HUAWEI

LANSWITCH 日常维护典型配置

LANSWITCH 基础应用典型配置

LANSWITCH 高级应用典型配置

Quidway®系列中低端 LANSWITCH

典型配置实例

技术支援网址：http://support.huawei.com 客户服务邮箱：support@huawei.com
客户服务电话：8008302118 0755-28560000 传真：0755-28560111
地址：深圳市龙岗区坂田华为总部办公楼 邮编：518129

声明

目 录

图表目录

表格目录

Quidway 系列中低端 LANSWITCH 典型配置

1 LANSWITCH 日常维护典型配置

1.1 基本操作

1. 常用命令新旧对照列表

表1 常用命令新旧对照表

旧	新		旧	新
show	**display**		access-list	**acl**
no	**undo**		acl	**eacl**
exit	**quit**			
write	**save**		show version	**disp version**
erase	**reset**		show run	**disp current-configuration**
			show tech-support	**disp diagnostic-information**
			show start	**disp saved-configuration**
router ospf	**ospf**			
router bgp	**bgp**			
router rip	**rip**			
hostname	**sysname**			
user	**local-user**			
0	**simple**			
7	**cipher**			
mode	**link-type**			
multi	**hybrid**			

⚠ 注意:

- disp 是 display 的缩写，在没有歧义时 LANSWITCH 会自动识别不完整词
- disp cur 显示 LANSWITCH 当前生效的配置参数
- disp 和 ping 命令在任何视图下都可执行，不必切换到系统视图
- 删除某条命令，一般的命令是 undo xxx，另一种情况是用其他的参数代替现在的参数，如有时虽然 xxx abc 无法使用 undo 删除，但是可以修改为 xxx def

1.2 LANSWITCH 配置注意事项

表2 LANSWITCH 配置注意事项

序号	注意项目	记录
1	登录交换机时请注意在超级终端中流控选择“无”	
2	启动时按”ctrl+B”可以进入到 boot menu 模式	
3	当交换机提示”Please Press ENTER”，敲完回车后请等待一下，设备需要一定的时间才能进入到命令行界面（具体的时间试产品而定）	
4	进入系统视图请输入”system-view”（输入”sys”即可）	
5	对使用的端口、vlan、interface vlan 进行详细的描述	
6	如果配置了 telnet 用户，一定要设置权限或配置 super 密码	
7	除了 S6500 系列，模块不可以带电插拔	
8	使用别的产品模块前请确认该模块是否可以混用	
9	配置 acl 时请注意掩码配置是否准确	
10	二层交换机配置管理 IP 后，请确保管理 vlan 包含了管理报文到达的端口	
11	配置完毕后请在用户视图下（即尖括号视图下）采用 save 命令保存配置	
12	请确保在设备保存配置的时候不掉电，否则可能会导致配置丢失	
13	如果要清除所有配置，请在用户视图下（即尖括号视图下）采用 reset saved-configuration，并重启交换机	

⚠ 注意：

其他配置需注意的地方请参考每部分内容后面的注明。

1.3 远程 telnet 登录

1. 功能需求及组网说明

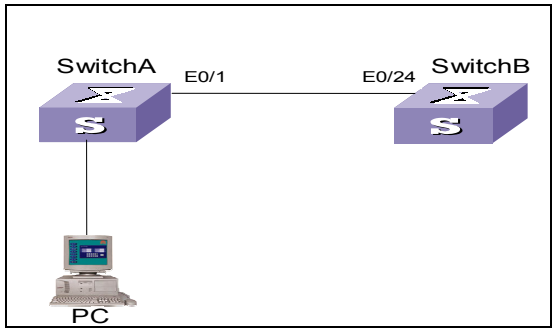


图1 telnet 配置

说明：

如图，交换机 SwitchA 通过以太网口 ethernet 0/1 和 SwitchB 的 ethernet0/24 实现互连。

PC 的 IP 地址为 10.10.10.10/24，SwitchA 的管理 IP 配置在 vlan100 的虚接口上，10.10.10.1/24，使用 vlan 10 与 SwitchB 进行互连，地址为 192.168.0.1/24，SwitchB 也使用 vlan 100 作为管理 vlan，地址为 192.168.0.2/24

需求:

(1) SwitchA 只能允许 10.10.10.0/24 网段的地址的 PC telnet 访问
(2) SwitchB 允许其它任意网段的地址 telnet 访问

2. 配置

表3 telnet 配置

配置过程	注释
SwitchA 交换机配置： [SwitchA]vlan 100 [SwitchA-vlan100] port Ethernet 0/10 to Ethernet 0/20 [SwitchA]interface Vlan-interface 100 [SwitchA-Vlan-interface100]ip address 10.10.10.1 255.255.255.0	#配置管理 vlan 100
[SwitchA]vlan 10 [SwitchA-vlan10] port Ethernet 0/1 [SwitchA]interface Vlan-interface 10 [SwitchA-Vlan-interface10]ip address 192.168.0.1 255.255.255.0	#配置与 SwitchB 互连的 vlan 10

配置过程	注释
[SwitchA]user-interface vty 0 4 [SwitchA-ui-vty0-4] [SwitchA-ui-vty0-4]authentication-mode password [SwitchA-ui-vty0-4]set authentication password simple Huawei	#设置 telnet 登录为密码验证方式。telnet 登录缺省为密码验证方式 #如果配置 telnet 登录为密码验证方式或使用缺省验证方式，必须配置登录密码，如果不配置密码，系统不允许登录。
[SwitchA-ui-vty0-4]user privilege level 3	#系统默认 VTY 登录方式用户级别为 0，设置为 3 才能进入系统视图
[SwitchA-ui-vty0-4] acl 2000 inbound [SwitchA]acl number 2000 [SwitchA-acl-basic-2000] [SwitchA-acl-basic-2000]rule permit source 10.10.10.0 0.0.0.255	#设置只允许 10.10.10.0 网段地址能够访问交换机 SwitchA
SwitchB 交换机配置： [SwitchA]vlan 100 [SwitchA-vlan100] port Ethernet 0/24 [SwitchB]interface Vlan-interface 100 [SwitchB-Vlan-interface100]ip address 192.168.0.2 255.255.255.0 [SwitchB]user-interface vty 0 4 [SwitchB-ui-vty0-4] [SwitchB-ui-vty0-4]authentication-mode password [SwitchB-ui-vty0-4]set authentication password simple Huawei [SwitchB-ui-vty0-4]user privilege level 3 [SwitchB]ip route-static 0.0.0.0 0.0.0.0 192.168.0.1	#允许其它任意网段的地址能够访问交换机需要启动路由协议或者加一条静态默认路由
telent访问控制.TXT	

⚠ 注意：

- 一共只可以设置 5 个 telnet 用户
- 缺省情况下 telnet 用户的权限是 0 级，如果没有配置 telnet 用户的权限，并且也没有配置 super 密码，则 telnet 用户只能对交换机执行有限的操作，无法配置交换机

1.4 远程 AUX 口登录

1. 功能需求及组网说明

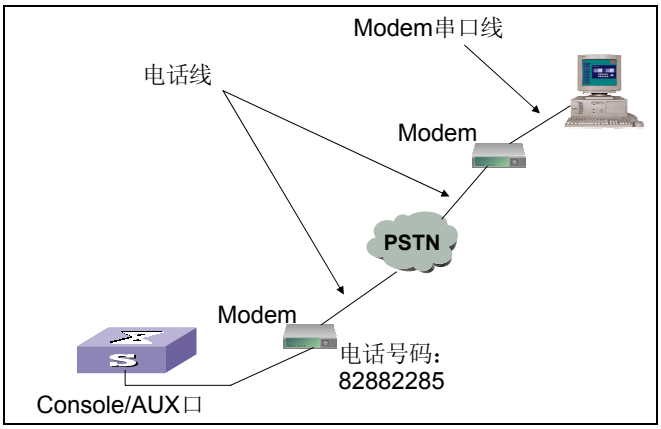


图2 通过 AUX 口远程登录交换机

需求：通过 AUX 口（即 console 口）登录到交换机进行配置

2. 配置

表4 通过 AUX 口远程登录配置

配置过程	注释
[Quidway] user-interface aux 0	#在交换机上执行 user-interface aux 0 进入 console
[Quidway-ui-aux0]modem	#键入 modem 进入 modem 状态。 #与计算机相连的modem为modemA，与交换机相连的modem为 modemB。 物理连接后在计算机上启用超级终端， com 端口选择和 modemA 相连的 com 口 在超级终端屏幕上键入命令 atdt 82882285（与交换机 modemB 的电话号码） 等待片刻就可以登录到交换机上。

⚠ 注意：

- 目前的命令行配置的交换机 console 口和 aux 口是合二为一的
- 连接交换机和 modem 要采用专用的 aux 线缆
- modem 要设置成自动应答方式

1.5 打开 debug 开关

1. 功能需求及组网说明

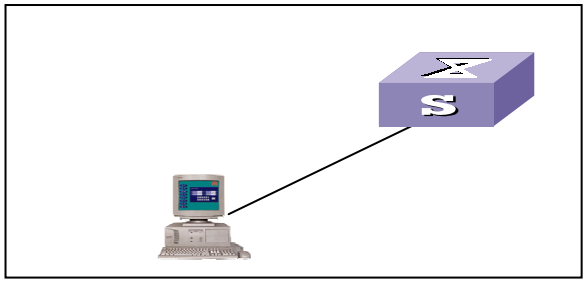


图3 Debug 系统调试

说明：如图，PC1 与交换机 A 的 Console 口或以太口相连。如果是通过以太口相连，要求 PC1 的 IP 地址和该以太端口所在的 VLAN Interface 在同一网段。在这里，我们假设 PC1 的地址是 10.110.53.247/21，交换机的以太网口所在 VLAN Interface 1 的 IP 地址是 10.110.53.248/21。

2. 配置

表5 打开 debug 开关

配置过程	注释
SwitchA 交换机配置： <Quidway>debbuging ? all All debugging functions arp ARP module bgp BGP module cluster Cluster module device Device manage dhcp-relay DHCP relay module dot1x Specify 802.1x configuration information	#在用户视图下面打开调试开关，选择所需要进行调试的模块参数。

配置过程	注释
ethernet Ethernet module fib FIB module ftp-server FTP server information garp GARP module gmrp GMRP module gvrp GVRP module habp HABP module hgmpserver HGMP server module igmp IGMP module ip IP module local-server Local authentication server information mac-address MAC address table information modem Modem module multicast Multicast module ndp NDP module ni NI module: NI Debuging information ntdp NTDP module ntp-service NTP module ospf OSPF module pim PIM module radius Radius module rip RIP module rmon RMON debugging switch snmp-agent SNMP module stp STP infomation tcp TCP module telnet TELNET module udp UDP module vfs Filesystem module vrrp VRRP module vtp VTP module vty VTY module	
<Quidway> debugging ip packet	#打开 IP 报文调试开关
<Quidway>terminal monitor	#在用户视图模式下打开屏幕输出开关。

配置过程	注释
% Current terminal monitor is on <Quidway>terminal debugging % Current terminal debugging is on <Quidway>	# 在用户视图模式下打开调试输出开关。

⚠ 注意：

- 调试结束后，用 undo debugging XXX, undo terminal monitor 和 undo terminal debugging 关闭所有的调试开关。
- 缺省情况下 debug 信息只向 console 口终端输成信息，如果是 telnet 到交换机，则需要在系统视图下执行 info-center monitor channel 0 命令，否则 debug 信息无法向 telnet 终端输出。

1.6 SNMP 配置

1. 功能需求及组网说明

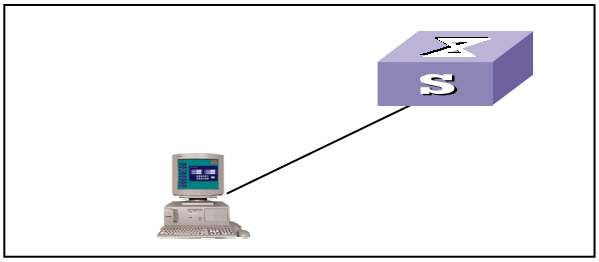


图4 SNMP 配置

说明：网管工作站（NMS）与以太网交换机通过以太网相连，网管工作站 IP 地址为 129.102.149.23，以太网交换机的 VLAN 接口 IP 地址为 129.102.0.1。在交换机上进行如下配置：设置团体名和访问权限、管理员标识、联系方法以及交换机的位置信息、允许交换机发送 Trap 消息。

2. 配置

表6 SNMP 配置

配置过程	注释
<Quidway>system-view [Quidway] snmp-agent community read public	# 进入系统视图 # 设置团体名和访问权限

配置过程	注释
[Quidway] snmp-agent community write private [Quidway]snmp-agent sys-info contact Mr.Wang-Tel:3306 [Quidway] snmp-agent sys-info location telephone-closet,3rd-floor [Quidway] snmp-agent trap enable [Quidway] snmp-agent target-host trap address udp-domain 129.102.149.23 udp-port 5000 params securityname public	# 设置管理员标识、联系方法以及物理位置 # 允许向网管工作站 129.102.149.23 发送 Trap 报文，使用的团体名为 public。

