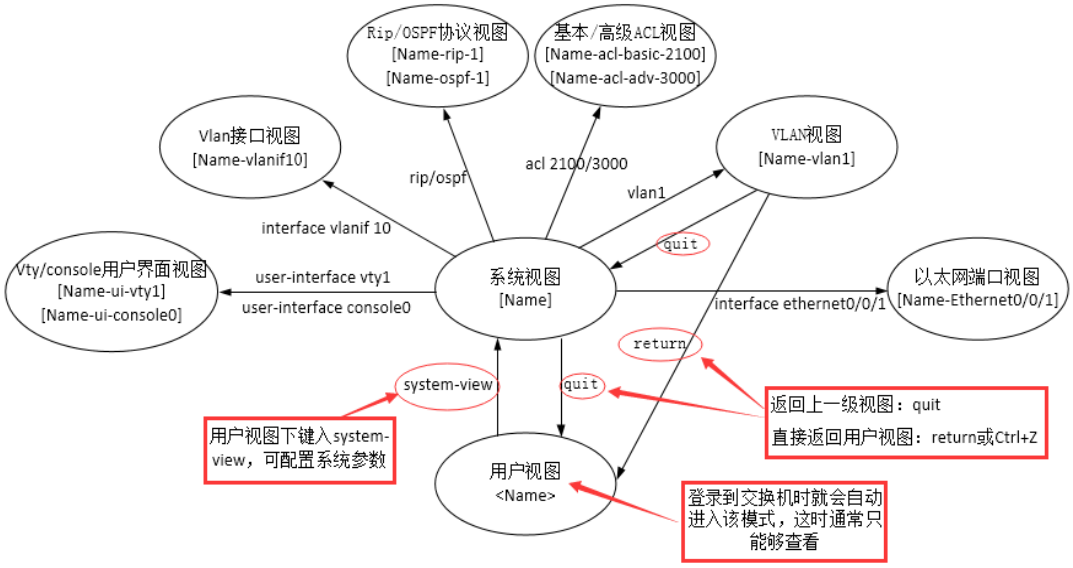
# 网络设备配置常见命令及注释

## 一、网络设备配置

### 1. 配置视图状态与转换




注：

1、配置文件

（1）运行配置文件：current-configuration 设备运行过程中的一些数据，当前配置。保存在 RAM 中

（2）启动配置文件：saved-configuration 经过保存了的配置数据，保存在非易失性 RAM----NVRAM 中

2、基本命令

（1）保存当前配置到启动配置：<HUAWEI> save

（2）查看命令：display

（3）<HUAWEI>display current-configuration //显示当前配置

（4）<HUAWEI>display saved-configuration //显示已保存配置

（5）启用 Telnet 并配置 vty 线路登录的验证方式

[HUAWEI]telnet server enable //使能 telnet 服务

[HUAWEI]user-interface vty 0 4 //开启 vty 线路（0-4）模式

[HUAWEI -ui-vty0-4]protocol inbound telnet //配置 vty 支持 telnet 协议

//设置认证模式为 aaa 认证或口令

[HUAWEI -ui-vty0-4]authentication-mode { aaa|password|none }

[HUAWEI] aaa　//进入 aaa 视图

//配置用户名和密码（密文|明文），用户不区分大小写，密码区分

[HUAWEI-aaa]local-user user1 password {irreversible-cipher|cipher} hello@123

//配置账号权限为 3（0~15 个级别，越大账号能做的操作越多）

[HUAWEI -aaa]local-user user1 privilege level 3

（6）配置 console 用户验证方式

[HUAWEI]user-interface console 0

[HUAWEI-ui-console0] authentication-mode {aaa|password|none}

当采用本地验证的话，配置密码：

[HUAWEI-ui-console0] Set authentication password [cipher password]

