S 系列框式交换机
常见配置命令指导

2019 年 11 月

Sundray TAC

信锐技术

文档密级：渠道合作伙伴

目录

1 Console 登录设备配置---------- 1
1.1 登录注意事项---------- 1
1.2 配置思路---------- 1
1.3 操作步骤---------- 1
2 基础配置命令---------- 3
2.1 基本操作命令---------- 3
2.2 用户名密码设置---------- 3
2.3 仅允许单个用户在 config 模式下---------- 4
2.4 查看光衰---------- 5
2.5 查看板卡---------- 6
3 常见配置命令---------- 7
3.1 管理 IP 配置---------- 7
3.2 telnet 配置---------- 7
3.3 SSH 配置---------- 8
3.4 VLAN 配置---------- 9
3.5 DHCP 服务相关配置---------- 10
3.6 链路聚合配置---------- 11
3.7 端口镜像---------- 12
3.8 虚拟化配置（堆叠）---------- 13
3.9 ACL 配置---------- 15
3.10 VRRP 配置---------- 17
3.11 生成树协议---------- 18
4 路由配置命令---------- 21
4.1 静态路由配置---------- 21

4.2 策略路由配置----------21
4.3 动态路由协议-RIP 配置----------24

1 Console 登录设备配置

通过 Console 口登录交换机是指使用专门的 Console 通信线缆将用户 PC 的串口与交换机的 Console 口相连，在该方式是登录交换机的最基本方式，也是其他登录方式（如：Telnet、STelnet）的基础，适用于首次登录交换机或无法远程登录交换机的场景。

准备好 Console 通信线缆。如果用户 PC 是笔记本电脑或者没有串口的电脑，还需要准备 USB 转串口的转接线，并按照说明书安装好随线光盘的驱动。

1.1 登录注意事项

准备好 PC 终端仿真软件。Windows 2000 系统的 PC 自带超级终端，可无需另行准备终端仿真软件。对于不自带终端仿真软件的系统，请您准备好 PC 终端仿真软件。

1.2 配置思路

采用如下思路配置通过 Console 口登录交换机：

1.配置终端仿真软件，设置连接接口及通信参数，登录交换机。

2.配置交换机的基本信息，包括日期、时间、时区及名称，以方便管理。

3.配置 Console 用户界面的认证方式，实现下次通过 Console 口登录交换机时需要本地认证。

4.配置管理 IP 地址和 Telnet 功能，便于后续对交换机进行远程维护。

1.3 操作步骤

1、将 Console 通信电缆的 DB9（孔）插头插入 PC 机的串口（COM）中，再将 RJ-45 插头端插入设备的 Console 口中；

2、配置终端仿真软件并登录交换机

在 PC 上打开终端仿真软件（以 MobaXterm、CRT 等），新建连接，设置连接的接口以及通信参数与交换机 Console 口缺省配置相同。

3、设置连接的接口及通信参数

初始配置时，需要用出厂附带的 console 线来连接配置（线序与普通 console 线线序不一样，如未用出厂附带的 console 线，会出现无任何输出的情况）

- 传输速率（speed）：9600
- 数据位（Data bits）：8
- 校验方式（Parity）：无
- 停止位（Stop bits）：1
- 流控方式（Flow control）：无

4、配置完成后，即可进入命令行配置

2 基础配置命令

2.1 基本操作命令

Switch>　　//通过 console 或远程登录进入交换机，按 enter 键进入用户模式

Switch>enable　　//通过 enable 命令进入管理模式

Switch#config　　//通过 config 命令进入配置模式

Switch_config#exit

Switch#　　//通过 exit 命令可以退出至上级模式

Switch_config#hostname Sundray_Switch　　//hostname 命令为交换机命名

Sundray_Switch_config#date

当前日期是 1970 年 1 月 7 日 10 时:7 分:58 秒

请输入新的日期(yyyy-mm-dd):2019-10-19

请输入新的时间(hh:mm:ss):10:14:30　　//data 命令配置设备时间

Sundray_Switch_config#english　　//修改交换机管理语言支持英文

Sundray_Switch_config#chinese　　//修改交换机管理语言支持中文

2.2 用户名密码设置

Sundray_Switch_config#username admin password 0 admin　　//配置本地用户及密码，0 为显示不加密，7 为显示加密

Sundray_Switch_config#enable password 0 admin level 1

Sundray_Switch_config#enable password 0 admin level 15　　//配置进入管理模式密码及权限，0 为显示不加密，7 为显示加密，level 代表特权级别（1-15）