⚠ 注意：

一般情况下只需设置团体名和访问权限设备即可被管理，其他为可选配置

1.7 WEB 网管配置

1. 功能需求及组网说明

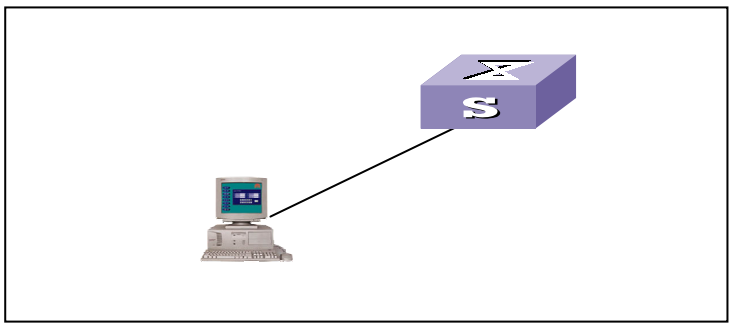


图5 WEB 网管配置

说明：PCA 连接在交换机 A 的端口 0/1

需求：PCA 使用 WEB 网管软件对交换机进行 WEB 管理

2. 配置

表7 WEB 网管配置

配置过程	注释
在 System 命令模式下进行下面配置	

配置过程	注释
[Quidway]ip http directory flash:/ [Quidway]int vlan 1 [Quidway-Vlan-interface1]ip address 13.0.0.1 255.255.255.0 [Quidway]local-user admin [Quidway-luser-admin]password simple 123 [Quidway-luser-admin]service-type telnet level 3	指定 web 网管文件的主目录 指导交换机的管理 IP 地址 建立一用户 设置用户的密码 设置用户的服务类型及级别
完成上述配置以后，在 PC 机打开浏览器，在地址栏输入交换机的 IP 地址，将在显示的页面中点击“图形管理界面”，就进入图形界面的 Web 网管。首先会弹出对话框，如果使用的是上面描述的配置，则用户名输入 wnm，认证方式选择 MD5，加密方式选择空，认证密码输入 123456，点击确定。后面就可以根据菜单和对话框的提示通过 Web 网管对交换机进行查询和配置了。	

注意：需要进行 web 网管配置，先得将 web 网管软件上传到交换机的 flash 并指定文件名为：WnmVfsFile.tar

现在有 S2000-EI、S2000/3000-SI、S3026E、S3026C、S3050、S3526E、S3526、S3528、S3552、S5000 等系列交换机支持 web 网管

2 LANSWITCH 基础应用典型配置

2.1 VLAN 配置

1. 功能需求及组网说明

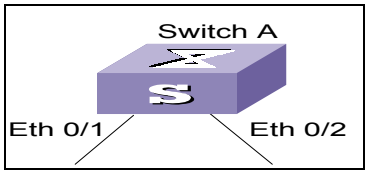


图6 VLAN 配置

需求：把交换机端口 Ethernet 0/1 加入到 VLAN 2 ，Ethernet 0/2 加入到 VLAN 3

2. 配置

表8 VLAN 配置

配置过程	注释
方法一： [Quidway]vlan 2 [Quidway-vlan2]port ethernet 0/1 [Quidway-vlan2]vlan 3	 #创建 VLAN 2 #将端口 1 加入到 VLAN 2 #创建 VLAN 3

[Quidway-vlan3]port ethernet 0/2 方法二： [Quidway]vlan 2 [Quidway-vlan2]quit [Quidway]interface ethernet 0/1 [Quidway-Ethernet1]port access vlan 2 [Quidway-Ethernet1]quit [Quidway]vlan 3 [Quidway-vlan3]quit [Quidway]interface ethernet 0/2 [Quidway-Ethernet2]port access vlan 3	#将端口 2 加入到 VLAN 3

⚠ 注意：

- 缺省情况下所有端口都属于 VLAN 1，并且端口是 access 端口，一个 access 端口只能属于一个 vlan;
- 如果端口是 access 端口，则把端口加入到另外一个 vlan 的同时，系统自动把该端口从原来的 vlan 中删除掉。

2.2 IP 地址配置

1. 功能需求及组网说明

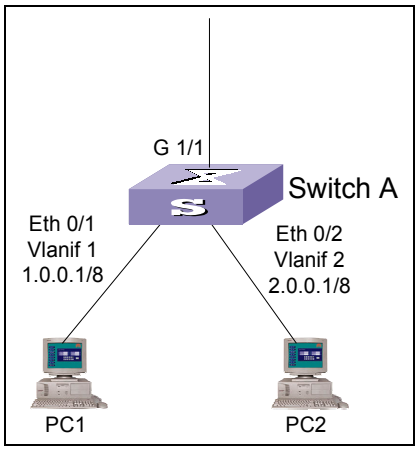


图7 IP 地址配置

说明：如图，三层交换机 SwitchA 有两个端口 ethetnet 0/1、ethernet 0/2，分别属于 vlan 2、vlan 3，vlan 2、vlan 3 的三层接口地址分别是 1.0.0.1/24、2.0.0.1/24，Pc1 和 Pc2 通过三层接口互通。

2. 配置

表9 IP 地址配置

配置过程	注释
[Quidway]vlan 2 [Quidway-vlan2]port ethernet 0/1 [Quidway-vlan2]interface vlan 2 [Quidway-Vlan-interface2]ip address 1.0.0.1 255.255.255.0 [Quidway]vlan 3 [Quidway-vlan3]port ethernet 0/2 [Quidway-vlan3]interface vlan 3 [Quidway-Vlan-interface3]ip address 2.0.0.1 255.255.255.0	#创建 VLAN 2 #增加端口 #给虚接口 VLAN 2 添加 IP 地址 #创建 VLAN 3 #增加端口 #给虚接口 VLAN 3 添加 IP 地址

注意：

- 对于交换机而言，地址只能配置在 vlan 虚接口上；但是 S6506 除外，它的 console 口旁边有一个管理以太网口（interface M-ethernet 0），可以直接配置 IP 地址。
- 该配置例是以三层交换机为例，如果是二层交换机，则只能配置一个 VLAN 虚接口。

2.3 端口的 trunk 属性配置

1. 功能需求及组网说明

图8 端口的 trunk 配置

说明：通过交换机端口的 trunk 功能来实现跨交换机之间的 vlan 互通

左边交换机为 A，右边交换机为 B。交换机 A 的 e0/1 接 vlan 10 pc；e0/2 接 vlan 20 pc; e0/3 接交换机 B 的 e0/3

需求：两台交换机之间的 vlan10 的 pc 可以互通，vlan 20 的 pc 可以互通。

2. 配置

表10 端口的 trunk 配置

配置过程	注释
SwitchA 交换机配置： [SwitchA] vlan 10 [SwitchA-vlan10]port Ethernet 0/1 [SwitchA]vlan 20 [SwitchA-vlan20]port Ethernet 0/2 [SwitchA-Ethernet0/3]port link-type trunk [SwitchA-Ethernet0/3]port trunk permit vlan all	 #创建 VLAN 10 #端口 e0/1 加入 VLAN 10 #创建 VLAN 20 #端口 e0/2 加入 VLAN 20 #配置端口 e0/3 trunk 端口，允许所有 VLAN 通过
SwitchB 交换机配置： [SwitchB] vlan 10 [SwitchB-vlan10]port Ethernet 0/1 [SwitchB]vlan 20 [SwitchB-vlan20]port Ethernet 0/2 [SwitchB-Ethernet0/3]port link-type trunk [SwitchB-Ethernet0/3]port trunk permit vlan all	 #创建 VLAN 10 #端口 e0/1 加入 VLAN 10 #创建 VLAN 20 #端口 e0/2 加入 VLAN 20 #配置端口 e0/3 trunk 端口，允许所有 VLAN 通过

⚠ 注意：

- 如果一个端口是 trunk 端口，则该端口可以属于多个 vlan;
- 缺省情况下 trunk 端口的 PVID 为 1，可以在端口模式下通过命令 port trunk pvid vlan *vlanid* 来修改端口的 PVID;
- 如果从 trunk 转发出去的数据报文的 vlan id 和端口的 PVID 一致，则该报文的 VLAN 信息会被剥去，这点在配置 trunk 端口时需要注意。
- 一台交换机上如果已经设置了某个端口为 hybrid 端口，则不可以再把另外的端口设置为 trunk 端口。

2.4 端口的 hybrid 属性配置

1. 功能需求及组网说明

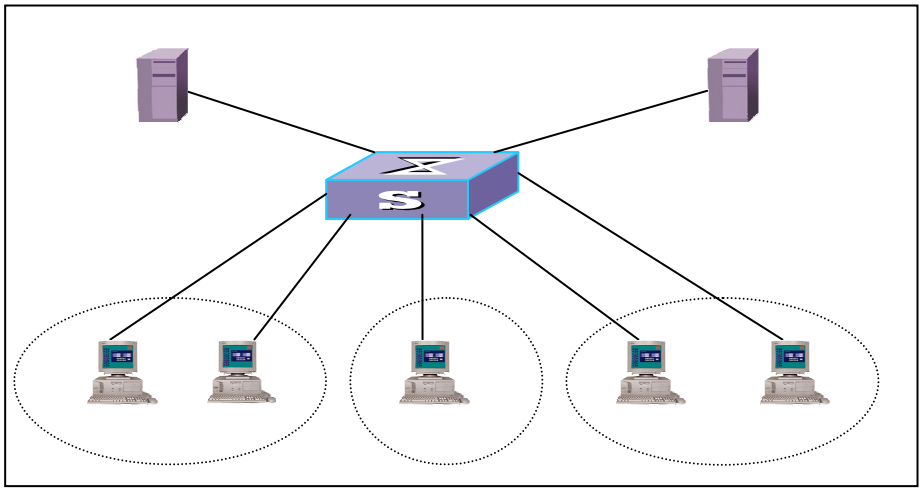


图9 端口 hybrid 属性的配置

说明：二层交换机之间利用端口的 hybrid 属性灵活实现 vlan 之间的灵活互访。

需求：所有设备的 ip 地址均在同一网段，要求三个 vlan 的 pc 均可以访问 server 1；只有 vlan 10、20 以及 vlan30 的 4 端口可以访问 server 2；同时 vlan 10 中的 2 端口的 pc 可以访问 vlan 30；vlan 20 可以访问 vlan 30 的 5 端口。

2. 配置

表11 端口 hybrid 属性配置

配置过程：	注释：
<Quidway>sys Enter system view , return user view with Ctrl+Z. [Quidway]vlan 10 [Quidway-vlan10]vlan 20 [Quidway-vlan20]vlan 30 [Quidway-vlan30]vlan 40 [Quidway-vlan40]vlan 50 [Quidway-vlan50]int e0/1 [Quidway-Ethernet0/1]port link-type hybrid [Quidway-Ethernet0/1]port hybrid pvid vlan 10 [Quidway-Ethernet0/1]port hybrid vlan 10 40 50	#首先创建业务需要的 vlan #每个端口，都配置为 hybrid 状态 #设置端口的 pvid 等于该端口所属的 vlan #将希望可以互通的端口的 pvid vlan，设置为 untagged vlan，这样从该端口发出的广播帧就可以到达本

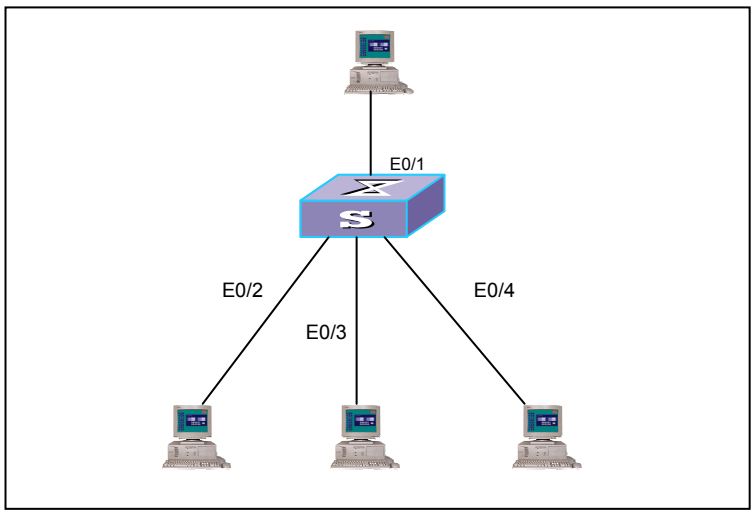
配置过程：	注释：
untagged [Quidway-Ethernet0/1]int e0/2 [Quidway-Ethernet0/2]port link-type hybrid [Quidway-Ethernet0/2]port hybrid pvid vlan 10 [Quidway-Ethernet0/2]port hybrid vlan 10 30 40 50 untagged [Quidway-Ethernet0/2]int e0/3 [Quidway-Ethernet0/3]port link-type hybrid [Quidway-Ethernet0/3]port hybrid pvid vlan 20 [Quidway-Ethernet0/3]port hybrid vlan 20 30 40 50 untagged [Quidway-Ethernet0/3]int e0/4 [Quidway-Ethernet0/4]port link-type hybrid [Quidway-Ethernet0/4]port hybrid pvid vlan 30 [Quidway-Ethernet0/4]port hybrid vlan 10 30 40 50 untagged [Quidway-Ethernet0/4]int e0/5 [Quidway-Ethernet0/5]port link-type hybrid [Quidway-Ethernet0/5]port hybrid pvid vlan 30 [Quidway-Ethernet0/5]port hybrid vlan 10 20 30 40 untagged [Quidway-Ethernet0/5]int e0/23 [Quidway-Ethernet0/23]port link-type hybrid [Quidway-Ethernet0/23]port hybrid pvid vlan 40 [Quidway-Ethernet0/23]port hybrid vlan 10 20 30 40 untagged [Quidway-Ethernet0/24]int e0/24 [Quidway-Ethernet0/24]port link-type hybrid [Quidway-Ethernet0/24]port hybrid pvid vlan 50 [Quidway-Ethernet0/24]port hybrid vlan 10 20 30 50 untagged	端口 #实际上，这种配置是通过 hybrid 端口的 pvid 来唯一的表示一个端口，接收端口通过是否将 vlan 设置为 untagged vlan，来控制是否与 pvid vlan 为该 vlan 的端口互通。
 配置信息显示.txt	

注意：

- 如果一个端口是 bybrid 端口，则可以指定 vlan 从这个端口转发出去的时候是否带 vlan 信息，如果带，则配置成 tagged 方式，否则配置成 untagged 方式；
- 一台交换机上如果已经设置了某个端口为 trunk 端口，则不可以再把另外的端口设置为 hybrid 端口。

