PS：以下是设备的简略命令配置。这个项目本身是我的毕业设计，以下内容也节选自我的论文，原本有详细的命令配置描述，但导师说命令太多了，所以进行了删减，因此可能存在命令缺失的问题，以及考虑到各位可能是为了毕业设计来此进行学习。为了大家的查重率以及论文抽检，以下一切内容仅供参考！

## VLAN管理相关配置

对各端口类型进行配置来管理VLAN的放行，其中除SW4与SW7连接AP的trunk端口需要配置pvid 100与101外，其余trunk端口只用于放行VLAN标签而不进行VLAN标签剥离，配置如表所示：

**VLAN**规划表

|  |  |  |  |
| --- | --- | --- | --- |
| 设备名 | 接口 | 接口类型 | 放行VLAN |
| SW2 | E0/0/1  E0/0/2  E0/0/3  E0/0/4 | trunk  trunk  access  access | 13  13  13  13 |
| SW3 | E0/0/1  E0/0/2  E0/0/3  E0/0/4 | trunk  trunk  access  access | 114  114  114  114 |
| SW4 | E0/0/1  E0/0/2  E0/0/3 | trunk  trunk  trunk | 24 100  24 100  24 100 |
| LSW1 | Eth0  G0/0/1  G0/0/2  G0/0/4  G0/0/6  G0/0/9 | trunk  access  trunk  trunk  trunk  trunk | 1-4094  18  13  24 100  1-4094  114 |
| LSW2 | Eth0  G0/0/1  G0/0/3  G0/0/4  G0/0/6  G0/0/7 | trunk  access  trunk  trunk  trunk  trunk | 1-4094  18  13  24 100  114  1-4094 |
| SW1 | E0/0/1  E0/0/3  E0/0/4  E0/0/5  E0/0/6 | trunk  trunk  access  access  trunk | 1-4094  17 100  16  110  1-4094 |
| AC6 | G0/0/1 | access | 16 |
| DHCP6 | G0/0/1 | trunk | 17 100 |
| SW7 | Eth0  E0/0/3  E0/0/4  E0/0/5 | trunk  access  trunk  access | 1-4096  37  57 101  37 |
| LSW4 | Eth0  Eth1  G0/0/1  G0/0/2 | trunk  trunk  access  access | 1-4094  1-4094  47  47 |
| SW8 | Eth1  E0/0/3  E0/0/4  E0/0/5 | trunk  trunk  trunk  access | 1-4094  34 101  45  124 |
| DHCP3 | G0/0/1 | trunk | 34 101 |
| AC5 | G0/0/1 | trunk | 45 |

## GVRP的实现

在各交换机上配置GVRP来动态学习VLAN，核心层与接入层交换机接口模式设置为normal模式，其余设置为fixed模式，关键命令如下：

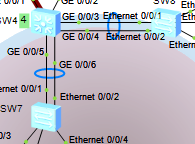
[LSW1]gvrp

//开启全局GVRP

[LSW1-GigabitEthernet0/0/4]gvrp registration normal

//在接口开启GVRP，模式选择normal

## 链路聚合的实现



链路聚合部分拓扑

在关键部分配置链路聚合以降低链路损坏时带来的影响，关键命令如下：

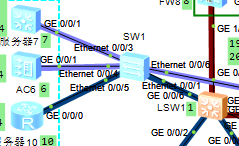
[LSW1-Eth-Trunk0]mode lacp-static

//配置为静态LACP模式

[LSW1-Eth-Trunk0]trunkport g0/0/3

//将g0/0/3与g0/0/5加入到链路聚合中

## DHCP以及DHCPv6的实现



总部及分部的DHCP服务器和中继

DHCP服务器7、3负责为公司总部、分部访客区分配地址，这部分DHCP配置在AC旁挂的实现部分详细讲解。DHCP服务器10负责为公司总部财务部、技术部分配地址，DHCP服务器12负责为公司分部技术部分配地址，为了指定LSW1与LSW4作为网关来方便配合VRRP，都采取地址池分配且配置中继，模式为全局模式，LSW1与LSW4为DHCP中继，DHCPv6采用有状态配置，因ENSP中DHCPv6无法做到在一台路由器上分配多个网段，因此总部技术部通过手动方式配置IPv6来模拟多网段分配，关键命令如下：

