G-LAB

G-CNP v2.0课程

讲师：沈老师

教学团队介绍

- 讲师：沈老师
- 班主任：Ella
- 上课时间：8天

  9：30 - 12:00 1:30 – 16：00

讲师介绍

沈彬　网络运维专家

苏州GLAB IT实验室---讲师
思科CCIE高级互联网专家认证
华为HCIE高级互联网专家认证
红帽RHCE工程师认证
技术宅

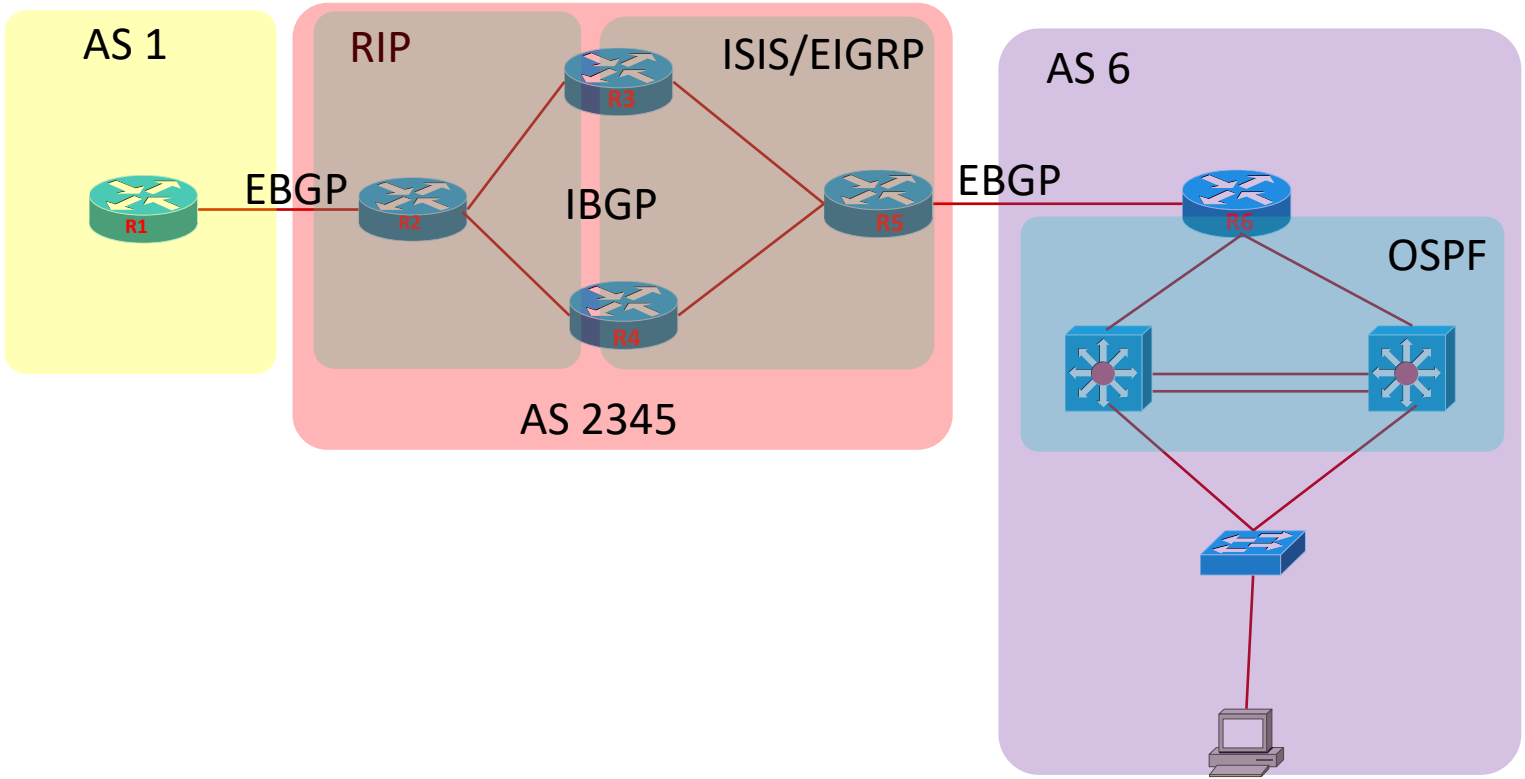
上课纪律要求

1. 不迟到、不早退、不无故缺勤
2. 缺勤3次或以上，将不通知重修（重要）
3. 课后作业按时完成
   - 作业格式：word
   - 作业包含：实验要求、实验拓扑、实验步骤、实验总结
   - 作业发送截止日期：每周六24 : 00

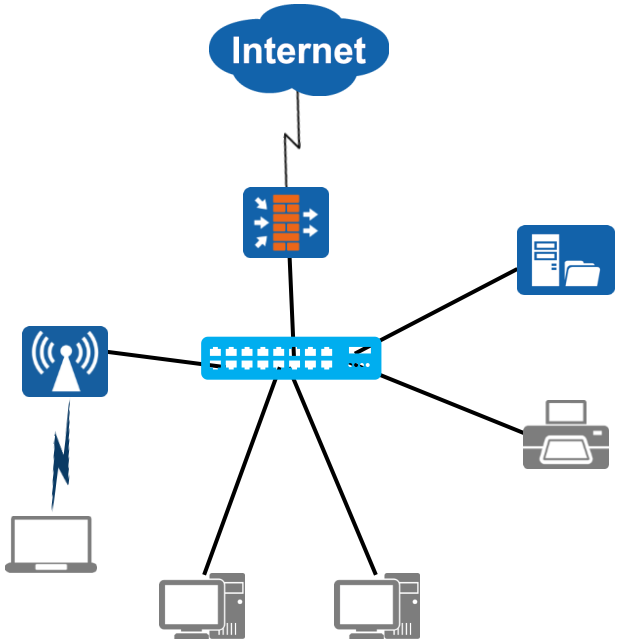
课程内容

A 局域网技术	B IGP技术	C BGP技术	D 路由重分布
E IPv6技术	F VPN技术	G 自动化运维	H 项目实战

课程目标



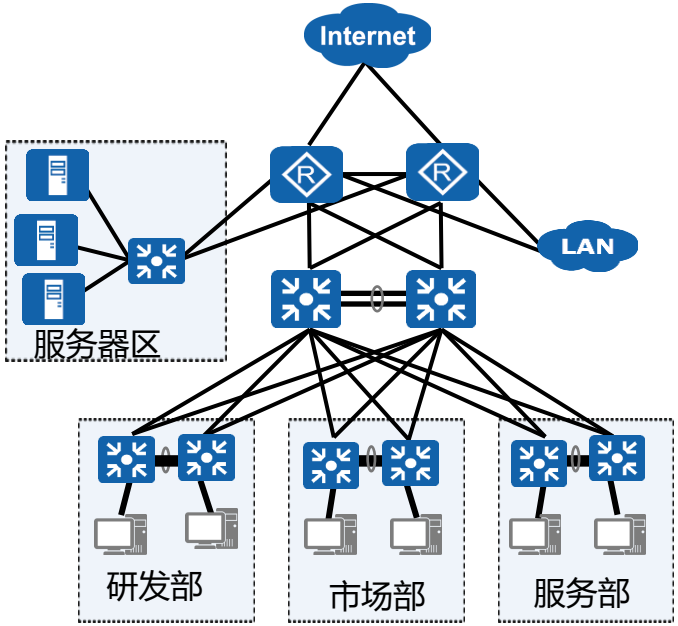
小型网络典型结构



特点：

- 用户数量较少
- 仅单个地点
- 网络无层次性
- 网络需求简单

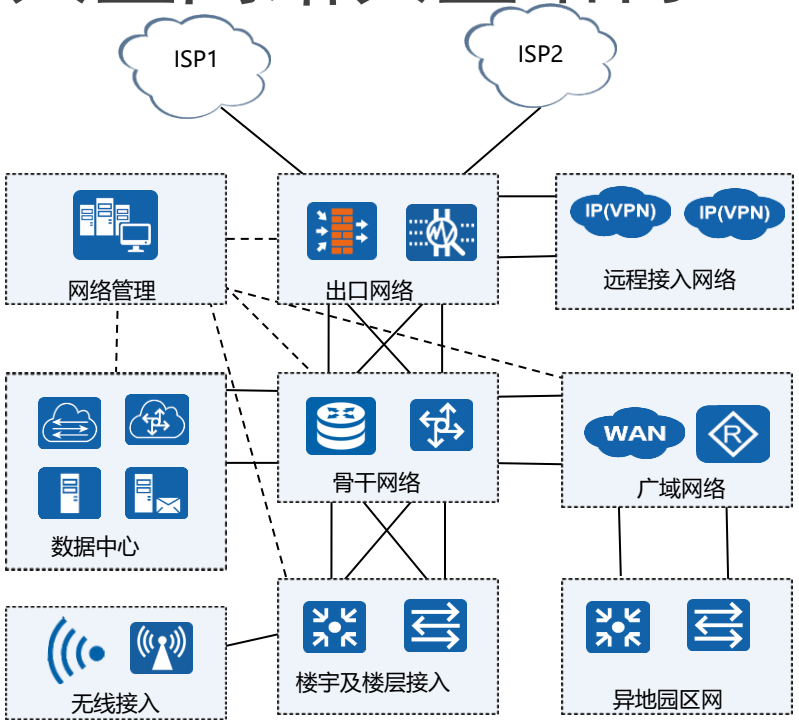
中型网络典型结构



特点：

- 规模中等
- 使用场合最多
- 功能分区
- 初步分层

大型网络典型结构



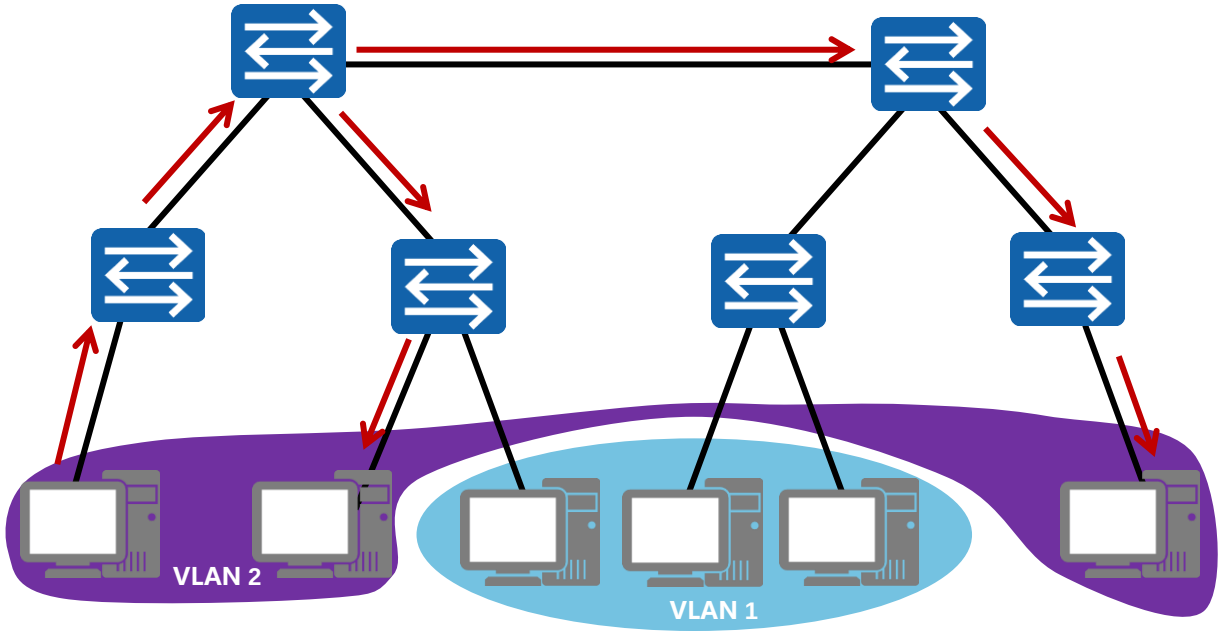
特点：

- 覆盖范围广
- 用户数量多
- 网络需求复杂
- 功能模块全
- 网络层次丰富

局域网技术回顾

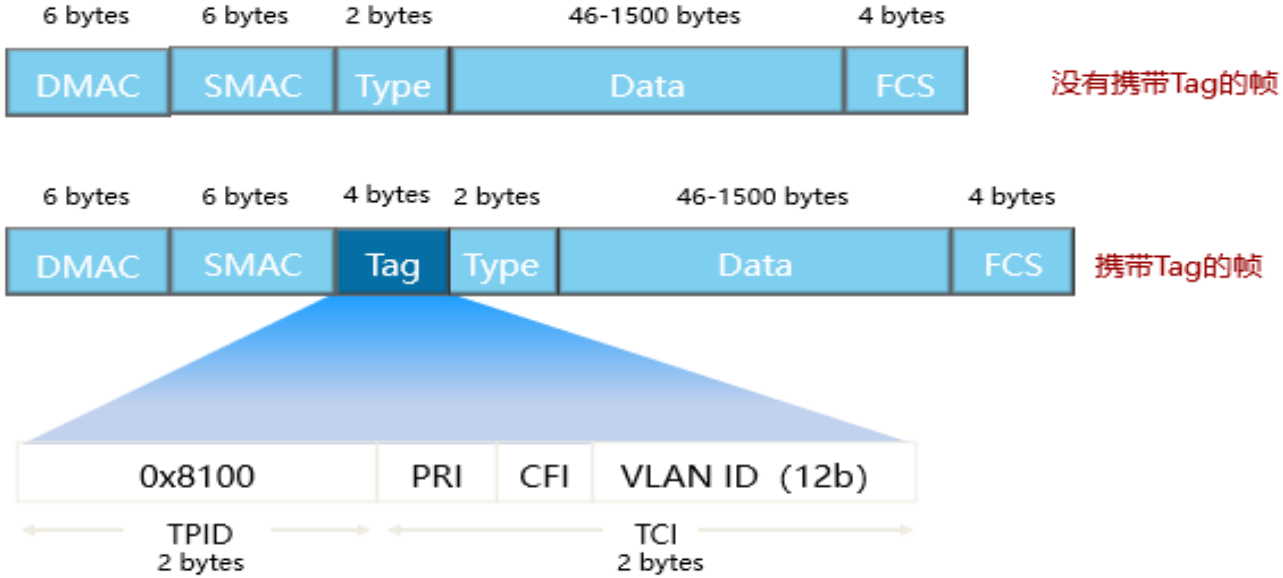
1. VLAN--Trunk
2. 局域网防环：STP--RSTP--MSTP--Ethernet-三层交换
3. 局域网网关冗余：HSRP--VRRP—GLBP