2.5 端口隔离的配置

组网图：



1. 功能需求及组网说明：

如上图，交换机端口 e0/2 to e0/4 之间的用户需要一一隔离，但端口 e0/2 to e0/4 的用户均需要与端口 e0/1 互通

2. isolate-user-vlan 方式：

配置过程	注释
[Quidway]vlan 11 [Quidway-vlan11]port e0/1 [Quidway-vlan11]isolate-user-vlan enable [Quidway-vlan11]vlan 12 [Quidway-vlan12]port e0/2 [Quidway-vlan12]vlan 13 [Quidway-vlan13]port e0/3 [Quidway-vlan13]vlan 14 [Quidway-vlan14]port e0/4	Isolate-user-vlan 的 vlan 不需要透传，所以 vlan 号只要在交换机内不重复即可。

配置过程	注释
[Quidway]isolate-user-vlan 11 secondary 12 to 14	
isolate-user-vlan的典型配置.txt	

Isolate-user-vlan 的方式适合 S2000/3000-SI、S2000、S3000、S3526、S3526E 系列交换机。

3. 端口 vlan 内隔离的方式：

配置过程	注释
[Quidway]vlan 2 [Quidway-vlan2]port e0/1 to e0/4 [Quidway-vlan2]port-isolate enable [Quidway-vlan2]int e0/1 [Quidway-Ethernet0/1]port-isolate uplink-port vlan 2 [Quidway-Ethernet0/1]	设置 vlan 内端口隔离 设置端口隔离 vlan 的上行端口
端口隔离的典型配置.txt	

端口 vlan 内隔离的方式适合 S2000-EI、S2000C、S3528、S3552 系列交换机。

2.6 端口汇聚配置

1. 功能需求及组网说明

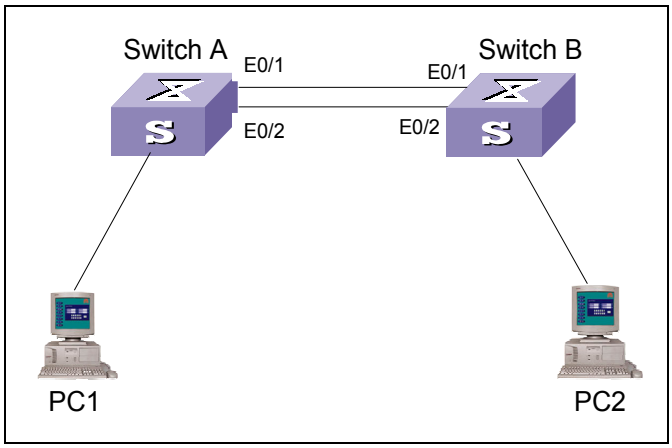


图10 端口汇聚配置

说明：如图，交换机 SwitchA 和 SwitchB 通过以太网口实现互连。其中 SwitchA 用于互连的端口为 e0/1 和 e0/2，SwitchB 用于互连的端口为 e0/1 和 e0/2。

需求：增加 SwitchA 的 SwitchB 的互连链路的带宽，并且能够实现链路备份，使用端口汇聚。

2. 配置

表12 端口汇聚配置

配置过程	注释
SwitchA 交换机配置： [SwitchA]interface Ethernet 0/1 [SwitchA-Ethernet0/1]duplex full [SwitchA-Ethernet0/1]speed 100 [SwitchA-Ethernet0/1]quit [SwitchA]interface Ethernet 0/2 [SwitchA-Ethernet0/2]duplex full [SwitchA-Ethernet0/2]speed 100 [SwitchA-Ethernet0/2]quit [SwitchA]link-aggregation Ethernet 0/1 to Ethernet 0/2 both SwitchB 交换机配置： [SwitchB]interface Ethernet 0/1 [SwitchB-Ethernet0/1]duplex full [SwitchB-Ethernet0/1]speed 100 [SwitchB-Ethernet0/1]quit [SwitchB]interface Ethernet 0/2 [SwitchB-Ethernet0/2]duplex full [SwitchB-Ethernet0/2]speed 100 [SwitchB-Ethernet0/2]quit [SwitchB]link-aggregation Ethernet 0/1 to Ethernet 0/2 both	#汇聚端口必须工作在全双工模式 #汇聚的端口速率要求相同，但不能是自适应 #可以对双向流量进行汇聚，也可以只对入流量进行汇聚
 端口汇聚配置案例.TXT	

⚠ 注意：

- 在一个端口汇聚组中，端口号最小的作为主端口，其他的作为成员端口。同一个汇聚组中成员端口的链路类型与主端口的链路类型保持一致，即如果主端口为 Trunk 端口，则成员端口也为 Trunk 端口；如主端口的链路类型改为 Access 端口，则成员端口的链路类型也变为 Access 端口。
- 不同的产品对端口汇聚时的起始端口号要求各有不同，请对照《操作手册》进行配置。

2.7 端口镜像配置

1. 功能需求及组网说明

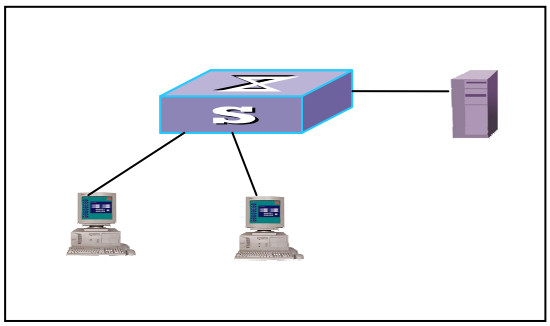


图11 端口镜像配置

说明：通过交换机端口镜像的功能使用 server 对两台 pc 的业务报文进行监控。

需求：按照不同的产品系列进行配置：

(1) 基于端口的镜像——3026
(2) 基于流的镜像——3526 和 F 系列
(3) 基于访问列表的镜像——E 系列

2. 配置

- 3026 产品

表13 3026 产品端口镜像配置

配置过程	注释
配置方法一： **[Quidway]monitor-port e0/8** **[Quidway]port mirror e0/1** **[Quidway]port mirror e0/2** 配置方法二：	 **#定义 e0/8 口为监控端口** **#定义 e0/1、e0/2 为被监控端口**

[Quidway]port mirror e0/1 to e0/2 observing-port e0/8	

- 3526/3526E/3526C/3026E/3026C 系列

表14 3526 端口镜像配置

配置过程	注释
[Quidway]acl number 3000 [Quidway-acl-adv-3000]rule 0 permit ip source 1.1.1.1 0 destination 2.2.2.2 0 [Quidway-acl-adv-3000]rule 1 permit ip source 2.2.2.2 0 destination 1.1.1.1 0 [Quidway-acl-adv-3000]quit [Quidway]mirrored-to ip-group 3000 interface e0/8	#定义一条扩展访问控制列表 #假定两台 pc 的 ip 地址分别为 1.1.1.1 和 2.2.2.2，定义分别以两台 pc 的 ip 地址做为源和目的的访问控制规则 #定义将两台 pc 的业务报文镜像到监控端口 e0/8 口上

- 3526/3526E/3526C/3026E/3026C 系列

表15 3526E 端口镜像配置

配置过程	注释
[Quidway]acl number 4000 [Quidway-acl-link-4000]rule 0 permit ingress interface Ethernet0/1 egress interface Ethernet0/2 [Quidway-acl-link-4000]rule 1 permit ingress interface Ethernet0/2 egress interface Ethernet0/1 [Quidway-acl-link-4000]quit [Quidway]mirrored-to link-group 4000 interface e0/8	#假定一台 pc 接在交换机 0/1 端口，另一台 pc 接在交换机 0/2 端口，假定 server 接在交换机 e0/8 口。

- S2000-SI/S3000-SI/S3050/S5000 系列

配置过程	注释
[Quidway]monitor-port Ethernet0/1 [Quidway] mirroring-port Ethernet0/2 both	定义观察端口 定义被镜像端口

⚠ 注意：

- S2026/S2016/S2008/S2403H 的端口镜像配置和 S3026 一致。

- S3026E/S3026C/3526E/S3526C/3526 均支持基于流的镜像，分别可对二层流、三层流做镜像。

2.8 堆叠管理配置

1. 功能需求及组网说明

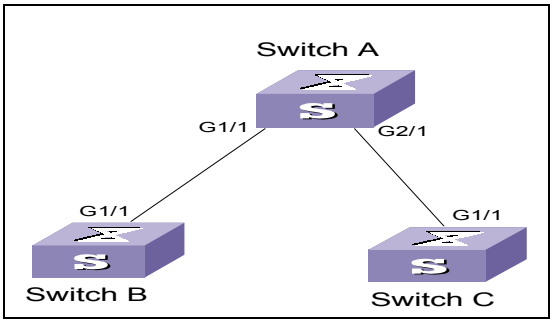


图12 堆叠管理配置

说明：如图，交换机 SwitchA 通过堆叠 1000M 口 GigabitEthernet 1/1 与 SwitchB 的 GigabitEthernet 1/1 连接，同时 SwitchA 通过堆叠 1000M 口 GigabitEthernet 2/1 与 SwitchC 的 GigabitEthernet 1/1 连接。

需求 1:SwitchA 作为堆叠主交换机管理 SwitchB 和 SwitchC，要求 SwitchA 使用 10.10.10.1/24 作为堆叠地址池。

2. 配置

表16 堆叠管理配置

配置过程	注释
SwitchA 交换机配置： [SwitchA]stacking ip-pool 10.10.10.1 3 [SwitchA]stacking enable 查看堆叠信息： [stack_0.SwitchA]display stack Main device for stack. Total members:2 查看堆叠成员信息： [stack_0.SwitchA]display stacking members Member number:0 Name:stack_0.SwitchA	 #指定堆叠管理地址池 #使能堆叠，几秒钟后两个从交换机加入。

配置过程	注释
Device:Quidway S3526 MAC Address:00e0-fc00-0003 Member status:Cmdr IP: 10.10.10.1/16 Member number:1 Name:stack_1.SwitchB Device:Quidway S3026 MAC Address:00e0-fc06-a045 Member status:Up IP: 10.10.10.2/16 Member number:2 Name:stack_1.SwitchC Device:Quidway S3026 MAC Address:00e0-fc06-a045 Member status:Up IP: 10.10.10.3/16 登录成员交换机 SwitchB： <stack_0.SwitchA>stacking 1 登录成员交换机 SwitchC <stack_0.SwitchA>stacking 2	#登录成员交换机 switchB #登录成员交换机 switchC
 堆叠管理的配置.txt	

⚠ 注意：

- 缺省情况下，堆叠地址池为空，建立堆叠必须先配置地址池;
- 缺省情况下堆叠会在成员交换机上创建 interface vlan 1，所以如果成员是二层交换机，请不要创建非 VLAN 1 的虚接口;
- S6500 系列交换机不支持堆叠。

2.9 HGMP V1 管理配置

1. 功能需求及组网说明

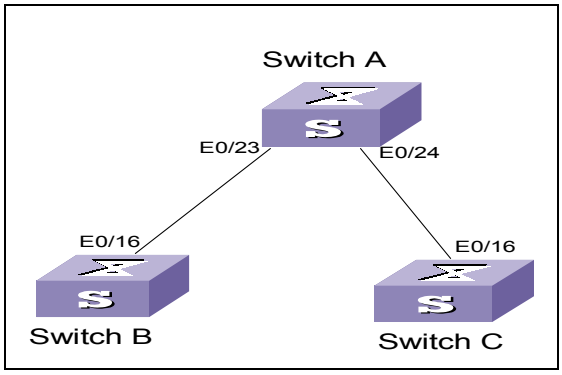


图13 HGMP V1 管理配置

说明：如图，交换机 SwitchA 通过 ethernet 0/23 与 SwitchB 的 ethernet 0/16 连接，同时 SwitchA 通过 ethernet 0/24 与 SwitchC 的 ethernet 0/16 连接。

需求 1:SwitchA 作为 HGMP Server 交换机管理 HGMP clinet 交换机 SwitchB 和 SwitchC，在 Switch A 上开启 HGMP server 的功能。

2. 配置

表17 HGMP V1 配置

配置过程	注释
SwitchA 交换机配置： [SwitchA] hgmp enable [SwitchA] interface e0/23 [SwitchA-Ethernet0/23]hgmpport enable [SwitchA] interface e0/24 [SwitchA-Ethernet0/23]hgmpport enable [SwitchA] hgmp enable [SwitchA-hgmp] display lanswitch all Lanswitch list..... ---------- No. 1 ---------- Position : LANSWITCH[0/0/23-/]	 #开启 HGMP Server 服务 #开启端口 HGMP 功能 #显示注册成功的 HGMP Client 交换机 #代表在 Switch A 上的 e0/23 上直接连接了一台交换机 S2016B，注册成功.