// cipher password 可选参数，如不使用，则采用交互方式输入明文密码

指定 cipher password，可输入密文密码

**2．交换机设备的配置**

1、二层技术原理性知识----局域网技术章节体现

2、VLAN 配置

（1）VLAN 的创建与删除

①[SWITCH] [undo] vlan *vlan-id*　　//删除/创建 *vlan-id*

②[SWITCH] vlan batch [*vlan-id*1 to *vlan-id2*]　　//批量创建 vlan

（2）设置端口类型

[SWITCH-Ethernet0/1]port link-type {access|trunk|hybrid}

// 接口模式设置为接入/中继/hybrid 模式

（3）设置端口可以通过的 VLAN 信息

①[SWITCH-Ethernet0/1]port default vlan *vlan-id*

//把端口加入到一个指定 vlan（access 模式下）

②[SWITCH-Ethernet0/1]port trunk allow-pass vlan [*vlan-id1* to *vlan-id2*|all]

//配置 trunk 中允许通过的 vlan（trunk 模式下）

③[SWITCH-Ethernet0/1]port hybrid tagged|untagged *vlan-id*

//指定 hybrid 端口以打标签/不打标签的方式加入 vlan（hyhrid 模式下）

（4）配置 VLAN 的逻辑接口（管理地址）

[SWITCH] interface vlanif *1*　　// 进入 Vlan 接口视图

[SWITCH--*vlanif1*]ip address 192.168.0.1 24　　//配置 vlan 管理地址

3、端口隔离配置

<Switch1>system-view

[Switch1] port-isolate mode l2　　//配置全局端口隔离模式为二层隔离

[Switch1]interface gigabitethernet 1/0/1

[Switch1- Gigabitethernet 1/0/1]port-isolate enable group1

//使能端口隔离功能，并将端口加入到隔离组 group1

[Switch1- Gigabitethernet 1/0/2]port-isolate enable group1

[Switch1- Gigabitethernet 1/0/2]quit　　//退出接口视图

[Switch1]　　//系统视图

即 Switch1 的两个端口实现了二层隔离

注意：需要相互隔离的两个端口一定要加入相同的隔离组。

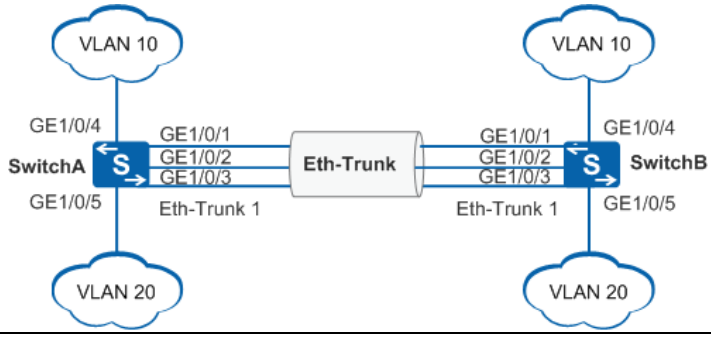
4、STP 和 GVRP 的配置

| | |
|---|---|
| GVRP | 通用属性注册协议 GARP 的应用 |
| 注册模式 | Normal：可学习、接收，发送 |
| | Fixed：不学习、接收，可发送 |
| | Forbidden：不学习，不接收，不发送 |
| 配置命令 | [HUAWEI] gvrp　//全局启用 GVRP<br>[HUAWEI-Ethernet0/1] gvrp　　//此接口启用 GVRP 功能<br>[HUAWEI-Ethernet0/1] gvrp registration [normal| fixed| forbidden]　　//配置接口 Ethernet0/1 GVRP 注册模式<br>< HUAWEI >display gvrp statistics //查看 GVRP 的统计信息 |
| STP | 目的：逻辑上阻塞冗余端口，消除网络中的环路。（二层防环） |
| 配置命令 | [HUAWEI]stp enable|disable　//全局开启|关闭 STP 功能 |

