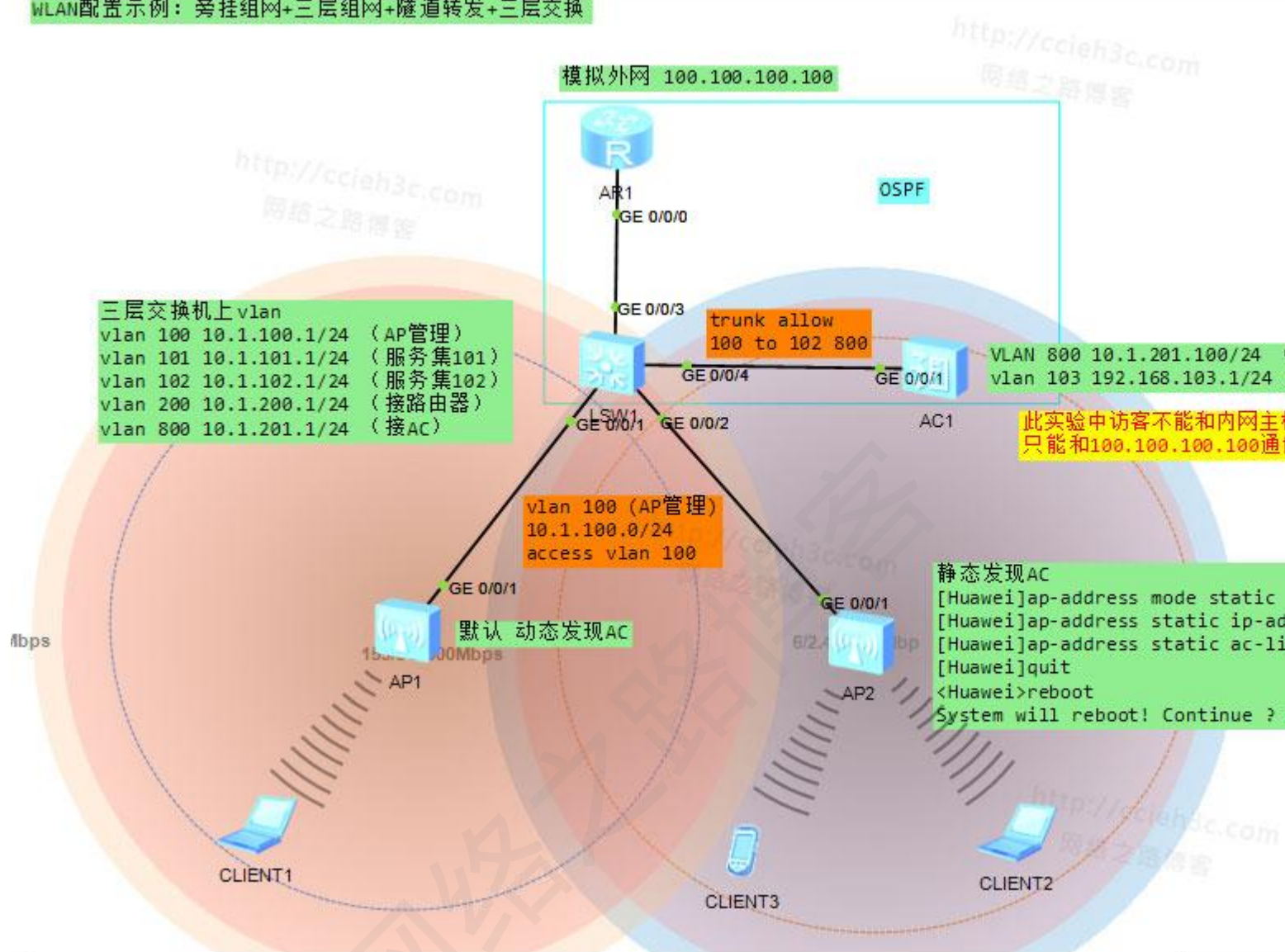


WLAN 配置示例 2（旁挂组网隧道 or 直接转发），这种方式比较适合中小型企业，AC 旁挂在三层交换机旁边，只是用于与 AP 建立 CAPWAP 隧道，下发业务给 AP，如果在隧道方式下的话，那么业务流量也会由 CAPWAP 隧道进行封装交给 AC 处理，再由 AC 来转发，而直接转发的话，则由 AP 本地交换了，不需要交给 AC，这样可以减轻 AC 的负担，具体使用可以根据需求来决定。

### 掌握目标

- 1、理解旁挂组网与直接 or 隧道转发的方式
- 2、AP 静态关联 AC 的方法【补充，之前都是以动态或者 option43 方式】
- 3、三层交换机配置
- 4、AC 的配置
- 5、只允许访客访问特定的流量，通过 ACL 下放