配置过程	注释
PortMode : TREE_MODE Lanswitch Name : Model : Quidway S2016B Device ID : Vf.30.1 MacAddr : 00e0-fc0c-0f44 Status : NORMAL [SwitchA-hgmp]lanswitch 0/0/23-/ [SwitchA-lanswitch0/0/23-/]	#进入 S2016B 的配置模式，对其相应的参数进行配置

⚠ 注意：

- 如果 client 端是 B 系列交换机，请在系统视图下配置 hgmp enable;
- 如果 client 端不是带 B 的交换机，在 boot menu 菜单下选择开启 HGMP 模式即可;
- HGMP CLENT 端的上行端口必须是指定的端口，否则无法管理。

2.10 集群管理（HGMP V2）配置

1. 功能需求及组网说明

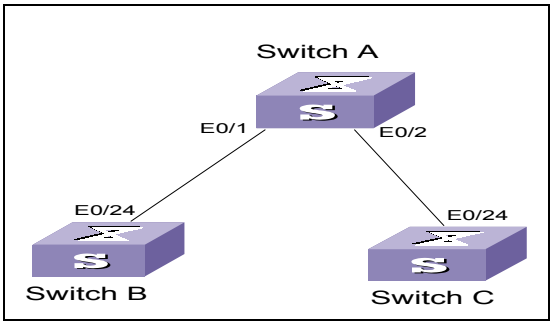


图14 集群管理配置

说明：如图，交换机 SwitchA 通过 ethernet 0/1 与 SwitchB 的 ethernet 0/24 连接，同时 SwitchA 通过 ethernet 0/2 与 SwitchC 的 ethernet 0/24 连接。

需求 1:SwitchA 作为命令交换机来管理成员交换机 SwitchB 和 SwitchC，要求使用 SwitchA 使用 10.10.10.1/24 作为集群地址池，集群的名称为 huawei。

2. 配置

表18 集群管理配置

配置过程	注释
SwitchA 交换机配置： [SwitchA]cluster [SwitchA-cluster]ip-pool 10.10.10.1 24 [SwitchA-cluster]build Huawei [huawei_0.SwitchA-cluster]auto-build Collecting candidate list, please wait... Candidate list: Name Hops MAC Address Device SwitchB 1 00e0-fc06-a045 Quidway S3026 SwitchC 2 00e0-fc06-a021 Quidway S3026 Add all to cluster?(Y/N)y Cluster auto-build Finish! 2 member(s) added successfully. 查看集群成员： [huawei_0.SwitchA-cluster]display cluster members SN Device MAC Address Status Name 0 Quidway S3526 00e0-fc00-0003 Admin Huawei_0.SwitchA 1 Quidway S3026 00e0-fc06-a045 Up Huawei_1.SwitchB 2 Quidway S3026 00e0-fc06-a021 Up Huawei_3.SwitchC [huawei_0.SwitchA-cluster] 登录成员交换机 SwitchB： <huawei_0.SwitchA>cluster switch-to 1 登录成员交换机 SwitchC <huawei_0.SwitchA>cluster switch-to 2	#指定集群内部使用的地址池 #配置集群名称 #使用命令自动加入成员 #此处输入 Y，将成员全部加入 #Up 表示成员正常 #登录成员交换机 swtichB #登录成员交换机 swtichC
 集群管理的配置.txt	

⚠ 注意：

缺省情况下集群会在成员交换机上创建 interface vlan 1，所以如果成员是二层交换机，请不要创建非 VLAN 1 的虚接口。

3 LANSWITCH 高级应用典型配置

3.1 STP 配置

1. 功能需求及组网说明

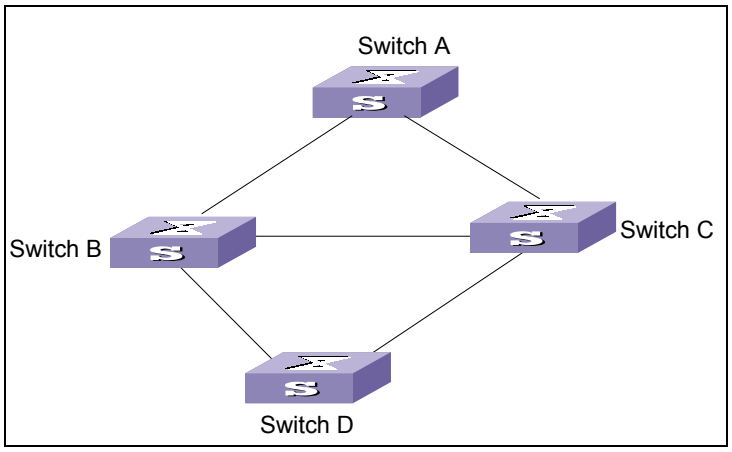


图15 STP 配置

说明：如图，交换机 SwitchA、SwitchB 和 SwitchC 都通过 GE 接口互连；SwitchB 和 SwitchC 交换机是核心交换机，要求主备。

需求：要求整个网络运行 STP 协议。

2. STP 配置

表19 STP 配置

配置过程	注释
SwitchA 交换机配置： [SwitchA]stp enable	 #启动生成树协议
SwitchB 交换机配置： [SwitchB]stp enable [SwitchB]stp root primary	 #启动生成树协议 #配置本桥为根桥
SwitchC 交换机配置： [SwitchC]stp enable [SwitchC]stp root secondary	 #启动生成树协议 #配置本桥为备份根桥
SwitchD 交换机配置： [SwitchD]stp enable	 #启动生成树协议

⚠ 注意：

- 缺省情况下交换机的优先级都是 32768，如果想人为指定某一台交换机为根交换机，也可以通过修改优先级来实现;
- 缺省情况下打开生成树后，所有端口都会开启生成树协议，请把接 PC 的端口改为边缘端口模式。

3.2 路由协议配置

1. 功能需求及组网说明

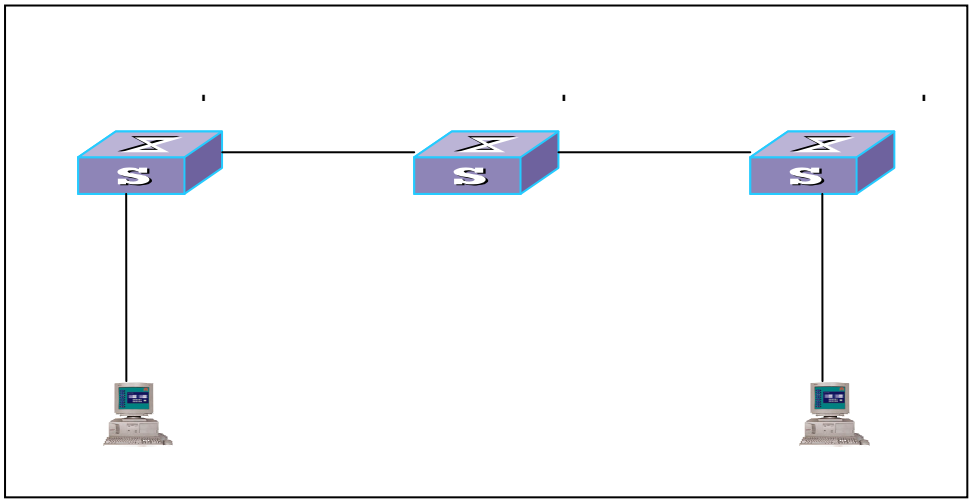


图16 路由协议配置

说明：如图，交换机 lanswitchA、lanswitchB、lanswitchC 实现互连。其中 lanswitchA 上 vlan 10 接局域网，interface vlan 10 的 IP 地址为为 10.1.1.1 /24，lanswitchA 和 lanswitchB 通过 VLAN 20 互连，lanswitchA 上 vlan 20 的虚接口地址为 20.1.1.1 /24，lanswitchB 上 vlan 20 的虚接口地址为 20.1.1.2 /24；lanswitchB 和 lanswitchC 通过 vlan 30 互连，lanswitchB 上 vlan 30 的虚接口地址为 30.1.1.1 /24，lanswitchC 上 vlan 30 的虚接口地址为 30.1.1.2/24；lanswitchC 上 vlan 40 接局域网，interface vlan 40 的 IP 地址为 40.1.1.1/24

需求: 交换机之间运行动态路由协议，保证 PC1 和 PC2 互通。

（PC1 的 IP 地址为 10.1.1.2/24，网关为 10.1.1.1；PC2 的 IP 地址为 40.1.1.2/24，网关为 40.1.1.2）

请分别写出运行 RIP、OSPF 的配置。

2. 配置

- rip：

表20 RIP 协议配置

配置过程	注释
LANSWITCHA： [SwitchA]VLAN 10 [SwitchA-vlan10]PORT （VLAN 10 的端口） [SwitchA-vlan10]Int vlan 10 [SwitchA-Vlan-interface10]Ip add 10.1.1.1 255.255.255.0	#配置相关 VLAN 信息

配置过程	注释
[SwitchA]Vlan 20 [SwitchA-vlan20]Port (vlan 20 的端口) [SwitchA-vlan20]Int vlan 20 [SwitchA-Vlan-interface20]Ip add 20.1.1.1 255.255.255.0 [SwitchA-Vlan-interface10]quit [SwitchA]rip [SwitchA-rip]Network 10.1.1.0 [SwitchA-rip]Network 20.1.1.0 LANSWTICHB： [SwitchB]VLAN 20 [SwitchB-vlan20]PORT （VLAN 20 的端口） [SwitchB-vlan20]Int vlan 20 [SwitchB-Vlan-interface20] Ip add 20.1.1.2 255.255.255.0 [SwitchB-Vlan-interface20]Vlan 30 [SwitchB-vlan30]Port (vlan 30 的端口) [SwitchB-vlan30]Int vlan 30 [SwitchB-Vlan-interface30] Ip add 30.1.1.1 255.255.255.0 [SwitchB-Vlan-interface30]quit [SwitchB]rip [SwitchB-rip]network 20.1.1.0 [SwitchB-rip]network 30.1.1.0 LANSWITCHC： [SwitchC]VLAN 30 [SwitchC-vlan30]PORT （VLAN 30 的端口） [SwitchC-vlan30]Int vlan 30 [SwitchC-Vlan-interface30]Ip add 30.1.1.2 255.255.255.0 [SwitchC-Vlan-interface30]Vlan 40 [SwitchC-vlan40]Port (vlan 40 的端口) [SwitchC-vlan40]Int vlan 40 [SwitchC-Vlan-interface40]Ip add 40.1.1.1 255.255.255.0 [SwitchC-Vlan-interface40]quit	#启动 RIP 协议 #从 10.1.1.0 网段的接口发布和接收 RIP 路由信息

配置过程	注释
[SwitchC]rip [SwitchC-rip] network 30.1.1.0 [SwitchC-rip] network 40.1.1.0	

- OSPF：

表21 OSPF 协议配置

配置过程	注释
LANSWITCHA： [SwitchA]VLAN 10 [SwitchA-vlan10]PORT （VLAN 10 的端口） [SwitchA-vlan10]Int vlan 10 [SwitchA-Vlan-interface10]Ip add 10.1.1.1 255.255.255.0 [SwitchA-Vlan-interface10]Vlan 20 [SwitchA-vlan20]Port (vlan 20 的端口) [SwitchA-vlan20]Int vlan 20 [SwitchA-Vlan-interface20]Ip add 20.1.1.1 255.255.255.0 [SwitchA-Vlan-interface10]quit [SwitchA]Ospf [SwitchA-ospf]Area 0 [SwitchA-ospf-area-0.0.0.0]Network 10.1.1.1 255.255.255.0 [SwitchA-ospf-area-0.0.0.0]Network 20.1.1.1 255.255.255.0 **LANSWTICHB：** [SwitchB]VLAN 20 [SwitchB-vlan20]PORT （VLAN 20 的端口） [SwitchB-vlan20]Int vlan 20 [SwitchB-Vlan-interface20]Ip add 20.1.1.2 255.255.255.0 [SwitchB-Vlan-interface20]Vlan 30 [SwitchB-vlan30]Port (vlan 30 的端口) [SwitchB-vlan30]Int vlan 30 [SwitchB-Vlan-interface30]Ip add 30.1.1.1 255.255.255.0 [SwitchB-Vlan-interface30]quit	**#配置相关 VLAN 信息** **#启动 OSPF 路由协议** **#指定区域号** **#从该网段的接口接收和发布路由信息**

配置过程	注释
[SwitchB]Ospf [SwitchB-ospf]Area 0 [SwitchB-ospf-area-0.0.0.0]Network 20.1.1.2 255.255.255.0 [SwitchB-ospf-area-0.0.0.0]Network 30.1.1.1 255.255.255.0 **LANSWITCHC：** [SwitchC]VLAN 30 [SwitchC-vlan30]PORT （VLAN 30 的端口） [SwitchC-vlan30]Int vlan 30 [SwitchC-Vlan-interface30]Ip add 30.1.1.2 255.255.255.0 [SwitchC-Vlan-interface30]Vlan 40 [SwitchC-vlan40]Port (vlan 40 的端口) [SwitchC-Vlan40]Int vlan 40 [SwitchC-Vlan-interface40]Ip add 40.1.1.1 255.255.255.0 [SwitchC-Vlan-interface30]quit [SwitchC]Ospf [SwitchC-ospf]Area 0 [SwitchC-ospf-area-0.0.0.0]Network 30.1.1.2 255.255.255.0 [SwitchC-ospf-area-0.0.0.0]Network 40.1.1.1 255.255.255.0	

3.3 组播配置

1. 功能需求及组网说明

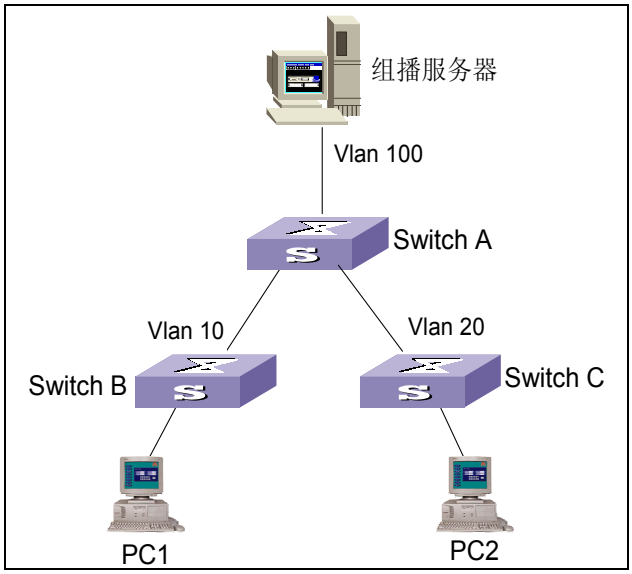


图17 三层交换机组播配置

说明：如图，三层交换机 SwitchA 通过上行口 G1/1 连接组播服务器，地址为 192.168.0.10/24，交换机连接组播服务器接口 interface vlan 100，地址为 192.168.0.1。vlan10 和 vlan20 下挂两个二层交换机 SwitchB 和 SwitchC，地址为 10.10.10.1/24 和 10.10.20.1/24。