2.3 仅允许单个用户在 config 模式下

设备仅允许单个用户在 config 模式下，当 config 下有用户登录时，config 命令无法进入全局模式，需要进行清除。

Sundray_Switch#config

Only 1 vty is permitted to enter config mode.　　//设备仅允许一个用户在配置模式下

console 0 is in configuring　　//目前串口 0 用户正在配置模式下

Sundray_Switch#clear line console 0　//通过命令清除当前通过串口登录在配置模式下的用户

Line 0 cleared　　//用户清除成功

Sundray_Switch#clear telnet 1　　//通过命令清除当前通过 telnet 登录在配置模式下的用户

Sundray_Switch#show telnet　　//查看当前通过 telnet 登录进去在配置模式下的用户信息

NO.　　Remote Addr　　Remote Port　　Local Addr　　Local Port

1　　172.16.196.185　　55100　　10.156.98.200　　23

2　　172.16.196.169　　59427　　10.156.98.200　　23

Sundray_Switch#show line console 0　　//查看当前通过 console 登录进去在配置模式下的用户信息

No. Type Len Width Terminal Remote-address　Interface

0　CTY　24　　80　　ANSI　　-　　-

2.4 查看光衰

Switch_config#ddm enable //开启查看光衰功能，**查看完后一定要关闭**，关闭命令：no ddm enable

Switch_config#show interface gigaEthernet 8/1 //查看接口信息，DDM info 为光衰信息

```
GigaEthernet8/1 is up, line protocol is up
  Ifindex is 78, unique port number is 1
  Hardware is Giga-FX-SFP, address is fcfa.f7f1.5b78 (bia fcfa.f7f1.5b78)
  MTU 1500 bytes, BW 1000000 kbit, DLY 10 usec
  Encapsulation ARPA
  Full-duplex,  Auto-Speed(1000Mb/s),  Flow-Control Off
  Transceiver Info:
    SFP,LC,1310nm,1000BASE-FX,SM 10KM            //光模块信息
   DDM:YES,vend name:OEM
  DDM info:
    TX power:-5.92 dBM, RX power:-5.75 dBM            //光衰信息
    SFP temperature:29.42 C,supply voltage :3.38V,Bias Current.:19.40mA
   5 minutes input rate 0 bits/sec, 0 packets/sec
  5 minutes output rate 513458973 bits/sec, 68054 packets/sec
  Real time input rate 0 bits/sec, 0 packets/sec
  Real time output rate 525233103 bits/sec, 69345 packets/sec
      Received 114815111401 packets, 21761914985401 bytes
      20466722514 broadcasts, 6146472414 multicasts
      8207556 discard, 0 error, 0 PAUSE
      0 align, 0 FCS, 0 symbol
      0 jabber, 0 oversize, 0 undersize
      0 carriersense, 0 collision, 0 fragment
      0 L3 packets, 0 discards, 0 Header errors
      Transmitted 73942011684 packets, 45548939322262 bytes
```

37079494 broadcasts, 722762024 multicasts

1 discard, 0 error, 0 PAUSE

0 sqettest, 0 deferred, 0 oversize

0 single, 0 multiple, 0 excessive, 0 late

0 L3 forwards

2.5 查看板卡

Sundray_Switch_config#show oir-information //查看业务板卡信息命令

Slot 1 type S75-LC-24GT-V3(present) //1 号板卡型号，present 为在线

Sundray_Switch_config#oir disable slot 1 //关闭 1 号业务板卡

3 常见配置命令

3.1 管理 IP 配置

Sundray_Switch#config //config 命令进入全局模式

Sundray_Switch_config#interface vlan 1 //进入到 VLAN 1 接口下

Sundray_Switch_config_v1#ip address 10.156.98.200 255.254.0.0 //配置 vlan 1 接口 ip 地址