## WLAN配置示例：旁挂组网+三层组网+隧道转发+三层交换



拓具体的 VLAN 信息与 IP 网段都包括，该实验主要是演示三层组网 旁挂+隧道或者直接转发方式的组网情况，并且包括怎么通过 AC 上面配置 ACL 来下放到 AP 上面限制客户端的流量。

### 1、理解旁挂组网与直接 or 隧道转发的方式

如果在隧道方式下的话，那么业务流量也会由 CAPWAP 隧道进行封装交给 AC 处理，再由 AC 来转发，而直接转发的话，

则由 AP 本地交换了，不需要交给 AC，这样可以减轻 AC 的负担，还可以配需华为的 feature，在 AC 失效后，AP 还能继续为客户端提供业务转发。

## 2、AP 静态关联 AC 的方法【补充，之前都是以动态或者 option43 方式】

```
静态发现AC
[Huawei]ap-address mode static
[Huawei]ap-address static ip-address 10.1.100.100 24 10.1.100.1
[Huawei]ap-address static ac-list 10.1.201.100
[Huawei]quit
<Huawei>reboot
System will reboot! Continue ? [y/n]:y
```

在 AP 上面配置模式为静态，配置自己的 IP 地址与网关，最后指定 AC 的地址在哪，重启设备即可。

## 3、三层交换机配置

dhcp enable

interface Vlanif100

ip address 10.1.100.1 255.255.255.0

dhcp select interface

dhcp server option 43 sub-option 3 ascii 10.1.201.100

这里配置了 option 43 , 指定 AC 的地址

#

interface Vlanif101

ip address 10.1.101.1 255.255.255.0

dhcp select interface

dhcp server dns-list 8.8.8.8

#

interface Vlanif102

ip address 10.1.102.1 255.255.255.0

dhcp select interface

dhcp server dns-list 8.8.8.8

#

interface Vlanif200

ip address 10.1.200.2 255.255.255.0

#

interface Vlanif800

ip address 10.1.201.1 255.255.255.0

#

interface MEth0/0/1

#

interface GigabitEthernet0/0/1

port link-type access

```
port default vlan 100
```

```
#
```

```
interface GigabitEthernet0/0/2
```

```
port link-type access
```

```
port default vlan 100
```

```
#
```

```
interface GigabitEthernet0/0/3
```

```
port link-type access
```

```
port default vlan 200
```

```
#
```

```
interface GigabitEthernet0/0/4
```

```
port link-type trunk
```

```
port trunk allow-pass vlan 100 to 102 200 800
```

说明：这里演示是以隧道方式组网演示的，所以交换机接 AP 的接口都为 Access 接口，如果是直接转发的话，那么必须为 hybrid 或者 trunk，其中 PVID 必须等于 AC 的源地址的 VLAN，也就是与 AP 建立 CAPWAP 隧道的 VLAN，为管理 VLAN，然后还需要放行业务 VLAN，否则 PC 关联不上，DHCP 获取不到地址。!!!

```
ospf 1 router-id 3.3.3.3
```

```
area 0.0.0.0
```

```
network 10.1.200.2 0.0.0.0
```

```
network 10.1.201.1 0.0.0.0
```