需求 1:在 SwitchA、SwitchB 和 SwitchC 上运行组播协议，要求 L3 上配置为 IP PIM-SM 模式。

2. 配置

表22 组播配置

配置过程	注释
switchA: [SwitchA]multicast routing-enable [SwitchA]int vlan 100 [SwitchA-Vlan-interface100]ip add 192.168.0.1 255.255.255.0 [SwitchA]int vlan 10 [SwitchA-Vlan-interface10]ip add 10.10.10.1 255.255.255.0 [SwitchA-Vlan-interface10]pim SM [SwitchA-Vlan-interface10]quit [SwitchA]interface Vlan-interface 20 [SwitchA-Vlan-interface20]ip add 10.10.20.1 255.255.255.0 [SwitchA-Vlan-interface20]pim SM [SwitchA-Vlan-interface20]quit [SwitchA]pim [SwitchA-pim]c-bsr vlan 100 24 [SwitchA-pim]c-rp vlan 100 swtichB,switchC 可以不配置，或者支持 IGMP SNOOPING，可以系统视图启动 multicast routing-enable。	#使能多播路由 #在接口上启动 PIM SM #在接口上启动 PIM SM #进入 PIM 视图 #配置候选 BSR #配置候选 RP
 三层交换机组播配置. txt	

⚠ 注意：

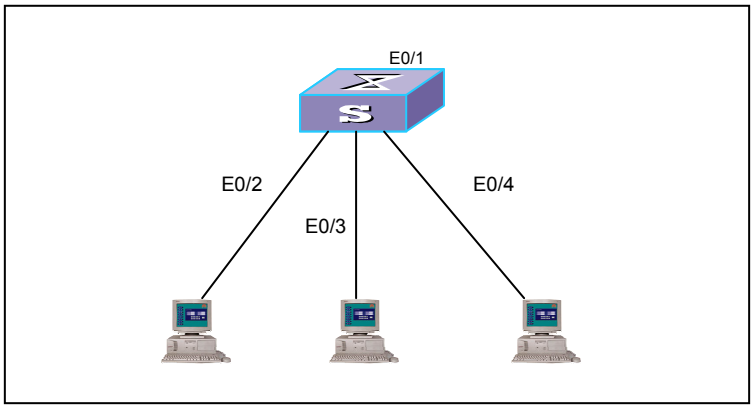
PIM-DM 的配置相对简单，只需两步：

- 在系统视图下配置 multicast routing-enable
- 在接口上配置 PIM-DM
- 不需要配置 c-bsr 和 c-rp

如果是二层交换机，则只需在系统视图下配置 igmp-snooping 即可；

目前交换机的 IGMP 只支持 V1/V2 版本。

3.4 DHCP-SERVER 配置



1. 功能需求组网说明：

如上图，交换机下挂 PC 通过交换机动态获取 IP 地址。端口 e0/2 to e0/4 均在 vlan2 里边，vlan2 的 IP 地址为 10.0.0.1/24

2. 配置：

配置过程	注释
Switch 交换机配置： [Quidway]vlan 2 [Quidway-vlan2]port e0/2 to e0/4 [Quidway-vlan2]int vlan 2 [Quidway-Vlan-interface2]ip add 10.0.0.1 255.255.255.0 [Quidway-Vlan-interface2]dhcp select interface [Quidway-Vlan-interface2]dhcp server dns-list 10.0.0.2 ? [Quidway-Vlan-interface2]dhcp server dns-list 10.0.0.2 [Quidway-Vlan-interface2]dhcp server domain-name huawei.com [Quidway-Vlan-interface2] dhcp server expired day 20 hour 10	

配置过程	注释
DHCPSERVER的典型配置.txt	

注意：低端交换机只有 S3526E 的 vrp3.10-0031 和以后的版本及 S3528/S3552 的 vrp3.10-0012 和以后的版本。

3.5 DHCP-RELAY 配置

1. 功能需求及组网说明

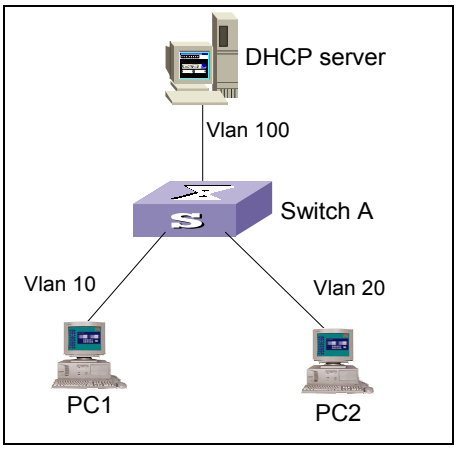


图18 DHCP 中继配置

说明：如图，交换机 SwitchA 通过上行口 G1/1 连接 DHCPserver，地址为 192.168.0.10/24，交换机连接 DHCP server 接口 interface vlan 100，地址为 192.168.0.1。下挂两个用户网段，vlan10 和 vlan20，vlan 10 包含的端口为 ethernet 0/1 到 ethernet 0/10，网段为 10.10.1.1/24，vlan 20 包含端口为 ethernet 0/11 到 ethernet 0/20，网段为 10.10.2.1/24。

需求：在 Switch 上配置 DHCP 中继

2. 配置

表23 DHCP 中继配置

配置过程	注释
SwitchA 交换机配置： [SwitchA]dhcp-server 0 ip 192.168.0.10 [SwitchA]vlan 100 [SwitchA-vlan100]port GigabitEthernet 1/1 [SwitchA-vlan100]q [SwitchA]interface Vlan-interface 100	 #指定 DHCP server0 的 IP 地址 #配置链接 DHCP server 的 vlan 。

配置过程	注释
[SwitchA-Vlan-interface100]ip address 192.168.0.1 255.255.255.0	
[SwitchA]vlan 10 [SwitchA-vlan10]port Ethernet 0/1 to Ethernet 0/10 [SwitchA-vlan10]q [SwitchA]interface Vlan-interface 10 [SwitchA-Vlan-interface10]ip address 10.10.1.1 255.255.255.0 [SwitchA-Vlan-interface10]dhcp-server 0 [SwitchA-Vlan-interface10]q	#添加 vlan10，网段地址为 10.10.1.1/24 #指定 vlan 10 使用 DHCP server0 的地址
[SwitchA-vlan10]vlan 20 [SwitchA-vlan20]port Ethernet 0/11 to Ethernet 0/20 [SwitchA]interface Vlan-interface 20 [SwitchA-Vlan-interface20]ip address 10.10.2.1 255.255.255.0 [SwitchA-Vlan-interface20]dhcp-server 0	#添加 vlan 20，网段地址为 10.10.2.1/24 #指定 vlan 20 使用 DHCP server0 的地址
DHCP中继配置.TXT	

3.6 802.1X 配置

1. 功能需求及组网说明

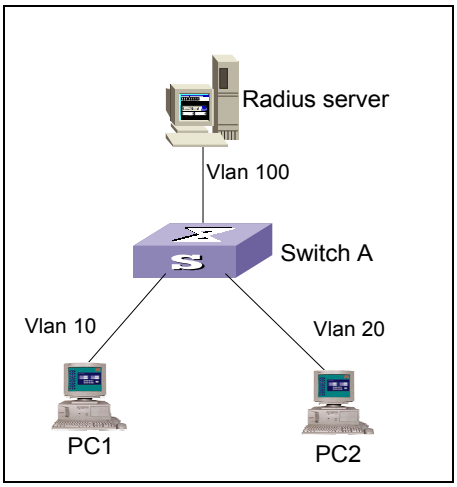


图19 802.1X 配置

说明：如图，交换机 SwitchA 通过上行口 G1/1 连接 RADIUS server，地址为 192.168.0.100/24，交换机连接 RADIUS server 接口 interface vlan 100，地址为 192.168.0.1。下挂两个用户网段，vlan10 和 vlan20，vlan 10 包含的端口为 ethernet 0/1 到 ethernet 0/10，网段为 10.10.1.1/24，vlan 20 包含端口为 ethernet 0/11 到 ethernet 0/20，网段为 10.10.2.1/24。

需求：在 Switch 上配置 802.1X

2. 配置

表24 802.1X 配置

配置过程	注释
本地认证配置： [SwitchA]vlan 100 [SwitchA-vlan100]port GigabitEthernet 1/1 [SwitchA-vlan100]quit	#本地认证不需要 RADIUS server，我们可以将图 1 中的 RADIUS server 去掉。
[SwitchA]interface Vlan-interface 100 [SwitchA-Vlan-interface100]ip address 192.168.0.1 255.255.255.0	#配置 vlan 100，地址为 192.168.0.1/24
[SwitchA]vlan 10 [SwitchA-vlan10]port Ethernet 0/1 to Ethernet 0/10 [SwitchA-vlan10]quit [SwitchA]interface Vlan-interface 10 [SwitchA-Vlan-interface10]ip address 10.10.1.1 255.255.255.0 [SwitchA-Vlan-interface10]quit	#添加 vlan10，网段地址为 10.10.1.1/24
[SwitchA-vlan10]vlan 20 [SwitchA-vlan20]port Ethernet 0/11 to Ethernet 0/20 [SwitchA]interface Vlan-interface 20 [SwitchA-Vlan-interface20]ip address 10.10.2.1 255.255.255.0	#添加 vlan 20，网段地址为 10.10.2.1/24
802.1X 相关配置： [SwitchA]dot1x [SwitchA]dot1x interface eth 0/1 to eth 0/10	#采用默认基于 MAC 的认证方式 #只在前 10 个端口上开启 802.1X #这里采用缺省域 system，并且缺省域引用缺省 radius 方案 system。 #如果不采用缺省域 system，可以以下面的“RADIUS 认证配置”为例设置，只不过服务器地址为 127.0.0.1，认证/计费端口分别为 1645/1646。 #添加本地用户 test，密码为 test（明文）
[SwitchA]local-user test [SwitchA-user-test]service-type lan-access	#前面的添加 vlan 和配置 IP 地址等和

配置过程	注释
[SwitchA-user-test]password simple test	本地配置相同，不再重复。只讲 802.1X 部分
	#设置认证方式为 RADIUS，RADIUS 认证不成功取本地认证。
RADIUS 认证配置	
[SwitchA]dot1x	#设置主认证服务器
[SwitchA]dot interface eth 0/1 to eth 0/10	
[SwitchA]radius scheme radius1	
[SwitchA-radius-radius1]primary authentication 192.168.0.100	#本例认证和计费在一个服务器中
[SwitchA-radius-radius1]primary accounting 192.168.0.100	#key 应该与服务器的设置一致
[SwitchA-radius-radius1]key authentication test	#交换机送给 RADIUS 报文去掉域名
[SwitchA-radius-radius1]key accounting test	#增加一个域
	#在域里引用前面设置的 radius 方案
[SwitchA-radius-radius1]user-name-format without-domain	
[SwitchA]domain Huawei	
[SwitchA-isp-huawei] radius-scheme radius1	
 802.1X配置.txt	

⚠ 注意：

- 一般情况下接入端用户名需要加上域，本例客户端认证的时候输入用户名时就需要加上域名；
- 可以在系统视图下通过命令 domain default enable *domain-name* 来指定缺省的域名，这样如果用户进行认证的时候没有输入用户名，则采用缺省指定域名来进行认证和计费；
- 新的版本支持对用户是否使用了代理进行检测，可以在系统视图下通过命令 dot1x supp-proxy-check xxx 实现；
- 新的版本也将支持多种认证方式（PAP、CHAP、EAP-MAD5），请在系统视图下通过命令 dot1x authentication-method xxx 来配置(如果命令行没有这条命令，这说明当前版本不支持多种认证方式，只支持缺省的 CHAP 认证方式。）

3.7 VRRP 配置

1. 功能需求及组网说明

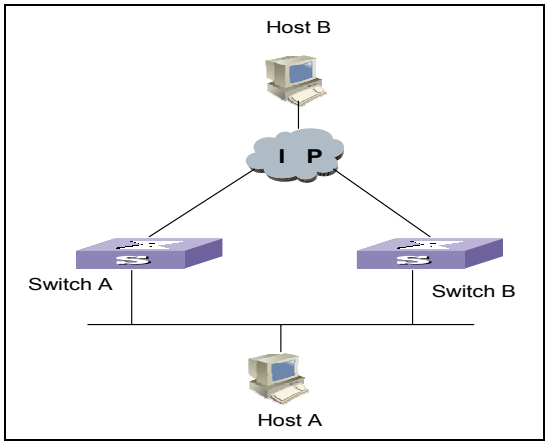


图20 VRRP 配置

说明：如图，交换机 SwitchA 通过 ethernet 0/24 与 SwitchB 的 ethernet 0/24 连接，同时连接 HostA,SwitchA 和 SwitchB 上分别创建两个虚接口，interface vlan 10 和 interface 20 做为三层接口，其中 interface vlan 10 分别包含 ethernet 0/24 端口，interface 20 包含 ethernet 0/23 端口，做为出口。

需求：SwitchA 和 SwitchB 之间做 VRRP，interface vlan 10 做为虚拟网关接口，Switch A 为主设备，允许抢占，SwitchB 为从设备，Host A 主机的网关设置为 VRRP 虚拟网关 IP192.168.100.1，进行冗余备份。访问远端主机 Host B10.1.1.1/24。

2. 配置

表25 VRRP 配置

配置过程	注释
SwitchA 交换机配置： [SwitchA] vlan 10 [SwitchA-vlan10] port Ethernet 0/24 [SwitchA]vlan 20 [SwitchA-vlan20]port Ethernet 0/23 [SwitchA-vlan20]int vlan 20 [SwitchA-Vlan-interface20]ip add 11.1.1.1 255.255.255.252 [SwitchA-Vlan-interface20]quit [SwitchA] interface vlan 10 [SwitchA-Vlan-interface10]ip address 192.168.100.2 255.255.255.0 [SwitchA-Vlan-interface10]vrrp vrid 1 virtual-ip 192.168.100.1 [SwitchA-Vlan-interface10]vrrp vrid 1 priority 120	#创建 vlan 10,vlan 20,虚拟接口 interface vlan 10,interface vlan 20. #接口实际 IP 地址 #创建 VRRP 组 1，虚拟网关为 192.168.100.1 #设置 VRRP 组优先级为 120，缺省为 100 #设置为抢占模式