VLAN技术



- VLAN能够隔离广播域。

VLAN帧格式

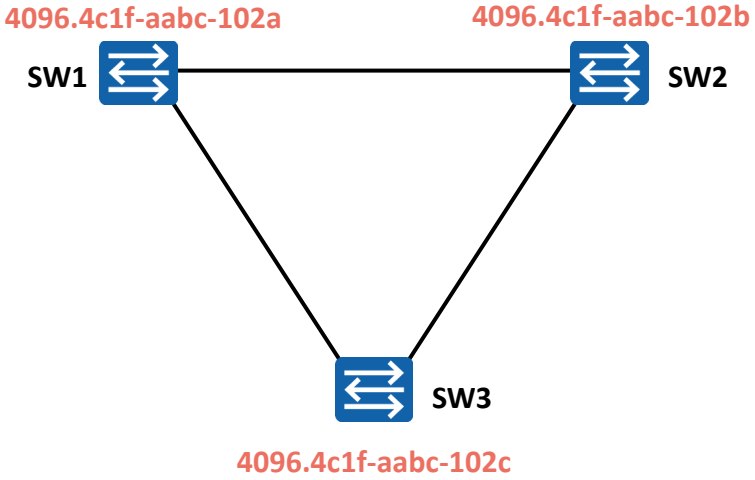


- 通过Tag区分不同VLAN。

接口模式

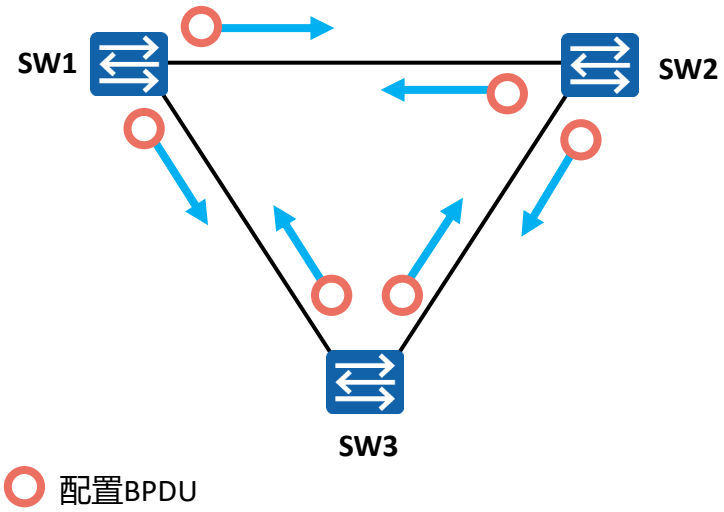
Access接口	Trunk接口	Hybrid接口
接收数据帧 ▫ Untagged数据帧，打上PVID，接收。 ▫ Tagged数据帧，与PVID比较，相同则接收；不同则丢弃。	接收数据帧 ▫ Untagged数据帧，打上PVID，且VID在允许列表中，则接收；VID不在允许列表，则丢弃。 ▫ Tagged数据帧，查看VID是否在允许列表中，在允许列表中，则接收；VID不在允许列表，则丢弃。	接收数据帧 ▫ Untagged数据帧，打上PVID，且VID在允许列表中，则接收；VID不在允许列表中，则丢弃。 ▫ Tagged数据帧，查看VID是否在允许列表中，在允许列表中，则接收；VID不在允许列表，则丢弃。
发送数据帧 ▫ VID与PVID比较，相同则剥离标签发送；不同则丢弃。	发送数据帧 ▫ VID在允许列表中，且VID与PVID一致，则剥离标签发送。 ▫ VID在允许列表，但VID与PVID不一致，则直接带标签发送。 ▫ 不在允许列表中，则直接丢弃。	发送数据帧 ▫ VID不在允许列表中，直接丢弃。 ▫ VID在Untagged列表中，剥离标签发送。 ▫ VID在Tagged列表中，带标签直接发送。

STP操作



1. 选举一个根桥。
2. 每个非根交换机选举一个根端口。
3. 每个链路上选举一个指定端口。
4. 阻塞非根、非指定端口。

STP的基本概念：BPDU



BPDU（Bridge Protocol Data Unit，网桥协议数据单元）

- BPDU是STP能够正常工作的根本。BPDU是STP的协议报文。
- STP交换机之间会交互BPDU报文，这些BPDU报文携带着一些重要信息，正是基于这些信息，STP才能够顺利工作。
- BPDU分为两种类型：
  - 配置BPDU（Configuration BPDU）
  - TCN BPDU（Topology Change Notification BPDU）
- 配置BPDU是STP进行拓扑计算的关键；TCN BPDU只在网络拓扑发生变更时才会被触发。

配置BPDU的报文格式

PID	PVI	BPDU Type	Flags	Root ID	RPC	Bridge ID	Port ID	Message Age	Max Age	Hello Time	Forward Delay

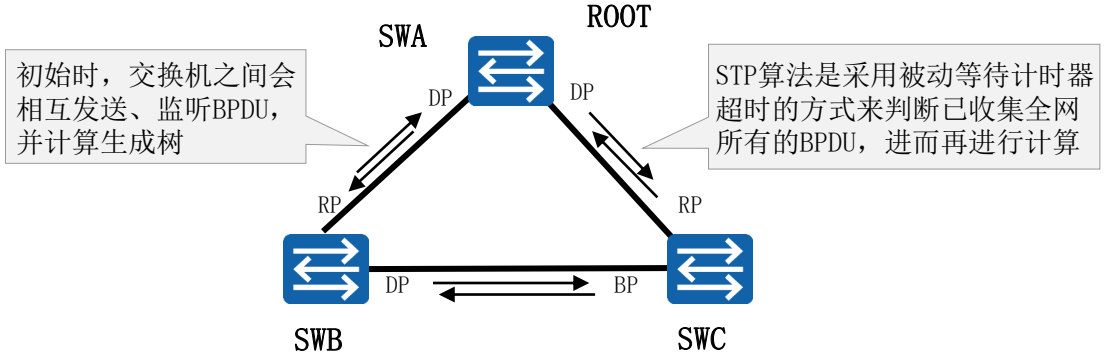
字节	字段	描述
2	PID	协议ID，对于STP而言，该字段的值总为0
1	PVI	协议版本ID，对于STP而言，该字段的值总为0
1	BPDU Type	指示本BPDU的类型，若值为0x00，则表示本报文为配置BPDU；若值为0x80，则为TCN BPDU
1	Flags	标志，STP只使用了该字段的最高及最低两个比特位，最低位是TC（Topology Change，拓扑变更）标志，最高位是TCA（Topology Change Acknowledgment，拓扑变更确认）标志
8	Root ID	根网桥的桥ID
4	RPC	根路径开销，到达根桥的STP Cost
8	Bridge ID	BPDU发送桥的ID
2	Port ID	BPDU发送网桥的接口ID（优先级+接口号）
2	Message Age	消息寿命，从根网桥发出BPDU之后的秒数，每经过一个网桥都减1，所以它本质上是到达根桥的跳数
2	Max Age	最大寿命，当一段时间未收到任何BPDU，生存期到达最大寿命时，网桥认为该接口连接的链路发生故障。默认20s
2	Hello Time	根网桥连续发送的BPDU之间的时间间隔，默认2s
2	Forward Delay	转发延迟，在侦听和学习状态所停留的时间间隔，默认15s

STP的接口状态

状态名称	状态描述
禁用（Disable）	该接口不能收发BPDU，也不能收发业务数据帧，例如接口为down
阻塞（Blocking）	该接口被STP阻塞。处于阻塞状态的接口不能发送BPDU，但是会持续侦听BPDU，而且不能收发业务数据帧，也不会进行MAC地址学习
侦听（Listening）	当接口处于该状态时，表明STP初步认定该接口为根接口或指定接口，但接口依然处于STP计算的过程中，此时接口可以收发BPDU，但是不能收发业务数据帧，也不会进行MAC地址学习
学习（Learning）	当接口处于该状态时，会侦听业务数据帧（但是不能转发业务数据帧），并且在收到业务数据帧后进行MAC地址学习。可以防止临时环路
转发（Forwarding）	处于该状态的接口可以正常地收发业务数据帧，也会进行BPDU处理。接口的角色需是根接口或指定接口才能进入转发状态

问题一：设备运行STP初始化场景

- STP从初始状态到完全收敛至少需经过30s：



listening → 15s → learning

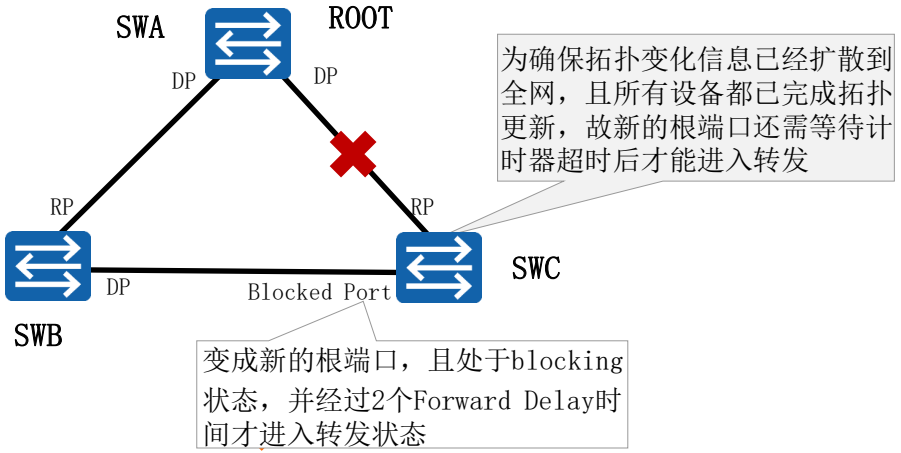
STP为避免临时环路，必须等待足够长的时间（即确保BPDU能同步发送至全网各节点）确保全网的端口状态全部确定，才能进入转发。

