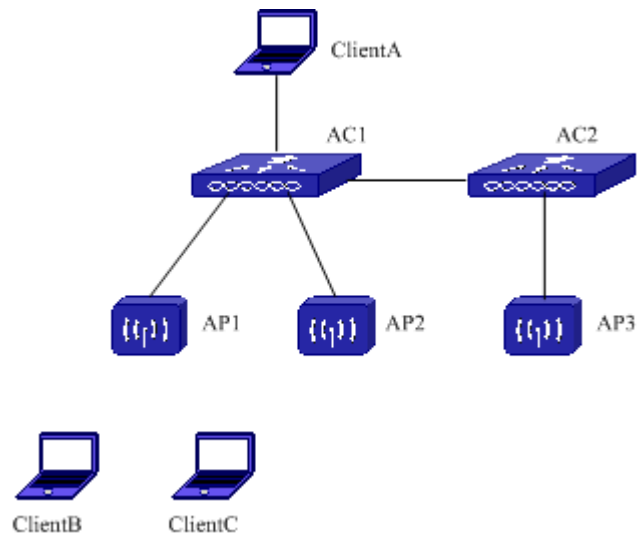


图 1-1 终端指纹识别典型案例

案例拓扑说明：如图 1-1 所示的拓扑，AC 通过二层网络连接到 AP，client B 和 client C 关联到 VAP0。VAP0 绑定 network 20。client A 通过有线连接到 AC1，Client A 的 IP 地址为 80.1.1.5，client B，client C 和 client A 二层互通。

案例配置说明：client B 和 client C 为不同的终端类型，在 AC 上配置一条匹配 client B 的终端指纹信息 x201 和一条匹配 client C 的终端指纹信息 apple。在 client B 指纹识别信息上绑定一条 ACL 列表 abc，禁止 client B 和 client A 之间数据通信，client C 的指纹识别信息上不绑定任何 ACL 列表。

案例结果说明：client B 和 client C 关联到 VAP0 获取地址后，他们的终端指纹信息都能在 AC 上正确识别，client B 和 client A 间数据不通，client C 和 client A 间数据互

通。

具体配置如下：

AC1 的配置序列：

1. 配置 ACL 列表

```
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. 配置终端指纹识别信息

```
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. 配置终端指纹信息为 x201 的绑定 ACL 规则

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

```
AC1 (config-device-finger)#access-control down ip abc
```

4. 开启终端识别识别开关

```
AC1 (config)#wireless
```

```
AC1 (config-wireless)#network 20
```

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

5. 在无线全局模式和 network 模式下开启 client qos 开关

```
AC1 (config-network)#client-qos enable
```

```
AC1 (config-network)#exit
```

```
AC1 (config-wireless)#ap client-qos
```

6. 把终端指纹识别配置下发到 AP

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

1.4 终端指纹识别排错帮助

在使用终端指纹识别功能时，可能会出现 ACL 列表失效，终端指纹识别失败等问题，请检查是否是如下原因：

- ☞ 当绑定的 ACL 失效，可以查看无线全局模式下 ap client-qos 和 network 模式下 client qos 开关是否打开；
- ☞ 当终端指纹识别失败，可以查看终端指纹识别信息是否正确在 AC 上配置，终端指纹识别开关是否在所关联的 network 下开启。