配置过程	注释
[SwitchA-Vlan-interface10]vrrp vrid 1 preempt-mode [SwitchA-Vlan-interface10]vrrp vrid 1 track Vlan-interface 20 reduced 30 [SwitchA-Vlan-interface10]quit [SwitchA]ip route-static 10.1.1.1 255.255.255.0 11.1.1.2 Switch B 配置： [SwitchA] vlan 10 [SwitchA-vlan10] port Ethernet 0/24 [SwitchA]vlan 20 [SwitchA-vlan20]port Ethernet 0/23 [SwitchA-vlan20]int vlan 20 [SwitchA-Vlan-interface20]ip add 12.1.1.1 255.255.255.252 [SwitchA-Vlan-interface20]quit [SwitchA] interface vlan 10 [SwitchA-Vlan-interface10]ip address 192.168.100.3 255.255.255.0 [SwitchA-Vlan-interface10]vrrp vrid 1 virtual-ip 192.168.100.1 [SwitchA-Vlan-interface10]vrrp vrid 1 preempt-mode [SwitchA-Vlan-interface10] [SwitchA-Vlan-interface10]quit [SwitchA]ip route-static 10.1.1.1 255.255.255.0 12.1.1.2	#设置监控端口为为interface vlan 20,如果端口Down 掉优先级降低 30 #配置一条到对方网段的静态路由

3.8 单向访问控制

1. 功能需求及组网说明

- 同网段单向访问控制

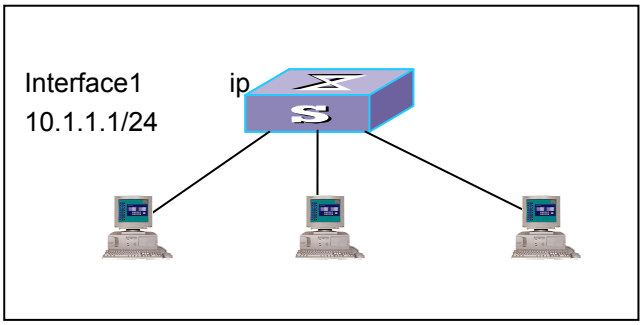


图21 单向访问控制

说明：如图，PCA、PCB 和 PCC 通过交换机互连。其中 PCA 的 IP 地址为 10.1.1.2/24,PCB 的 IP 地址为 10.1.1.3/24，PCC 的 IP 地址为 10.1.1.4/24

需求:PCA、PCB 和 PCC 之间完成单向访问，即 PCA 可以访问 PCB、PCC，但是 PCB、PCC 不能访问 PCA

- 不同网段单向访问控制

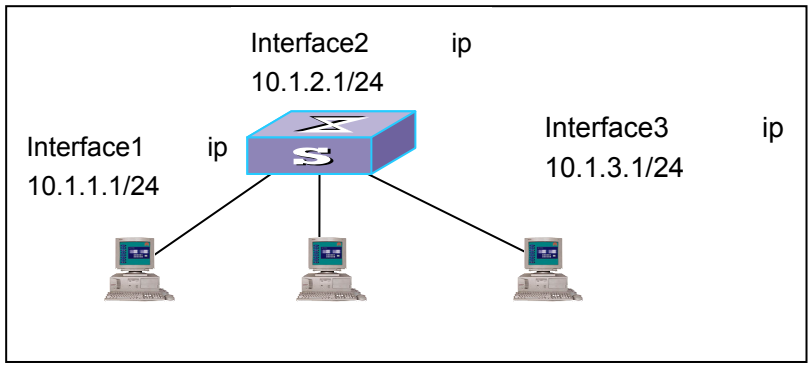


图22 不同网段单向访问控制

说明：如图，PCA、PCB 和 PCC 通过交换机互连。其中 PCA 的 IP 地址为 10.1.1.2/24,PCB 的 IP 地址为 10.1.2.2/24，PCC 的 IP 地址为 10.1.3.2/24，对应的网关地址分别为 10.1.1.1/24、10.1.2.1/24 和 10.1.3.1/24

需求:PCA、PCB 和 PCC 之间完成单向访问，即 PCA 可以访问 PCB、PCC，但是 PCB、PCC 不能访问 PCA

2. 配置

- 同网段单向 ping 配置

以 S3526E 为例：

表26 同一网段 PING 单向访问控制

配置过程	注释
PCA 与交换机的 e0/1 端口相连，配置如下： [Quidway]acl number 3000	#配置二层访问控制规则

[Quidway-acl- adv-3000]rule deny icmp source 1.1.1.1 0 destination 1.1.1.2 0 icmp-type echo	#配置二层访问控制子规则，禁止从任何端口的入报文出端口到 e0/1
[Quidway]packet-filter ip-group 3000	#激活该规则

以 6506 为例:

配置过程	注释
PCA 与交换机的 e4/0/1 端口相连，配置如下： [Quidway]acl number 3000	＃配置扩展访问控制规则
[Quidway-acl-adv-3000]rule 0 deny icmp source 1.1.1.1 0 destination 1.1.1.2 0	＃配置扩展访问控制子规则，禁止 1.1.1.1 Ping 通 1.1.1.2
[Quidway-acl-adv-3000]int e4/0/1	#进入端口模式
[Quidway-Ethernet4/0/1] packet-filter inbound ip-group 3000 rule 0	＃激活该规则

以 5516 为例：

配置过程	注释
PCA 与交换机的 e0/1 端口相连，配置如下： [Quidway]acl number 3000	＃配置二层访问控制规则
[Quidway-acl-adv-3000]rule deny icmp source 1.1.1.3 0 destination 1.1.1.2 0	＃配置访问控制子规则，禁止主机 pcb 访问 pca
[Quidway-acl-adv-3000]rule deny icmp source 1.1.1.4 0 destination 1.1.1.2 0	＃配置访问控制子规则，禁止主机 pcc 访问 pca
[Quidway]packet-filter ip-group 3000	＃激活该规则

(2) 同网段 TCP 单向访问配置

以 S3526E 为例：

表27 同一网段 TCP 单向访问控制

配置方法	注释
[Quidway]acl number 3000	#配置三层访问控制规则
[Quidway-acl-adv-3000]rule deny tcp established source 1.1.1.1 0 destination 1.1.1.2 0	#主机 ip 地址为 1.1.1.1 的 PC 无法向 1.1.1.2 的 PC 发起 TCP 连接建立请求
[Quidway]packet-filter ip-group 3000	#激活该规则

以 6506 为例：

配置方法	注释
PCA 与交换机的 e4/0/1 端口相连，配置如下： [Quidway]acl number 3000	＃配置扩展访问控制规则
[Quidway-acl-adv-3000] rule 1 deny tcp established source 1.1.1.1 0 destination 1.1.1.2 0	＃主机 ip 地址为 1.1.1.1 的 PC 可以 ping 通 1.1.1.2 的 PC，但是不能通过网上邻居查找到 1.1.1.2，反之则可以
[Quidway-acl-adv-3000]int e4/0/1	#进入端口模式
[Quidway-Ethernet4/0/1] packet-filter inbound ip-group 3000 rule 1	＃激活该规则

以 5516 为例：

配置方法	注释
[Quidway]acl number 3000	＃配置三层访问控制规则
[Quidway-acl-adv-3000]rule deny tcp source 1.1.1.3 0 destination 1.1.1.2 0 destination-port eq 139	＃主机 ip 地址为 1.1.1.3 的 PC 可以 ping 通 1.1.1.2 的 PC，但是不能通过网上邻居查找到 1.1.1.2，反之则可以
[Quidway]packet-filter ip-group 3000	＃激活该规则

⚠ 注意：

- 不同网段的单向访问配置类似，请参考上面的配置。

- 单向访问控制一般只能对 PING 和 TCP 报文进行控制，无法对 UDP 报文进行控制。如果要对 UDP 报文进行控制，必须知道 UDP 报文的端口号。

3.9 双向访问控制

1. 功能需求及组网说明

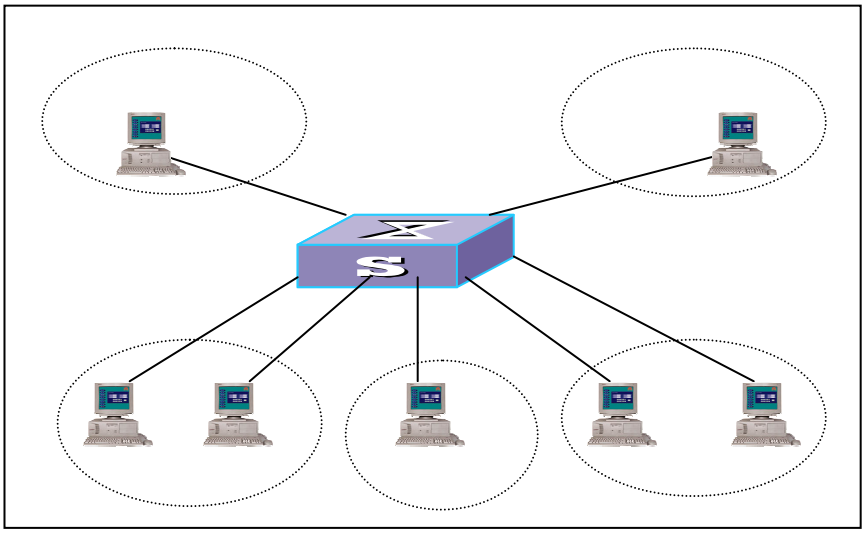


图23 双向访问控制

说明：通过配置三层交换机的 acl 来实现 vlan 之间的访问控制

需求：组网和 vlan 分配如图所示，要求 vlan 10、20、30 均可以访问 server 1，但是只有 vlan 10 和 vlan 20 可以访问 server 2，同时 vlan 10、20、30 之间不能互访。

2. 配置

以 S3526E 为例：

表28 双向访问控制

配置过程	注释
交换机配置： [Switch] vlan 10 [Switch-vlan10] interface Vlan-interface 10 [Switch-Vlan-interface10]ip address 10.10.1.1 255.255.0.0 [Switch] vlan 20 [Switch-vlan20] interface Vlan-interface 20 [Switch-Vlan-interface20]ip address 10.20.1.1 255.255.0.0	 #配置 VLAN 10 #配置 VLAN 10 虚接口 #配置 VLAN 20 #配置 VLAN 20 虚接口

配置过程	注释
[Switch] vlan 30	
[Switch-vlan30] interface Vlan-interface 30	#配置 VLAN 30
[Switch-Vlan-interface30]ip address 10.30.1.1 255.255.0.0	#配置 VLAN 30 虚接口
[Switch] vlan 100	
[Switch-vlan100] interface Vlan-interface 100	#配置 VLAN 100
[Switch-Vlan-interface100]ip address 10.100.1.1 255.255.0.0	#配置 VLAN 100 虚接口
[Switch] vlan 200	
[Switch-vlan200] interface Vlan-interface 200	
[Switch-Vlan-interface200]ip address 10.200.1.1 255.255.0.0	#配置 VLAN 200 #配置 VLAN 200 虚接口
[Switch] acl num 3000	
[Switch-acl-adv-3000]rule deny ip source 10.10.1.1 0.0.255.255 destination 10.20.1.1 0.0.255.255	#配置 acl 访问控制列表禁止网段 10.10.0.0 访问网段 10.20.0.0
[Switch-acl-adv-3000]rule deny ip source 10.10.1.1 0.0.255.255 destination 10.30.1.1 0.0.255.255	#禁止网段 10.10.0.0 访问网段 10.30.0.0
[Switch-acl-adv-3000]rule deny ip source 10.20.1.1 0.0.255.255 destination 10.10.1.1 0.0.255.255	#禁止网段 10.20.0.0 访问网段 10.10.0.0
[Switch-acl-adv-3000]rule deny ip source 10.20.1.1 0.0.255.255 destination 10.30.1.1 0.0.255.255	#禁止网段 10.20.0.0 访问网段 10.30.0.0
[Switch-acl-adv-3000]rule deny ip source 10.30.1.1 0.0.255.255 destination 10.10.1.1 0.0.255.255	#禁止网段 10.30.0.0 访问网段 10.10.0.0
[Switch-acl-adv-3000]rule deny ip source 10.30.1.1 0.0.255.255 destination 10.20.1.1 0.0.255.255	#禁止网段 10.30.0.0 访问网段 10.20.0.0
[Switch-acl-adv-3000]rule deny ip source 10.30.1.1 0.0.255.255 destination 10.200.1.1 0.0.255.255	#禁止网段 10.30.0.0 访问网段 10.200.0.0 #下发访问控制列表
[Switch]packet-filter ip 3000	

以 6506 为例:

配置过程	注释
交换机配置： [Switch] vlan 10 [Switch-vlan10] interface Vlan-interface 10 [Switch-Vlan-interface10]ip address 10.10.1.1 255.255.0.0	 #配置 VLAN 10 #配置 VLAN 10 虚接口
[Switch] vlan 20 [Switch-vlan20] interface Vlan-interface 20 [Switch-Vlan-interface20]ip address 10.20.1.1 255.255.0.0	#配置 VLAN 20 #配置 VLAN 20 虚接口
[Switch] vlan 30 [Switch-vlan30] interface Vlan-interface 30 [Switch-Vlan-interface30]ip address 10.30.1.1 255.255.0.0	#配置 VLAN 30 #配置 VLAN 30 虚接口
[Switch] vlan 100 [Switch-vlan100] interface Vlan-interface 100 [Switch-Vlan-interface100]ip address 10.100.1.1 255.255.0.0	#配置 VLAN 100 #配置 VLAN 100 虚接口
[Switch] vlan 200 [Switch-vlan200] interface Vlan-interface 200 [Switch-Vlan-interface200]ip address 10.200.1.1 255.255.0.0	#配置 VLAN 200 #配置 VLAN 200 虚接口
[Switch] acl num 3000 [Switch-acl-adv-3000]rule 0 deny ip source 10.10.1.1 0.0.255.255 destination 10.20.1.1 0.0.255.255	#配置 acl 访问控制列表禁止网段 10.10.0.0 访问网段 10.20.0.0
[Switch-acl-adv-3000]rule 1 deny ip source 10.10.1.1 0.0.255.255 destination 10.30.1.1 0.0.255.255	
[Switch-acl-adv-3000]rule 2 deny ip source 10.20.1.1 0.0.255.255 destination 10.10.1.1 0.0.255.255	#禁止网段 10.10.0.0 访问网段 10.30.0.0
[Switch-acl-adv-3000]rule 3 deny ip source 10.20.1.1 0.0.255.255 destination 10.30.1.1 0.0.255.255	#禁止网段 10.20.0.0 访问网段 10.10.0.0
[Switch-acl-adv-3000]rule 4 deny ip source 10.30.1.1 0.0.255.255 destination 10.10.1.1 0.0.255.255	#禁止网段 10.20.0.0 访问网段 10.30.0.0
[Switch-acl-adv-3000]rule 5 deny ip source 10.30.1.1 0.0.255.255 destination 10.20.1.1 0.0.255.255	
[Switch-acl-adv-3000]rule 6 deny ip source 10.30.1.1 0.0.255.255 destination 10.200.1.1 0.0.255.255	#禁止网段 10.30.0.0 访问网段 10.10.0.0