3.2 telnet 配置

开启 telnet，使用本地用户数据库鉴别用户身份。

switch_config#aaa authentication login admin local //创建认证方法列表，配置名为 admin 的认证方法列表

switch_config#aaa authentication enable default none //配置进入用户管理模式（enable）是否需要认证，可选配置

enable --使用 enable 密码进行认证

group --使用服务器组进行认证

line --使用 line 密码进行认证

none --不需要 AAA 服务）

switch_config#aaa authorization exec default local //定义了 exec 授权的默认方法列表，该方法列表自动运用于所有需要进入 EXEC shell 的用户，可选配置，详细可参考配置手册

switch_config#line vty 0 4

switch_config_line#login authentication admin //进入 vty 线路，设置本地用户认证

switch_config#username admin password admin　//创建本地用户

Switch_config#enable password admin　//创建 enable 密码

3.3 SSH 配置

配置只允许 IP 为 192.168.246.117 的主机访问 ssh server，使用本地用户数据库鉴别用户身份。

switch_config#aaa authentication login auth-ssh local　//创建认证方法列表，配置名为 auth-ssh

switch_config#ip sshd auth-method auth-ssh　//将 auth-ssh 的认证方法列表应用于 ssh server

switch_config#aaa authentication enable default none　//配置进入用户管理模式（enable）是否需要认证，可选配置，默认可选（enable 使用 enable 密码进行认证，group 使用服务器组进行认证，line 使用 line 密码进行认证，none 不需要 AAA 服务）

switch_config#aaa authorization exec default local　//定义了 exec 授权的默认方法列表，该方法列表自动运用于所有需要进入 EXEC shell 的用户，可选配置，详细可参考配置手册

switch_config#ip access-list standard ssh-accesslist

switch_config_std#permit 192.168.246.117

switch_config#ip sshd access-class ssh-accesslist　//配置一个名为 ssh-accesslist 的访问控制列表，并将其应用于 sshserver

switch_config#ip sshd enable　//开启 ssh 功能

switch_config#username admin password admin　//创建本地用户

Switch_config#enable password admin　//创建 enable 密码

3.4 VLAN 配置

switch_config#vlan 10　　//创建 vlan 10

switch_config#vlan 10-100　//创建 vlan 10-100

- **access 接口配置**

Switch_config#interface GigaEthernet1/6

Switch_config_tg1/6#switchport mode access

Switch_config_tg1/6#switchport pvid 20　　//进入 GigaEthernet1/6 配置为 access 口划到 vlan20

- **trunk 接口配置**

Switch_config#interface GigaEthernet1/5

Switch_config_tg1/5#switchport mode trunk

Switch_config_tg1/5#switchport pvid 10

Switch_config_tg1/5#switchport trunk vlan-allowed 1-100　//进入 GigaEthernet1/5 配置为 trunk 口，pvid10，允许 vlan1-100 通过

- **hybrid 接口口**

将接口 TGigaEthernet1/4 配置为 trunk 口，pvid10，允许 vlan1-100 通过，其中 VLAN 1-10 不打标签通过：

Switch_config# interface TGigaEthernet1/4

Switch_config_tg1/4# switchport mode trunk

Switch_config_tg1/4# switchport pvid 10

Switch_config_tg1/4# switchport trunk vlan-allowed 1-100

Switch_config_tg1/4# switchport trunk vlan-untagged 1-10

3.5 DHCP 服务相关配置

Switch_config#ip dhcpd enable //打开 DHCP 服务

Switch_config#ip dhcpd pool vlan100 //添加 DHCP 地址池

Switch_config_dhcp#network 100.1.1.0 255.255.255.0 //配置用于自动分配的地址池的网络地址

Switch_config_dhcp#range 100.1.1.100 100.1.1.150 //配置用于自动分配的地址池范围

Switch_config_dhcp#default-router 100.1.1.1 //配置给客户端分配的网关地址

Switch_config_dhcp#dns-server 114.114.114.114 //配置给 DNS 地址

Switch_config_dhcp#lease 1 12 0 //配置租期

Switch#show ip dhcpd statistic //显示 DHCP 的统计信息，包括各类报文的数量和自动分配、手动分配的地址数 。

- **核心配置中继服务器**

Switch_config#int vlan100 //进入对应 vlan

Switch_config_v100#ip helper-address 100.1.1.253 //配置 dhcp 服务器或中继服务器地址

- **dhcp snooping 配置**

DHCP-snooping 的任务就是对 DHCP 报文进行判断，防止伪造的 DHCP 服务器提供 DHCP 服务，维护接口上 MAC 地址与 IP 地址的对应绑定关系。

从信任端口接收的 DHCP 报文无需校验即可转发。典型的设置是将信任端口连接 DHCP 服务器或者 DHCP relay 代理。非信任端口连接 DHCP 客户端，交换机将转发从非信任端口接收的 DHCP 请求报文，不转发从非信任端口接收的 DHCP 回应报文。如果从非信任端口接收 DHCP 回应报文，进行丢弃 DHCP 回应报文。

