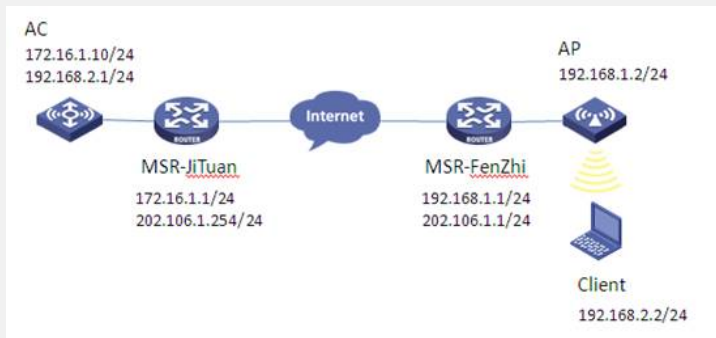


WX系列AC+Fit AP穿越NAT典型配置 (集中转发)

一、组网需求:

WX系列AC、FIT AP、路由器、便携机 (安装有无线网卡)

二、组网图:



本典型配置举例中AC使用WX5004无线控制器，版本为R2308P07。AC和AP分别位于私网内，通过集团路由器和分支路由器穿越Internet实现互通。

分支侧MSR-FenZhi作为AP网关 (192.168.1.1/24) 并设置互联地址 (202.106.1.1/24)，配置DHCP Server为AP分配IP地址，在外网口配置动态地址转换将AP的IP地址映射公网IP地址。

集团侧MSR-JiTuan作为AC网关 (172.16.1.1/24) 并设置互联地址 (202.106.1.254/24)，在外网口配置静态地址转换将AC的IP地址一对一静态映射为公网IP地址。无线控制器AC作为用户业务网关 (192.168.2.1/24)，配置DHCP Server为Client分配IP地址。

三、特性介绍:

AC和AP间穿越NAT通过AC同时纪录AP的IP地址和端口号信息，实现处于NAT设备内部的AP注册到AC。

AP与AC之间共要建立两条隧道，控制隧道和数据隧道。穿过NAT后，两条隧道的AP端IP地址和端口号都会被转换。AC会面临两个问题：第一，如何建立控制隧道和数据隧道的对应关系；第二，在数据隧道没有数据传送时，如何保活NAT会话。解决方式：数据隧道新增一类报文“数据保活报文”，通过周期性的发送来保活NAT会话；然后其携带的session id帮助AC实现数据隧道和控制隧道的关联。AC的B96版本默认支持AP到AC之间穿越NAT，不需要任何配置。

在MSR-JiTuan侧配置静态地址转换将私网AC的IP地址一对一静态映射为公网IP地址，可以实现AC位于私网内的应用环境。

四、配置信息:

1. AC的配置信息:

```
#  
version 5.20, Release 2308P07  
#  
sysname AC  
#  
domain default enable system  
#  
telnet server enable  
#  
port-security enable  
#  
vlan 1  
#
```

```
vlan 2
#
domain system
access-limit disable
state active
idle-cut disable
self-service-url disable
#
dhcp server ip-pool vlan2
network 192.168.2.0 mask 255.255.255.0
gateway-list 192.168.2.1
#
user-group system
group-attribute allow-guest
#
local-user admin
password simple admin
authorization-attribute level 3
service-type telnet
#
wlan rrm
dot11a mandatory-rate 6 12 24
dot11a supported-rate 9 18 36 48 54
dot11b mandatory-rate 1 2
dot11b supported-rate 5.5 11
dot11g mandatory-rate 1 2 5.5 11
dot11g supported-rate 6 9 12 18 24 36 48 54
#
wlan service-template 1 clear
ssid h3c-nat
bind WLAN-ESS 1
service-template enable
#
interface NULL0
#
interface Vlan-interface1
ip address 172.16.1.10 255.255.255.0
#
interface Vlan-interface2
ip address 192.168.2.1 255.255.255.0
#
interface GigabitEthernet1/0/1
#
interface GigabitEthernet1/0/2
#
interface GigabitEthernet1/0/3
#
interface GigabitEthernet1/0/4
#
interface Ten-GigabitEthernet1/0/5
#
interface WLAN-ESS1
port access vlan 2
#
wlan ap ap1 model WA2610i-GN id 1
trap enable
serial-id 219801A0CLC124000294
```

```
radio 1
service-template 1
radio enable
#
ip route-static 202.106.1.0 255.255.255.0 172.16.1.1
#
undo info-center logfile enable
#
dhcp server forbidden-ip 192.168.2.1
#
dhcp enable
#
arp-snooping enable
#
load xml-configuration
#
user-interface con 0
user-interface vty 0 4
authentication-mode scheme
user privilege level 3
#
Return
```