[DHCP10]ip pool pool30

//创建IPv4地址池pool30

[DHCP10-ip-pool-pool30]gateway-list 192.168.0.254

//设置地址池网关为192.168.0.254

[DHCP10-ip-pool-pool30]network 192.168.0.0 mask 255.255.255.0

//分发192.168.0.0/24网段的IPv4地址

[DHCP10]dhcpv6 pool pool10

//创建IPv6地址池pool10，ENSP中DHCPv6不支持指定IPv6网关，只能自

//动选择本地链路地址作为网关

[DHCP10-dhcpv6-pool-pool10]address prefix 2001:DB8::/64

//分发2001:0db8::/64网段，但因ENSP问题，分发下去的IPv6地址会

//变为128

[DHCP10-GigabitEthernet0/0/0]dhcp select global

//接口开启全局模式

[DHCP10-GigabitEthernet0/0/0]dhcpv6 server pool10

//选择有状态配置，pool10作为IPv6地址池

[LSW1-Vlanif13]undo ipv6 nd ra halt

//取消IPv6 邻居发现报文的禁用

[LSW1-Vlanif13]ipv6 nd autoconfig managed-address-flag

//告诉接口从 DHCPv6 服务器获取 IPv6 地址

[LSW1-Vlanif13]ipv6 nd autoconfig other-flag

//告诉接口从其他途径获取配置选项，而不是从自动配置过程中获取

[LSW1-Vlanif13]dhcp select relay

//将该接口配置为DHCP中继

[LSW1-Vlanif13]dhcp relay server-ip 192.168.110.10

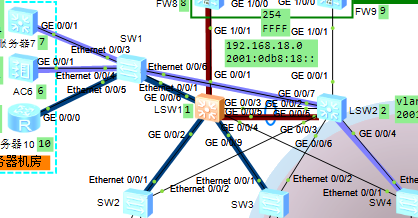
//指定DHCP服务器地址为192.168.110.10

[LSW1-Vlanif13]dhcpv6 relay destination 2001:DB8:110::10

//将该接口配置为DHCPv6中继，指定DHCPv6服务器地址为2001:0db8:11

//0::10

## MSTP的实现



MSTP配置区域拓扑

在MSTP中配置了实例1与实例2，VLAN 13、114、110属于实例1，VLAN 17、16、24、100属于实例2，在实例1中LSW1作为根桥，优先级为0，LSW2优先级为4096，在实例2中LSW2作为根桥，优先级为0，LSW1优先级为4096，LSW4优先级为0作为分部的根桥，其余优先级统一配置为8192，边缘部分则配置边缘端口，关键命令如下：

**[LSW1]stp instance 1 priority 0**

**//LSW1在实例1中的优先级为0，即为根桥**

**[LSW1]stp instance 2 priority 4096**

**//LSW1在实例2中的优先级为4096**

**[LSW1]stp region-configuration**

**//进入MSTP配置**

**[LSW1-mst-region]region-name Huawei**

**//指定区域名词为Huawei**

**[LSW1-mst-region]instance 1 vlan 13 110 114**

**//将VLAN 13 110 114划入实例1**

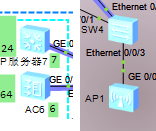
**[LSW1-mst-region]instance 2 vlan 16 to 17 24 100**