示例：

Switch_config#ip dhcp-relay snooping //全局开启 dhcp snooping 功能

Switch_config#int gigaEthernet 1/24 //进入连接 dhcp 服务器接口

Switch_config_g7/6#dhcp snooping trust //将该接口配置为信任端口

3.6 链路聚合配置

端口链路聚合是将几个具有相同属性的端口捆绑为一个逻辑端口，而这个捆绑过程可以通过 Lacp 协商，也可以不用通过协商而强制的捆绑到一起。

如果使用 static 静态聚合，要保证捆绑的端口的属性是相同的，即同为全双工，相同的速度，同时还要保证捆绑的端口的连接都是点对点连接，并且点对点连接的对端端口同样是捆绑在一个逻辑端口。

配置端口聚合时，可选择 LACP 协商模式，在 Active 模式下，端口将会主动的发送 LACP 报文，进行 LACP 协商；在 Passive 模式下，端口只会被动的响应 LACP 报文，被动的进行 LACP 协商。

示例：

TGigaEthernet1/6 和 TGigaEthernet1/7 接口做链路聚合，使用 lacp 主动模式：

Switch_config#interface port-aggregator 3 //创建聚合口，接口号取值范围 1-32

Switch_config#interface range TGigaEthernet1/6-7 //同时进入 6、7 两个接口

Switch_config_if_range#aggregator-group 3 mode lacp active //使用 lacp 主动模式

Switch_config#interface port-aggregator 3

Switch_config_p3#aggregator-group load-balance both-mac //支持目的 MAC 地址、源 MAC 地址、源 MAC 与目的 MAC 地址、目的 IP 地址、源 IP 地址，源 IP 地址与目的 IP 地址、源端口这 7 种方式做负载分担

TGigaEthernet1/8 和 TGigaEthernet1/9 接口做链路聚合，使用静态模式：

Switch_config#interface port-aggregator 1 //创建聚合口，接口号取值范围 1-32

Switch_config#interface range TGigaEthernet1/8-9 //同时进入 8、9 两个接口

Switch_config_if_range#aggregator-group 1 mode static //使用静态模式

Switch_config#interface port-aggregator 1

Switch_config_p1#aggregator-group load-balance both-mac //支持目的 MAC 地址、源 MAC 地址、源 MAC 与目的 MAC 地址、目的 IP 地址、源 IP 地址，源 IP 地址与目的 IP 地址、源端口这 7 种方式做负载分担

通过 show aggregator-group [id] {detail|brief|summary}　　//查看详细的聚合信息。

3.7 端口镜像

为了方便对交换机进行管理，可以通过配置端口镜像，使用交换机某一个端口来对流经一组端口的流量进行观察。

示例：

Switch_config# mirror session 1 source interface g1/24 both　　//选择 g1/24 作为源端口，可选择该接口下的入方向、出方向或双向的流量(both 为双向，rx 监控接收流量，tx 监控发送流量）

Switch_config# mirror session 1 destination interface g1/2　　//选择 g1/2 作为目的端口

Switch_config# mirror session 1 source interface g1/20,g1/21 both　　//选择 g1/20、g1/21 作为源端口，可选择该接口下的入方向、出方向或双向的流量(both 为双向，rx 监控接收流量，tx 监控发送流量）

Switch_config# mirror session 1 destination interface g1/2　　//选择 g1/2 作为目的端口

Switch#show mirror　　//查看镜像状态

Sundray_Switch_config#show mirror session 1　　//查看镜像会话 1 的状态

Session 1

Destination Ports: g1/23

Source Ports:

RX Only:　　None

TX Only:　　None

Both:　　g1/20 g1/21

3.8 虚拟化配置（堆叠）

虚拟化技术是一种集中管理的端口扩展技术。用户可以把启用虚拟化功能的交换机，利用虚拟化线卡及连接线把它们连接在一起构成虚拟设备。

示例：

- A 机器

Switch#

Switch#config //进入全局模式

Switch#_config#bvss //进入虚拟化配置模块

Switch#_config_bvss#bvss enable //开启虚拟化功能

Switch#_config_bvss#bvss mode normal //模式选择正常（2 台用正常模式，2 台以上用 enhanced）

Switch#_config_bvss#bvss domain-id 100 //创建虚拟化域 100（随便数字，2 台一致即可）

Switch#_config_bvss#bvss member-id 1 //虚拟化域里面的 1 号成员(另一台写 2 就行)