配置过程	注释
[Switch]int e4/0/1	#禁止网段 10.30.0.0 访问网段 10.20.0.0
[Switch]packet-filter inbound ip 3000 not-care-for-interface	#禁止网段 10.30.0.0 访问网段 10.200.0.0
	#进入端口模式，（假设图中所有端口与 e4/0/1 在同一个芯片上）
	#下发访问控制列表

以 5516 为例：

配置过程	注释
交换机配置： [Switch] vlan 10 [Switch-vlan10] interface Vlan-interface 10 [Switch-Vlan-interface10]ip address 10.10.1.1 255.255.0.0	 #配置 VLAN 10 #配置 VLAN 10 虚接口
[Switch] vlan 20 [Switch-vlan20] interface Vlan-interface 20 [Switch-Vlan-interface20]ip address 10.20.1.1 255.255.0.0	 #配置 VLAN 20 #配置 VLAN 20 虚接口
[Switch] vlan 30 [Switch-vlan30] interface Vlan-interface 30 [Switch-Vlan-interface30]ip address 10.30.1.1 255.255.0.0	 #配置 VLAN 30 #配置 VLAN 30 虚接口
[Switch] vlan 100 [Switch-vlan100] interface Vlan-interface 100 [Switch-Vlan-interface100]ip address 10.100.1.1 255.255.0.0	 #配置 VLAN 100 #配置 VLAN 100 虚接口
[Switch] vlan 200 [Switch-vlan200] interface Vlan-interface 200 [Switch-Vlan-interface200]ip address 10.200.1.1 255.255.0.0	 #配置 VLAN 200 #配置 VLAN 200 虚接口
[Switch] acl num 3000 [Switch-acl-adv-100]rule deny ip source 10.10.1.1 0.0.255.255 destination 10.20.1.1 0.0.255.255	
[Switch-acl-adv-3000]rule deny ip source 10.10.1.1 0.0.255.255 destination 10.30.1.1 0.0.255.255	#配置 acl 访问控制列表禁止网段 10.10.0.0 访问网段 10.20.0.0

配置过程	注释
[Switch-acl-adv-3000]rule deny ip source 10.20.1.1 0.0.255.255 destination 10.10.1.1 0.0.255.255	
[Switch-acl-adv-3000]rule deny ip source 10.20.1.1 0.0.255.255 destination 10.30.1.1 0.0.255.255	#禁止网段 10.10.0.0 访问网段 10.30.0.0
[Switch-acl-adv-3000]rule deny ip source 10.30.1.1 0.0.255.255 destination 10.10.1.1 0.0.255.255	#禁止网段 10.20.0.0 访问网段 10.10.0.0
[Switch-acl-adv-3000]rule deny ip source 10.30.1.1 0.0.255.255 destination 10.20.1.1 0.0.255.255	#禁止网段 10.20.0.0 访问网段 10.30.0.0
[Switch-acl-adv-3000]rule deny ip source 10.30.1.1 0.0.255.255 destination 10.200.1.1 0.0.255.255	
[Switch]packet-filter ip 3000	#禁止网段 10.30.0.0 访问网段 10.10.0.0
	#禁止网段 10.30.0.0 访问网段 10.20.0.0
	#禁止网段 10.30.0.0 访问网段 10.200.0.0
	#下发访问控制列表

⚠ 注意：

如果是低端交换机同一网段内的双向访问控制，也可以通过端口的 hybrid 属性来实现，具体的内容可以参考第二章关于端口 bybrid 属性的配置部分。

3.10 IP+MAC+端口绑定

1. 功能需求及组网说明

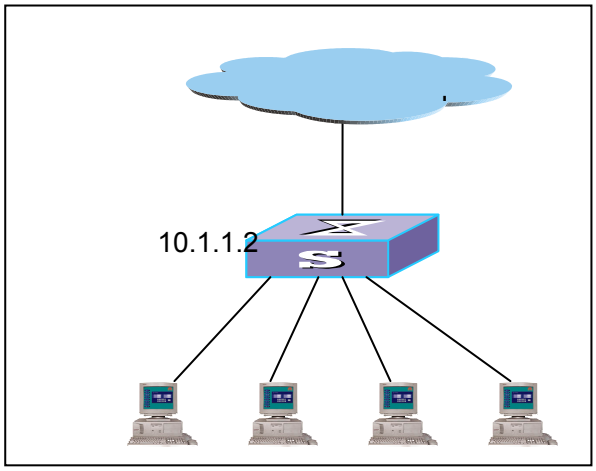


图24 IP 地址绑定

说明：通过对三层交换机进行 ip＋mac＋端口的绑定，实现对合法用户上网的保护，访问恶意用户通过修改地址上网。

需求：对合法的用户进行 ip＋mac＋端口的绑定，防止恶意用户通过更换自己的地址上网的行为。

2. 配置

表29 IP+MAC+端口的绑定

配置过程	注释
配置方法一：采用 DHCP-SECURITY 来实现： [Quidway]mac-address static 00e0-fca0-6500 interface e0/1 vlan 1 [Quidway] dhcp-security static 10.1.1.2 00e0-fca0-6500 [Quidway-Vlan-interface1]dhcp-server 1 [Quidway-Vlan-interface1]address-check enable	#配置端口的静态 MAC 地址 #配置 IP 和 MAC 对应表 #配置 dhcp-server 组号(否则不允许执行下一步，此 dhcp-server 组不用在交换机上创建也可) #使能三层地址检测 #完成此配置即可使 10.1.1.2 这台 pc 只有接到 e0/1 才可以上网
配置方法二：采用 AM 命令来实现 [Quidway]am enable	#使能 AM 功能

配置过程	注释
[Quidway]int e0/1 [Quidway-Ethernet0/1]am ip-pool 10.110.91.129 10	#该端口只允许起始 IP 地址为 10.110.91.129 的 10 IP 地址上网 #上面的配置把 IP 地址和端口绑定起来了，MAC 地址和端口的绑定参照上面的配置。IP 和 MAC 的绑定可以通过静态 ARP 来实现。

配置方法三：

[Quidway]am user-bind ip-addr 1.1.1.1 mac-addr 00-00-01 interface Ethernet 0/1 将端口和 ip、mac 捆绑。

或者：

[Quidway]am user-bind ip-addr 1.1.1.1 interface Ethernet 0/1 将端口与 ip 捆绑。

也可以：

[Quidway]am user-bind mac-addr 00-00-10 interface Ethernet 0/1 将 mac 和端口捆绑。

⚠ 注意：

- 该配置以 3526-0021 版本为例
- 三层交换机中目前只有 S3526/3526E 系列支持使用 AM 命令来进行 IP 地址和端口的绑定。并且如果 S3526 系列交换机要采用 AM 命令来实现绑定功能，则交换机必须是做三层转发（即用户的网关应该在该交换机上）。
- 用配置方法三来实现捆绑支持的设备为 3026EFGTC/ 3526EFGTC /3050/以最新版本为例。

不支持同时对一个端口做“PORT+IP+MAC”和“PORT+IP”绑定

3.11 各种接入控制的配置

1. 功能需求及组网说明

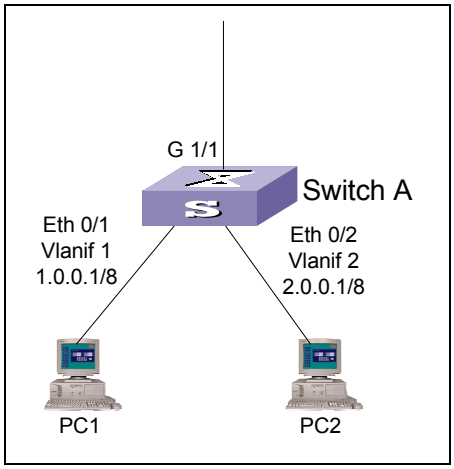


图25 各种接入控制的配置

说明：如图，三层交换机 SwitchA 有两个端口 ethetnet 0/1、ethernet 0/2 分别属于 vlan 1、vlan 2，vlan 1、vlan 2 的三层接口地址分别是 1.0.0.1/8、2.0.0.1/8，上行口 G 1/1 是 trunk 端口，并允许 vlan 3 通过。

需求：

(1) 静态 mac、端口捆绑：端口 ethetnet 0/1 仅仅允许 pc1（mac：0.0.1）接入。
(2) 动态 mac、端口捆绑：端口 ethetnet 0/1 仅仅允许一个主机（任何 mac 地址）接入。
(3) ip、端口捆绑：端口 ethetnet 0/1 仅仅允许 ip 地址为（ip：1.0.0.2）的主机接入
(4) ip、mac 捆绑：vlan 1 下的主机 pc1（mac：0.0.1）必须使用 ip 地址（ip：1.0.0.2）才可以通过交换机。
(5) mac、ip、端口捆绑：端口 ethetnet 0/1 仅仅允许 mac 地址为（mac：0.0.1）而且 ip 地址为（ip：1.0.0.2）的主机接入。

2. 配置

表30 接入控制配置

配置过程	注释
需求 1： [Quidway]acl num 4000 [Quidway-acl-link-4000]rule deny ingress any egress any [Quidway-acl-link-4000]rule permit ingress 00-00-01 00-00-00 interface Ethernet 0/1 egress any [Quidway-acl-link-4000]quit	#静态 mac、端口捆绑 #命令举例以 S3526E 为例。 #这里必须严格 rule 规则的顺序，否则不生效。 #3528/3552 在端口下发

配置过程	注释
[Quidway]packet-filter link-group 4000	
需求 2： [Quidway-Ethernet0/2]mac-address max-mac-count 1	#动态 mac、端口捆绑
需求 3： [Quidway]acl number 2000 [Quidway-acl-basic-2000]rule permit source 1.0.0.2 0 [Quidway-acl-basic-2000]quit [Quidway]acl num 4000 [Quidway-acl-link-4000] rule 0 deny ingress interface Ethernet 0/1 egress any [Quidway-acl-link-4000]rule 1 permit ingress interface e0/1 egress any [Quidway-acl-link-4000]quit [Quidway]packet-filter ip-group 2000 rule 0 link-group 4000 rule 0 [Quidway]packet-filter ip-group 2000 rule 1 link-group 4000 rule 1	#ip、端口捆绑 注：这是用 QACL 命令实现的，该功能在 S3526 系列交换机上可以使用用静态 dhcp 和 am 命令分别实现，也具体情况请参考上面的内容。
需求 4： [Quidway]acl number 2000 [Quidway-acl-basic-2000]rule 0 permit source 1.0.0.2 0 [Quidway-acl-basic-2000]quit [Quidway]acl number 4000 [Quidway-acl-link-4000]rule 1 permit ingress 1 0000-0000-0001 0000-0000-0000 egress any [Quidway-acl-link-4000]rule 0 deny ingress 1 0000-0000-0001 0000-0000-0000 egress any [Quidway-acl-link-4000]quit [Quidway]packet-filter ip-group 2000 rule 0 link-group 4000 rule 1 [Quidway]packet-filter link-group 4000 rule 0	#ip、mac 捆绑 #命令举例以 S3526E 为例。
需求 5： [Quidway]acl number 2000 [Quidway-acl-basic-2000]rule 0 permit source 1.0.0.2 0 [Quidway-acl-basic-2000]quit [Quidway]acl number 4000 [Quidway-acl-link-4000]rule 0 deny ingress interface Ethernet0/1 egress any [Quidway-acl-link-4000]rule 1 permit ingress 1 0000-0000-0001 0000-0000-0000 egress any [Quidway-acl-link-4000]quit [Quidway]packet-filter link-group 4000 rule 0 [Quidway]packet-filter ip-group 2000 rule 0 link-group 4000 rule 1	#命令举例以 S3526E 为例。

3.12 基于端口限速的配置

1. 功能需求及组网说明

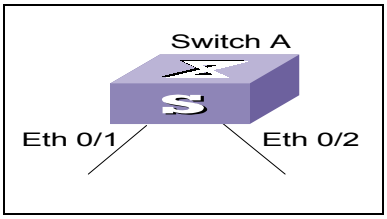


图26 端口限速配置

说明：如图，交换机 SwitchA 有两个端口 ethetnet 0/1、ethernet 0/2。

需求：

(1) 对进入 ethetnet 0/1 的流量做限速；
(2) 对从 ethernet 0/2 出的流量做限制（流量的粒度与产品有关）。

2. 配置

表31 端口限速配置

配置过程	注释
需求 1： [Quidway]acl num 4000 [Quidway-acl-link-4000]rule 0 permit ingress any egress any [Quidway-acl-link-4000]quit [Quidway]interface e0/1 [Quidway-Ethernet0/1]traffic-limit inbound link-group 4000 8 需求 2： [Quidway-Ethernet0/1]interface e0/2 [Quidway-Ethernet0/2]line-rate 8	#命令举例以 S3526E 为例。 该例对 6506 也适用，还可以使用 outbound 对出端口做限制

以 5516 为例：

配置过程	注释
需求 1： [Quidway]acl num 4000 [Quidway-acl-link-4000]rule permit ingress int e0/1 egress any [Quidway-acl-link-4000]quit [Quidway]interface eth 0/1	#需求：对从 ethernet 0/1 进入的流量做限制 1M #进入 acl 配置模式配置规则 #退出 acl 配置模式 #下发流量限制

