

知 某局点终端无法接入hybrid-remote-ap的经验案例

AC备份 AP管理 wlan接入 杨海严 2017-08-15 发表



某局点总部部署无线控制器WX5540E（Version 5.20, Release 2609P58），分支部署WA2620i-AGN，配置hybrid-remote-ap，做本地转发，AP和AC正常连接时，终端接入正常，数据转发正常；但是当AP和AC断开连接时，分支的无线终端始终无法接入。

1、收集现场配置，查看是否有明显错误

（1）map文件hybrid-remote-ap.txt内容

system-view

vlan 10 //业务vlan10

interface GigabitEthernet1/0/1

port link-type trunk //上行口设置为trunk口

undo port trunk permit vlan 1

port trunk permit vlan 10 //放通业务vlan10

（2）无线关键配置

#

interface WLAN-ESS10

port link-type hybrid //配置为hybrid口

undo port trunk permit vlan 1

port hybrid vlan 10 untagged //业务vlan10 untagged

port hybrid pvid vlan 10 //pvid设置为业务vlan10

port-security port-mode psk

port-security tx-key-type 11key

port-security preshared-key pass-phrase simple 12345678

#

wlan service-template 10 crypto

ssid hybrid-remote-ap

bind WLAN-ESS 10 //绑定ESS接口

cipher-suite ccmp

security-ie rsn

client forwarding-mode local vlan 10 //本地转发

authentication-mode backup //认证模式为backup

wlan ap hybrid-remote-ap01 model WA2620i-AGN

map-configuration hybrid-remote-ap.txt //下发map文件

serial-id 219801A0CMC146000765

hybrid-remote-ap enable //开启hybrid-remote-ap功能

radio 1

service-template 10 //绑定服务模板

radio enable //开启射频口

radio 2

service-template 10

radio enable

查看WX5540E上的配置都是正常的，未发现问题。

2、根据现场配置实验室复现问题

（1）和现场一样的配置，问题复现，当AP和AC断开连接时，分支的无线终端始终无法接入。

（2）尝试配置不加密的无线服务模板

#

interface WLAN-ESS20

port link-type hybrid

undo port trunk permit vlan 1

port hybrid vlan 10 untagged

port hybrid pvid vlan 10

```
#
wlan service-template 20 clear
ssid hybrid-remote-ap- clear
bind WLAN-ESS 20
    client forwarding-mode local vlan 10
authentication-mode backup

wlan ap hybrid-remote-ap01 model WA2620i-AGN
    radio 1
    service-template 20
    radio enable
    radio 2
    service-template 20
    radio enable
```

测试：AP和AC正常连接时，终端接入正常，数据转发正常；当AP和AC断开连接时，分支的无线终端能正常连接无线网络，应该和加密的无线服务模板有关。

（3）authentication-mode backup 即AC和AP的连接出现故障后如果有新的终端接入，将自动使用AP本地认证，也就是说AP需要承担终端认证的功能，登录AP上查看配置：

```
#
version 5.20, Release 1508P08
#
sysname hybrid-remote-ap01
.....
#
telnet server enable
#
password-recovery enable
.....
```

AP上没有配置port-security enable，而CCMP+RSN+PSK是必须配置端口安全的，这和之前的现象符合，不加密的无线服务不涉及端口安全，所以能正常接入。

（4）在AP上配置port-security enable
当AP和AC断开连接时，分支的无线终端能正常连接无线网络，可以判断是没有配置端口安全导致。

map文件hybrid-remote-ap.txt内容增加port-security enable即可。

- （1）明确认证模式backup的含义，即 AP和AC连接正常时，使用AC集中式认证；AC和AP的连接出现故障后，原有的客户端不会下线，如果有新的客户端需要接入，将自动使用AP本地认证。
- （2）遇到问题要大胆猜想，小心求证，注意技术点之间的关联。