Switch#_config_bvss#bvss priority 100 //交换机的优先级（优先级高的为 master）

Switch#_config_bvss#bvss slot 7 //指定第几块板卡为堆叠板卡（堆叠版卡装在哪里就写几就行，如该项目堆叠版装在卡槽 1，那就是 slot1，如果是卡槽 2 就是 solt2）

Switch#_config_bvss#bvss sgnp neighbour-timeout 10 //超时时间 10 分钟

Switch#write bvss-config //使用 write 保存虚拟化配置**（注意，直接 write 命令不能保存虚拟化配置）**，再重启设备**（需要通过直接断电重启设备，不要 reboot 命令重启，reboot 会清空全部堆叠配置）**

Switch# Switch#config //进入全局模式

Switch#_config#bvss

Switch#_config_bvss#interface TGigaEthernet7/1 //进入堆叠口，

Switch#_config_bvss_tg1/1#bvss-link-group 2 //关联虚拟化端口组 2（对端写 1）！

Switch#_config_bvss#interface TGigaEthernet7/2 //进入堆叠口（如果只用到 1 个堆叠口，不用配置）

Switch#_config_bvss_tg1/2#bvss-link-group 2 //关联虚拟化端口组 2（对端写 1）

Switch#write bvss-config //再次保存配置，否则重启会丢失配置

- B 机器

Switch#

Switch#config //进入全局模式

Switch#_config#bvss //进入虚拟化配置模块

Switch#_config_bvss#bvss enable //开启虚拟化功能

Switch#_config_bvss#bvss mode normal //模式选择正常（2 台用正常模式，2 台以上用 enhanced）

Switch#_config_bvss#bvss domain-id 100 //创建虚拟化域 100（随便数字，2 台一致即可）

Switch#_config_bvss#bvss member-id 2 //虚拟化域里面的 2 号成员（交换机 A 是 1）

Switch#_config_bvss#bvss priority 80 //交换机的优先级（比交换机 A 低即可）

Switch#_config_bvss#bvss slot 7 //指定第几块板卡为堆叠板卡（堆叠版卡装在哪里就写几就行，比如该项目堆叠版装在卡槽 1，那就是 slot1，如果是卡槽 2 就是 solt2）

Switch#_config_bvss#bvss sgnp neighbour-timeout 10 //超时时间 10 分钟

Switch#_write bvss-config //使用 write 保存虚拟化配置**（注意，直接 write 命令不能保存虚拟化配置）**，再重启设备**（需要通过直接断电重启设备，不要 reboot 命令重启，reboot 会清空全部堆叠配置）**

Switch#

Switch#config //进入全局模式

Switch#_config#bvss

Switch#_config_bvss#interface TGigaEthernet7/1 //进入堆叠口，

Switch#_config_bvss_tg1/1#bvss-link-group 1 //关联虚拟化端口组 2（对端写 2）

Switch#_config_bvss#interface TGigaEthernet7/2 //进入堆叠口（如果只用到 1 个堆叠口，

不用配置）

Switch#_config_bvss_tg1/2#bvss-link-group 1　　//关联虚拟化端口组 2（对端写 2）

Switch#write bvss-config　　//再次保存配置，否则重启会丢失配置

Switch#show bvss current-config　　//查看虚拟化状态

bvss configuration information:

bvss enable: TRUE　　//当前虚拟化使能状态

bvss domain-id: 100　　//域 id 为 100

bvss member-id : 1　　//虚拟化域里面的成员 1

bvss mode: normal　　//虚拟化模式为普通模式

bvss priority: 100　　//交换机优先级

bvss mac-address mode: use-active-member

bvss slot1: 7, slot2: 0　　//slot1：7 表示当前配置虚拟化使用的为 7 号板卡；slot2：0 表示当前使用普通模式，只使用一款虚拟化板卡

3.9 ACL 配置

- 标准 ACL
  - 基于源 ip 地址控制数据包
  - 允许和拒绝完整的协议
- 扩展 ACL
  - 基于源 ip 地址 目的 ip 地址 端口号 协议类型
  - 允许和拒绝特定的协议和端口号

注意：ACL 由一个隐含的 deny 规则结束

1、配置基于物理端口 IP 访问列表

IP 访问列表是应用 IP 地址的允许和禁止条件的有序集合。交换机的软件系统在访问列表中逐个按规则测试地址。第一个匹配决定是否该软件接受或拒绝该地址。因为在第一个匹