learning → 15s → forwarding

在STP进入转发前还需根据收到的用户流量构建MAC地址表，仍需等待计时器超时才能进入转发。

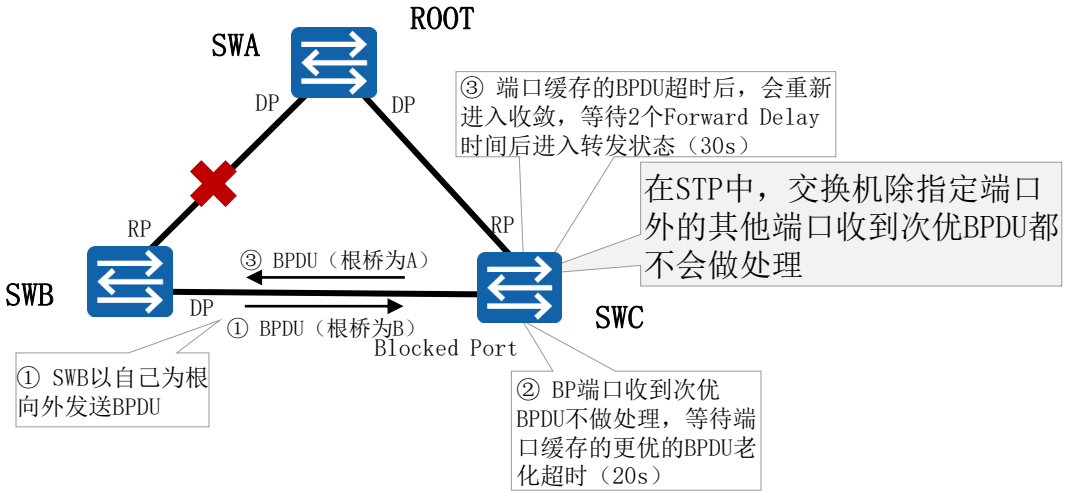
问题二：交换机有BP端口，RP端口down掉场景

- SWC与SWA的直连链路down掉，其BP端口切换成RP端口并进入转发状态至少需要经过30s：



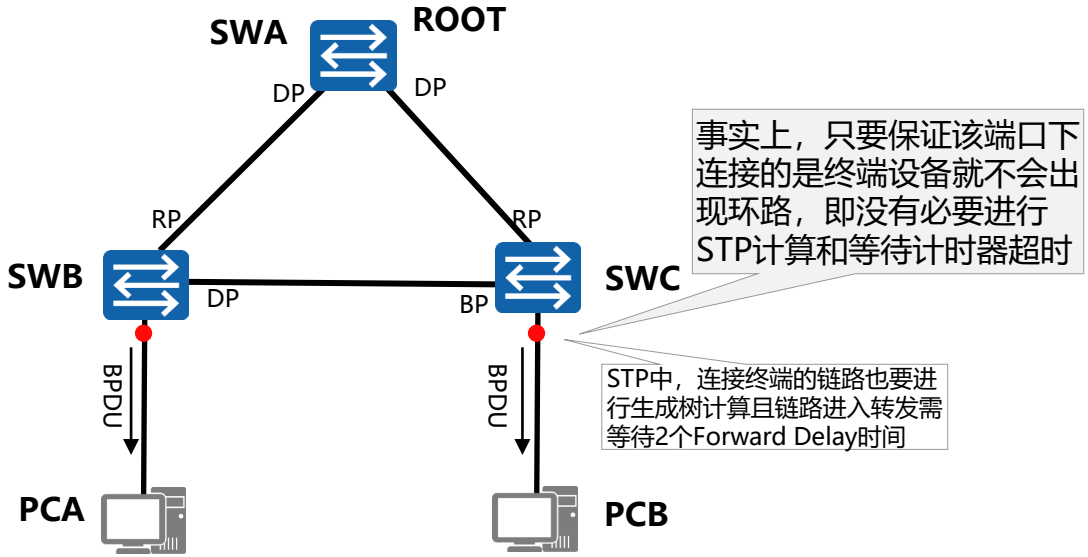
问题三：交换机无BP端口，RP端口down掉场景

- SWB与SWA的直连链路down掉，则SWC的BP端口切换成DP端口并进入转发状态大约需要50s：



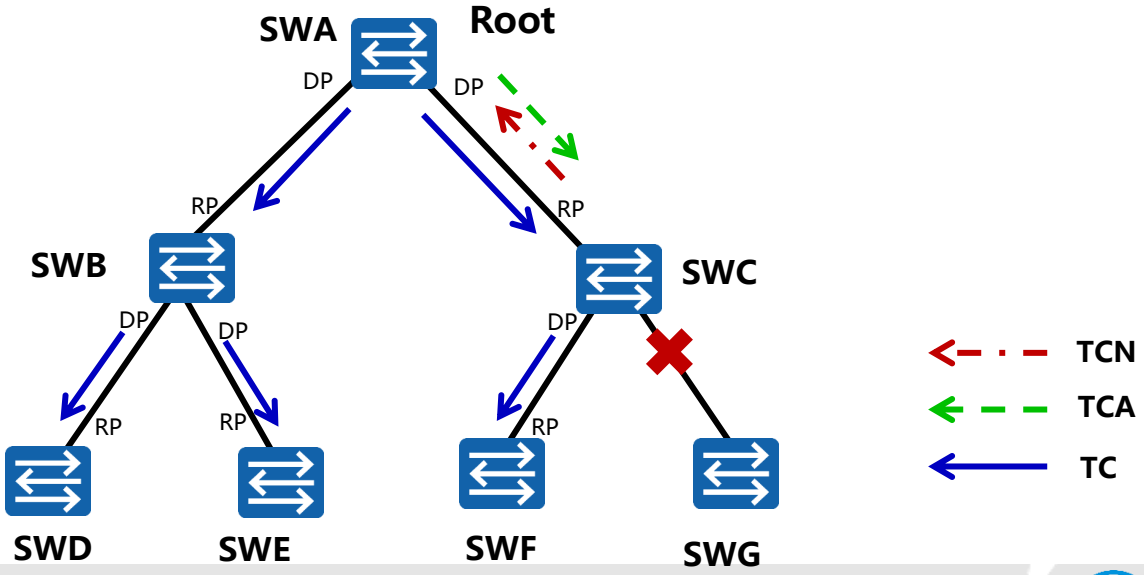
问题四：运行STP的交换机连接用户终端的场景

- 交换机连接终端的链路进入转发需要经过30s：



问题五：STP的拓扑变更机制

- 先由变更点朝根桥方向发送TCN消息，收到该消息的上游交换机就会回复TCA消息进行确认；最后TCN消息到达根桥后，再由根桥发送TC消息通知设备删除桥MAC地址表项，机制复杂，效率低下。



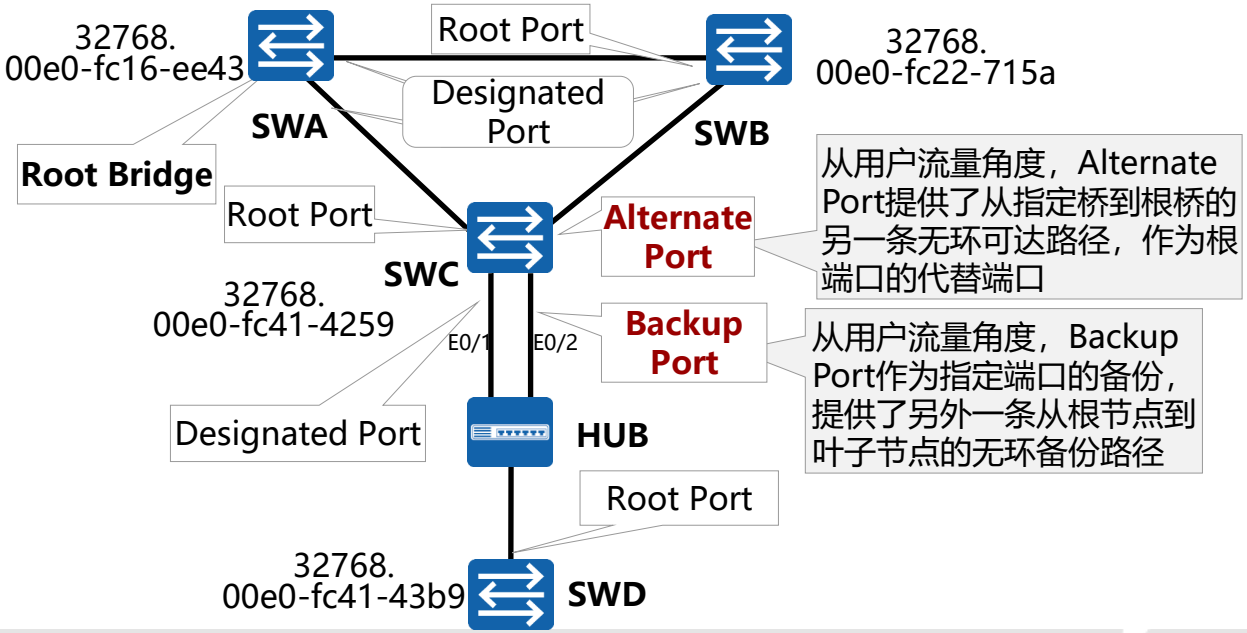
STP的其他不足之处 – 端口状态

STP端口状态	端口状态对应的行为
Disabled	不转发用户流量也不学习MAC地址
Blocking	
Listening	
Learning	不转发用户流量但是学习MAC地址
Forwarding	既转发用户流量又学习MAC地址

三种端口状态从用户使用的角度对应的行为都相同，但呈现出不同的状态，这样反而增加了使用难度

端口角色的重新划分

- RSTP定义了两种新的端口角色：备份端口（Backup Port）和预备端口（Alternate Port）。



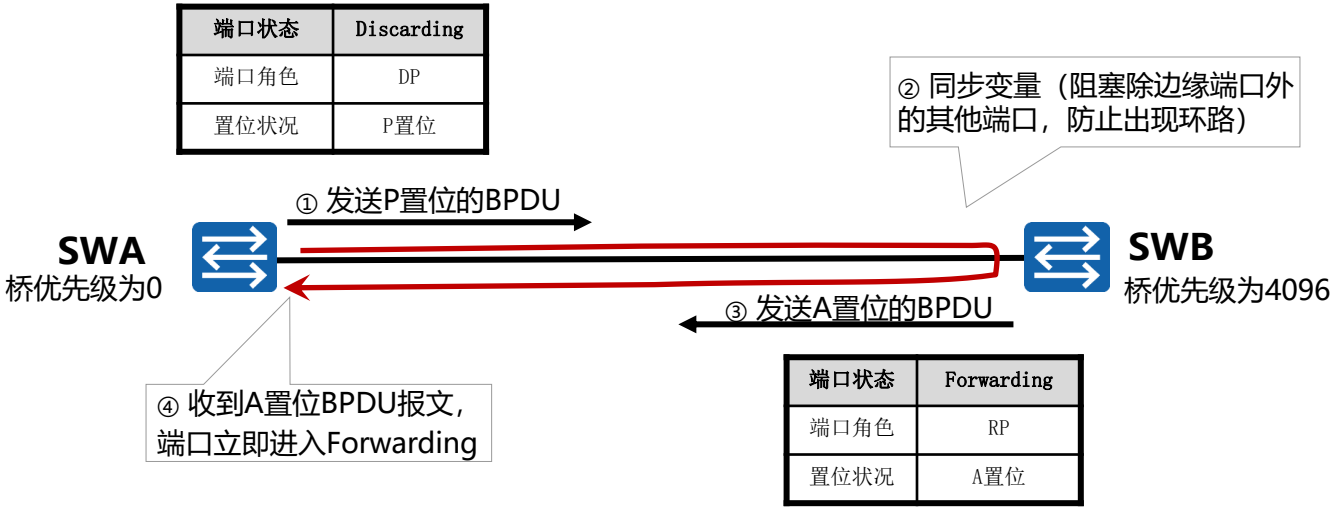
端口状态的重新划分

- RSTP的状态规范把原来的5种状态缩减为3种：

STP端口状态	RSTP端口状态	端口状态对应的行为
Disabled	Discarding	如果不转发用户流量也不学习MAC地址，那么端口状态就是Discarding状态。
Blocking		
Listening		
Learning	Learning	如果不转发用户流量但是学习MAC地址，那么端口状态就是Learning状态。
Forwarding	Forwarding	如果既转发用户流量又学习MAC地址，那么端口状态就是Forwarding状态。

针对问题一：P/A机制（1）

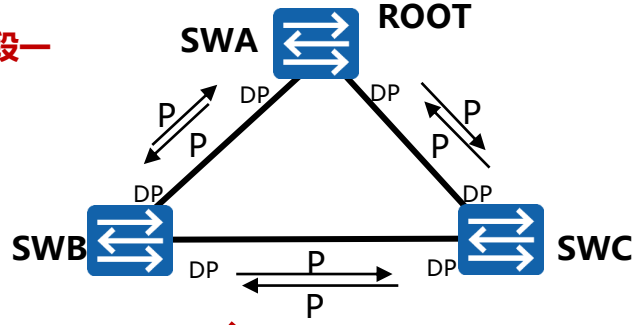
- P/A机制基本原理



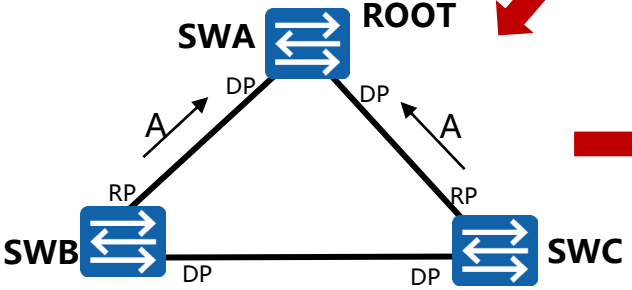
- 特点：由于有来回确认机制和同步变量机制，就无需依靠计时器来保障无环。

针对问题一：P/A机制（2）

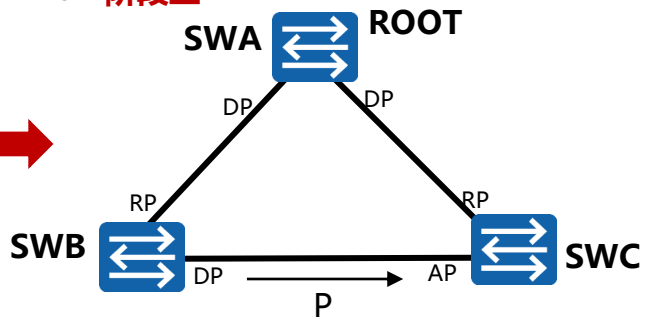
- 阶段一



- 阶段二



- 阶段三

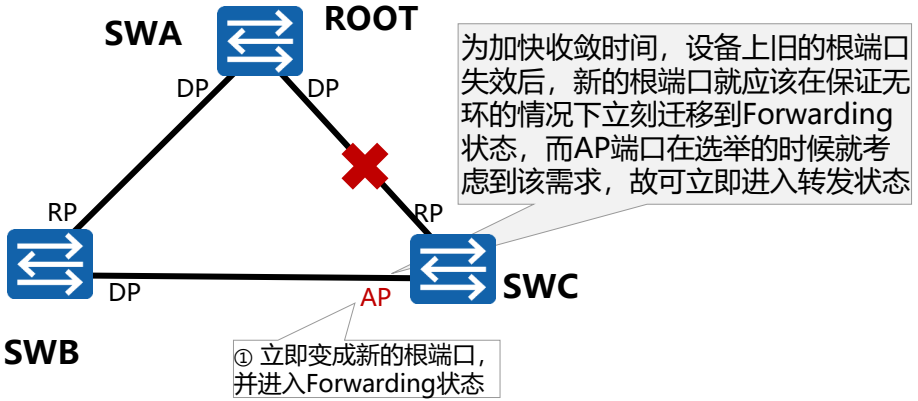


针对问题一：P/A机制（3）

- RSTP选举原理和STP本质上相同：选举根交换机-选举非根交换机上的根端口-选举指定端口-选举预备端口和备份端口。
- 但是RSTP在选举的过程中加入了“发起请求-回复同意”（P/A机制）这种确认机制，由于每个步骤有确认就不需要依赖计时器来保证网络拓扑无环才去转发，只需要考虑BPDU发送报文并计算无环拓扑的时间（一般都是秒级）。