**area 0.0.0.1**

**network 10.1.100.1 0.0.0.0**

**network 10.1.101.1 0.0.0.0**

**network 10.1.102.1 0.0.0.0**

## 4、AC 的配置

**acl number 3001**

**rule 5 permit ip destination 10.1.201.100 0**

**rule 10 deny ip destination 10.0.0.0 0.255.255.255**

**rule 15 permit ip**

**说明：拒绝访客访问内部员工网络**

**interface Vlanif103**

**ip address 192.168.103.1 255.255.255.0**

**traffic-filter inbound acl 3001**

**dhcp select interface**

**dhcp server dns-list 8.8.8.8**

**#**

**interface Vlanif800**

**ip address 10.1.201.100 255.255.255.0**

**#**

**ospf 1 router-id 2.2.2.2**

**area 0.0.0.0**

**network 10.1.201.100 0.0.0.0**

**area 0.0.0.103**

**network 192.168.103.1 0.0.0.0**

**interface GigabitEthernet0/0/1**

**port link-type trunk**

**port trunk allow-pass vlan 100 to 102 800**

**interface Wlan-Ess0**

**port hybrid untagged vlan 101**

**#**

**interface Wlan-Ess1**

**port hybrid untagged vlan 102**

**#**

**interface Wlan-Ess2**

**port hybrid untagged vlan 103**

**说明：该接口用来关联每一个服务集的，下发的时候告诉下面的 AP 打上什么样的 VLAN。**

**wlan**

**wlan ac source interface vlanif800**

**ap id 0 type-id 19 mac 00e0-fc03-d740 sn 2102354483106C6FFC3E** 【采用 MAC 认证方式来让 AP 上线】

**ap id 1 type-id 19 mac 00e0-fc03-1360 sn 210235448310646DC543**

**wmm-profile name wmm id 0**

**traffic-profile name tra id 0**

**security-profile name sec id 0**

**service-set name valn101 id 0** 【创建一个服务集，它的转发方式为 tunnel，关联了 WLAN-ESS0 接口，SSID 为 VLAN 101】

**forward-mode tunnel**

**wlan-ess 0**

**ssid vlan101**

**traffic-profile id 0**

**security-profile id 0**

**service-vlan 101**

**service-set name vlan102 id 1**

**forward-mode tunnel**

**wlan-ess 1**

**ssid vlan102**

**traffic-profile id 0**

**security-profile id 0**



**service-vlan 102**

**service-set name guest103 id 2**

**forward-mode tunnel**

**wlan-ess 2**

**ssid vlan103**

**user-isolate**

**traffic-profile id 0**

**security-profile id 0**

**service-vlan 103**

**radio-profile name 2g11n id 0**                   **【指定射频类型为 2.4G 的，关联 WMM】**

**radio-type 80211bgn**

**wmm-profile id 0**

**radio-profile name 5g11n id 1**                   **【指定射频类型为 5G 的，关联 WMM】**

**radio-type 80211an**

**wmm-profile id 0**

**ap 0 radio 0**                   **【在 ap 的射频下，0 表示 2.4G，关联刚刚的射频 profile，然后关联服务集，服务集是可以关**  
**联多个的，可以多个 SSID】**

**radio-profile id 0**

**service-set id 0 wlan 1**

**service-set id 1 wlan 2**

**service-set id 2 wlan 3**

**ap 0 radio 1**

**radio-profile id 1**

**channel 40MHz-minus 153**

**service-set id 0 wlan 1**

**service-set id 1 wlan 2**

**service-set id 2 wlan 3**

**ap 1 radio 0**

**radio-profile id 0**

**channel 20MHz 6**

**service-set id 0 wlan 1**

**service-set id 1 wlan 2**

**service-set id 2 wlan 3**

**ap 1 radio 1**

**radio-profile id 1**

**channel 40MHz-minus 161**

**service-set id 0 wlan 1**

**service-set id 1 wlan 2**

**service-set id 2 wlan 3**

**说明：注意频段不要冲突，这里要手工修改下，模拟器不支持自动分配。**

这里用的的 tunnel 转发模式的，默认情况下为直接，所以如果想为直接的转发模式，可以不需要配置 forward-mode tunnel，如果为直接转发的话，那么交换机注意不能为 Access 接口，必须为 hybrid 或者 trunk，PVID=AC 与 AP 建立 CAWPWAP 隧道的 VLAN，然后给业务 VLAN 打上 Tag，否则会出现客户端连接不了 AP，获取不到地址的情况。

## 5、只允许访客访问特定的流量，通过 ACL 下放

在 tunnel 的模式下，所有的流量都是会经过 AC 上面的 VLAN 接口的，所以策略是在 AC 的 VLAN 接口下做，但是如果是直接转发就不一样了。

```
acl number 3001
```

```
rule 5 permit ip destination 10.1.201.100 0
```

```
rule 10 deny ip destination 10.0.0.0 0.255.255.255
```

```
rule 15 permit ip
```

说明：拒绝访客访问内部员工网络

```
service-set name guest103 id 2
```

```
traffic-filter inbound acl 3001
```

它会在 AP 关联的时候，就会自动下发给 AP，那么 AP 的接口上面就会有该 ACL，直接在 AP 上面对客户端的流量做限制。

所以在做控制的时候，一定要区分是在什么方式下，是直接转发还是隧道转发，不同的模式，策略应用的方式也不一样。

[AC6005]dis service-set id 0

```
-----
Service-set ID           : 0
Service-Set name         : valn101
SSID                     : vlan101
Hide SSID                : disable
User isolate             : disable
Type                     : service
Maximum number of user   : 32
Association timeout(min) : 5
Traffic profile name     : tra      ccieh3c.qzone.qq.com
Security profile name    : sec
User profile name        : -
Wlan-ess interface       : Wlan-ess0
Igmp mode                : off
Forward mode             : tunnel
Service-vlan             : 101
DHCP snooping            : disable
DHCP snooping option id  : -
IPSG switch              : disable
DHCP trust port          : disable
DAI switch               : disable
ARP attack threshold(pps): 15
Protocol flag            : all
Offline-management switch: disable
~'                        ~' ~'
```

```
<ap-1>dis capwap link state
```

