S9503&S9150&SI9100 交换机简明开局手册

1. 工业交换机

1.1 EAPS 开局

EAPS 快速以太环网保护协议是一个特殊的链路层协议，专门用于构建环状的以太网拓扑。以太环网保护协议在环网拓扑完整的情况下阻塞一条链路，防止出现数据环路形成广播风暴。在出现链路中断的情况下，协议迅速恢复之前阻断的链路，使环网各节点之间恢复通信。

环网保护协议和生成树协议都用于链路层拓扑控制。生成树协议适用于各种复杂的网络，它使用逐跳的方法传播网络拓扑的变化。环网保护协议专用于环状的拓扑，并使用扩散法传播拓扑变化信息。因此，在环状网络中，环网保护协议的收敛性能优于生成树协议。在网络状况良好的情况下，环网保护协议恢复网络通信的时间甚至可以少于 50 毫秒。

如图 1.1.1 所示，其中 SW1 为主节点，SW2，SW3 为传输节点。

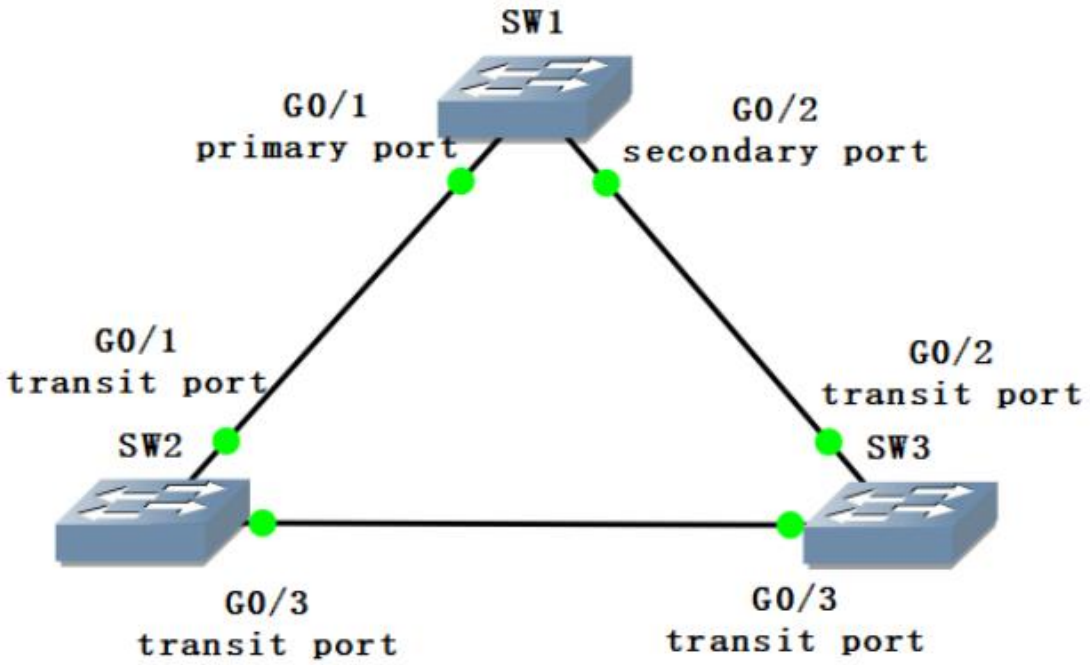

图 1.1 EAPS

配置命令如下：

SW1:

SW1_config#no spanning-tree　　//关闭生成树

SW1_config#ether-ring 1　　//配置环网节点实例 1，进入节点配置模式

SW1_config_ring1#control-vlan 2　　//控制 vlan2

SW1_config_ring1#master-node　　//配置环网节点为主节点

SW1_config_ring1#hello-time 2　　//主节点发送环网探测报文的周期时间为 2s，缺省 1s

SW1_config_ring1#fail-time 6　　//主节点次端口等待环网探测报文时限为 6s，缺省 3s

SW1_config_ring1#exit　　//退出节点配置模式

SW1_config#interface gigaEthernet 0/1

SW1_config_g0/1#ether-ring 1 primary-port　　//配置 g0/1 为主节点的主端口

SW1_config_g0/1#exit

SW1_config#interface gigaEthernet 0/2

SW1_config_g0/2#ether-ring 1 secondary-port　　//配置 g0/2 为主节点的次端口

SW1_config_g0/2#exit

SW1_config#vlan 2

SW1_config_vlan2#exit

SW1_config#interface range g0/1 , 2

SW1_config_if_range#switchport mode trunk

SW1_config_if_range#exit

SW2:

SW2_config#no spanning-tree　　//关闭生成树

SW2_config#ether-ring 1　　//配置环网节点实例 1，进入节点配置模式

SW2_config_ring1#control-vlan 2　　//控制 vlan2

SW2_config_ring1#transit-node　　//配置环网节点为传输节点

SW2_config_ring1#pre-forward-time 8　　//传输端口保持预转发状态时间为 8s，缺省 3s

SW2_config_ring1#exit　　//退出节点配置模式

SW2_config#interface gigaEthernet 0/1

SW2_config_g0/1#ether-ring 1 transit-port　　//配置 g0/1 为传输节点的传输端口

SW2_config_g0/1#exit

SW2_config#interface gigaEthernet 0/3

SW2_config_g0/3#ether-ring 1 transit-port　　//配置 g0/3 为传输节点的传输端口

SW2_config_g0/3#exit

SW2_config#vlan 2

SW2_config_vlan2#exit

SW2_config#interface range gigaEthernet 0/1 , 3

SW2_config_if_range#switchport mode trunk

SW2_config_if_range#exit

SW3:

SW3_config#no spanning-tree　　//关闭生成树

SW3_config#ether-ring 1　　//配置环网节点实例 1，进入节点配置模式

SW3_config_ring1#control-vlan 2　　//控制 vlan2

SW3_config_ring1#transit-node　　//配置环网节点为传输节点

SW3_config_ring1#pre-forward-time 8　　//传输端口保持预转发状态时间为 8s，缺省 3s

SW3_config_ring1#exit　　//退出节点配置模式

```
SW3_config#interface gigaEthernet 0/2
SW3_config_g0/2#ether-ring 1 transit-port      //配置 g0/2 为传输节点的传输端口
SW3_config_g0/2#exit
SW3_config#interface gigaEthernet 0/3
SW3_config_g0/3#ether-ring 1 transit-port      //配置 g0/3 为传输节点的传输端口
SW3_config_g0/3#exit

SW3_config#vlan 2
SW3_config_vlan2#exit
SW3_config#interface range gigaEthernet 0/2 , 3
SW3_config_if_range#switchport mode trunk
SW3_config_if_range#exit
```

配置完成后，可通过如下配置查看环网保护协议状态：

```
show ether-ring id      //查看环网保护协议和环网端口的摘要信息，id 为环网实例号

Switch#show ether-ring 1

Ethernet Automatic Protection Switching

ether-ring 1
  Configured    Role              Master-node(主节点)
                Control-Vlan      2
                Node ID           BC60.6BA6.0000
                Hello Time 2 sec  Fail Time 6 sec  Pre-forward Time 3 sec

  Running       State             Idle
                Mode              Independent
                Complete          True
                Health Check      True
                Hello While 1 sec  Fail While 5 sec
```

```
Interface           Role          State          Pre-fwd    Status
--------------- ---------- ----------- -------- ----------------------
g0/1                Primary      FWD              0          Enabled, Link-Up
g0/2                Secondary    BLK              0          Enabled, Link-Up
                              (主节点在次端口阻塞数据报文)

传输节点:
Switch#show ether-ring 1

Ethernet Automatic Protection Switching

ether-ring 1
  Configured    Role              Transit-node(传输节点)
                Control-Vlan      2
                Node ID           1807.12F0.0A00
                Hello Time 1 sec  Fail Time 3 sec  Pre-forward Time 8 sec

  Running       State             Links-Up
                Mode              Independent
                Master ID         BC60.6BA6.0000
                Complete          True

Interface           Role          State          Pre-fwd    Status
--------------- ---------- ----------- -------- ----------------------
g0/1                Transit      FWD              0          Enabled, Link-Up
g0/3                Transit      FWD              0          Enabled, Link-Up
```

```
show ether-ring id detail      //查看环网保护协议和环网端口的详细信息
```

1.2 ERPS 开局

ERPS 以太网多环保护技术，是 ITU-T 定义的一种二层破环协议标准，标准号为 ITU-T G.8032/Y1344，因此又称为 G.8032。它定义了 RAPS 协议报文和保护倒换机制。

ERPS 是具备高可靠性和稳定性的以太环网链路层技术。它在以太网环完整时能够防止数据环路引起的广播风暴，而当以太网环发生链路故障时能迅速恢复环网上各个节点之间的通信通路，具备较高的收敛速度。