配之后，软件停止了匹配规则，所以条件的先后次序是重要的。如果没有规则匹配，拒绝该地址。在使用访问列表中有以下两个步骤：

（1）通过指定访问列表名及访问条件，建立访问列表。

（2）将访问列表应用到端口

配置过程：

建立标准的和扩展的 IP 访问列表

用一个字符串建立 IP 访问列表。注意：标准的访问列表和扩展的访问列表不能用相同的名字。

❖ 为了建立标准的访问列表，在全局配置下执行下列命令。

ip access-list standard name //使用名字定义一个标准的 IP 访问列表。

deny {source [source-mask] | any} or permit {source [source-mask] | any} //在标准访问列表配置模式下，指定一个或多个允许或不允许条件。这决定该包通过还是不通过。

exit //退出访问列表配置模式。

❖ 为建立扩展的访问列表，在全局配置态执行下列命令：

ip access-list extended name //使用名字定义一个扩展的 IP 访问列表。

{deny | permit} protocol source source-mask src-port destination destination-mask dst-port [precedence precedence] [tos tos] {deny | permit} protocol any any //在扩展访问列表配置模式下，指定一个或多个允许或不允许条件。这决定该包通过还是不通过。（precedence 表示 ip 包优先级，TOS 表示 Type of Service）

Exit //退出访问列表配置模式。

当建立了访问列表后，可以将它应用到一个或多个 vlan 端口上，过滤访问交换机的报文。在端口配置态使用以下命令：

ip access-group {access-list-name}{in | out} //将访问列表应用到端口。

对于标准的入口访问列表，在接收到包之后，对照访问列表检查包的源地址。对于扩展

的访问列表，该路由交换机也检查目标地址。如果访问表允许该地址，那么软件继续处理该包。如果访问表不允许该地址，该软件放弃包并返回一个 ICMP 主机不可到达报文。

如果指定的访问列表不存在，所有的包允许通过。

2、基于接口 ACL 配置示例：

在以下例子中，第一行允许新来的 TCP 与主机 130.2.1.2 的 SMTP 端口连接。

Sundray_Switch_config#ip access-list extended smtp //建立名称为 smtp 的扩展访问列表

Sundray_Switch_config_ext#permit tcp any 130.2.1.2 255.255.255.255 eq 25 //允许任何主机的 tcp 协议与主机 130.2.1.2 的 SMTP 端口连接

Sundray_Switch_config#interface g5/0 //进入到需要应用该 acl 的接口

Sundray_Switch_config_g5/0#ip access-group smtp //将名称为 smtp 的访问列表应用于 interface g5/0，默认在入口方向，egress 配置在出口方向，stat-packet 使能报文统计，stat-byte 使能报文字节的统计。

Sundray_Switch_config#ip access-list standard ssh_access //创建标准访问控制列表 ssh_access

Sundray_Switch_config_std#permit 192.168.20.40 //允许 192.168.20.40 主机从下接口通过

3、基于 VLAN ACL 配置示例：

Sundray_Switch_config#ip access-list extended smtp //建立名称为 smtp 的扩展访问列表

Sundray_Switch_config#ip access-group smtp vlan 1 //将名称为 smtp 的访问列表应用于 vlan 1，默认在入口方向，egress 配置在出口方向，stat-packet 使能报文统计，stat-byte 使能报文字节的统计。

3.10 VRRP 配置

配置 VRRP 组

1、在 SwitchA 上创建 VRRP 备份组 1，配置 SwitchA 在该备份组中的优先级为 120，并配置抢占时间为 20 秒。

switchA_config#int vlan 1 //进入 vlan1 接口

switchA_config_v1# vrrp 1 associate 10.1.1.1 255.255.255.0 //创建 vrrp 组，ID 为 1，配置 vrrp 虚拟 ip 地址为 10.1.1.1

switchA_config_v1# vrrp 1 priority 120 //配置 vrrp 1 主机优先级为 120

switchA_config_v1#vrrp 1 preempt delay 20 //vrrp 组抢占的延时时间为 20S

switchA_config_v1#exit

2、在 SwitchB 上创建 VRRP 备份组 1，其在该备份组中的优先级采用缺省值 100（不需要配置）。

switchB_config#int vlan 1 //进入 vlan1 接口

switchB_config_v1# vrrp 1 associate 10.1.1.1 255.255.255.0 //创建 vrrp 组，ID 为 1，配置 vrrp 虚拟 ip 地址为 10.1.1.1

switchB_config_v1# vrrp 1 priority 100 //配置 vrrp 1 备机优先级为 100

switchB_config_v1#exit

3.11 生成树协议

MSTP 配置

交换机所处的多生成树区域，由配置名称、修订号以及 VLAN 与 MSTI 映射关系这三项属性决定，通过区域配置命令可以分别对其进行设置。需要注意的是，三项属性中任何一项的变化都会导致交换机所处区域的变化。