2. MSR-JiTuan的配置信息:

```
#
version 5.20, Release 2209P15
#
sysname MSR-JiTuan
#
domain default enable system
#
dar p2p signature-file flash:/p2p_default.mtd
#
port-security enable
#
vlan 1
#
domain system
access-limit disable
state active
idle-cut disable
self-service-url disable
#
user-group system
group-attribute allow-guest
#
local-user admin
password cipher $c$3$40gC1cxf/wlJNa1ufFPjsjKAof+QP5aV
authorization-attribute level 3
service-type telnet
#
cwmp
undo cwmp enable
#
interface Aux0
async mode flow
link-protocol ppp
#
```

```
interface Cellular0/0
  async mode protocol
  link-protocol ppp
#
interface Ethernet0/0
  port link-mode route
  ip address 172.16.1.1 255.255.255.0
#
interface Ethernet0/1
  port link-mode route
  nat outbound static
  ip address 202.106.1.254 255.255.255.0
#
interface NULL0
#
#
voice-setup
#
sip
#
sip-server
#
  call-rule-set
#
  call-route
#
dial-program
  default entity fax protocol standard-t38
  default entity fax protocol standard-t38 hb-redundancy 0
  default entity fax protocol standard-t38 lb-redundancy 0
#
aaa-client
#
gk-client
#
  nat static 172.16.1.10 202.106.1.253
#
  load xml-configuration
#
  load tr069-configuration
#
user-interface tty 12
user-interface aux 0
user-interface vty 0 4
  authentication-mode scheme
#
Return
3. MSR-FenZhi的配置信息
#
  version 5.20, Release 2104P02
#
  sysname MSR-FenZhi
#
  nat address-group 1 202.106.1.2 202.106.1.10
#
  domain default enable system
#
```

```
dar p2p signature-file flash:/p2p_default.mtd
#
port-security enable
#
acl number 2001
rule 0 permit source 192.168.1.0 0.0.0.255
rule 5 deny
#
vlan 1
#
domain system
access-limit disable
state active
idle-cut disable
self-service-url disable
#
dhcp server ip-pool ap
network 192.168.1.0 mask 255.255.255.0
gateway-list 192.168.1.1
option 43 hex 80070000 01CA6A01 FD //AC地址为202.106.1.253
#
user-group system
#
local-user admin
password cipher .J@USE=B,53Q=^Q`MAF4<1!!
authorization-attribute level 3
service-type telnet
#
cwmp
undo cwmp enable
#
interface Aux0
async mode flow
link-protocol ppp
#
interface Cellular0/0
async mode protocol
link-protocol ppp
#
interface NULL0
#
interface Vlan-interface1
ip address 192.168.1.1 255.255.255.0
#
interface GigabitEthernet0/0
port link-mode route
nat outbound 2001 address-group 1
ip address 202.106.1.1 255.255.255.0
#
interface GigabitEthernet0/1
port link-mode bridge
#
interface GigabitEthernet0/2
port link-mode route
#
interface GigabitEthernet0/3
port link-mode route
```

```
#
interface GigabitEthernet0/4
 port link-mode route
#
ip route-static 0.0.0.0 0.0.0.0 202.106.1.254
#
dhcp server forbidden-ip 192.168.1.1
#
dhcp enable
#
load xml-configuration
#
load tr069-configuration
#
user-interface tty 12
user-interface aux 0
user-interface vty 0 4
 authentication-mode scheme
#
Return
```