如图 1.2.1 所示，其中 SW1 为 RPL 保护节点，SW2,SW3 为普通节点。

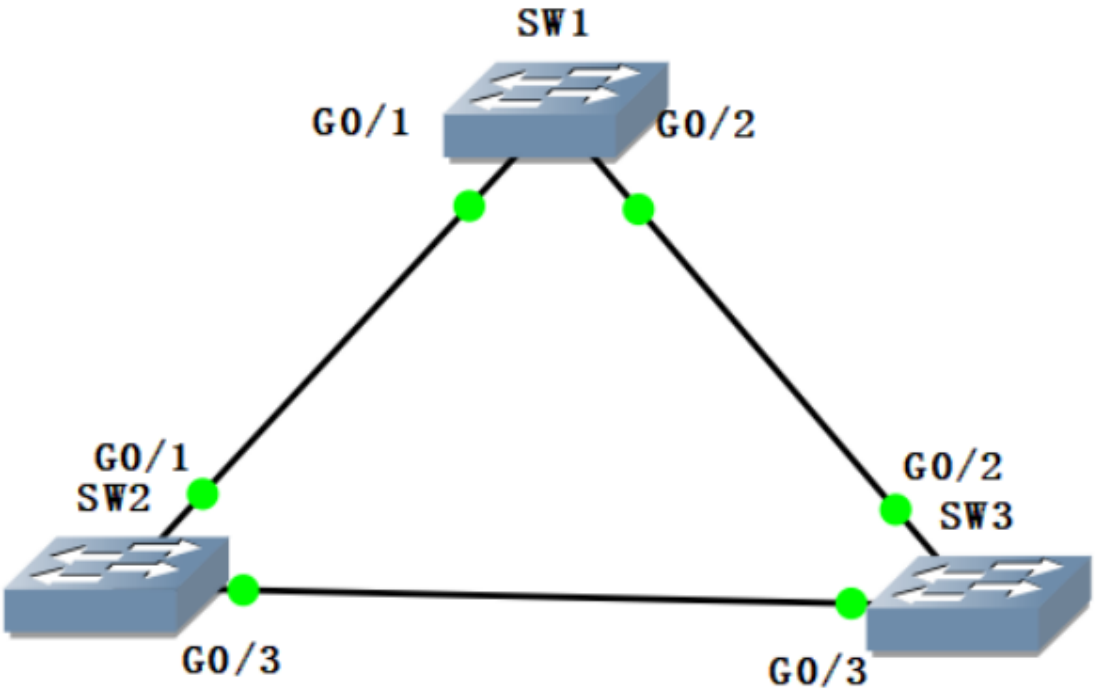

图 1.2 ERPS

配置命令如下：

```
SW1:
link scan fast 10      //配置快速链路扫描时间为 10s
!
!
 ethernet cfm ENABLE      //开启全局 cfm
!
!
erps nimble-mode      //开启 erps 配置简化和倒换加速模式
erps 1      //配置环网节实例 1 并进入节点配置模式
  control-vlan 4094      //配置环网节点控制 vlan4094
exit
!
interface GigaEthernet0/1
 switchport enhanced-link      //配置增强的链路状态检测
```

```
 switchport mode trunk
 ethernet cfm ENABLE     //使 g0/1 的 cfm 功能生效
 erps 1 rpl     //配置环网保护链路
 erps 1 cfm-disable     //配置环网节点实例 1cfm 失效功能
!
interface GigaEthernet0/2
 switchport enhanced-link     //配置增强的链路状态检测
 switchport mode trunk
 ethernet cfm ENABLE     //使 g0/2 的 cfm 功能生效
 erps 1 ring-port     //配置环网端口
 erps 1 cfm-disable     //配置环网节点实例 1cfm 失效功能
!
vlan 1-4094
```

```
SW2:
link scan fast 10     //配置快速链路扫描时间为 10s
!
!
 ethernet cfm ENABLE     //开启全局 cfm
!
!
!
erps nimble-mode     //开启 erps 配置简化和倒换加速模式
erps 1     //配置环网节实例 1 并进入节点配置模式
  control-vlan 4094     //配置环网节点控制 vlan4094
exit
!
interface GigaEthernet0/1
 switchport enhanced-link     //配置增强的链路状态检测
 switchport mode trunk
 ethernet cfm ENABLE     //使 g0/1 的 cfm 功能生效
```

```
 erps 1 ring-port     //配置环网端口
 erps 1 cfm-disable     //配置环网节点实例 1cfm 失效功能
!
interface GigaEthernet0/3
 switchport enhanced-link     //配置增强的链路状态检测
 switchport mode trunk
 ethernet cfm ENABLE     //使 g0/3 的 cfm 功能生效
 erps 1 ring-port     //配置环网端口
 erps 1 cfm-disable     //配置环网节点实例 1cfm 失效功能
!
vlan 1-4094
!
```

```
SW3:
link scan fast 10     //配置快速链路扫描时间为 10s
!
!
 ethernet cfm ENABLE     //开启全局 cfm
!
!
!
erps nimble-mode     //开启 erps 配置简化和倒换加速模式
erps 1     //配置环网节实例 1 并进入节点配置模式
  control-vlan 4094     //配置环网节点控制 vlan4094
exit
!
interface GigaEthernet0/2
 switchport enhanced-link     //配置增强的链路状态检测
 switchport mode trunk
 ethernet cfm ENABLE     //使 g0/2 的 cfm 功能生效
 erps 1 ring-port     //配置环网端口
```

```
 erps 1 cfm-disable      //配置环网节点实例 1cfm 失效功能
!
interface GigaEthernet0/3
 switchport enhanced-link      //配置增强的链路状态检测
 switchport mode trunk
 ethernet cfm ENABLE      //使 g0/3 的 cfm 功能生效
 erps 1 ring-port      //配置环网端口
 erps 1 cfm-disable      //配置环网节点实例 1cfm 失效功能
!
vlan 1-4094
!
```