#配置过程

（1）配置多生成树区域

spanning-tree mstp name string //设置多生成树配置名称。

string 表示配置名称字符串，最多可包含 32 个字符，大小写敏感。默认值为交换机 MAC 地址的字符串形式。

no spanning-tree mstp name //设置多生成树配置名称为默认值。

spanning-tree mstp revision value //设置多生成树配置修订号。value 表示修订号，范围：

0 – 65535，默认值 0。

no spanning-tree mstp revision　　//设置多生成树修订号为默认值。

spanning-tree mstp instance instance-id vlan vlan-list　　//将 VLAN 映射到 MSTI；instance-id：生成树实例号，表示一个 MSTI；vlan-list：映射到该生成树的 VLAN 列表。范围 1 – 4094；instance-id 为单独的值，仅表示一个生成树实例；vlan-list 可以表示一组 VLAN，比如："1,2,3"、"1-5"、"1,2,5-10"等。

no spanning-tree mstp instance instance-id　　//取消 MSTI 的 VLAN 映射，停止生成树实例；instance-id：生成树实例号，表示一个 MSTI。

使用下面的命令查看多生成树协议的区域设置：

show spanning-tree mstp region　　//显示多生成树协议的区域设置

（2）配置网络根桥

spanning-tree mstp instance-id root primary [diameter net-diameter [hello-time seconds]]

//设置交换机在指定生成树实例中为根；instance-id：生成树实例号；net-diameter：可选参数，网络直径，当 instance-id 为 0 时有效，范围：2 – 7；seconds：可选参数，Hello Time，范围：1 – 10 秒。

no spanning-tree mstp instance-id root　　//取消交换机在生成树中的根桥设置；instance-id：生成树实例号。

使用下面的命令查看多生成树协议信息：

show spanning-tree mstp [instance instance-id]　　//查看多生成树实例的信息

配置示例：

Switch_config#spanning-tree mode mstp　　//启动 mstp 多生成树协议

Switch_config#spanning-tree mstp instance 1 root primary/secondary　//设置交换机在指定生成树实例中为根/备根

Switch_config#spanning-tree mstp name MST　　//命名 mstp 生成树协议为 MST

Switch_config#spanning-tree mstp revision 1　　//设置多生成树修订号为 1

Switch_config#spanning-tree mstp instance 1 vlan 10,20-21　　//将对应 vlan 映射到 MSTI

Switch_config#spanning-tree mstp 1 priority 4096　　//设置 MSTP 优先级为 4096

4 路由配置命令

4.1 静态路由配置

Sundray_Switch#ip route default 10.157.255.254 //缺省路由，即指定到任意网段的报文的下一跳地址为 10.157.255.254

Sundray_Switch#ip route 111.11.11.0 255.255.255.0 100.0.1.2 //静态路由，指定到网段 111.11.11.0/24 的报文的下一跳地址为 100.0.1.2

Sundray_Switch#ip route 10.0.0.0 255.0.0.0 vlan 1 //静态路由，指定到网段 10.0.0.0/8 的报文的出端口为 interface vlan 1

4.2 策略路由配置

PBR 是策略路由(Policy Based Routing)的英文缩写。PBR 使得用户可以依靠某种策略来进行路由，而不是依赖路由协议。PBR 目前支持的策略是：ip 报文大小、源 ip 地址。用户可以为符合策略的报文指定下一跳 ip address 或者下一跳端口。PBR 支持负载均衡，对符合策略的报文可以应用多个下一跳 ip 地址或端口。

PBR 应用下一跳的规则如下：

1、如果配置了 set ip next-hop，并且 nexthop 是可到达的，则采用 nexthop。如果有多个 nexthop，则采用第一个可到达的 nexthop，如果多个 nexthop 是 load-balance 方式，则轮流选择这些 nexthop。

2、 如果配置了 set interface，并且 interface 处于可路由(端口协议 up，配置了 ip 地址)状态，则采用该端口作为下一跳端口。如果有多个 interface，则采用第一个可路由的端口，