五、主要配置步骤：

1. AC配置：

```
#创建VLAN，并配置VLAN接口IP地址。
system-view
[AC] vlan 2
[AC -vlan2] quit
[AC] interface Vlan-interface1
[AC-Vlan-interface1] ip address 172.16.1.10 255.255.255.0
[AC-Vlan-interface1] quit
[AC] interface Vlan-interface2
[AC-Vlan-interface2] ip address 192.168.2.1 255.255.255.0
[AC-Vlan-interface2] quit
#配置DHCP server。
[AC] dhcp enable
[AC] dhcp server ip-pool vlan2
[AC- dhcp server ip-pool vlan2] network 192.168.2.0 mask 255.255.255.0
[AC- dhcp server ip-pool vlan2] gateway-list 192.168.2.1
[AC- dhcp server ip-pool vlan2] quit
[AC] dhcp server forbidden-ip 192.168.2.1
#使能ARP Snooping功能。
[AC] arp-snooping enable
#配置静态路由。
[AC] ip route-static 202.106.1.0 255.255.255.0 172.16.1.1
#配置WLAN ESS接口。
[AC] interface WLAN-ESS1
[AC-WLAN-ESS1] port access vlan 2
[AC-WLAN-ESS1]quit
#配置service-template服务模板。
[AC] wlan service-template 1 clear
[AC-wlan-st-1] ssid h3c-nat
[AC-wlan-st-1] bind WLAN-ESS 1
[AC-wlan-st-1] service-template enable
[AC-wlan-st-1] quit
#配置ap1。
[AC] wlan ap ap1 model WA2610i-GN
[AC-wlan-ap-ap1] serial-id 219801A0CLC124000294
```

```
[AC-wlan-ap-ap1] radio 1
[AC-wlan-ap-ap1-radio-1] service-template 1
[AC-wlan-ap-ap1-radio-1] radio enable
[AC-wlan-ap-ap1-radio-1] quit
[AC-wlan-ap-ap1] quit
```

2. MSR-JiTuan配置:

#配置以太网接口IP地址。

```
system-view
[MSR-JiTuan] interface Ethernet0/0
[MSR-JiTuan - Ethernet0/0] ip address 172.16.1.1 255.255.255.0
[MSR-JiTuan - Ethernet0/0] quit
[MSR-JiTuan] interface Ethernet0/1
[MSR-JiTuan - Ethernet0/1] ip address 202.106.1.254 255.255.255.0
[MSR-JiTuan - Ethernet0/1] quit
```

#配置一对一静态地址转换映射

```
[MSR-JiTuan] nat static 172.16.1.10 202.106.1.253
[MSR-JiTuan] interface Ethernet0/1
[MSR-JiTuan - Ethernet0/1] nat outbound static
[MSR-JiTuan - Ethernet0/1] quit
```

3. MSR-FenZhi配置:

#切换以太网接口的工作模式，并配置以太网接口及VLAN接口IP地址。

```
system-view
[MSR-FenZhi] interface GigabitEthernet0/1
[MSR-FenZhi - GigabitEthernet0/1] port link-mode bridge
[MSR-FenZhi - GigabitEthernet0/1] quit
[MSR-FenZhi] interface GigabitEthernet0/0
[MSR-FenZhi - GigabitEthernet0/0] ip address 202.106.1.1 255.255.255.0
[MSR-FenZhi - GigabitEthernet0/0] quit
[MSR-FenZhi] interface Vlan-interface1
[MSR-FenZhi - Vlan-interface1] ip address 192.168.1.1 255.255.255.0
[MSR-FenZhi - Vlan-interface1] quit
```

#配置DHCP server，并设置option 43 属性，AC地址为202.106.1.253。

```
[MSR-FenZhi] dhcp enable
[MSR-FenZhi] dhcp server ip-pool ap
[MSR-FenZhi - dhcp server ip-pool ap] network 192.168.1.0 mask 255.255.255.0
[MSR-FenZhi - dhcp server ip-pool ap] gateway-list 192.168.1.1
[MSR-FenZhi - dhcp server ip-pool ap] option 43 hex 80070000 01CA6A01 FD
[MSR-FenZhi - dhcp server ip-pool ap] quit
[MSR-FenZhi] dhcp server forbidden-ip 192.168.1.1
```