配置完成后，可通过如下配置查看环网保护协议状态：

```
show erps id      //查看环网保护协议和环网端口的摘要信息，id 为环网实例号

保护节点:
Switch#show erps 1

Ethernet Ring Protection Switching

Ring1
                This node is the RPL Owner
  Node ID       Role            RPL（保护节点）
                Address          1807.12F0.0A00
                Control Vlan     4094
                Version          1
                RAPS Virtual Channel:       True
                Revertive Mode:       Revertive
                State   Idle                WTR   True
                Signal Fail   False         Sending   NR-RB
                WTR time 0/20 sec   WTB time 0/6 sec
                Guard time 0/500 ms   Send time 2/5 sec

Status code: D - LINK DOWN, F - SIGNAL FAIL
Interface          Role              State          Status          MEP Role
---------------- ------------- ----------- ----------- ---------------
g0/1               RPL               BLK                           NULL
```

```
g0/2                Ring-Port       FWD                             NULL

普通节点:
Switch_config#show erps 1

Ethernet Ring Protection Switching

Ring1
  Node ID      Role            Normal(普通节点)
               Address         BC60.6B30.EF23
               Control Vlan    4094
               Version         1
               RAPS Virtual Channel:      True
               Revertive Mode:      Revertive
               State   Idle
               Signal Fail   False       Sending   None
               WTR time 0/20 sec   WTB time 0/6 sec
               Guard time 0/500 ms   Send time 0/5 sec

Status code: D - LINK DOWN, F - SIGNAL FAIL
Interface          Role            State          Status         MEP Role
---------------- ------------- ----------- ----------- --------------
g0/1               Ring-Port       FWD                             NULL
g0/3               Ring-Port       FWD                             NULL
```

```
show erps id detail      //查看环网保护协议和环网端口的详细信息
```

2. 框式及盒式交换机

以简要企业网络园区网络架构为例，三层架构包括接入层、汇聚层、核心层，两层架构包裹接入层、核心层，在实际应用中可根据具体的网络规模及业务需求来选择两层或三层架构。

2.1 S9503 框式交换机堆叠

2.1.1 堆叠

堆叠是指将一台以上的交换机组合起来共同工作，相当于逻辑上将多台交换机合并成一台交换机。

如图 2.1.所示，使用 SW1 与 SW2 两台框式交换机堆叠作为核心，注意 S9503 只支持三槽位做堆叠，槽位排列顺序为自下而上。仅支持万兆及以上光口作为堆叠口。

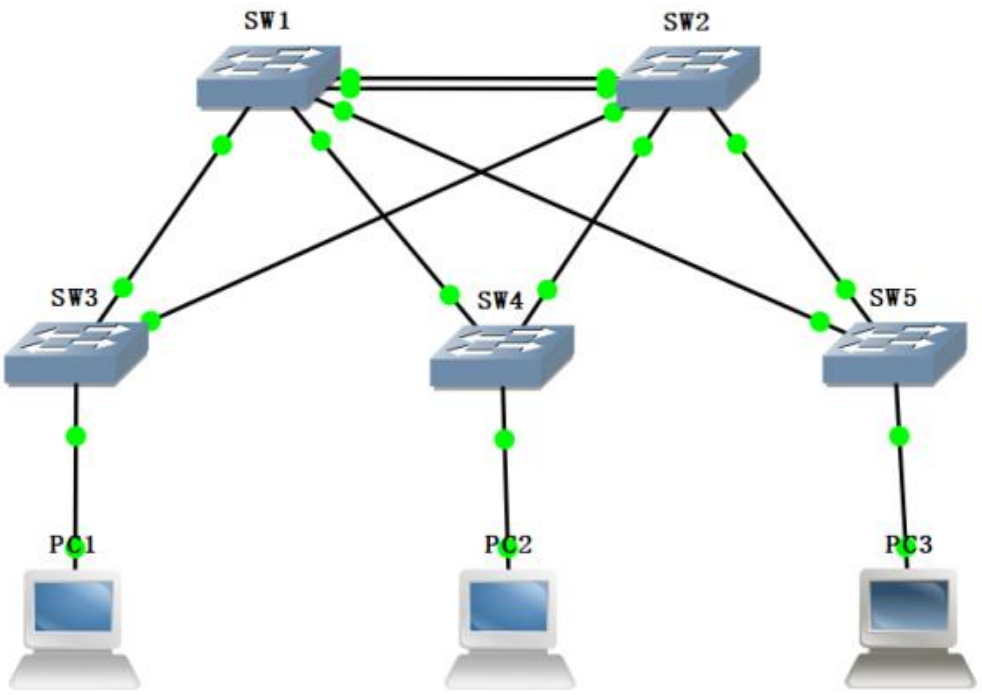

图 2.1 堆叠

配置命令如下：

SW1:

config 模式下输入 bvss 进入 config_bvss 模式。

以下命令在 config_bvss 模式下输入

bvss enable　　//开启 BVSS

bvss mode normal　　//配置堆叠模式为普通模式，普通模式只支持 2 台堆叠，也可配置为增强模式，增强模式支持最多四台设备堆叠，**注意！堆叠设备的模式应保持一致**

bvss domain-id 254　　//配置堆叠域

bvss member-id 1　　//配置堆叠成员 ID

bvss priority 255　　//配置堆叠设备优先级，优先级越高越优

bvss slot 3　　//配置虚拟化线卡，**注意！只支持三槽位堆叠！**

bvss sgnp neighbour-timeout 10　　//配置 SGNP 邻居超时时间值，如在这个时间内没收到对端信息，则认为对端断开，单位为 s

bvss rnp old-master-timeout 10　　//配置 RNP 旧主设备超时时间值，在主备切换后，新的主设备（原备设备）启动定时器，如在这个时间内，原主设备起来了并参与了协商，原主设备就会协商为备设备。如果原来的主设备在这个时间内没有参与协商为备设备，就有可能重新参与协商为主设备，单位为 min

bvss interface 1 slot 3 port 1　　//配置 slot 3/1 为虚拟化端口

bvss interface 2 slot 3 port 2　　//配置 slot 3/2 为虚拟化端口

interface TGigaEthernet3/1

bvss-link-group 1　　//配置堆叠口 group，**注意！互联的两个端口 group 必须不一致！**

interface TGigaEthernet3/2

bvss-link-group 1　　//配置堆叠口 group，**注意！互联的两个端口 group 必须不一致！**

write bvss-config　　//保存堆叠配置

SW2:

config 模式下输入 bvss 进入 config_bvss 模式。

以下命令在 config_bvss 模式下输入

bvss enable　　//开启 BVSS

bvss mode normal　　//配置堆叠模式为普通模式，普通模式只支持 2 台堆叠，堆叠设备的模式应保持一致

bvss domain-id 254　　//配置堆叠域

bvss member-id 2　　//配置堆叠成员 ID

bvss priority 254　　//配置堆叠设备优先级，优先级越高越优

```
bvss slot 3        //配置虚拟化线卡，注意！只支持三槽位堆叠！
bvss sgnp neighbour-timeout 10      //配置 SGNP 邻居超时时间值，如在这个时间内没收到对端信息，则认为对端断开，单位为 s
bvss rnp old-master-timeout 10      //配置 RNP 旧主设备超时时间值，在主备切换后，新的主设备（原备设备）启动定时器，如在这个时间内，原主设备起来了并参与了协商，原主设备就会协商为备设备。如果原来的主设备在这个时间内没有参与协商为备设备，就有可能重新参与协商为主设备，单位为 min

bvss interface 1 slot 3  port 1      //配置 slot 3/1 为虚拟化端口
bvss interface 2 slot 3  port 2      //配置 slot 3/2 为虚拟化端口

interface TGigaEthernet3/1
bvss-link-group 2      //配置堆叠口 group，注意！互联的两个端口 group 必须不一致！
interface TGigaEthernet3/2
bvss-link-group 2      //配置堆叠口 group，注意！互联的两个端口 group 必须不一致！

write bvss-config      //保存堆叠配置
```

TIPS：

①保存堆叠配置后，需要等待 15 分钟，等他们之间的配置同步完成之后断电重启俩台设备，设备重启完成后会自动开始堆叠。

②重启后可通过 show bvss rnp 查看是否可以看到所有堆叠成员信息以确认堆叠是否成功。堆叠成功后备机无法进入 config 模式。

```
Switch#show bvss rnp
  RNP is running. CfgPri 255, SwitchType 0x107b, Slot 0
  System started, ignoreTimeoutCnt 0
  DomainId 1, MemberId 1, LoopTopology 0, Merge 0, Master State
```

MasterMemId 1, BackupMemId 2, MasterGlbMacAddr 00e0.0f62.0035
OldMasterMemberId 0, OldMasterWhile 0, txAdvPduCnt 3353
bvss link group 1 is usable, bvss link group 2 is not usable.
Pri info for member **1** (SwitchType 107b, slot 0):
Priority 255, RunningTime 17097, MAC 00e0.0f62.0035
//成员 1 优先级，运行时间，MAC 地址
Pri info for member **2** (SwitchType 107b, slot 0):
Priority 254, RunningTime 4198, MAC fcfa.f736.c300
//成员 1 优先级，运行时间，MAC 地址