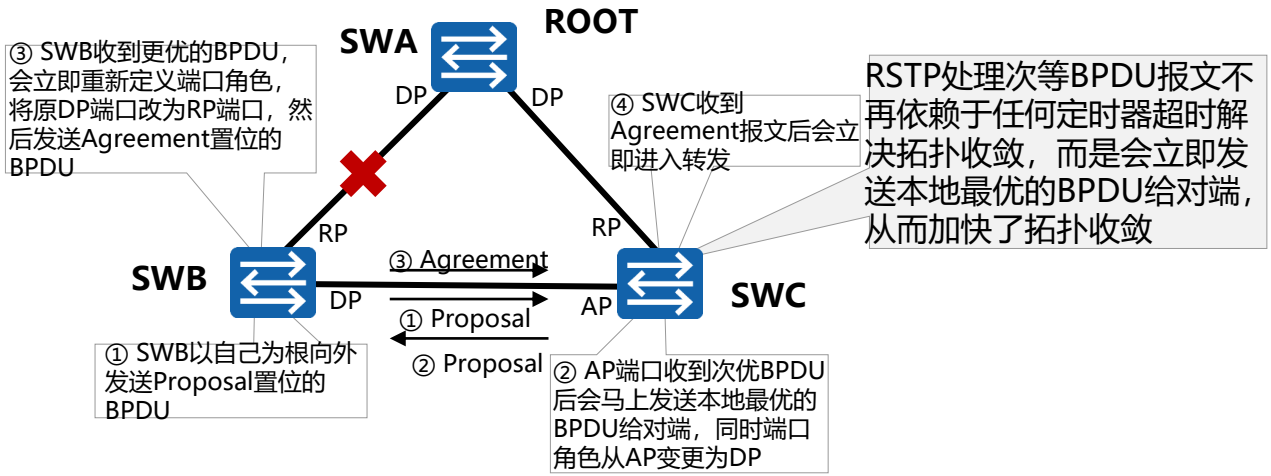
针对问题二：根端口快速切换机制

- SWC与SWA的直连链路down掉，其AP端口切换成RP端口并进入转发状态可在秒级时间内完成收敛：



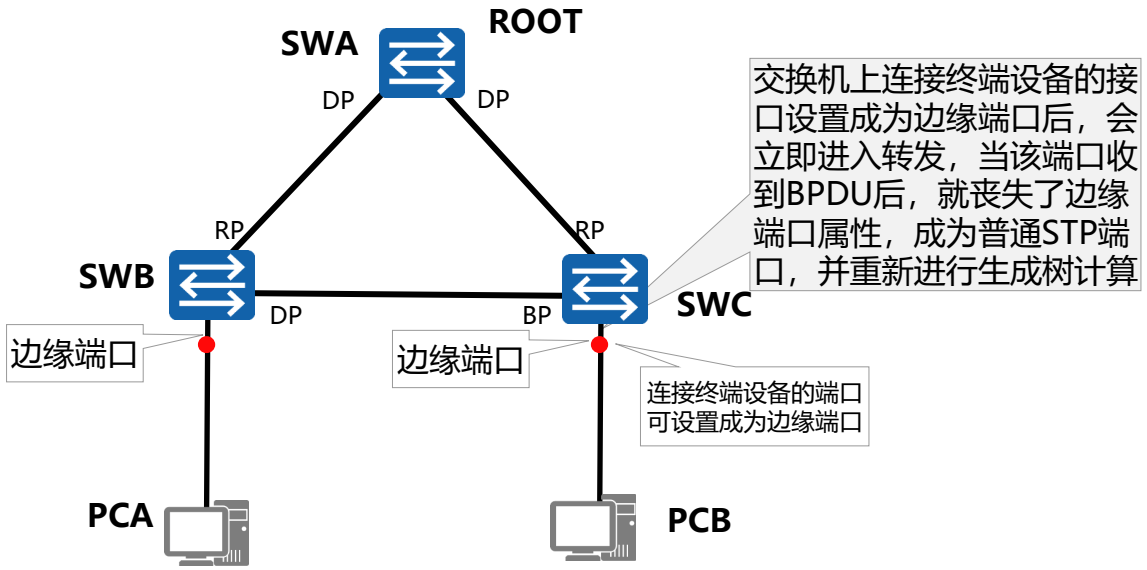
针对问题三：次等BPDU处理机制

- SWB与SWA的直连链路down掉，SWC的AP端口切换成DP端口并进入转发状态可在秒级时间内完成：



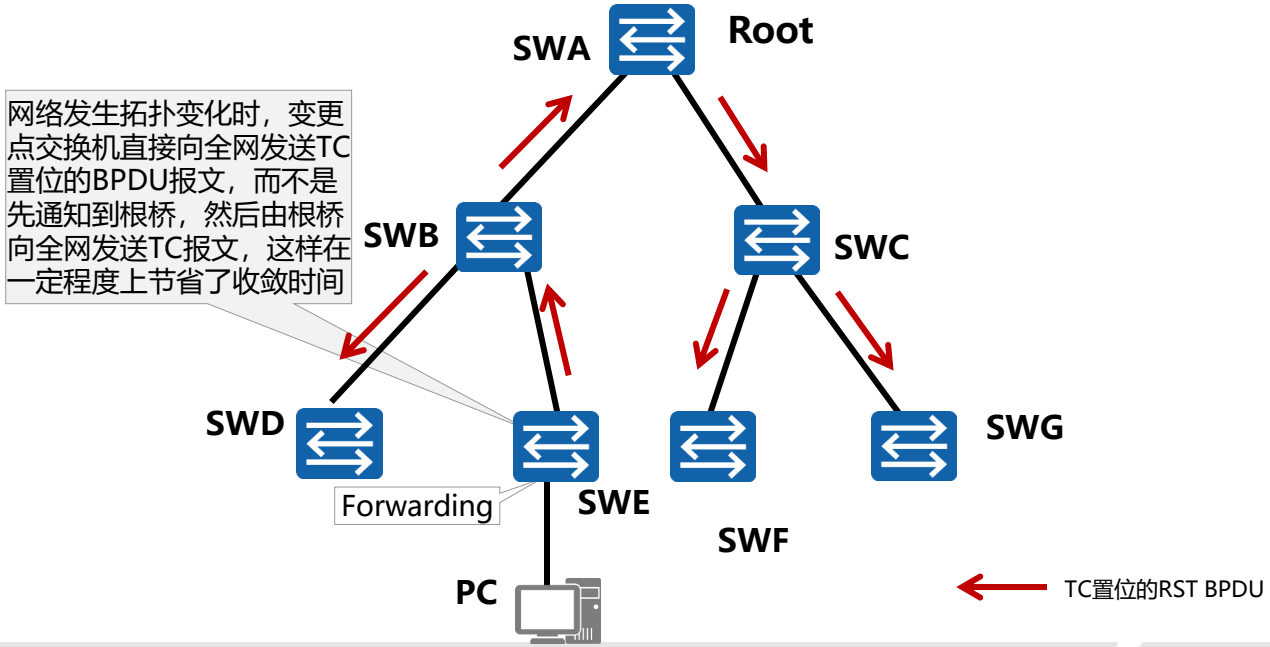
针对问题四：边缘端口的引入

- 在RSTP中，交换机连接终端的链路可立即进入转发状态：

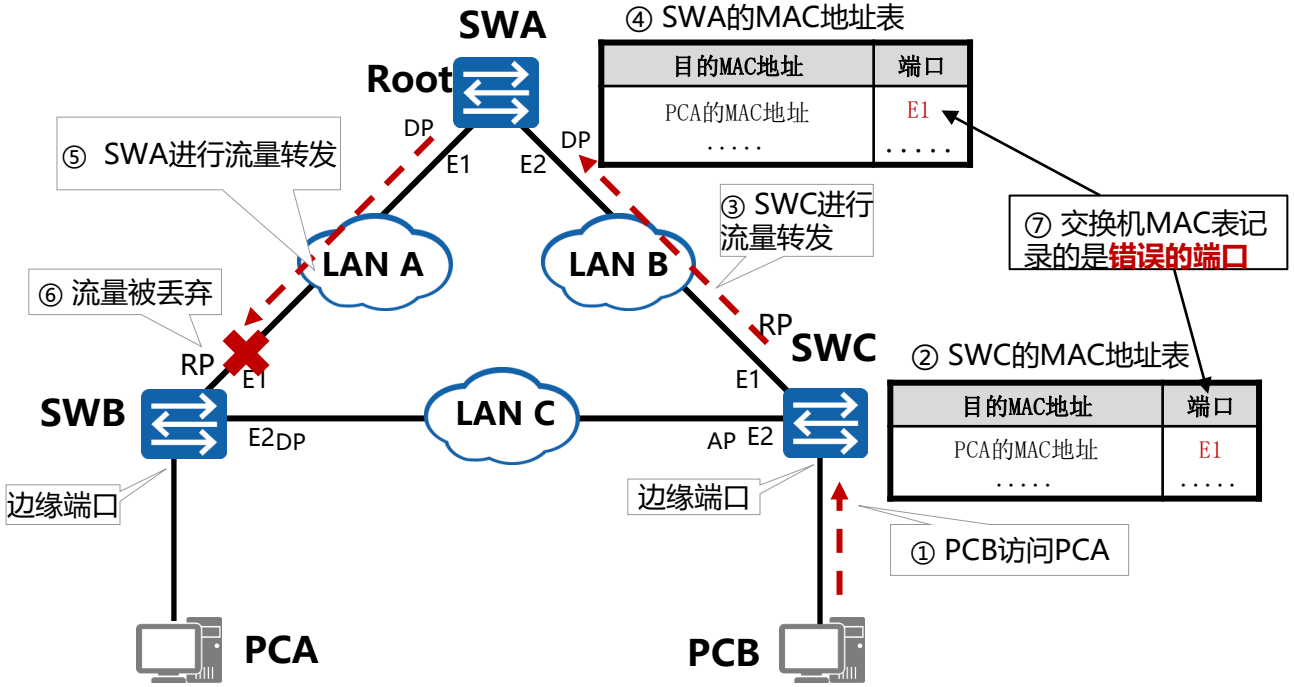


针对问题五：拓扑变更机制的优化

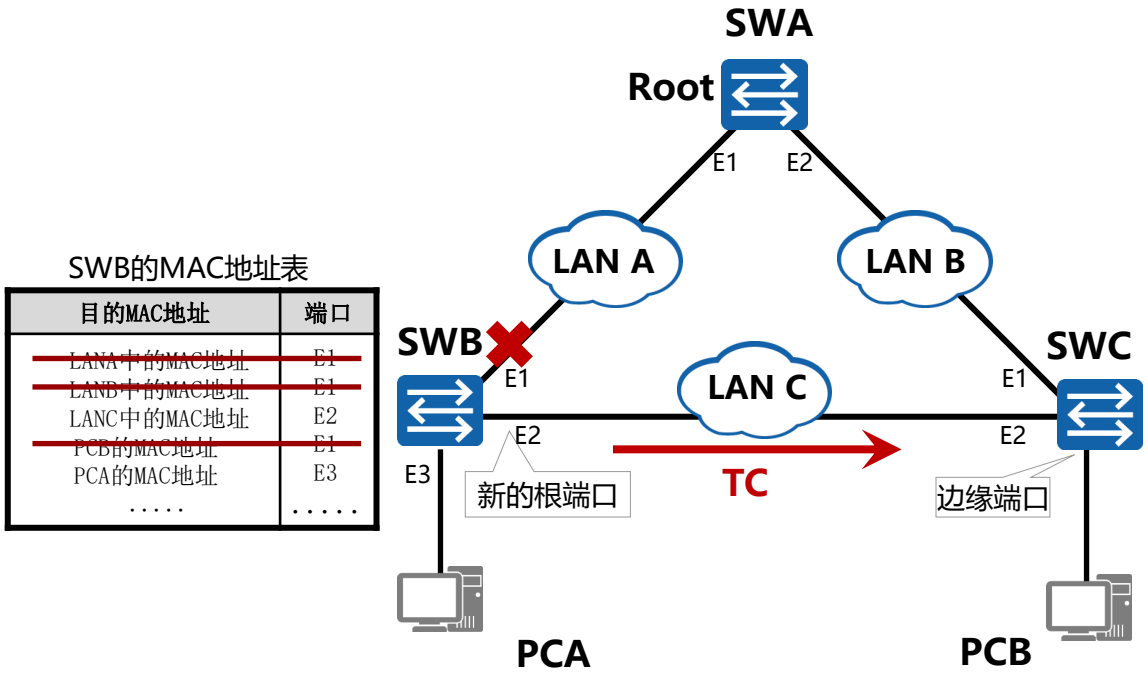
- 判断拓扑变化唯一标准：一个非边缘端口迁移到Forwarding状态。



拓扑变化引发的问题



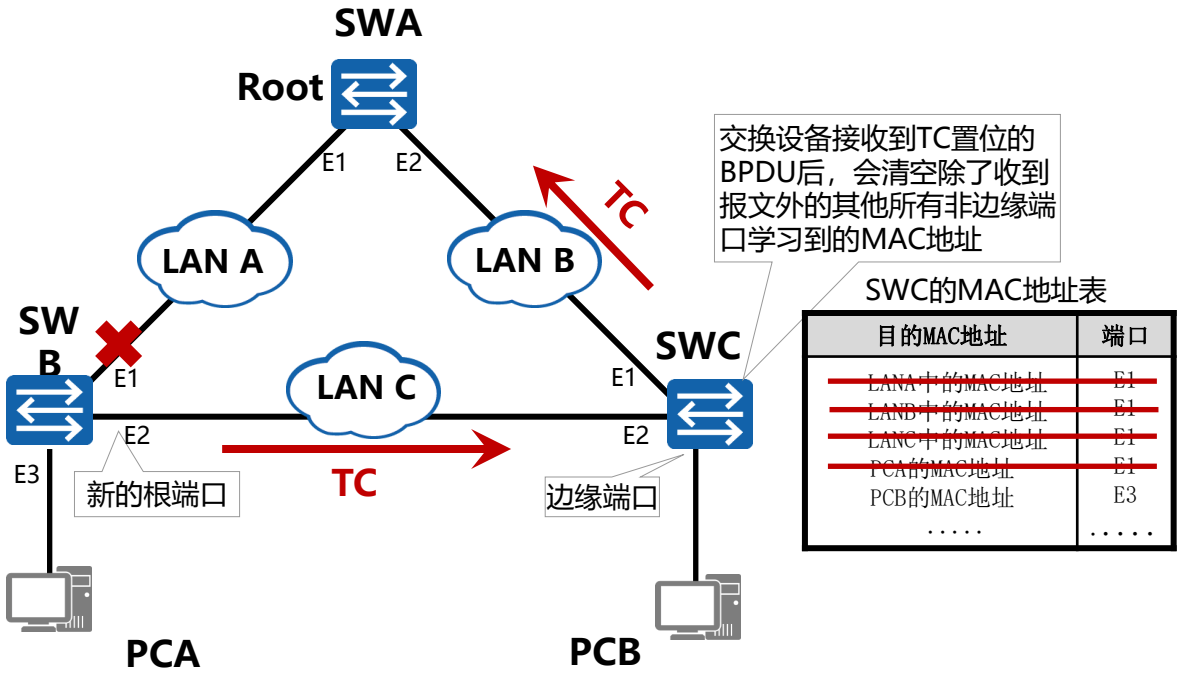
拓扑变化处理（1）



SWB的MAC地址表

目的MAC地址	端口
~~LANA中的MAC地址~~	~~E1~~
~~LANB中的MAC地址~~	~~E1~~
LANC中的MAC地址	E2
~~PCB的MAC地址~~	~~E1~~
PCA的MAC地址	E3
.....	.....