| | |
|---|---|
| | [HUAWEI]stp mode stp\|rstp //运行生成树 stp/rstp 模式<br>[HUAWEI]stp root {primary\|secondary}<br>// 设置为根桥或备份根桥<br>[HUAWEI]stp priority 优先级数值<br>//设置网桥优先级，要为 4096 的倍数<br>[HUAWEI-Ethernet0/1]stp cost 端口开销值 //设置端口开销<br>[HUAWEI-Ethernet0/1]stp port priority 优先级数值<br>//设置端口优先级<br>[HUAWEI-Ethernet0/1]stp edged-port enable<br>//配置端口为边缘端口（连接 pc）<br>[HUAWEI-Ethernet0/1]stp bpdu-filter enable<br>//启用端口 BPDU 报文过滤功能 |

5、链路聚合（在 SwitchA 和 SwitchB 上创建 Eth-Trunk 接口并加入成员接口）

| | |
|---|---|
| 链路聚合 | 将多个物理端口汇聚在一起，形成一个逻辑端口，以实现提高可靠性，提高带宽，实现负载均衡 |
| 配置命令 | <HUAWEI> system-view<br>[HUAWEI] sysname SwitchA<br>[SwitchA] interface eth-trunk 1 //创建逻辑接口 eth-trunk 1<br>[SwitchA-Eth-Trunk1] trunkport gigabitethernet 1/0/1 to 1/0/3<br>//将 gigabitethernet 1/0/1 to 1/0/3 汇聚成逻辑接口<br>[SwitchA-Eth-Trunk1] quit //退出接口模式 |

| | |
|---|---|
| | <HUAWEI> system-view<br>[HUAWEI] sysname SwitchB<br>[SwitchB] interface eth-trunk 1　　//创建逻辑接口 eth-trunk 1<br>[SwitchB-Eth-Trunk1] trunkport gigabitethernet 1/0/1 to 1/0/3<br>//将 gigabitethernet 1/0/1 to 1/0/3 汇聚成逻辑接口<br>[SwitchB-Eth-Trunk1] quit //退出接口模式<br>  |

备考攻略：

1、二层技术原理性知识点已经在局域网技术章节体现，原理性知识点在上午常考

2、下午常考配置类大题，常以填空题形式出现，可以依据上下文来判断正确填写的内容

例如：修改后的设备名（sysname）；进入的端口号（interface）；退回的界面视图（用户视图、系统视图、接口视图）等等。

填写命令尽量写全称，毕竟简写给不给分还是看阅卷老师心情的，无法作保障。

其次有实验环境条件的同学建议通过敲击一些命令来记忆语句，没有条件的同学建议自己在草稿纸上，手写命令来熟悉内容；

3、VLAN 的配置是需要重点掌握的内容

4、STP 和 GVRP 的配置需要做基本了解

5、可以参考华为华三官网的配置指导文件熟悉配置命令，协助学习。

### 3. 路由器 DHCP 的配置(举例)

[HUAWEI] dhcp enable　　//全局启用路由 DHCP 功能
[HUAWEI] ip pool pool1　　//创建全局地址池 pool1
//配置全局地址池中可用 IP 地址范围
[HUAWEI-ip-pool-pool1] network 192.168.10.0 mask 255.255.255.0
//配置自动分配给 DHCP 客户端的网关 IP
[HUAWEI-ip-pool-pool1] gateway-list 192.168.10.1
//配置租约信息：3 天 10 小时
[HUAWEI-ip-pool-pool1] lease day 3 hour 10
//启用接口采用全局地址池的 DHCP 服务器功能
[HUAWEI-Ethernet0/1]dhcp select global

DHCP 中继配置：
[HUAWEI-Ethernet0/1]dhcp select relay
//配置 DHCP 中继所连接的 DHCP 服务器 IP 地址
[HUAWEI-Ethernet0/1]dhcp relay server-ip ip-address

