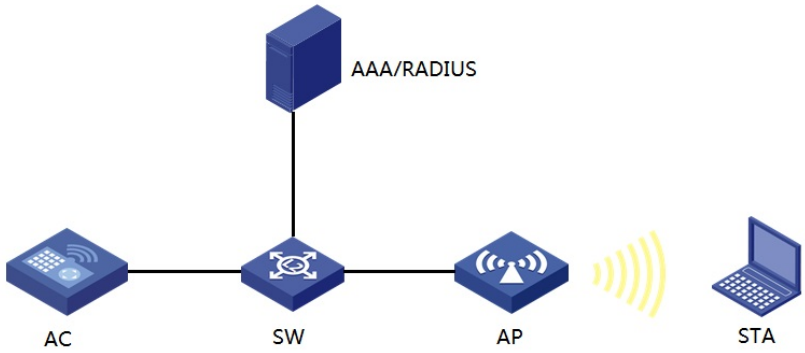
H3C无线控制器AC远程Portal下发ACL典型配置举例(V7)

ACL Portal 陈少华 2017-12-27 发表

1.AP通过交换机与AC相连,在AC开启DHCP server功能，为AP和客户端分配IP地址。
2.AP注册到AC上，业务网段属于vlan 161，需portal认证通过后才能访问网络资源，但是访问不能访问192.168.164.0段。

图1 AC启用portal认证对接imc 实现用户接入认证



(1).AC主要配置：

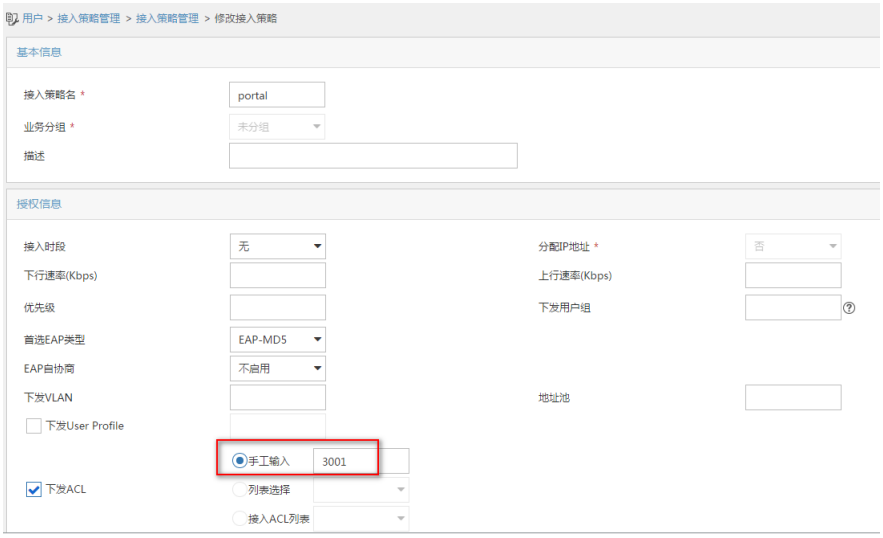
```
#
 portal server guest ip 192.168.21.15 port 2000 key simple portal url http://192.168.21.15:8080/portal/
server-type imc
#
acl number 3001                          //下发acl的编号
 description imc下发acl
 rule 0 deny ip destination 192.168.164.0 0.0.0.255
 rule 5 permit ip
#
vlan 161                                 //业务vlan
#
radius scheme 3245
 server-type extended
 primary authentication 192.168.21.15 key cipher $c$3$d2c4IKdo6KSApXrZLyzE9aN9Aeo/6Ic=
 primary accounting 192.168.21.15 key cipher $c$3$mgPsxHtnU22ArZGNRyZZbGDFAA7rEjw=
 user-name-format without-domain
 nas-ip 192.168.160.2
domain portal
 authentication portal radius-scheme 3245
 authorization portal radius-scheme 3245
 accounting portal radius-scheme 3245
 access-limit disable
 state active
 idle-cut disable
 self-service-url disable
#
dhcp server ip-pool 161
 network 192.168.161.0 mask 255.255.255.0
 gateway-list 192.168.161.1
 dns-list 8.8.8.8
#
wlan service-template 10 crypto
 ssid 2-portal
 bind WLAN-ESS 10
 cipher-suite ccmp
 security-ie rsn
 service-template enable
#
interface Vlan-interface161
```

```
 ip address 192.168.161.1 255.255.255.0
 portal server guest method direct
 portal domain portal
 portal nas-ip 192.168.161.1
#
interface WLAN-ESS10
 port link-type hybrid
 undo port hybrid vlan 1
 port hybrid vlan 161 untagged
 port hybrid pvid vlan 161
 mac-vlan enable
 port-security port-mode psk
 port-security tx-key-type 11key
 port-security preshared-key pass-phrase simple 12345678
#
wlan ap wa4330-acn model WA4330-ACN id 1
 serial-id 210235A1K6C161001123
 radio 1
  service-template 10
  radio enable
#
 dhcp enable
#
 arp-snooping enable
```