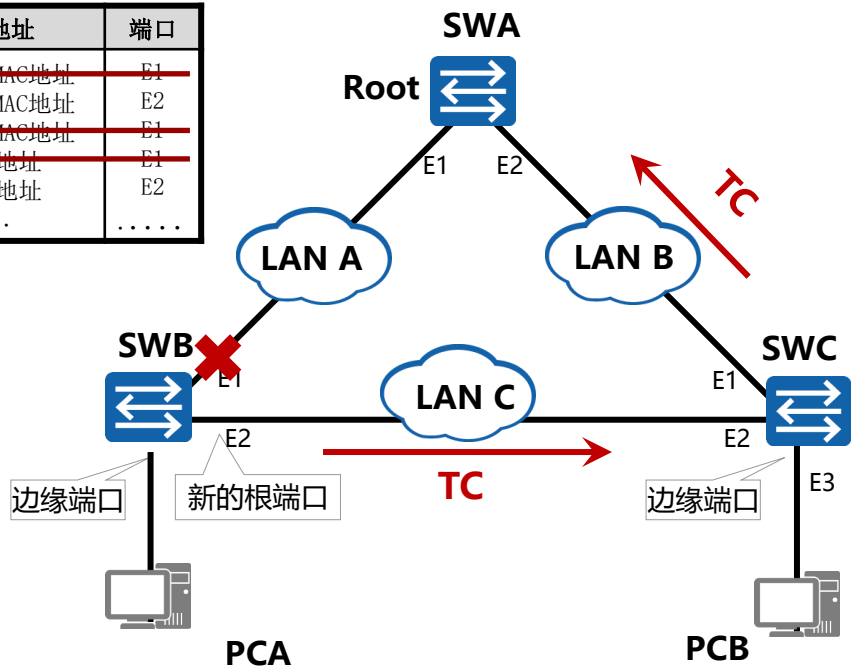
拓扑变化处理 (2)



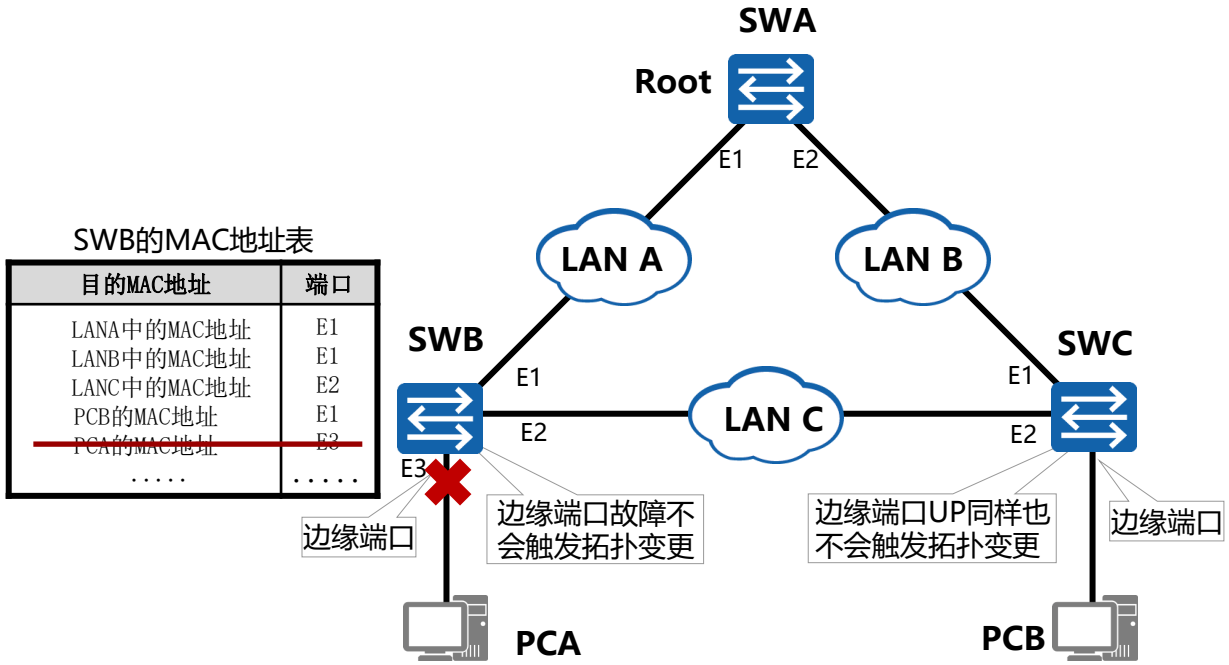
拓扑变化处理（3）

SWA的MAC地址表

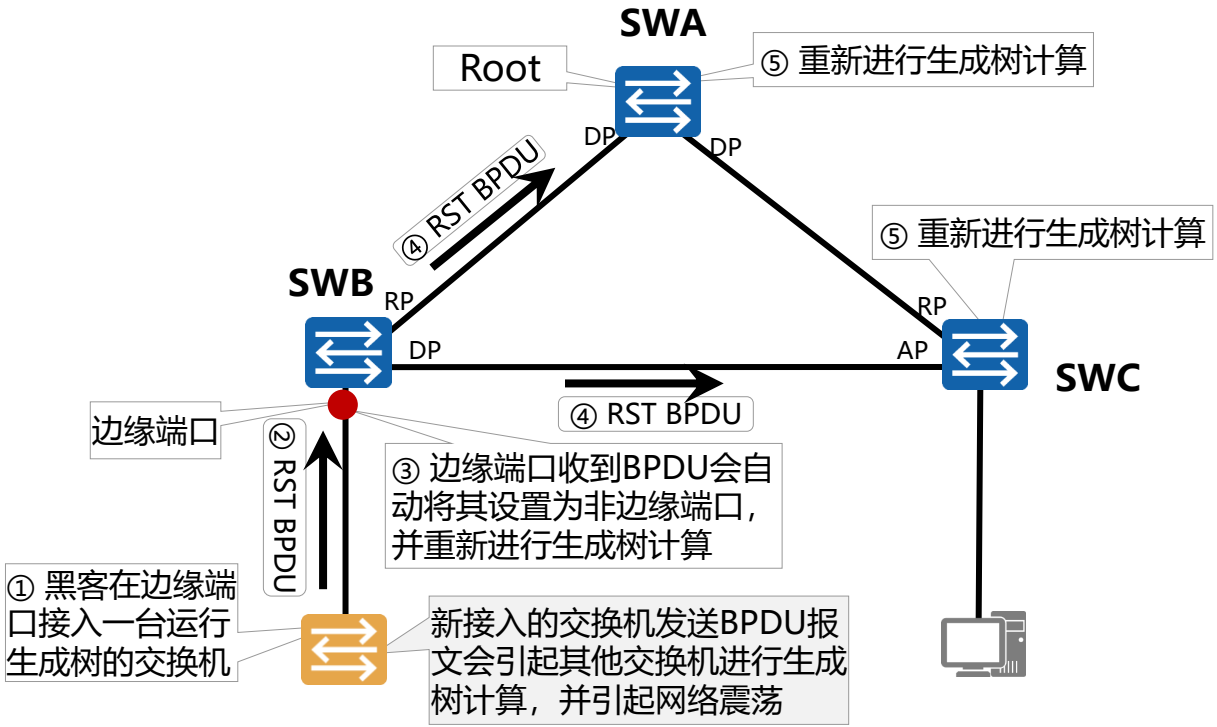
目的MAC地址	端口
~~LANA中的MAC地址~~	~~E1~~
LANB中的MAC地址	E2
~~LANC中的MAC地址~~	~~E1~~
~~PCA的MAC地址~~	~~E1~~
PCB的MAC地址	E2
.....	.....