#配置访问控制列表2001，仅允许内部网络中192.168.1.0/24网段的用户可以访问Internet。

```
[MSR-FenZhi] acl number 2001
[MSR-FenZhi - acl-basic-2001] rule 0 permit source 192.168.1.0 0.0.0.255
[MSR-FenZhi - acl-basic-2001] rule 5 deny
[MSR-FenZhi - acl-basic-2001] quit
```

#配置IP地址池1。

```
[MSR-FenZhi] nat address-group 1 202.106.1.2 202.106.1.10
# 在出口接口GigabitEthernet0/0上配置ACL 2001与IP地址池1相关联。
[MSR-FenZhi] interface GigabitEthernet0/0
[MSR-FenZhi - GigabitEthernet0/0] nat outbound 2001 address-group 1
[MSR-FenZhi - GigabitEthernet0/0] quit
```

#配置默认路由。

```
[MSR-FenZhi] ip route-static 0.0.0.0 0.0.0.0 202.106.1.254
```

六、结果验证:

- (1) 查看分支路由器nat会话表项。

```
<MSR-FenZhi>display nat session

There are currently 2 NAT sessions:

Protocol      GlobalAddr  Port      InsideAddr  Port      DestAddr  Port
UDP           202.106.1.5 12291     192.168.1.3 12222     202.106.1.253 12222
status:11     TTL:00:04:00 Left:00:03:58  VPN:---

UDP           202.106.1.5 12288     192.168.1.3 12223     202.106.1.253 12223
status:11     TTL:00:04:00 Left:00:03:59  VPN:---
```

(2) 查看集团路由器nat会话表项。

```
<MSR-JiTuan>display nat session

There are currently 2 NAT sessions:

Pro   GlobalAddr:Port      LocalAddr:Port      DestAddr:Port
UDP   202.106.1.253:12222  172.16.1.10:12222   202.106.1.5:12291
      GlobalVPN: ---     LocalVPN: ---
      status: 9         TTL: 00:04:00      Left: 00:03:58

UDP   202.106.1.253:12223  172.16.1.10:12223   202.106.1.5:12288
      GlobalVPN: ---     LocalVPN: ---
      status: 9         TTL: 00:04:00      Left: 00:03:53
```

(3) 查看AP信息。

```
<AC>display wlan ap all
Total Number of APs configured      : 1
Total Number of configured APs connected : 1
Total Number of auto APs connected   : 0
AP Profiles
State : I = Idle, J = Join, JA = JoinAck, IL = ImageLoad
       C = Config, R = Run, KU = KeyUpdate, KC = KeyCfm
-----
AP Name      State Model      Serial-ID
-----
ap1          R/M  WA2610i-GN      219801A0CLC124000294
-----
```

(5) 查看客户端信息。

```
<AC>display wlan client
Total Number of Clients      : 1
Client Information
SSID: h3c-nat
-----
MAC Address  User Name      APID/RID IP Address      VLAN
-----
0024-d636-16b2 -NA-      1 /1  192.168.2.2      2
-----
```

(6) 客户端获取IP地址信息，并能ping通网关。

```
C:\Documents and Settings\08903>ipconfig

Windows IP Configuration

Ethernet adapter 无线网络连接:

Connection-specific DNS Suffix . :
IP Address . . . . . : 192.168.2.2
Subnet Mask . . . . . : 255.255.255.0
IP Address . . . . . : fe80::224:d6ff:fe36:18b2%4
Default Gateway . . . . . : 192.168.2.1
```

```
C:\Documents and Settings\08903>ping 192.168.2.1

Pinging 192.168.2.1 with 32 bytes of data:

Reply from 192.168.2.1: bytes=32 time=8ms TTL=255
Reply from 192.168.2.1: bytes=32 time=13ms TTL=255
Reply from 192.168.2.1: bytes=32 time=2ms TTL=255
Reply from 192.168.2.1: bytes=32 time=2ms TTL=255

Ping statistics for 192.168.2.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 13ms, Average = 6ms
```