2.1.2 MAD 检测

虚拟化链路故障会导致一个虚拟化域分裂成两个虚拟化域。这两个虚拟化域拥有相同的 MAC 地址、IP 地址，会引起地址冲突，导致网络震荡。为了提高系统的稳定性，当虚拟化域分裂时，我们需要一种机制检测出网络中同时存在的两个虚拟化域，并进行相应的处理，尽量降低虚拟化域分裂对业务的影响。MAD（Multi-Active Detection，多主检测）就是这样一种检测和处理机制。当 MAD 检测出双主后，会将其中一个虚拟化域中所有的普通业务端口 shutdown。

配置 LACP MAD 需要使用一台支持 Multi-Active Relay 的辅助设备与虚拟化域中的主备设备跨设备进行聚合。

配置如下：

注：开启 MAD 堆叠双主检测的设备需要使用 LACP 进行连接

堆叠主设备：

```
int port-aggregator 1
multi-active-detection      //开启 LACP MAD 检测功能
```

辅助设备：

```
int port-aggregator 1
multi-active-relay      //开启 LACP Multi-Active Relay 检测功能
```

2.2 链路聚合

以图 2.1 中 SW1，SW2，SW3 为例，在堆叠环境下做跨设备链路聚合。

配置命令如下：

堆叠主设备： int port-aggregator 1 exi int range g1/1/1,g2/1/2 aggregator-group 1 mode static/lacp
SW3： int port-aggregator 1 exi int range g0/1,g0/2 aggregator-group 1 mode static/lacp

配置完成后，可通过如下配置查看链路聚合状态：

show interface port-aggregator 1　　//查看聚合口 1 具体信息
show aggregator-group 1 {detail|brief|summary}　　//查看逻辑端口 1 的具体信息 Switch#show aggregator-group 1 brief Aggregator-group brief infomation ---------- Group: 1 ---------- System ID : 32768 8479.73B5.0603　Partner : 0 0000.0000.0000 Group ID : 32768 8479.73B5.0632　state : lineUp Max Ports : 8　ports : 2 ---------- Flags: D - down　A - Use In port-aggregator U - Up　I - Not In port-aggregator d - default **g0/1(UA)　g0/2(UA)**

```
UA 表示该端口在端口聚合组中，端口也是 up 的；DI 表示该端口是 down 的也不在端口聚合组中
```

2.3 DHCP

可根据现网情况及客户需求选择是否配置在核心交换机上。

配置命令如下：

```
ip dhcpd enable      //开启 dhcp server 服务
ip dhcpd pool 1     //添加 dhcp server 地址池 1
network 192.168.2.0 255.255.255.0       //配置用于自动分配的地址池的网络地址
range 192.168.2.10 192.168.2.100       //配置用于自动分配的地址范围
default-router 192.168.2.1       //该网段的网关地址
dns-server 8.8.8.8       //配置分配给客户机的 DNS 服务器地址
```

配置完成后，可通过如下配置查看 DHCP 相关信息：

```
show ip dhcpd pool {binding|pool|statistic}      //查看 DHCP Server 地址绑定信息|地址池信息|统计信息
```

TIPS：可通过 range 的方式排除不需要被被分配出去的地址，但一个地址池只支持配置 8 个地址范围。

DHCP 中继配置如下：

```
int vlan 1
ip helper-address X.X.X.X      //在网关地址上配置
```

2.4 静态路由

在交换机上配置缺省静态路由指向出口路由器，或用于不同网段间通信等。

配置命令如下：

```
ip route 目的 ip 掩码 下一跳
```

TIPS：

①一般情况下两个设备之间的通信是双向的，因此路由也必须是双向的，在本端配置完静态路由以后，请不要忘记在对端设备上配置回程路由。

②在企业网络双出口的场景中，通过配置两条等价的静态路由可以实现负载分担，流量可以均衡的分配到两条不同的链路上。

BFD 联动静态路由

BFD 双向转发检测是一套全网统一的检测机制，用于快速检测、监控网络中链路或者 IP 路由转发的连通状况。为了提升现有网络性能，相邻协议之间必须能快速检测到通信故障，从而更快的建立起备用通道恢复通信。

BFD 在两台机器上建立会话，用来监测两台机器间的双向转发路径，为上层协议服务。需要服务的上层协议通知其该与谁建立会话，通过 3 次握手会话建立后如果在检测时间内没有收到对端的 BFD 控制报文或回声报文丢失报文的数量超过配置允许的最大值则认为发生故障，通知被服务的上层协议，上层协议进行相应的处理。

配置命令如下：

ip route bfd static next-hop　　//启动静态路由 ping 方式下一跳检测机制（单向检测）
ip route bfd static X.X.X.X(网关地址) X.X.X.X(远端地址)

配置完成后，可通过如下配置确认：

如以一下配置为例,当检测到 192.168.0.6 这个地址不通后,进行默认路由的切换至 4.4.4.1:

```
ip route default 3.3.3.1
ip route default 4.4.4.1 200
ip route bfd static next-hop
ip route bfd static 3.3.3.1 192.168.0.6
```