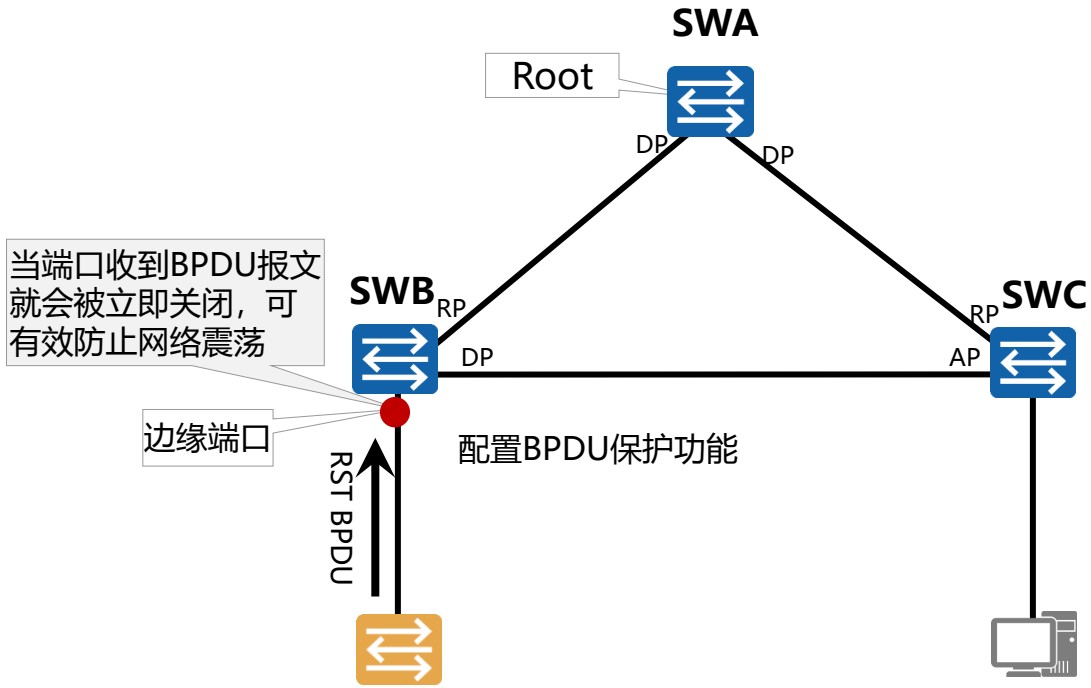
拓扑变化处理（4）



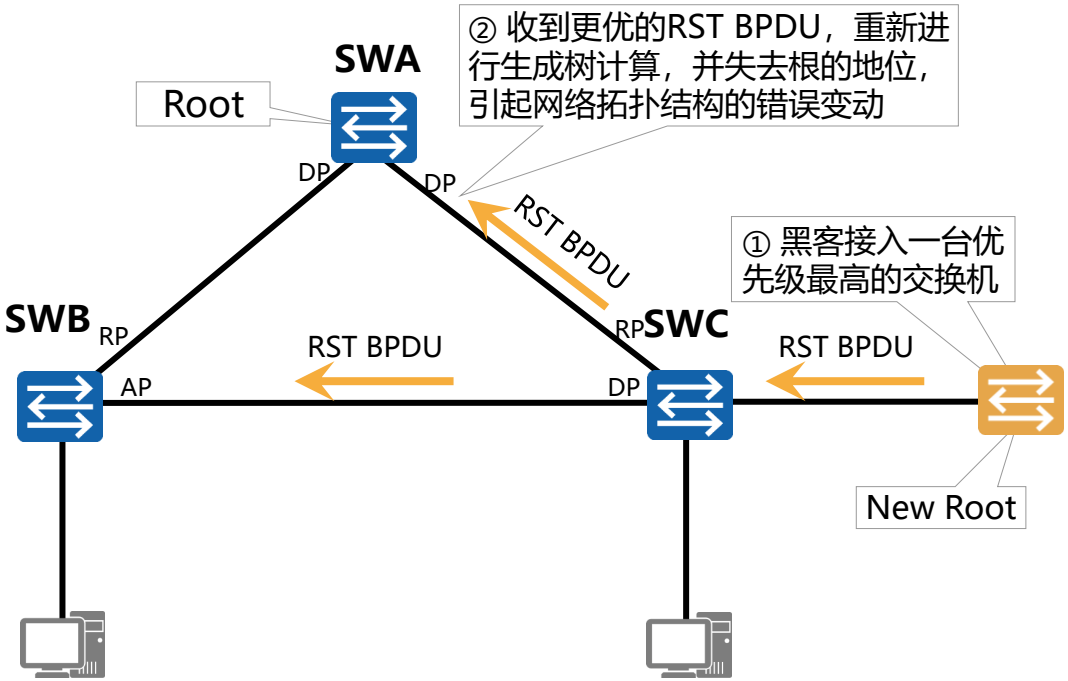
BPDU保护（1）



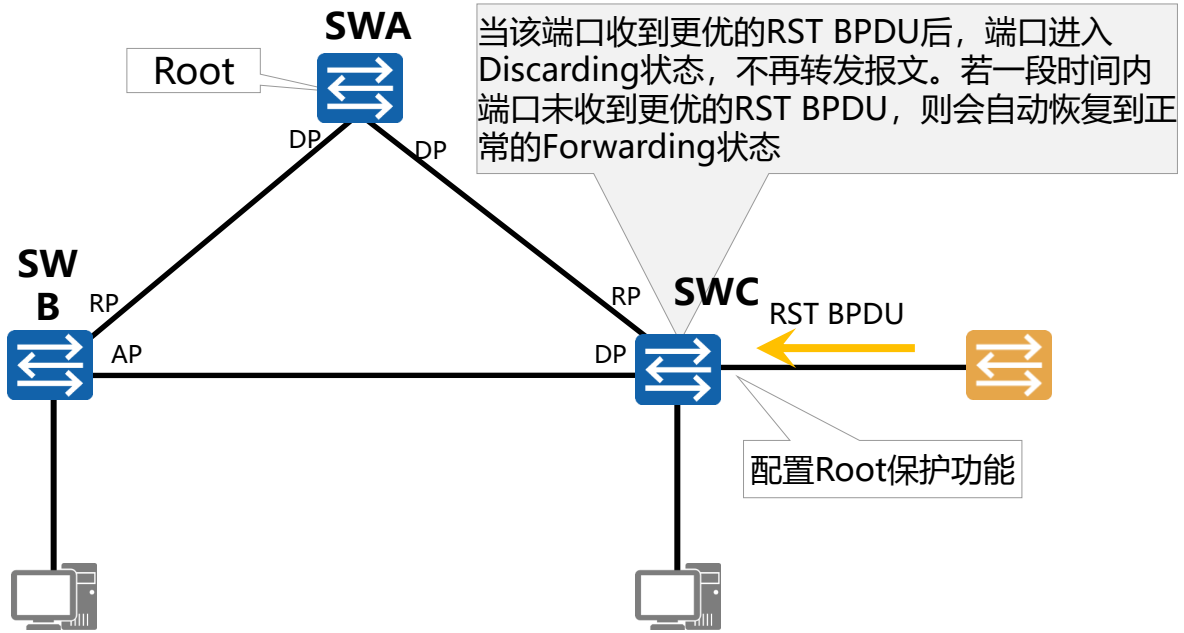
BPDU保护（2）



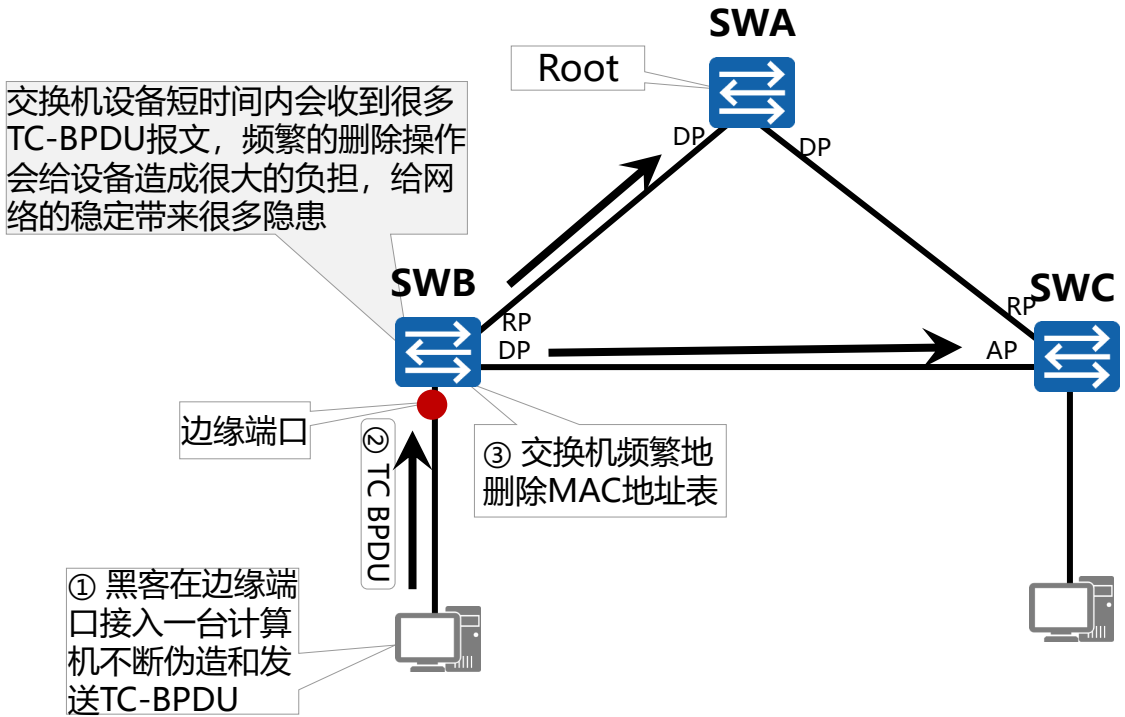
根保护（1）



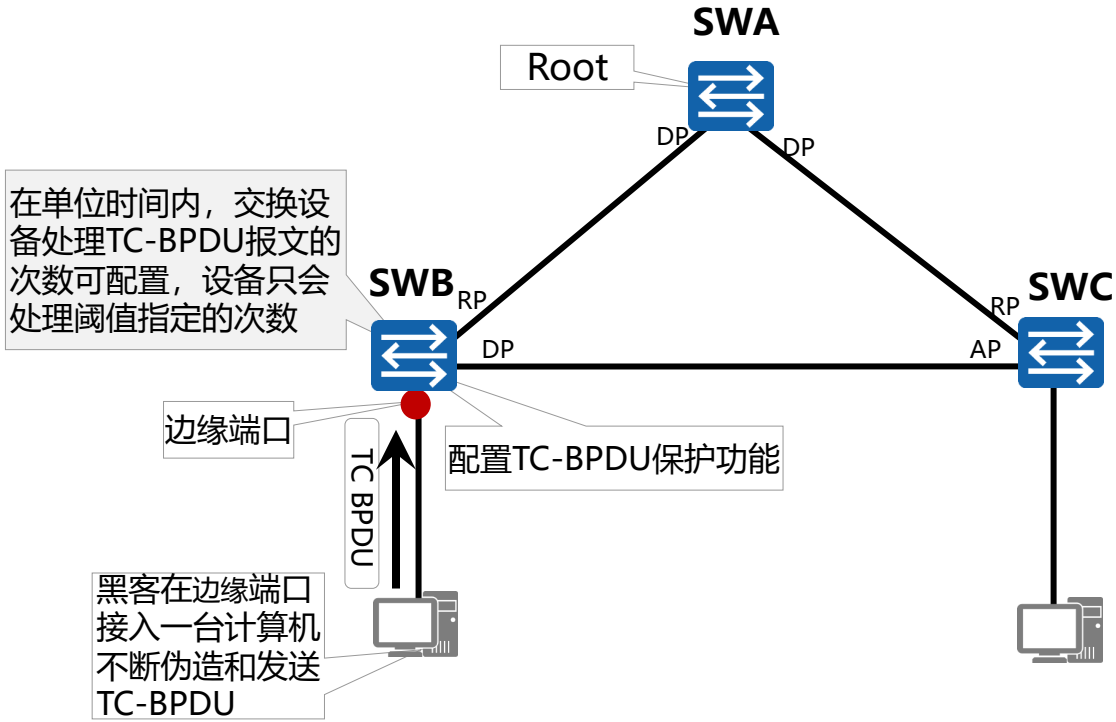
根保护（2）



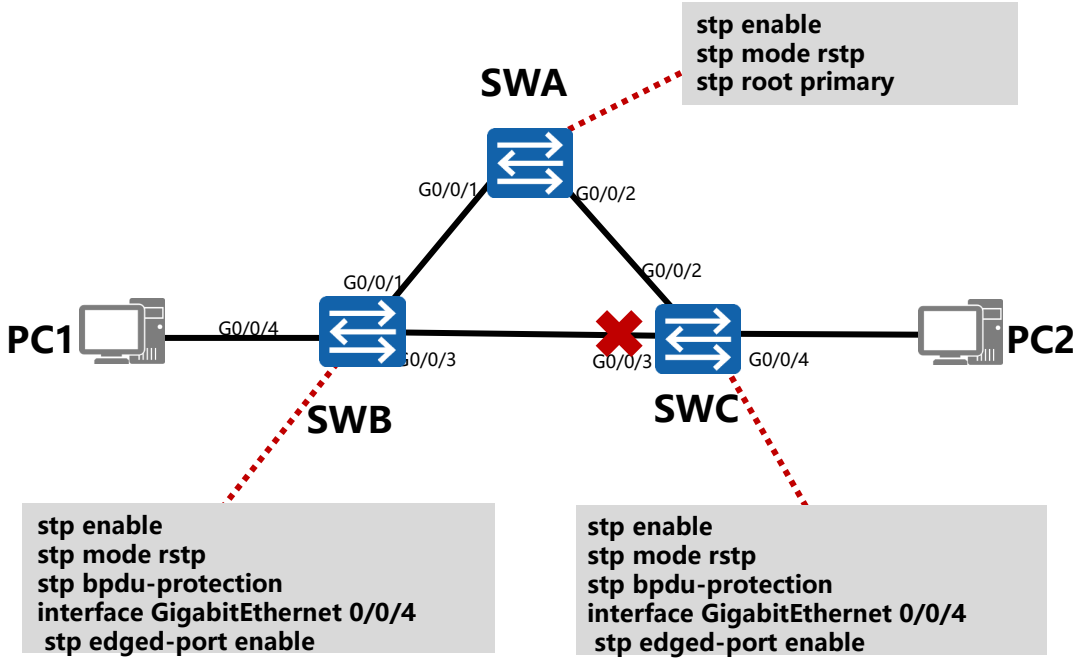
TC-BPDU泛洪保护（1）



TC-BPDU泛洪保护（2）

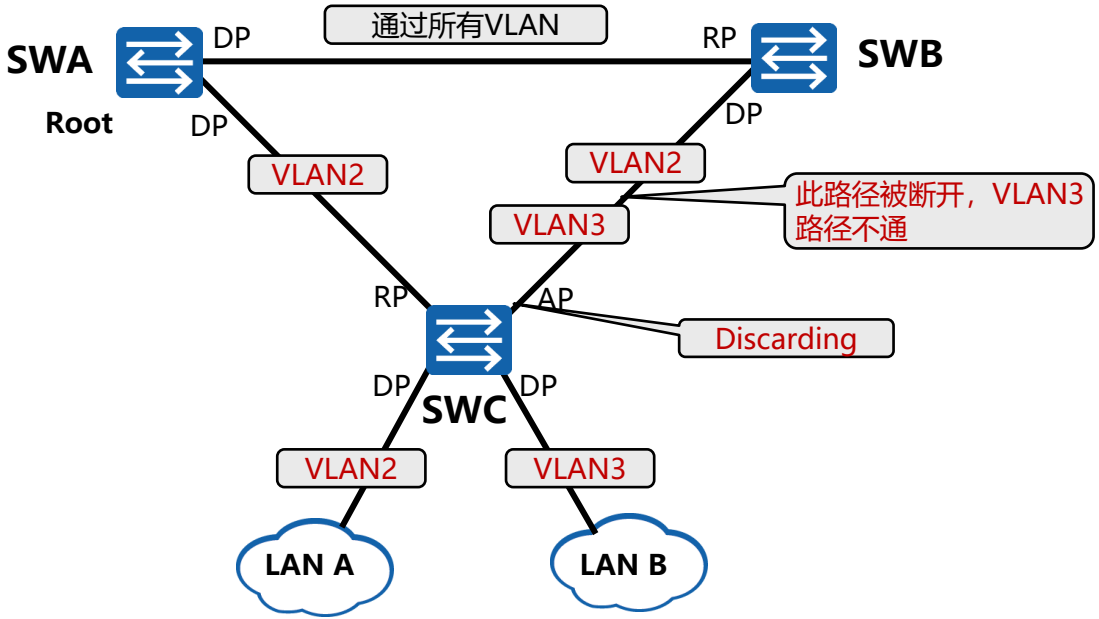


RSTP配置实现

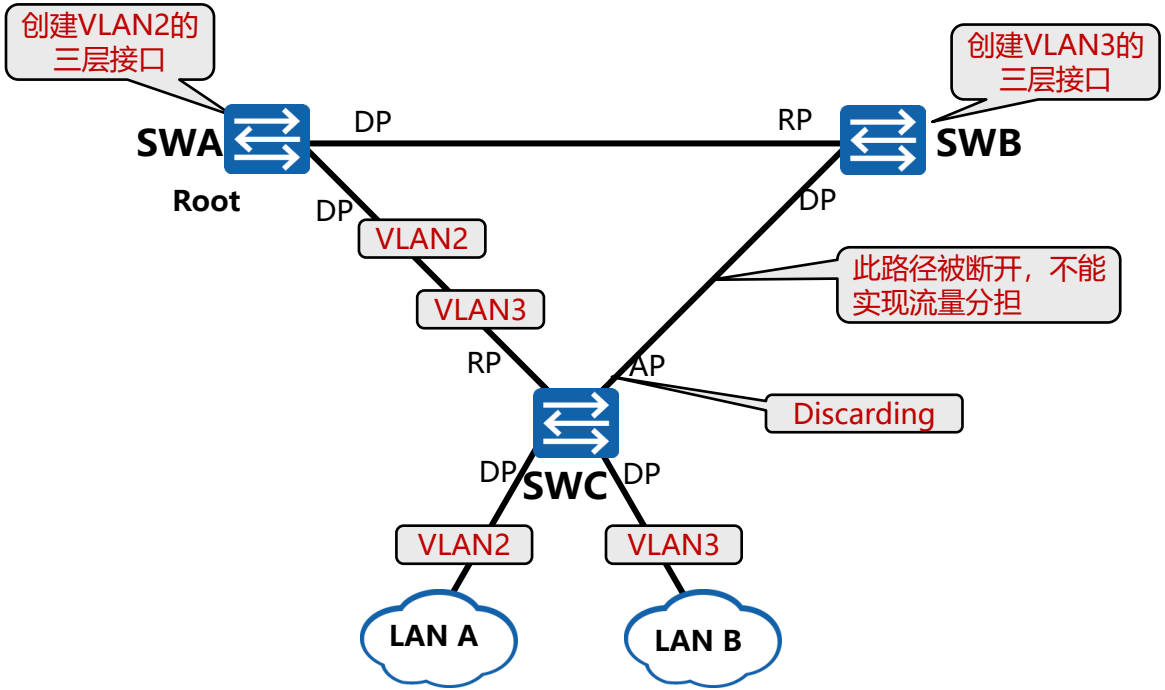


RSTP配置实现

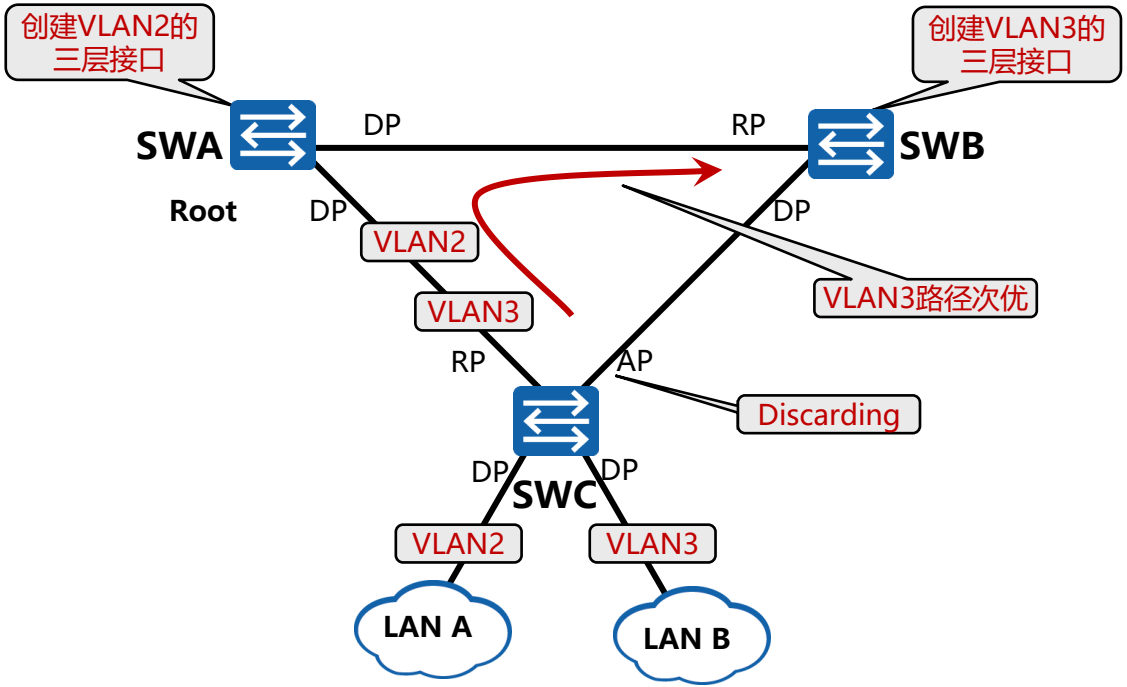
单生成树的弊端 – 部分VLAN路径不通



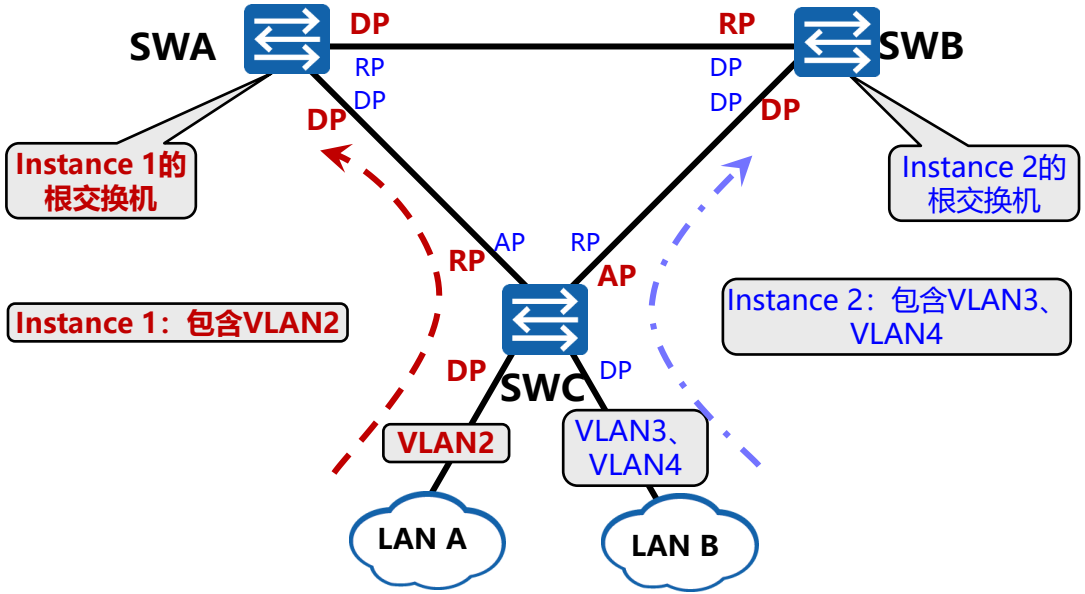
单生成树的弊端 – 无法实现流量分担



单生成树的弊端 – 次优二层路径



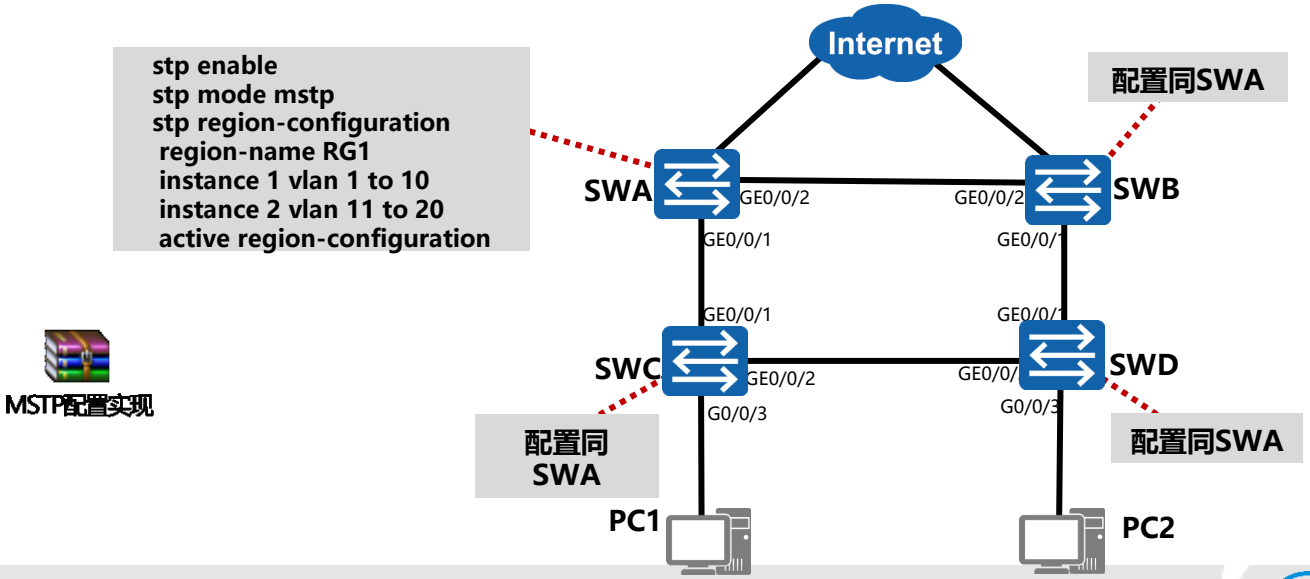
多生成树实例解决单生成树弊端



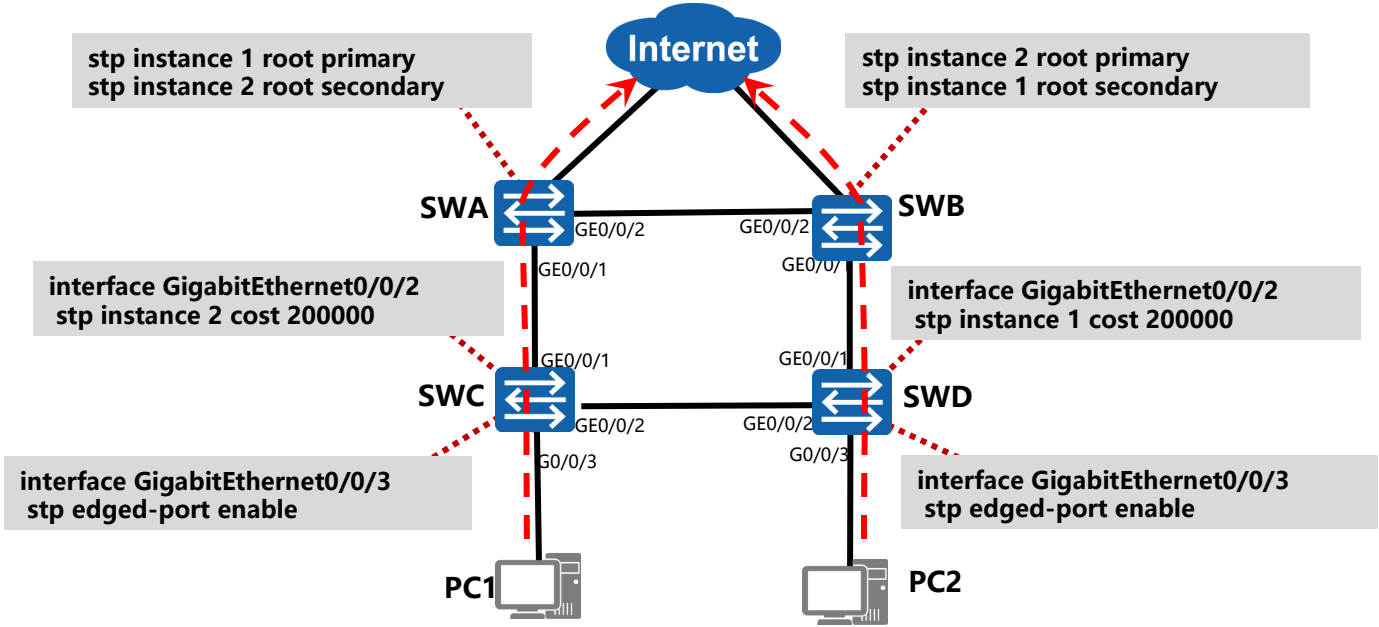