**//将VLAN 16 17 24 100划入实例2**

**[LSW1-mst-region]active region-configuration**

**//激活上述配置**

## AC旁挂的实现



无线部分拓扑

DHCP服务器7业务VLAN配置地址池、全局模式加中继实现下发地址，管理VLAN DHCP配置为接口模式，AC通过MAC认证方式绑定AP，通过组方式配置多业务，旁挂方式接入，ENSP中无线不支持IPv6，因此不配置相关IPv6。关键命令如下：

[DHCP7-Vlanif100]dhcp select interface

//DHCP配置为接口模式

[DHCP7-Vlanif100]dhcp server option 43 sub-option 3 ascii 192.168

16.6

//为DHCP服务器指定AC位置为192.168.16.6

[AC6]capwap source interface vlan 16

//配置CAPWAP的源接口为 VLAN 16

[AC6-wlan-view]ap auth-mode mac-auth

//配置AP认证模式为mac认证

[AC6-wlan-view]ap-id 1 ap-mac 00E0-FC6C-7090

//绑定AP的mac地址为00E0-FC6C-7090

[AC6-wlan-view]ssid-profile name ssid01

//创建一个名为ssid01的服务集标识配置文件

[AC6-wlan-ssid-prof-ssid01]ssid wifivlan20

//配置WIFI的名称为wifivlan20

[AC6-wlan-view]vap-profile name vap01

//创建一个名为vap01的虚拟接入点配置文件

[AC6-wlan-vap-prof-vap01]ssid-profile ssid01

//关联之前创建的ssid01

[AC6-wlan-vap-prof-vap01]service-vlan vlan 24

//配置服务vlan为vlan 20

[AC6-wlan-view]ap-group name group01

//创建一个名为group01的AP组

[AC6-wlan-ap-group-group01]vap-profile vap01 wlan 1 radio 0

//将vap01应用到 WLAN 1，并开启2.4G频段

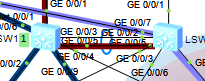
[AC6-wlan-ap-group-group01]vap-profile vap01 wlan 1 radio 1

//将vap01应用到 WLAN 1，并开启5G频段

[AC6-wlan-ap-1]ap-group group01

//将接入点配置到group01的AP组中

## VRRP以及VRRP6的实现



VRRP配置部分拓扑

为每个接入LSW1与LSW2的设备配置VRRP与VRRP6，其中DHCP服务器7、AC6、总部访客区以LSW2为主，LSW1为备，DHCP服务器10、总部财务部、总部技术部以LSW1为主，LSW2为备，ENSP中无线不支持IPv6，所以不配置无线部分的VRRP6。关键命令如下：

[LSW1-Vlanif13]vrrp vrid 13 virtual-ip 192.168.0.254

//配置vrid为13的VRRP的虚拟网关为192.168.0.254

[LSW1-Vlanif13]vrrp vrid 13 priority 101

//优先级设为101，使其为主

[LSW1-Vlanif13]vrrp vrid 13 track interface GigabitEthernet0/0/1

//追踪g0/0/1状态，只在主上配置，用于链路断开时切换主备关系

[LSW1-Vlanif13]vrrp6 vrid 13 virtual-ip FE80::13 link-local

//配置vrid为13的VRRP6的虚拟本地链路地址为FE80::13

[LSW1-Vlanif13]vrrp6 vrid 13 virtual-ip 2001:DB8::FFFF

//虚拟网关为2001:0db8::FFFF

//因ENSP问题，若主机手动配置IPv6地址与网关会导致无法ping通虚

//拟网关，可使用DHCPv6自动分配或手动将后缀改为128位，网关改为

//VRRP6主的本地链路地址解决，但实际意义不大

[LSW1-Vlanif13]vrrp6 vrid 13 priority 101

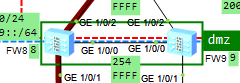
[LSW1-Vlanif13]vrrp6 vrid 13 track interface GigabitEthernet0/0/1