## 4.静态路由

基本概念

| 路由类型 | 描述 |
| --- | --- |
| 静态路由 | 管理员手动配置路由表项（人工指路）<br>ip route-static 目的 IP 地址 掩码 {下一跳 IP 地址/端口}<br>默认路由：[RB] ip route-static　0.0.0.0 0.0.0.0　10.0.0.1<br>//配置一条默认路由下一跳为 10.0.0.1<br>主机静态路由：[RB] ip route-static 192.168.3.1 255.255.255.255 192.168.2.1<br>//配置一条主机静态路由下一跳为 192.168.2.1 |
| 浮动静态路由 | 作用：路由备份，保证可靠性。通过指定优先级来实现，静态路由优先级默认为 60<br>[RB]ip route-static 192.168.1.0 255.255.255.0 192.168.2.1<br>[RB]ip route-static 192.168.1.0 255.255.255.0 192.168.20.1 preference 62　//配置一条浮动静态路由 |

**5.动态路由**

| 路由类型 | | 描述 |
|---|---|---|
| 动态路由(协议) | RIP | 内部网关路由协议&距离矢量路由协议<br>以跳数作为度量值，最大跳数 15 跳<br>定期发送更新，更新时间 30s，为避免路由环路要使用到水平分割、路由下毒（反向下毒）、触发更新等技术<br>两个版本：RIPv1 和 RIPv2<br>其中 v1 只支持有类别路由，广播通告路由信息；v2 支持无类别路由，支持认证，以组播地址 224.0.0.9 通告路由信息<br>传输层使用 UDP，520 端口 |
| | OSPF | 内部网关路由协议&链路状态路由协议<br>以开销 COST 作为度量值（与带宽有直接关系），带触发更新，使用 SPF 算法计算路由<br>通过使用区域为自治系统分段，Area0 是必要的主干区域<br>直接使用 IP 报文传输 |
| | BGP | 边界网关协议<br>运行于 TCP 179 上的一种自治系统间路由协议 |

RIP 配置命令：

| | |
|---|---|
| RIP | 基本配置：<br>[R1]rip 1　　//进入 RIP 视图，进程号未输入默认开启进程 1<br>[R1-rip-1]network 192.168.3.0　//宣告直连网络<br>[R1-rip-1]version 2　//配置 rip v2 版本<br>[R1-rip-1]undo summary　//取消路由聚合功能<br><R1>display rip 1 route　//查看 rip 协议的路由信息<br><R1>display ip routing-table //查看路由表信息 |
| | BFD 联动：双向转发检测，实现路由的快速收敛<br>[R1]bdf　　//全局使能 BFD 功能<br>[R1-rip-1]bfd all-interfaces enable //所有接口启用 BFD 功能 |

| | |
|---|---|
| OSPF | [R1]router-id 1.1.1.1 //指定 R1 的 router-id 为 1.1.1.1<br>[R1]ospf 1 //进入 ospf 视图，进程号未输入默认开启进程 1<br>[R1-ospf-1]area 0 //创建并进入 ospf 区域视图<br>[R1-ospf-1-area-0.0.0.0]network 192.168.3.0 0.0.0.255 //宣告直连网段<br><R1>display ospf routing //查看 ospf 路由信息 |

### 6. 虚拟路由冗余协议 VRRP

VRRP 基本配置

| | |
|---|---|
| VRRP | **作用：实现可靠性&负载均衡**<br>基本配置：<br>[R1] interface Gigabitethernet 0/0/1 //进入接口视图<br>[R1-Gigabitethernet 0/0/1] ip address 192.168.1.1 255.255.255.0 //给接口配置 IP 地址<br>[R1-Gigabitethernet 0/0/1] vrrp vrid 10 virtual-ip 192.168.1.254 //配置 VRRP 组号 10，并指定虚拟网关 IP<br>[R1-Gigabitethernet 0/0/1] vrrp vrid 10 priority 200<br>//配置 R1 的优先级为 200<br>[R1-Gigabitethernet 0/0/1] vrrp vrid 10 preempt-mode timer delay 10 //配置 R1 为延迟抢占方式，延时时间 10s<br>[R1-Gigabitethernet 0/0/1] vrrp vrid 10 track interface Gigabitethernet 0/0/2 reduced 60<br>//配置 VRRP 与上行接口 G0/0/2 的状态联动，如上行接口出故障 R1 优先级降低 60 |