如果这些多个 interface 是 load-balance 方式，则轮流选择这些端口。如果同时配置 set ip next-hop 和 set interface，优先选择 set ip next-hop。

3、set ip default next-hop 或 set default interface 仅在基于目的 ip 地址的路由表查找失败的情况下有效。

对以下报文，不会应用策略路由：

1、对于目的地址是本地的报文。

2、multicast 报文

3、本地直连广播报文

配置过程：

创建访问列表

创建 route-map

将 route-map 应用到端口

案例配置：

server1 走 13.1.1.254

server2 走 14.1.1.254

server3 负载均衡同时走 13.1.1.254 和 14.1.1.254

配置示例：

Switch_config#ip pbr //默认情况下 pbr 是关闭的，需要先开启

1、创建 ACL

Switch_config#ip access-list standard server1 //创建标准访问控制列表，名称为 server1

Switch_config_std#permit 10.1.1.1 255.255.255.255 //允许主机 10.1.1.1

Switch_config#ip access-list standard server2 //创建标准访问控制列表，名称为 server2

Switch_config_std#permit 10.1.1.2 255.255.255.255 //允许主机 10.1.1.2

Switch_config#ip access-list standard server3 //创建标准访问控制列表，名称为 server3

Switch_config_std#permit 10.1.1.3 255.255.255.255 //允许主机 10.1.1.3

2、创建 route-map

Switch_config#route-map pbr 1 permit //创建 Route-map 的允许项，Route-map 条目的序号为 1

Switch_config_route_map#match ip address server1 //匹配 server1 ip 地址的访问控制列表名

Switch_config_route_map#set ip next-hop 13.1.1.254 // 设置 server1 的下一跳 IP 为 13.1.1.254

Switch_config#route-map pbr 2 permit //创建 Route-map 的允许项，Route-map 条目的序号为 2

Switch_config_route_map#match ip address server2 //匹配 server2 ip 地址的访问控制列表名

Switch_config_route_map#set ip next-hop 14.1.1.254 // 设置 server2 的下一跳 IP 为 14.1.1.254

Switch_config#route-map pbr 3 permit //创建 Route-map 的允许项，Route-map 条目的序号为 3

Switch_config_route_map#match ip address server3 //匹配 server3 ip 地址的访问控制列表名

Switch_config_route_map#set ip next-hop 13.1.1.254 14.1.1.254 load-balance // 设置 server3 的多个下一跳地址，并进行负载分担

Switch_config#route-map pbr 4 permit //创建 Route-map 的允许项，Route-map 条目的序号为 4

Switch_config_route_map#set ip default next-hop 13.1.1.254 // 设置缺省的下一跳地址为 13.1.1.254

3、将 route-map 应用到端口

Switch_config#interface Vlan1 //进入需要应用策略路由的接口

Switch_config_v1#ip policy route-map pbr //打开策略路由，并指定路由映射的名称为 pbr

通过 show ip pbr，显示策略路由所有的配置信息

4.3 动态路由协议-RIP 配置

两台 75 系列交换机，配置如下：

1、交换机 A：

Switch_config#interface vlan1 //进入 vlan 1 接口

Switch_config_v1#ip address 192.168.20.81 255.255.255.0 //配置 vlan 1 接口 ip 地址

Switch_config_v1#ip rip 1 enable //vlan 1 接口下开启 rip，进程号为 1

Switch_config#interface loopback 0 //进入 loopback 0 接口

Switch_config_l0#ip address 10.1.1.1 255.0.0.0 //配置 lo 接口 ip 地址

Switch_config_l0#ip rip 1 enable //l0 接口下开启 rip，进程号为 1

Switch_config#router rip 1 //全局开启 rip 协议，进程号为 1

2、交换机 B：

Switch_config#interface vlan1 //进入 vlan 1 接口

Switch_config_v1#ip address 192.168.20.82 255.255.255.0 //配置 vlan 1 接口 ip 地址

Switch_config_v1#ip rip 1 enable //vlan 1 接口下开启 rip，进程号为 1

Switch_config#interface loopback 0 //进入 loopback 0 接口

Switch_config_l0#ip address 20.1.1.1 255.0.0.0 //配置 lo 接口 ip 地址

Switch_config_l0#ip rip 1 enable //l0 接口下开启 rip，进程号为 1

Switch_config#router rip 1 //全局开启 rip 协议，进程号为 1