[LSW2-Vlanif13]vrrp vrid 13 virtual-ip 192.168.0.254

//配置vrid为13的VRRP的虚拟网关为192.168.0.254，默认优先级为

//100，使其为备

## 防火墙双机热备的实现



防火墙双机热备配置部分拓扑

出口层中FW8与FW9、FW7与FW11进行双机热备，其中FW8、FW7作为主，FW9、FW11作为备。关键命令如下：

[FW8-GigabitEthernet1/0/1]vrrp vrid 18 virtual-ip 192.168.18.254

Active

//配置VGMP，虚拟网关为192.168.18.254，为主

[FW8-GigabitEthernet1/0/1]vrrp6 vrid 18 virtual-ip FE80::18 link-

local active

//虚拟本地链路为FE80::18，为主

[FW8-GigabitEthernet1/0/1]vrrp6 vrid 18 virtual-ip 2001:DB8:18::F

FFF

[FW9-GigabitEthernet1/0/1]vrrp vrid 18 virtual-ip 192.168.18.254

Standby

//配置为备

[FW9-GigabitEthernet1/0/1]vrrp6 vrid 18 virtual-ip FE80::18 link-

local standby

[FW9-GigabitEthernet1/0/1]vrrp6 vrid 18 virtual-ip 2001:DB8:18::F

FFF

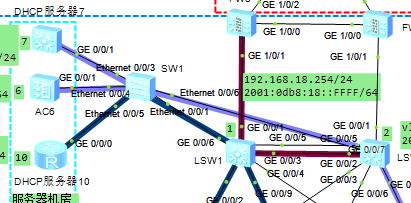
[FW8]hrp interface g1/0/0 remote 192.168.89.9

//指定心跳口与对端IP

[FW8]hrp enable

//开启HRP

## OSPF以及OSPFV3的实现



OSPF及OSPFv3配置部分拓扑

公司总部整体配置OSPF与OSPFv3，全部网段宣告在区域0下，并配置边缘端口优化网络。关键命令如下：

[LSW1-ospf-1-area-0.0.0.0]network 192.168.16.0 0.0.0.255

//宣告192.168.0.0/24 IPv4网段

[LSW1-ospfv3-1]router-id 1.0.1.1

//配置OSPFv3的router-id为1.0.1.1

[LSW1-Vlanif13] ospfv3 1 area 0

//在接口下开启OSPFv3进程1，宣告该接口下的IPv6网段到区域0

//为使内网访问公网，需配置默认路由并宣告，因此需在防火墙上进行额外

//配置，配置如下

HRP\_M[FW8]ip route-static 0.0.0.0 0.0.0.0 112.0.18.1

//配置IPv4默认路由用于访问公网

HRP\_M[FW8]ipv6 route-static :: 0 2001:DB8:112:18::1

//配置IPv6默认路由

HRP\_M[FW8-OSPF-1]default-route-advertise

//向其他邻居发布默认路由

HRP\_M[FW8-ospfv3-1]default-route-advertise

//因ENSP中，RIPng存在一定问题，其在防火墙上无法与默认路由共存，

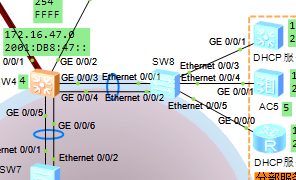
//因此FW7、11与LSW4上也配置OSPFv3，在LSW4/上导入RIPng来间接完

//成分部的连通，配置如下

[LSW4-ospfv3-1]import-route ripng 1

//将RIPng进程1的路由导入OSPFv3

## RIP以及RIPng的实现



RIP及RIPng配置部分拓扑

公司分部采用RIP与RIPng来进行连通，RIP使用version 2。关键命令如下：

[LSW4-rip-1]version 2

//使用版本2

[LSW4-rip-1]network 172.16.0.0

//因为LSW4上的IPv4地址都是B类地址，因此通过B类地址方式宣告

[LSW4-rip-1]silent-interface Eth-Trunk0

//同样设置静默端口

[LSW4-ripng-1]import-route ospfv3 1

//向RIPng引入OSPFv3进程1

[LSW4-Vlanif34]ripng 1 enable

//在接口下开启RIPng 进程1

//为使内网访问外网，也需进行额外配置，配置如下

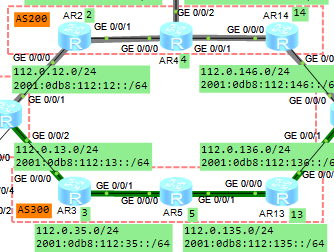
HRP\_M[FW7]ip route-static 0.0.0.0 0.0.0.0 112.0.67.6