### 7. 三层交换机

三层交换机配置

| | |
|---|---|
| 三层交换机 | **作用：带路由功能的交换机**<br>基本配置：<br>[huawei]interface Vlanif 10 //进入 vlanif10 接口视图<br>[huawei-Vlanif10]ip address 192.168.0.1 255.255.255.0 // 配置 vlanif10 接口的 IP 地址<br>[huawei]interface Vlanif 20<br>[huawei-Vlanif20]ip address 10.10.10.1 255.255.255.0 //配置 vlanif20 接口的 IP 地址 |

**8. ACL、NAT**

1、ACL 访问控制列表

表 ACL 类型

| ACL 类型 | 编号范围 | 规则描述 | 部署位置 |
|---|---|---|---|
| 基本 ACL | 2000~2999 | 基于源 ip 进行过滤 | 接近数据流的**目的**地方 |
| 高级 ACL | 3000~3999 | 基于五元组（源目 ip、源目端口、协议类型）进行过滤 | 接近数据流的**源的**地方 |

注：ACL 在**系统视图**下配置，并且需要**被应用在具体接口**才能生效

ACL 除了可以通过编号区分，还可以通过命名来区分。

表 ACL 配置命令

| | |
|---|---|
| 基本 ACL 配置 | [huawei] acl number 2002 //创建基本 ACL2002<br>[huawei-acl-basic-2002] rule permit source 202.110.10.0 0.0.0.255 //允许源 IP 是 202.110.10.0/24 网段的报文通过<br>[huawei-acl-basic-2002] rule deny source any<br>//拒绝其它网段的报文通过 |
| 高级 ACL 配置 | [huawei] acl number 3000 //创建一个编号为 3000 的高级 ACL<br>[huawei-acl-adv-3000] rule permit tcp source 202.110.10.0 0.0.0.255 destination 179.100.17.10 0.0.0.0 eq 80<br>//允许源 IP 是 202.110.10.0/24 到目的 IP 是 179.100.17.10 的 HTTP 报文通过 |

| | |
|---|---|
| ACL 应用 | Traffic-filter 传输过滤（端口，个别）<br>[Huawei-gigabitethernet 1/0/3] traffic-filter inbound acl 2002<br>//在接口 G1/0/3 的入方向上应用 ACL2002<br>注意：应用 ACL 一定要指定方向，inbound 入方向，outbound 出方向 |
| 基于时间的 ACL | [Huawei]time-range mytime 09:00 to 12:00 working-day<br>//定义一个 mytime 的时间段<br>[Huawei]acl 2000<br>[Huawei-acl-basic-2000]rule permit source 192.168.20.1 0 time-range mytime //将 ACL 的规则与时间进行关联 |
| 流分类<br>流行为<br>流策略 | [R1] traffic classifier *cname* // 创建流分类<br>//将 ACL 与流分类关联<br>[R1-classifier-*cname*] if-match acl *acl-number*<br>[R1] traffic behavior *bname* //创建流行为<br>[R1-behavior-*bname*] peimit\|deny<br>//配置流行为动作为允许\|拒绝报文通过<br>[R1] traffic policy *pname* // 创建流策略<br>//将流分类与流行为进行关联<br>[R1-trafficpolicy-*pname*] classifier *cname* behavior *bname*<br>//流策略应用在接口**入方向**<br>[R1-GigabitEthernet1/0/1] traffic-policy *pname* **inbound** |
| 策略路由 | 作用：可按管理员的意愿来实现报文转发的路径<br>通过 QOS 流策略中通过流行为中的重定向来实现<br>[Switch] traffic behavior b1<br>[Switch-behavior-b1] redirect ip-nexthop 10.1.20.1<br>//重定向到下一跳 10.1.20.1<br>其它流分类与流策略的配置同上。 |