可通过 show ip route 进行查看:

```
Switch_config#show ip route
max_rtlimit:512 static_nh_limit:8
Codes: C - connected, S - static, R - RIP, B - BGP, BC - BGP connected
```

```
        D - BEIGRP, DEX - external BEIGRP, O - OSPF, OIA - OSPF inter area
        ON1 - OSPF NSSA external type 1, ON2 - OSPF NSSA external type 2
        OE1 - OSPF external type 1, OE2 - OSPF external type 2
        DHCP - DHCP type, L1 - IS-IS level-1, L2 - IS-IS level-2, IA - ISIS inter-level
        I - IPSEC type

VRF ID: 0

S       0.0.0.0/0           [1,0] via 3.3.3.1(on VLAN3)
C       3.3.3.0/24          is directly connected, VLAN3
C       4.4.4.0/24          is directly connected, VLAN4


Switch_config#show ip route
max_rtlimit:512 static_nh_limit:8
Codes: C - connected, S - static, R - RIP, B - BGP, BC - BGP connected
        D - BEIGRP, DEX - external BEIGRP, O - OSPF, OIA - OSPF inter area
        ON1 - OSPF NSSA external type 1, ON2 - OSPF NSSA external type 2
        OE1 - OSPF external type 1, OE2 - OSPF external type 2
        DHCP - DHCP type, L1 - IS-IS level-1, L2 - IS-IS level-2, IA - ISIS inter-level
        I - IPSEC type

VRF ID: 0

S       0.0.0.0/0           [200,0] via 4.4.4.1(on VLAN4)
C       3.3.3.0/24          is directly connected, VLAN3
C       4.4.4.0/24          is directly connected, VLAN4
```

2.5 OSPF

OSPF 开放最短路径优先协议，是一种基于链路状态的动态路由协议，其协议号为89，属于内部网关协议，OSPF 协议的路由收敛速度较快，可在较短时间内实现路由信息的更新。OSPF 通过划分区域对网络进行管理，分为骨干和非骨干区域。是最具代表性的 LS 协议。

配置命令如下：

```
router ospf 100      //启动并进入 ospf 100

router-id 1.1.1.1      //指定设备的 router-id

network 192.168.10.0 255.255.255.0 area 0      //在区域 0 内宣告网段
```

```
redistribute protocol process-id [metric-type [1 | 2] | metric cost |
tag tag |route-map WORD]     //引入外部路由信息
```

配置完成后，可通过如下配置确认：

```
show ip ospf [process-id]     //显示 ospf 路由进程的一般信息
```

```
show ip ospf [process-id] database[router|network| summary| asbr-
summary|external| database-summary]{ link-state-id|self-originate|
adv-router[ip-address]}      //显示 ospf 数据库的相关信息
Switch#show ip os database
------------------------------------------------------------------------
                OSPF process: 100（ospf 进程号）
                (Router ID: 1.1.1.1)

                    AREA: 0（区域）
                Router Link States（LSA 名称）
Link ID         ADV Router      Age         Seq Num       Checksum Link Count
1.1.1.1         1.1.1.1         110         0x80000004 0x67d9     1
2.2.2.2         2.2.2.2         1521        0x80000003 0x2b0e     1
                    Net Link States
Link ID         ADV Router      Age         Seq Num       Checksum
192.168.10.1    1.1.1.1         110         0x80000003 0xf7bd
------------------------------------------------------------------------
```

```
show ip ospf neighbor      //显示 ospf 的邻居信息
Switch#show ip ospf neighbor
------------------------------------------------------------------------
                OSPF process: 100（ospf 进程号）
                    AREA: 0（区域）
（邻居 id）（优先级）  （状态）    （死亡时间）    （邻居地址）    （接口）
Neighbor ID   Pri     State       DeadTime    Neighbor Addr   Interface
2.2.2.2         1     FULL/BDR    31          192.168.10.2    VLAN10
------------------------------------------------------------------------
```

2.6 ACL 访问控制列表

ACL 访问控制列表用于过滤网络流量，可以基于源/目标地址、端口、协议等条件

进行控制，可用于实现安全性、流量控制和网络分割等。

可分为基于 IP 进行控制的 ACL 和基于 MAC 进行控制的 ACL，其中基于 IP 的 ACL 可分为标准 ACL 和扩展 ACL。

配置命令如下：

标准 ACL： ip access-list standard acl1　　//定义名为 acl1 的标准访问控制列表 permit/deny　192.168.1.0　255.255.255.0　　// 允 许 或 拒 绝 源 为 192.168.1.0/24 的流量 int g0/1 ip access-group acl1 in/out
扩展 ACL： ip access-list extended acl2　　//定义名为 acl2 的标准访问控制列表 permit/deny　ip　192.168.1.0　255.255.255.0　192.168.2.0　255.255.255.0 //允许或拒绝来自 192.168.1.0/24 目的 192.168.2.0/24 的流量 int g0/1 ip access-group acl2 in/out
基于 MAC 访问控制列表： mac access-list 3　　//定义名为 3 的 mac 访问控制列表 permit/deny H.H.H[源 mac] H.H.H H.H.H[目的 mac] H.H.H int g0/1 mac access-group 3 in/out