HRP\_M[FW7]ipv6 route-static :: 0 2001:DB8:112:67::6preference 200

HRP\_M[FW7-rip-1]default-route originate

//将IPv4默认路由通过RIP下发

## ISIS以及ISISv6的实现



ISIS及ISISv6配置部分拓扑

同一AS区域内使用ISIS与ISISv6进行连通，统一使用level-2。关键实现命令如下：

[AR2-isis-1]network-entity 49.0000.0000.0002.00

//配置网络实体名称为49.0000.0000.0002.00，其中统一使用49，2则是

//自己设备序号以方便记忆

[AR2-isis-1]is-level level-2

//配置level类型为level-2

[AR2-isis-1]ipv6 enable

//开启IPv6功能

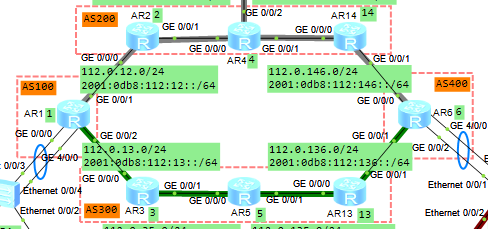
[AR2-LoopBack0]isis enable 1

//开启ISIS进程1

[AR2-LoopBack0]isis ipv6 enable 1

//开启ISISv6进程1

## BGP的实现



BGP配置部分拓扑

配置BGP时，使用物理端口来建立EBGP邻居关系，使用环回口建立IBGP邻居关系，将AR4与AR5配置为路由反射器来模拟公网设备众多的情况。关键命令如下：

[AR1]bgp 100

//创建BGP 100

[AR1-bgp]peer 112.0.12.2 as-number 200

//与AR2通过物理端口，IPv4地址建立EBGP邻居关系

[AR1-bgp]peer 112.0.13.3 as-number 300

//与AR3通过物理端口，IPv4地址建立EBGP邻居关系

[AR1-bgp]peer 2001:DB8:112:12::2 as-number 200

//与AR2通过物理端口，IPv6地址建立EBGP邻居关系

[AR1-bgp]peer 2001:DB8:112:13::3 as-number 300

//与AR3通过物理端口，IPv6地址建立EBGP邻居关系

[AR1-bgp]network 112.0.18.0 255.255.255.0

//在BGP中宣告112.0.18.0/24网段

[AR1-bgp]ipv6-family unicast

//开启处理IPv6单播路由信息

[AR1-bgp-af-ipv6]peer 2001:DB8:112:12::2 enable

//允许与AR2通过IPv6建立邻居关系

[AR1-bgp-af-ipv6]peer 2001:DB8:112:13::3 enable

//允许与AR2通过IPv6建立邻居关系

[AR1-bgp-af-ipv6]network 2001:DB8:112:18:: 64

//在BGP中宣告2001:0db8:112:18::/64网段

[AR4-bgp]peer 2.2.2.2 reflect-client

//将AR4配置为反射器，AR2为AR4的反射器客户端

[AR2-bgp-af-ipv6]peer 2::2 reflect-client

## BFD的实现

配置BFD与OSPF、VRRP、VRRP6、RIP、ISIS、ISISv6、BGP进行联动，因ENSP中不支持BFD与OSPFv3(只有防火墙上可配置)、RIPng进行联动，所以没有配置相应BFD，且因ENSP问题，AC只有与设备直连时，其BFD才会生效，因此AC上也不配置BFD。关键命令如下：