2、NAT 网络地址翻译----缓解网络地址的紧张

在内部网络中使用私有地址，通过 NAT 把内部地址翻译成合法的公有 IP 地址在 Internet 上使用。

<table>
<tr><td rowspan="5">NAT 类型</td><td>静态 NAT</td><td colspan="2">一对一固定映射</td></tr>
<tr><td rowspan="3">动态 NAT</td><td>Basic NAT</td><td>可动态映射公网地址池中的某个 IP</td></tr>
<tr><td>NAPT</td><td>基于端口变量，实现多对一映射</td></tr>
<tr><td>EASY-IP</td><td>无需创建地址池，转换为路由器接口公有 IP 地址</td></tr>
<tr><td>NAT Server</td><td colspan="2">需要对外网提供服务的内网服务器的 NAT 方式</td></tr>
<tr><td>NAT 配置</td><td colspan="3">1）//静态 NAT 配置(必须是数据的出端口)<br>[R1-Ethernet0/1]nat static global 公网 ip 地址 inside 私有 ip 地址<br>2））动态 NAT：Basic NAT<br>[Huawei] nat address-group 1 192.1.1.2 192.1.1.4<br>//定义公网地址池<br>[Huawei] acl 2000 //定义 ACL 2000<br>[Huawei-acl-basic-2000]rule permit source 10.1.1.0 0.0.0.255<br>//指定源为 10.1.1.0/24 网段的报文允许转发<br>[Huawei-acl-basic-2000] quit<br>[Huawei] interface Ethernet 0/0/1<br>[Huawei-Ethernet0/0/1] nat outbound 2000 address-group 1 no-pat<br>//实现 ACL2000 中定义的 IP 可以与地址池中的地址进行一对一转换<br><br>3）NAPT 配置与 Basic NAT 类似，只在最后 一条命令中无需要设置 no-pat<br>[Huawei-Ethernet0/0/1] nat outbound 2000 address-group 1<br>//实现 ACL2000 中定义的 IP 与地址池中的地址进行 NAPT 转换<br><br>4）NAT-Server<br>[Huawei-Ethernet0/0/1] nat server protocol tcp global 192.1.1.2 www inside 10.1.1.2 www<br>//指定访问公网 IP 地址为 192.1.1.2 www 的报文，地址转换为私有 IP 地址 10.1.1.2 www 的报文。</td></tr>
</table>

**9. IPSec-VPN**

IPSEC VPN 配置命令(五步)

| | |
|---|---|
| 配置安全 ACL | 1、通过 ACL 定义需要保护的数据流<br>[RA] acl number 3000 //创建高级 ACL3000<br>[RA-acl-adv-3000]rule permit ip source 50.50.50.0 0.0.0.255 destination 60.60.60.0 0.0.0.255<br>//指定从源网段 50.50.50.0/24 去往目的网段 60.60.60.0/24 的数据流 |
| 配置 ipsec 安全提议 | 2、配置 Ipsce 安全提议（封装模式、安全协议、加密算法和验证算法）<br>[RA]ipsec proposal tran1 //进入 ipsec 安全提议视图<br>[RA-ipsec-proposal-tran1] Encapsulation-mode tunnel<br>//指定封装模式为隧道<br>[RA-ipsec-proposal-tran1] Transform esp<br>//指定安全协议为 ESP<br>[RA-ipsec-proposal-tran1] esp encryption-algorithm 3des<br>//指定加密算法为 3des<br>[RA-ipsec-proposal-tran1] esp authentication-algorithm sha1<br>//指定验证算法为 SHA1<br>[RA-ipsec-proposal-tran1]quit<br>//退出 ipsec 安全提议视图 |
| 配置 IKE | 3、配置 IKE 对等体（指定 VPN 隧道终点）<br>[RA]ike peer peer1 //进入 IKE 对等体视图<br>[RA-ike-peer-peer1] pre-shared-key simple Huawei<br>//配置预共享密钥<br>[RA-ike-peer-peer1]remote-address 20.20.20.1 //指定对端 IP<br>[RA-ike-peer-peer1]quit //退出 IKE 对等体视图 |