TIPS：注意！每个 acl 都会有一条隐式拒绝所有的策略，如不需要，在配置完相关的策略后加 permit ip any any

2.7 策略路由

策略路由 PBR（policy based routing），支持 ip 访问列表策略和下一跳 ip address 规则，优先级最高。在配置了多个下一跳情况下，选择第一个有效下一跳， 只有在没有任何有效下一跳的情况下才会丢弃报文。

配置命令如下：

```
ip pbr    //开启 ip-pbr 功能
创建访问控制列表：
ip access-list extended 2
deny   ip 192.168.2.0 255.255.255.0 192.168.8.0 255.255.252.0
permit ip 192.168.2.0 255.255.255.0 any
创建 route map：
route-map pbr(route-map 名) 10(默认序列号 10) permit
match ip address 2(访问列表名)
set ip next-hop 192.168.20.1
应用：
interface VLAN2
ip address 192.168.2.1 255.255.255.0
no ip directed-broadcast
ip policy route-map pbr
```

2.8 NTP

NTP 网络时间协议（Network Time Protocol）是用来使计算机时间同步化的一种协议，可用于分布式时间服务器和客户端之间进行时间同步。它可以提供高精度的时间校正，且可通过加密认证方式防止恶意的协议攻击。客户端和服务器端采用 UDP 协议进行通信，端口号为 123。

配置命令如下：

```
server：
ntp master primary     //配置设备作为原始 NTP 服务器（stratum = 1），在设备无上级 NTP 服务器的情况下采用该配置
ntp master secondary     //配置设备作为次级 NTP 服务器，在设备配置了上级 NTP 服务器的情况下采用该配置[需配置 ntp server 命令，且时间能够同步到指定服务器，否则设备无法给 NTP 客户端提供时间同步服务]
```

```
client：
```

```
ntp client enable      //开启 ntp 客户端功能
```

2.9 端口绑定

为保证接入用户的安全性，可在端口上同时绑定 ip 地址和 mac 地址，也可只绑定 ip 或 mac 地址。

配置命令如下：

```
int g0/1
sw port-security port-security bind/block {ip/arp/both-arp-ip A.B.C.D
/ mac H.H.H}
```

TIPS:

①bind 只允许符合绑定要求的报文通过，其他的报文拒绝；block 只拒绝符合绑定要求的报文，其他的允许通过。

②ip 表示只对符合绑定要求的 ip 报文起作用；Arp 表示只对符合绑定要求的 arp 报文起作用；both-arp-ip 表示对符合绑定要求的 ip 和 arp 报文都起作用。

2.10 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。

端口镜像配置命令如下：

```
将端口 1 的发送和收方向，复制一份给 2 口：
mirror session 1 source interface g0/1 both
mirror session 1 destination interface g0/2
```

2.11 端口物理特性

配置命令如下：

```
速率：
```

int g0/1 Speed 10/100/1000/10000/auto
双工模式： duplex full/half/auto

TIPS：注意再强制速率前需关闭自适应 no fiber-auto-config。

2.12 等保

等保相关配置如下：

密码规则设置： localpass [name]　　//本地密码策略配置 element number lower-letter upper-letter special-character　　//指定口令组成成分，可组合选择，也可选择单个 min-length [1-127]　　//口令最小长度，1-127 为最小密码长度值 validity [1d2h3m4s]　　//密码有效时长，以天、小时、分钟、秒的格式
关闭 telnet 且开启 ssh： no ip telnet enable ip sshd enable 创建三个不同权限的用户(创建的用户名和密码不区分是 ssh 登录还是 console 登录) localauthor test（名称） exec privilege default 14 privilege exec 14 show running-config 创建 14 权限 localauthor bug（名称） exec privilege default 13 创建 13 权限 username admin password 0 admin；该 admin 账户权限最高可以操作交换机所有命令 username Y password 0 K author-group test；该 Y 账号只限于进入 enable 模式，可执行 enable 下可操作的命令 username L password 0 P author-group bug；该 L 账号只限于进入 enable 模式，除了无

法执行 show run（查看所有配置），其他 enable 下的命令都可执行

登录失败 5 次锁定 10 分钟：

ip sshd auth-retries 5

ip sshd silence-period 600

配置登录 ACL：

ip access-list extended UsersLogin

permit ip <源网段> <掩码> <目的网段> <掩码>

exit

设置登录超时 10 分钟退出、登录 ACL 引用：

line vty 0 7

exec-timeout 600

ip sshd access-class UsersLogin

配置日志服务器：

logging on

logging X.X.X.X

配置 NTP、SNMP：

ntp client enable

ntp server X.X.X.X

snmp-server community 0 public RW

snmp-server host 10.36.6.13 version V2C public authenticatio configure snmp