[LSW1]bfd

//开启BFD

[LSW1-ospf-1]bfd all-interfaces enable

//使BFD与OSPF进行联动，OSPFv3同样如此

//其余设备也在OSPF进程中开启BFD即可，不予说明

[LSW1]bfd 13 bind peer-ip 192.168.0.2 source-ip 192.168.0.1 auto

//配置BFD进程13，对端IP为192.168.0.2，自身IP为192.168.0.1，自

//动配置会话标识符

[LSW1-Vlanif17]vrrp vrid 17 track bfd-session session-name 17 inc

reased 40

[LSW1-Vlanif17]vrrp6 vrid 17 track bfd-session session-name 17 in

creased 40

//在VRRP 17上应用BFD进程17，若发生断连，则会使LSW1的VRRP 17与

//VRRP6 17的优先级增加40，使其快速成为主

[LSW2]bfd 13 bind peer-ip 192.168.0.1 source-ip 192.168.0.2 auto

[LSW4-rip-1]]bfd all-interfaces enable

//使RIP与BFD联动，RIPng也是如此

[AR2-isis-1]bfd all-interfaces enable

//使ISIS、ISISv6与BFD联动

[AR1-bgp]peer 112.0.12.2 bfd enable

//与112.0.12.2建立BFD

## GRE over IPsec的实现

**在防火墙上配置GRE over IPsec，使内网之间可跨公网进行访问并进行加密，因GRE支持同时封装IPv4与IPv6，所以无需对IPv6进行额外处理，IPsec通过ipsec profile对GRE进行加密，其中IPsec默认使用的全部认证与加密算法安全性已经较为优秀，因此不做改动。关键命令如下：**