- MST域内可以生成多棵生成树，每棵生成树都称为一个MSTI。MSTI之间彼此独立，且每个MSTI的计算过程基本与RSTP的计算过程相同。

MSTP配置实现（1）

- 为实现分别属于不同VLAN的PC访问Internet的流量能够进行负载均衡，可采用MSTP来实现，VLAN1~10为一组，VLAN11~20为另一组。



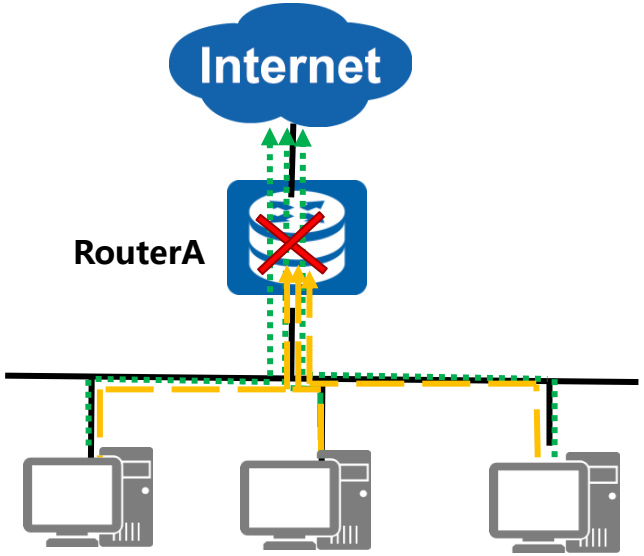
MSTP配置实现（2）



网关冗余

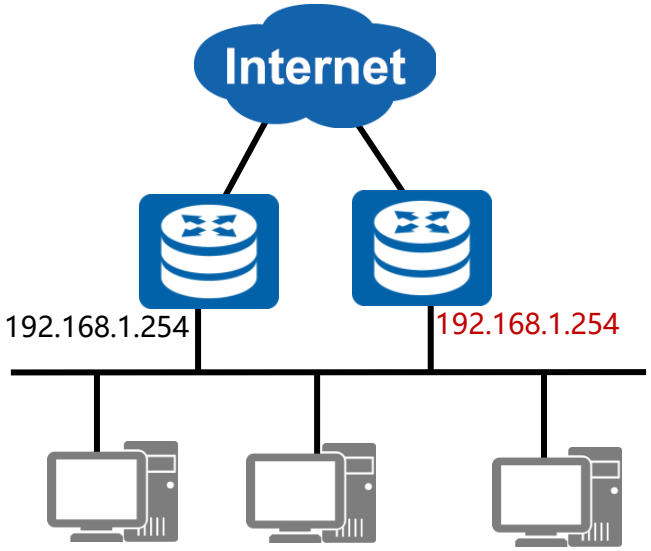
- 局域网中的用户终端通常采用配置一个默认网关的形式访问外部网络，如果此时默认网关设备发生故障，将中断所有用户终端的网络访问，这很可能会给用户带来不可预计的损失，所以可以通过部署多个网关的方式来解决单点故障问题，那么如何让多个网关能够协同工作但又不会互相冲突就成了最迫切需要解决的问题。
- 于是VRRP应运而生，它既可以实现网关的备份，又能解决多个网关之间互相冲突的问题。那么VRRP的工作原理是如何实现的？在网络中又该如何配置呢？

单网关的缺陷



- 当网关路由器RouterA出现故障时，本网段内以该设备为网关的主机都不能与Internet进行通信。

多网关存在的问题



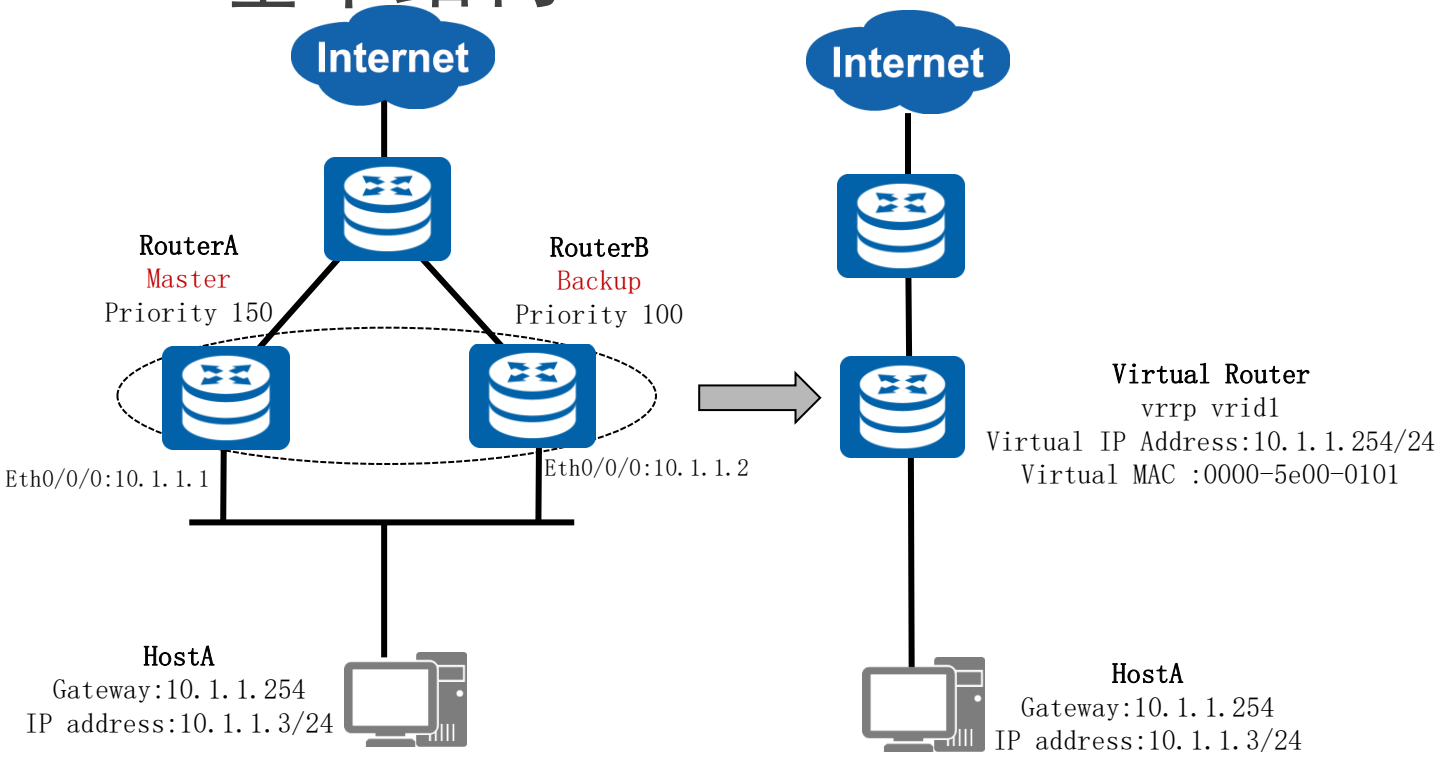
- 通过部署多网关的方式实现网关的备份。
- 但多网关可能会出现一些问题：网关间IP地址冲突；主机会频繁切换网络出口。