LINK ID	AP IPAddr	AP CPort	AP DPort	InIf Index
0	10.1.100.254	50232	50233	0

```
<ap-1>dis system-information
```

```
System Information
```

```
Serial Number      : 210235448310646DC543
System Time        : 2024-06-04 22:42:33
System Up time     : 0:03
System Name        : ap-1
Country Code       : CN
MAC Address        : 00:e0:fc:03:13:60
Radio 2.4GHz MAC Address : 00:e0:fc:03:13:60
Radio 5GHz MAC Address : 00:e0:fc:03:13:70
IP Address         : 10.1.100.254
Subnet Mask        : 255.255.255.0
Default Gateway    : 10.1.100.1
Management VLAN ID(AP) : 1
IP MODE           : dhcp
Slot Status       : Dual band(an/bgn)
AP Type           : AP6010DN-AGN
Board Type        : AP6010DN
Board Serial Number :
```

329 256.793000 10.1.101.254 100.100.100.100 ICMP Echo (ping) request (id=0x2416, seq(be/le)=1/256, ttl=64)

- Frame 329: 136 bytes on wire (1088 bits), 136 bytes captured (1088 bits) on interface 0
- Ethernet II, Src: HuaweiTe\_03:13:60 (00:e0:fc:03:13:60), Dst: HuaweiTe\_39:b5:0a (4c:1f:cc:39:b5:0a)
- Internet Protocol, Src: 10.1.100.254 (10.1.100.254), Dst: 10.1.201.100 (10.1.201.100)
- User Datagram Protocol, Src Port: 50233 (50233), Dst Port: capwap-data (5247)
- Control And Provisioning of Wireless Access Points
  - Preamble
    - Version: 0
    - Type: CAPWAP Header (0)
  - Header
    - Ethernet II, Src: HuaweiTe\_cf:52:6a (54:89:98:cf:52:6a), Dst: HuaweiTe\_39:b5:0a (4c:1f:cc:39:b5:0a)
    - 802.1Q Virtual LAN, PRI: 0, CFI: 0, ID: 101
    - Internet Protocol, Src: 10.1.101.254 (10.1.101.254), Dst: 100.100.100.100 (100.100.100.100)
    - Internet Control Message Protocol

0028 00000000 00000000 00000000 00100000 00000000 00010000 00000000 00000000 .....






0030 00000000 00000000 00000110 00000000 11110000 11111100 00000011 00010011 .....9..

0038 01100000 00000000 01001100 00011111 11001100 00111001 10110101 00001010 T...Rj..

0040 01010100 10001001 10011000 11001111 01010010 01101010 10000001 00000000 .e..E..<


0048 00000000 01100101 00001000 00000000 01000101 00000000 00000000 00111100 ca


0050 00010110 00100100 01000000 00000000 10000000 00000001 10101011 11010101


 86E93332-9182-467b-9C2F-8E114F08BD6D  
 4737F688-B9E1-4161-987D-D45367819E37  
 53368F15-09FC-462a-A966-FED11450B9FB  
 A6453261-8DBB-4834-A7C8-F880BDF11F61  
 D85E3E67-A91C-4a23-BA91-1113CEA02677


 AC1


 AR1


 SW1


 WLAN配置示例 (旁挂组网隧道转发)

 WLAN配置示例2 (旁挂组网隧道转发)

 WLAN配置示例2 (旁挂组网隧道转发) 0

 WLAN配置示例2 (旁挂组网隧道转发) 1

 WLAN配置示例2 (旁挂组网隧道转发) 2

 WLAN配置示例2 (旁挂组网隧道转发) 3

模拟器可以  
直接加载

博主也只是业余时间写写技术文档，请大家见谅，大家觉得不错的话，可以推荐给朋友哦，博主会努力推出更好的系列文档的。如果大家有任何疑问或者文中有错误跟疏忽的地方，欢迎大家留言指出，博主看到后会第一时间修改，谢谢大家的支持，更多技术文章尽在网络之路博客，<http://ccieh3c.com>。



您的支持，是我们努力收集与分享的最大动力



微信公众平台

订阅第一时间享受  
最新文章更新通知



远程设备调试服务

有需要的朋友可以  
加微信聊



## 更多联系方式

QQ : 1914756383

邮箱 : 1914756383@qq.com

微信 : ciscohuawei3c

博客地址: <http://ccieh3c.com>

远程调试服务 : <https://1914756383.taobao.com>