**HRP\_M[FW8]ike proposal 1 (+B)**

**//创建ike安全提议1，其中算法使用默认配置**

**HRP\_M[FW8]ike peer FW117 (+B)**

**//创建ike邻居，名为FW117**

**HRP\_M[FW8-ike-peer-FW117]pre-shared-key huawei@123 (+B)**

**//配置预共享密钥为huawei@123**

**HRP\_M[FW8-ike-peer-FW117]ike-proposal 1 (+B)**

**//绑定ike安全提议1**

**HRP\_M[FW8-ike-peer-FW117]remote-address 112.0.67.254 (+B)**

**//指定对端地址为112.0.67.254，因使用了双机热备所以是虚拟地址**

**HRP\_M[FW8]ipsec proposal 1 (+B)**

**//创建IPsec安全提议1，采用默认配置**

**HRP\_M[FW8]ipsec profile gre (+B)**

**//配置IPsec 配置文件，名为gre**

**HRP\_M[FW8-ipsec-profile-gre]ike-peer FW117 (+B)**

**//绑定对端邻居**

**HRP\_M[FW8-ipsec-profile-gre]proposal 1 (+B)**

**//绑定IPsec安全提议1**

**HRP\_M[FW8-Tunnel0]ip address 192.168.78.8 24**

**HRP\_M[FW8-Tunnel0]ipv6 address 2001:0db8:78::8/64**

**HRP\_M[FW8-Tunnel0]tunnel-protocol gre**

**//制定隧道协议为GRE**

**HRP\_M[FW8-Tunnel0]source 112.0.18.254**

**//指定源IP为112.0.18.254**

**HRP\_M[FW8-Tunnel0]destination 112.0.67.254**

**//指定目的IP为112.0.67.254**

**HRP\_M[FW8-Tunnel0]ipsec profile gre (+B)**

**//绑定IPsec配置文件，使IPsec对GRE隧道进行加密**

[FW8-zone-dmz]add interface **Tunnel0**

**HRP\_M[FW8-Tunnel0]ip route-static 172.16.47.0 255.255.255.0 Tunne**

**l0**

**//使用静态路由进行引流，将需要通过隧道的流量引向隧道**

## ACL及路由策略的实现

**配置ACL以禁止财务部与访客区对服务器机房的访问，因ENSP原因，关于IPv6的ACL只在路由器上进行示范配置。在BGP上配置路由策略来更改引入的路由优先级，使隧道的流量走下方链路。关键命令如下：**

**[SW1]acl 3001**

**//创建ACL 3001，因只对ICMP进行限制，所以需要使用高级ACL**

**[SW1-acl-adv-3001]rule deny icmp source 192.168.1.0 0.0.0.255**

**//创建禁止源地址网段192.168.1.0/24，协议为ICMP的报文通过的规则**

**[SW1-acl-adv-3001]rule deny icmp source 192.168.0.0 0.0.0.255**

**[SW1-Ethernet0/0/1]traffic-filter inbound acl 3001**

**//在入接口方向绑定ACL 3001**

**[DHCP10]acl ipv6 3001**

**//创建IPv6版本的ACL 3001**

**[DHCP10-acl6-adv-3001]rule deny icmpv6 source 2001:DB8::/64**

**[DHCP10-GigabitEthernet0/0/0]traffic-filter inbound ipv6 acl 3001**

**[AR1]route-policy FW78 permit node 10**

**//创建路由策略FW78，设为允许通过，结点为10**

**[AR1-route-policy]if-match acl 2001**

**//如果匹配ACL 2001**

**[AR1-route-policy]apply preferred-value 200**

**//则将路由优先级改为200**

**[AR1-bgp]peer 112.0.13.3 route-policy FW78 import**

**//在邻居112.0.13.3的入方向绑定路由策略FW78**

**[AR1-bgp-af-ipv6]peer 2001:DB8:112:13::3 route-policy FW78-6**

**import**

## NAPT、NAT Server及NAT64的实现

**在防火墙上设置NAPT、NAT64进行地址转换以访问公网，在平台服务器配置NAT Server将私网地址映射为公网地址进行发布。关键命令如下：**

**HRP\_M[FW8]nat address-group napt**

**//创建NAPT用的地址池**

**HRP\_M[FW8-address-group-napt]mode pat**

**//设置为pat模式**

**HRP\_M[FW8-address-group-napt]section 112.0.18.20 112.0.18.30**

**//地址池范围为112.0.18.20-30**

**HRP\_M[FW8-policy-security]default action permit(+B)**

**//为方便默认全部放行通过，实际请勿这样操作，应按所需要求进行放行**

**HRP\_M[FW8-policy-nat]rule name napt (+B)**

**//规则名为napt**

**HRP\_M[FW8-policy-nat]source-zone trust**

**//源区域为trust**

**HRP\_M[FW8-policy-nat]destination-zone untrust**

**//目的区域为untrust**

**HRP\_M[FW8-policy-nat]source-address 192.168.0.0 mask255.255.255.0**

**//源地址网段为192.168.0.0/24**

**HRP\_M[FW8-policy-nat]action source-nat address-group napt**

**//选择源NAT模式，绑定napt地址池**

**HRP\_M[FW8]nat64 enable**

**//开启NAT64服务**

**HRP\_M[FW8-GigabitEthernet1/0/1]nat64 enable**

**//在拥有IPv6地址一端的接口也开启**

**HRP\_M[FW8]nat64 prefix 3001:: 96**

**//指定IPv4转为IPv6所用的前缀，其中96是固定的**

**HRP\_M[FW8-policy-nat-rule-nat64]nat-type nat64**

**//指定NAT类型为NAT64**

**[AR15-GigabitEthernet0/0/0]nat server protocol tcp global 112.0.1**

**54.1 www inside 10.0.151.1 www**

**//指定只将TCP流量转发，公网IP地址为112.0.154.1，并监听外网上的**

**//TCP端口80，内网的目标主机为10.0.151.1，并且这个主机将接收来自**

**//NAT的TCP 端口80流量。**