| | |
|---|---|
| 配置 Ipsce 安全策略 | 4、配置 Ipsce 安全策略（并将 ACL、ipsec 安全提议、IKE 对等体进行关联）<br>[RA] ipsec policy csaimap 1 isakmp<br>//进入 Ipsce 安全策略 csaimap 视图<br>[RA-ipsec-policy-isakmp-csaimap-1]proposal tran1<br>//关联 ipsec 安全提议<br>[RA-ipsec-policy-isakmp-csaimap-1]security acl 3000<br>//关联 ACL<br>[RA-ipsec-policy-isakmp-csaimap-1]ike-peer peer1<br>//关联 IKE 对等体<br>[RA-ipsec-policy-isakmp-csaimap-1]quit<br>//退出 Ipsce 安全策略视图 |
| 在接口应用安全策略 | 5、在接口上应用 IPsec 安全策略组<br>[RA-serial 0/0] ipsec policy csaimap |

**10. IPV6 配置**

IPv6 通信隧道配置命令

| | |
|---|---|
| 手动隧道 | 1、IPV6-OVER-IPV4 GRE 隧道配置——适用 IPV6 网络的主机需要通过 IPV4 网络通信。在双协议栈路由器上配置，手动指定隧道的源目地址。<br>GRE 隧道相关配置命令<br>[RA]Interface tunnel 0 //创建 Tunnel 接口<br>[RA-tunnel0]Tunnel protocol gre //指定 Tunnel 为 GRE 模式<br>[RA-tunnel0]Source e0 //指定 Tunnel 的源接口<br>[RA-tunnel0]Destination 192.168.50.1<br>//指定 Tunnel 的目的地址<br>[RA-tunnel0]ipv6 enable //使能接口的 IPV6 功能<br>[RA-tunnel0]Ipv6 address 3001::1 64<br>//设置 Tunnel 接口的 IPV6 地址<br>[RA]ipvr route-static 3003::1 64 tunnel 0<br>//设置发往隧道接口的 IPV6 静态路由 |

| | |
|---|---|
| 自动隧道 | 2、只需指定隧道源地址（ISATAP 隧道&IPV4 兼容 IPV6 自动隧道&6 to 4 隧道）<br>ISATAP 隧道的地址，其格式为:　　::0:5efe:w.x.y.z<br>与 IPv4 兼容的地址，0:0:0:0:0:0:w.x.y.z 或 ::w.x.y.z<br>6 to 4 地址：48 位格式前缀（2002:a.b.c.d::/48）<br><br>ISATAP 隧道相关配置命令：<br>[Router] interface tunnel 0/0/2　　//增加 tunnel 接口<br>[Router-Tunnel0/0/2] tunnel-protocol ipv6-ipv4 isatap<br>//配置 tunnel 接口隧道协议为 ISATAP<br>[Router-Tunnel0/0/2] ipv6 enable<br>[Router-Tunnel0/0/2] ipv6 address 2001::/64 eui-64<br>//配置 tunnel 接口的 IPV6 地址<br>[Router-Tunnel0/0/2] source gigabitethernet 2/0/0<br>//指定 tunnel 的源接口<br>[Router-Tunnel0/0/2] undo ipv6 nd ra halt<br>//使能系统发布 RA 报文功能<br>[Router-Tunnel0/0/2] quit |

备考攻略：

1、配置 IP 地址和静态路由：一定要写子网掩码。

2、配置 OSPF 和 ACL：一定要写反向子网掩码。

3、配置 RIP：宣告直连网段时，只要写 IP 网络地址，不需要写掩码。