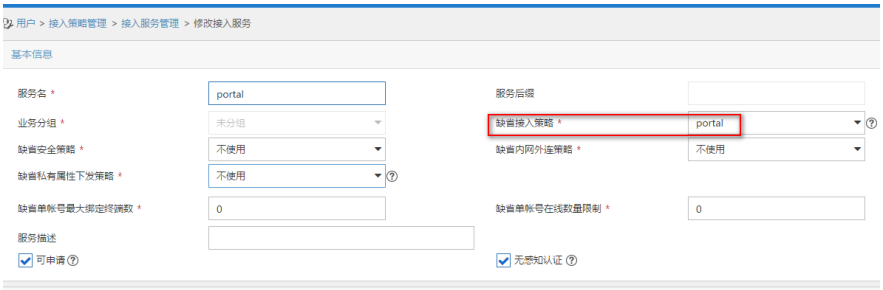
(2). imc上主要配置

添加接入设备，密钥与设备radius方案中配置一致

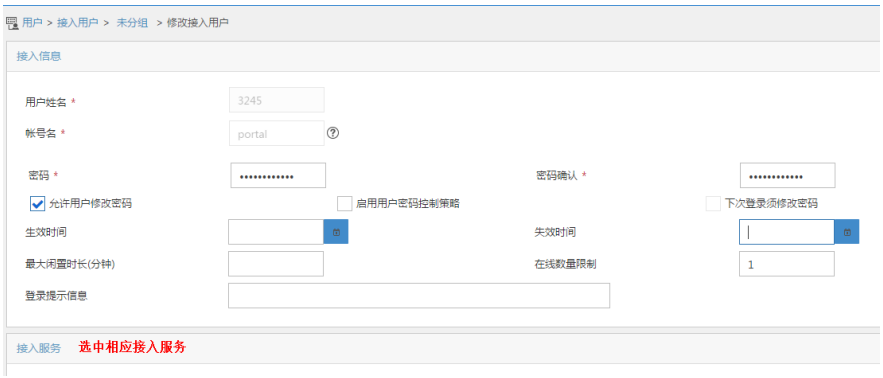
接入策略下发acl编号



创建接入服务，关联接入策略

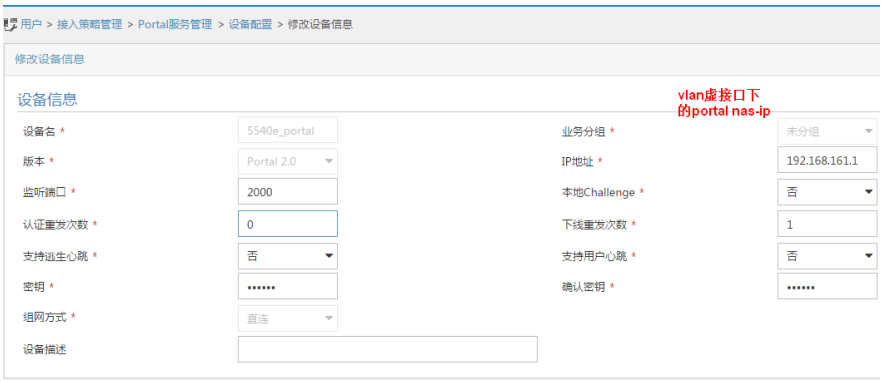


创建接入用户

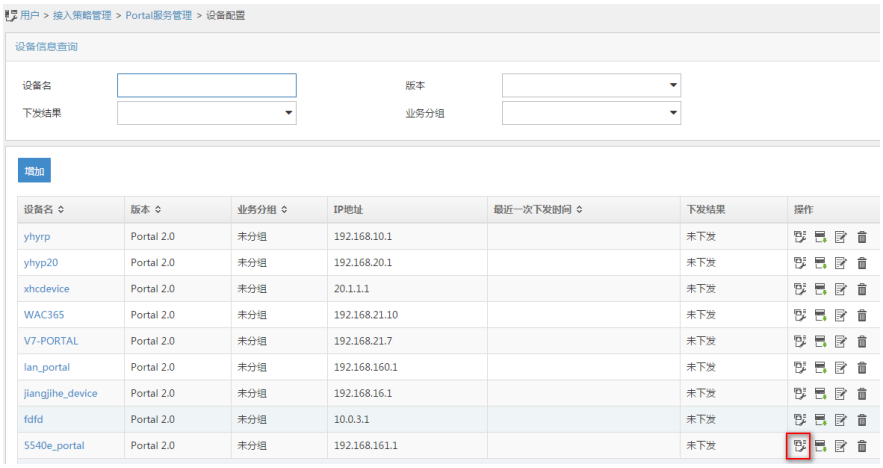


portal服务器相关配置
ip地址组配置，认证网段ip

添加portal设备



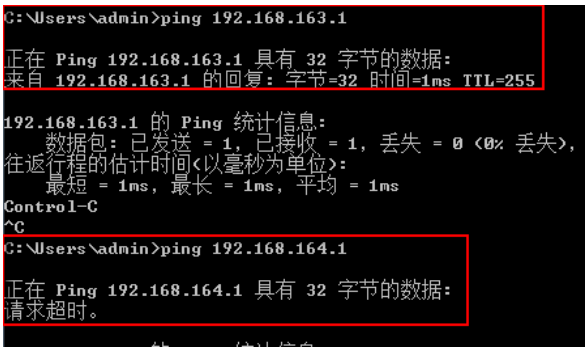
添加端口组



点增加，绑定ip地址组

验证配置：

(1).连接成功后，不能访问192.168.164.0段的ip



(2).设备上显示，下发acl3001成功

<wx5540e>dis conn

Index=5321,Username=NGAOTksENy92TBsxdlZ5JiYWd9E= portal@portal

MAC=5C-E0-C5-AC-52-79

IP=192.168.161.2

IPv6=N/A

Online=00h07m16s

Total 1 connection(s) matched.

(3).通过索引查看具体信息：

<wx5540e>dis conn uc 5321

Index=5321, Username=NGAOTksENy92TBsxdlZ5JiYWd9E= portal@portal

MAC=5C-E0-C5-AC-52-79

IP=192.168.161.2

IPv6=N/A

Access=PORTAL ,AuthMethod=CHAP

Port Type=Wireless-802.11,Port Name=Vlan-interface161

Initial VLAN=161, Authorization VLAN=N/A

ACL Group=3001

User Profile=N/A
CAR=Disable
Traffic Statistic:
  InputOctets =108961 OutputOctets =37550
  InputGigawords=0 OutputGigawords=0
Priority=Disable
SessiOnTimeout=85953(s), Terminate-Action=Default
Start=2016-05-01 17:42:24 ,Current=2016-05-01 17:49:51 ,Online=00h07m27s
 Total 1 connection matched.