配置过程	注释
[Quidway-Ethernet0/1]traffic-limit link-group 4000 1024	
需求 2： [Quidway]acl num 4000 [Quidway-acl-link-4000]rule permit ingress any egress int e0/2 [Quidway-acl-link-4000]quit [Quidway]interface eth 0/1 Quidway-Ethernet0/1]traffic-limit link-group 4000 1024	需求：对从 ethernet 0/2 出去的流量做限制 1M #进入 acl 配置模式配置规则 #退出 acl 配置模式 #下发流量限制

2000-EI 端口限速：

[Quidway-Ethernet0/1]line-rate inbound <1-127>

[Quidway-Ethernet0/1]line-rate outbound <1-127>

S2000/3000-SI 的出入端口限速：

[Quidway-Ethernet0/1]line-rate inbound <1-8>

[Quidway-Ethernet0/1]line-rate outbound <1-8>

3528/3552 出端口限速：

[Quidway-Ethernet0/1]traffic－shap 650（该参数为各位要配置的参数） 4 256

3528/3552 入端口限速：

[Quidway]acl num 4000

[Quidway-acl-link-4000]rule 0 permit ingress any egress any

[Quidway-Ethernet0/1] traffic-limit inbound link 4000 1000 125000 125000 1000

注意：目前低端交换机中只有 S3X00E 和 S3050 系列交换机支持端口限速，S3X00E 和 S3050 百兆口的粒度为 1M，千兆口的粒度为 8M。

对于 2000-EI：报文速率限制级别取值为 1～127。如果速率限制级别取值在 1～28 范围内，则速率限制的粒度为 64Kbps，这种情况下，如果用户设置的级别为 N，则端口上限制的速率大小为 N*64K；如果速率限制级别取值在 29～127 范围内，则速率限制的粒度为 1Mbps，这种情况下，如果用户设置的级别为 N，则端口上限制的速率大小为(N-27)*1Mbps。

对于 S2000/3000-SI 系列交换机：target-rate：对端口发送或接收报文限制的总速率，这里以 8 个级别来表示，取值范围为 1～8，含义为：端口工作在 10M 速率时，

1～8 分别表示 312K，625K，938K，1.25M，2M，4M，6M，8M；端口工作在 100M 速率时，1～8 分别表示 3.12M，6.25M，9.38M，12.5M，20M，40M，60M，80M。

3552/3528【参数配置说明】

在配置 CBS　EBS 参数时，建议 CBS=EBS=(CIR /8 KBYTES）×(1～1.5)

如配置 cir＝1000Kbites/S，则 CBS=EBS=（1000/8)*1～1.5 =(125～180)Kbytes，注意在命令行上该参数的单位为 bytes。CBS EBS 的最大值则参考命令行提示。

如果未按照该建议配置，则会出现限速不准确的现象。

另外，如果配置 pir 参数，建议 pir=cir,此为双速率，实测的限速值等于配置的限速值。如果没有配置 pir 参数，则为单速率，实测的限速值为配置的限速值的二倍。

3.13 基于流限速的配置

1. 功能需求及组网说明

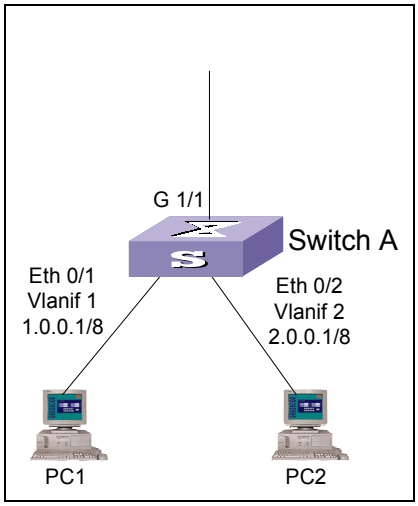


图27 基于流限速的配置

说明：如图，三层交换机 SwitchA 有两个端口 ethetnet 0/1、ethernet 0/2 分别属于 vlan 1、vlan 2，vlan 1、vlan 2 的三层接口地址分别是 1.0.0.1/8、2.0.0.1/8，上行口 G 1/1 是 trunk 端口，并允许 vlan 3 通过。

需求：

- 对位于 ethetnet 0/1 下的 pc1（mac：0.0.1）进入端口的流量做限速。
- 对位于 ethetnet 0/1 下的 pc1（mac：0.0.1）访问本 vlan 的流量做限速。
- 对位于 ethetnet 0/2 下的 pc2（ip：2.0.0.2）进入端口的流量做限速。
- 对 pc1 到 pc2 的流量做限速。
- 在上行口对 vlan 3 外出的流量做限速。

2. 配置

表32 基于流的限速配置

配置过程	注释
需求 1： [Quidway]acl num 4000 [Quidway-acl-link-4000]rule 0 permit ingress 0.0.1 0-0-0 egress any [Quidway-acl-link-4000]quit [Quidway]interface e0/1 [Quidway-Ethernet0/1]traffic-limit inbound link-group 4000 8	#命令举例以 S3526E 为例。
需求 2： [Quidway]acl num 4000 [Quidway-acl-link-4000]rule 0 permit ingress 0.0.1 egress 1 [Quidway-acl-link-4000]quit [Quidway]interface e3/0/1 [Quidway-Ethernet3/0/1]traffic-limit inbound link-group 4000 20480	#命令举例以 S6506 为例。S3526E 不支持目的 vlan，而 S6506、S5516 支持。 #假设 FE 在 3 槽位
需求 3： [Quidway]acl num 4000 [Quidway-acl-link-4000]rule 0 permit ingress 0.0.2 0-0-0 egress any [Quidway-acl-link-4000]quit [Quidway]interface e0/2 [Quidway-Ethernet0/2]traffic-limit inbound link-group 4000 6	#命令举例以 S3526E 为例。
需求 4： [Quidway]acl num 4000 [Quidway-acl-link-4000]rule 0 permit ingress interface e0/1 egress interface e0/2 [Quidway-acl-link-4000]quit [Quidway]interface e0/1 [Quidway-Ethernet0/1]traffic-limit inbound link-group 4000 6	#命令举例以 S3526E 为例。
需求 5： [Quidway]acl num 4000 [Quidway-acl-link-200]rule 0 permit ingress 3 egress any [Quidway-acl-link-4000]quit [Quidway]interface e3/0/3 [Quidway-Ethernet3/0/3]traffic-limit outbound link-group 4000 20480	#命令举例以 S6506 为例。S3526E 不支持出限速，而 S6506 支持。 #假设 FE 板在 3 槽位

以 5516 为例：

配置过程	注释
需求 1： [Quidway]acl num 3000 [Quidway-acl-adv-100]rule p ip source 1.0.0.1 0.255.255.255 destination 2.0.0.2 0.255.255.255 [Quidway-acl-adv-3000]quit [Quidway] [Quidway]traffic-l ip 1024	#该需求对 pc1 到 pc2 的流量做限速(1M) #配置流从 1.0.0.2 到 2.0.0.2 #退出到系统模式 #下发带宽管理配置

3.14 其他流动作的配置

1. 功能需求及组网说明

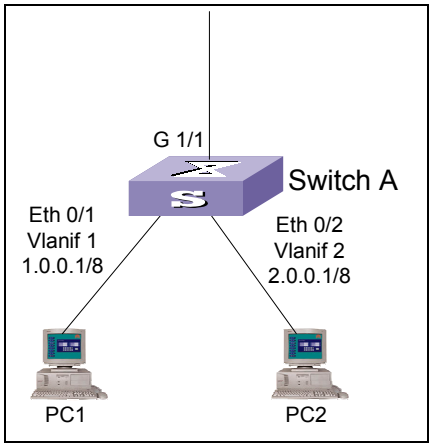


图28 各种流动作的配置

说明：如图，三层交换机 SwitchA 有两个端口 ethetnet 0/1、ethernet 0/2 分别属于 vlan 1、vlan 2，vlan 1、vlan 2 的三层接口地址分别是 1.0.0.1/8、2.0.0.1/8，上行口 G 1/1 是 trunk 端口，并允许 vlan 3 通过。

需求：

- 访问控制：允许位于 ethetnet 0/1 下的 pc1（ip：1.0.0.2）进入端口的流量，拒绝 pc3（ip：1.0.0.3）的流量通过端口进入交换机。
- 带宽保证：保证位于 ethetnet 0/1 下的主机（ip 网段：1.0.0.0/8）在上行口端口有 70mbps 带宽。
- 拥塞避免：位于 ethetnet 0/1 下的主机（ip 网段：1.0.0.0/8）在上行口端口有 70mbps 带宽，当流量超过时，为了避免同步丢失，启用 RED。

- 优先级标记：对源于 pc1（ip：1.0.0.2）的报文打上 ef 标记，并在上行口启用 diff 以保证 pc1 发出的流量得到相应的服务登记。
- 队列调度：当上行口发生拥塞时，保证 pc2（ip：2.0.0.2）发出的报文得到优先转发。
- 流量统计：对主机 pc1（ip：1.0.0.2）进入端口的流量进行统计，以作为计费依据。
- 流重定向：将 pc1 到 pc2 的报文重定向到 cpu。

2. 配置

以 S3526E 为例：

表33 其他流动作的配置

配置过程	注释
需求 1：	#该配置请参考本章第八部分，此处不再重复。
需求 2：	#S3526E 能实现基于流的随即丢弃
需求 3：	#S3526E 不能实现基于流的随即丢弃
需求 4： [Quidway]acl num 2000 [Quidway-acl-basic-2000]rule 0 permit source 1.0.0.2 0 [Quidway-acl-basic-2000]quit [Quidway]traffic-priority ip-group 2000 dscp ef	
需求 5： [Quidway]acl num 2000 [Quidway-acl-basic-2000]rule 0 permit source 1.0.0.2 0 [Quidway-acl-basic-2000]quit [Quidway]traffic-priority ip-group 2000 local-precedence 7 [Quidway] queue-scheduler strict-priority	
需求 6： [Quidway]acl num 2000 [Quidway-acl-basic-1]rule 0 permit source 1.0.0.2 0 [Quidway-acl-basic-2000quit [Quidway]acl num 4000 [Quidway-acl-link-4000]rule 0 permit ingress interface e0/1 egress any [Quidway-acl-link-4000]quit [Quidway]traffic-statistic ip-group 2000 link-group 4000 rule 0	
需求 7：	

配置过程	注释
[Quidway]acl num 4000 [Quidway-acl-link-4000]rule 0 permit ingress interface e0/1 egress interface e0/2 [Quidway-acl-link-4000]quit [Quidway] traffic-redirect link-group 4000 cpu	

以 6506 为例:

配置过程	注释
需求 1： [Quidway]acl num 2000 [Quidway-acl-basic-2000]rule 0 permit source 1.0.0.2 0 [Quidway-acl-basic-2000]rule 1 deny source 1.0.0.3 0 [Quidway]int e1/0/1 [Quidway-Ethernet1/0/1]packet-filter ip-group 2000 rule 0 [Quidway-Ethernet1/0/1]packet-filter ip-group 2000 rule 1	
需求 2： [Quidway]acl num 2000 [Quidway-acl-basic-1]rule 0 permit source 1.0.0.2 0.255.255.255 [Quidway-acl-basic-2000]quit [Quidway]inter e1/0/1 [Quidway-Ethernet1/0/1]traffic-bandwidtch outbound ip-group 2000 rule 71680 102400 100	
需求 3： [Quidway]acl num 2000 [Quidway-acl-basic-2000]rule 0 permit source 1.0.0.2 0.255.255.255 [Quidway-acl-basic-2000]quit [Quidway]inter e1/0/1 [Quidway-Ethernet1/0/1]traffic-red outbound ip-group 2000 rule 0 64 128 80	
需求 4： [Quidway]acl num 2000 [Quidway-acl-basic-2000]rule 0 permit source 1.0.0.2 0 [Quidway-acl-basic-2000]quit [Quidway]inter e1/0/1 [Quidway-Ethernet1/0/1]traffic-priority ip-group outbound 2000 rule 0 dscp ef	
需求 6： [Quidway]acl num 2000 [Quidway-acl-basic-2000]rule 0 permit source 1.0.0.2 0	

配置过程	注释
[Quidway-acl-basic-2000]quit [Quidway]int e1/0/1 [Quidway-Ethernet1/0/1]traffic-statistic ip-group 2000 rule 0	
需求 7：	此需求 6506 不支持

以 5516 为例：

配置过程	注释
需求 1：访问控制 [Quidway]acl num 3000 [Quidway-acl-adv-3000]rule permit ip source 1.0.0.2 0 [Quidway-acl-adv-3000]rule deny ip destination 1.0.0.3 0 [Quidway-acl-adv-3000]quit [Quidway]packet-filter ip-group 3000	#进入 acl 配置模式 #允许 pc1（ip：1.0.0.2）进入端口的流量 #拒绝 pc3（ip：1.0.0.3）的流量 #退出到系统模式 #下发配置
需求 2：队列调度 [Quidway]acl num 3000 [Quidway-acl-adv-3000]rule p ip source 1.0.0.2 0 [Quidway-acl-adv-3000]q [Quidway]traffic-pri ip 3000	进入 acl 配置模式 允许 pc1（ip：1.0.0.2）进入端口的流量 退出到系统模式 下发配置
需求 3：队列调度 [Quidway]acl num 3000 [Quidway-acl-adv-3000]rule p ip source 1.0.0.2 0 [Quidway-acl-adv-3000]q [Quidway]traffic-sta ip 3000	进入 acl 配置模式 允许 pc1（ip：1.0.0.2）进入端口的流量 退出到系统模式 下发配置
需求 4：优先级标记 [Quidway]acl nu 3000 [Quidway-acl-adv-3000]rule p ip source 1.0.0.2 0 dscp ef [Quidway-acl-adv-3000]q	进入 acl 配置模式 允许 pc1（ip：1.0.0.2）进入端口的流量并将报文打上 ef 标记 退出到系统模式

配置过程	注释
[Quidway] pa ip 3000	下发配置