VRRP基本概述

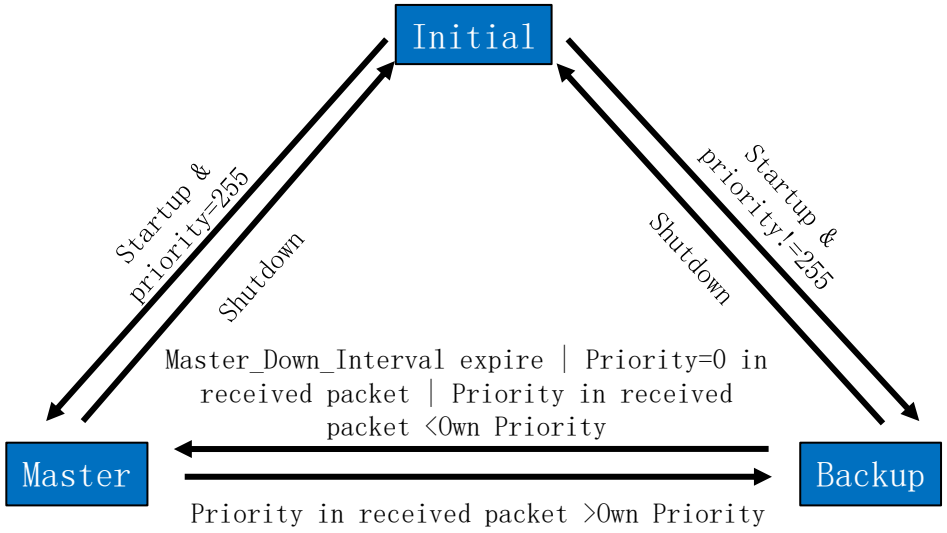
- VRRP能够在不改变组网的情况下，将多台路由器虚拟成一个虚拟路由器，通过配置虚拟路由器的IP地址为默认网关，实现网关的备份。
- 协议版本：VRRPv2（常用）和VRRPv3：
- VRRPv2仅适用于IPv4网络，VRRPv3适用于IPv4和IPv6两种网络。
- VRRP协议报文：

  Advertisement报文：其目的IP地址是224.0.0.18，目的 MAC地址是01-00-5e-00-00-12，协议号是112。

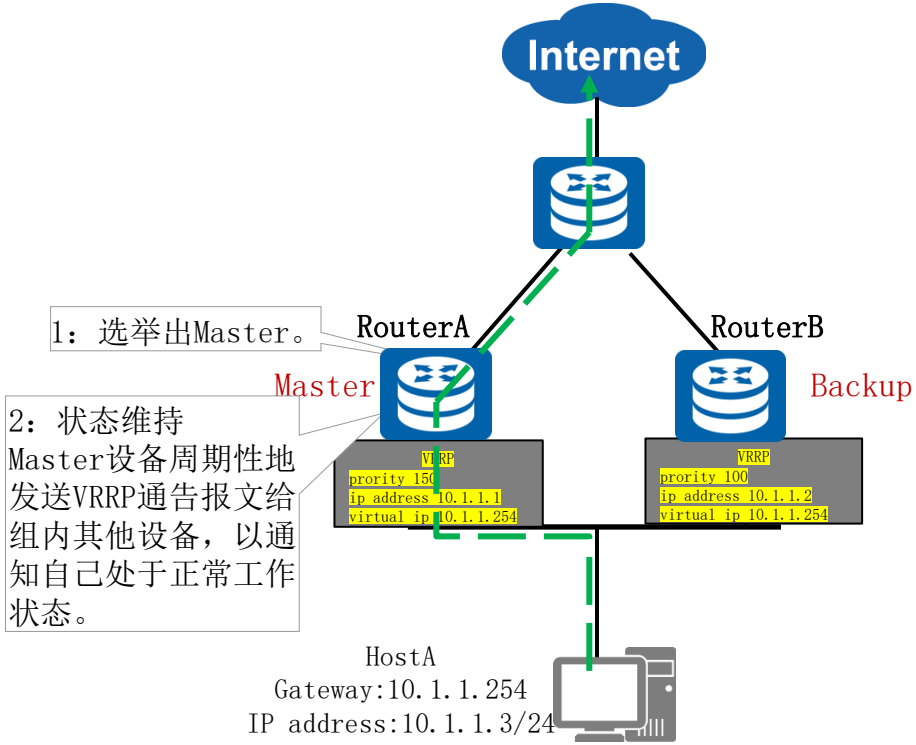
VRRP基本结构



状态机

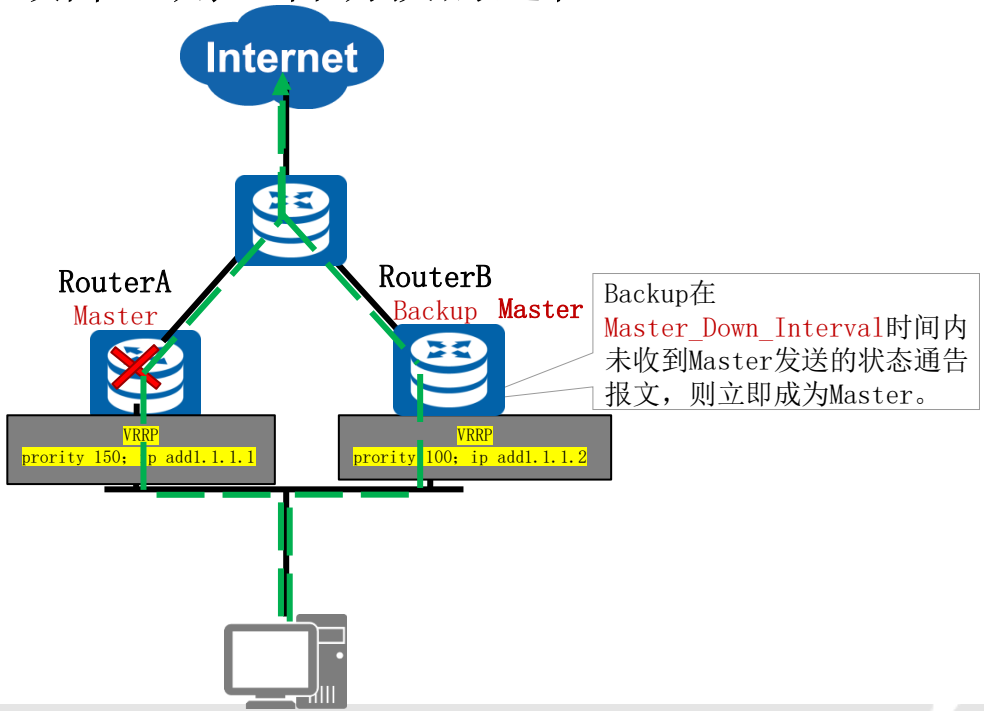


VRRP主备备份工作过程



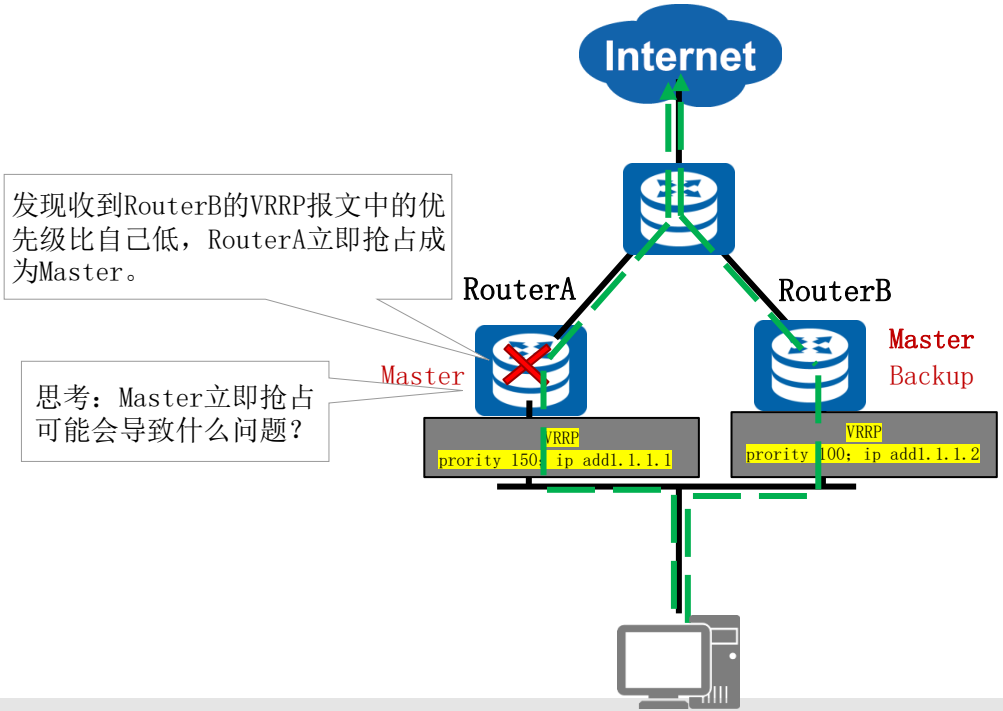
VRRP主备路由器切换过程（1）

- 如果Master发生故障，则主备切换的过程：

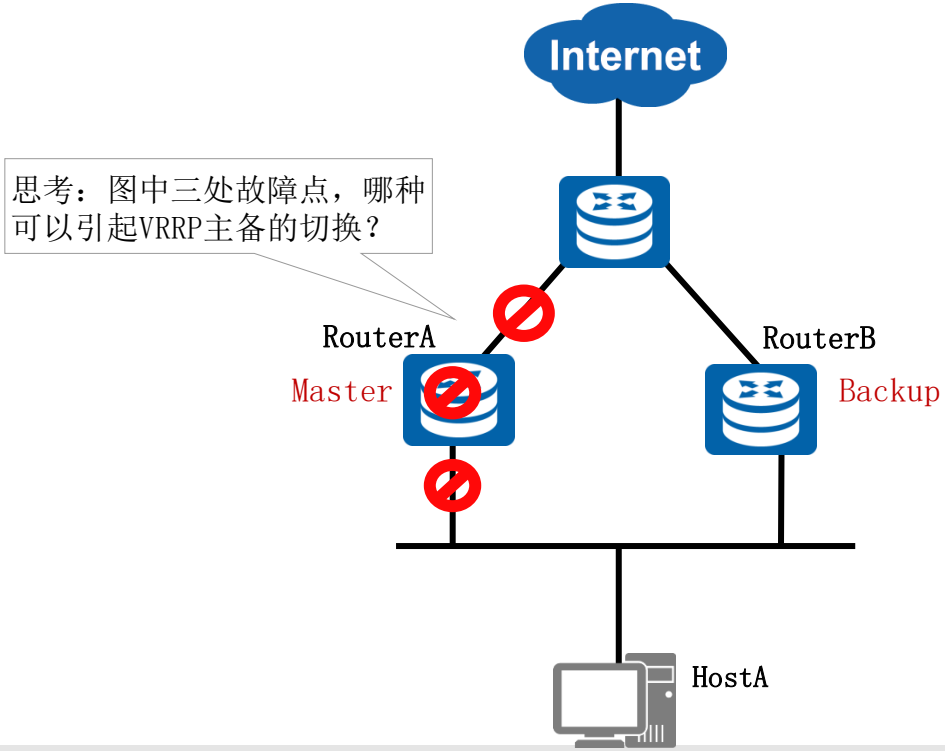


VRRP主备路由器切换过程（2）

- 如果原Master故障恢复，则主备回切的过程：

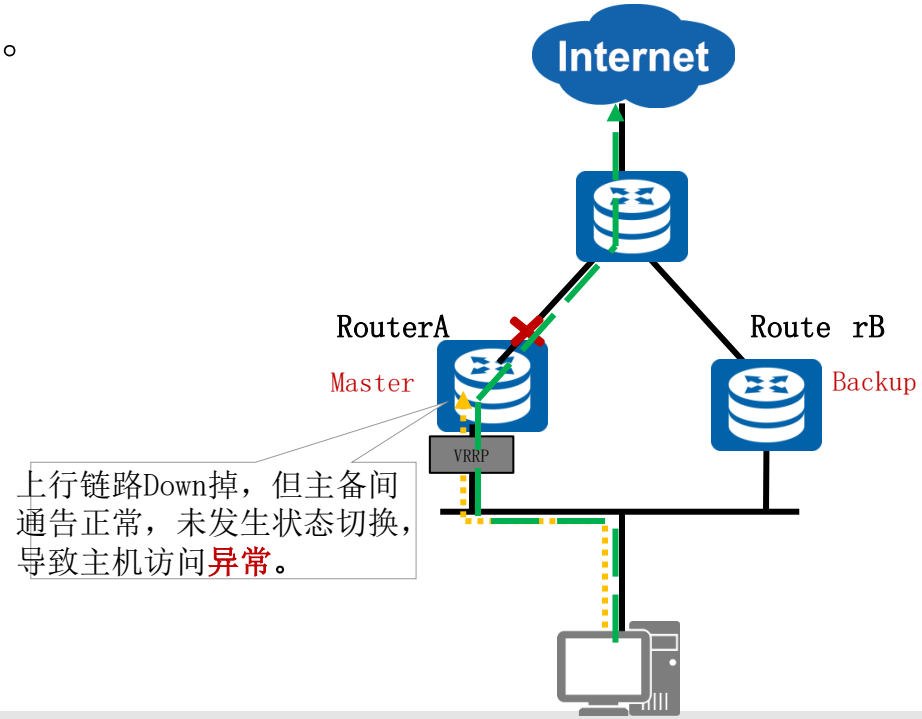


VRRP故障场景

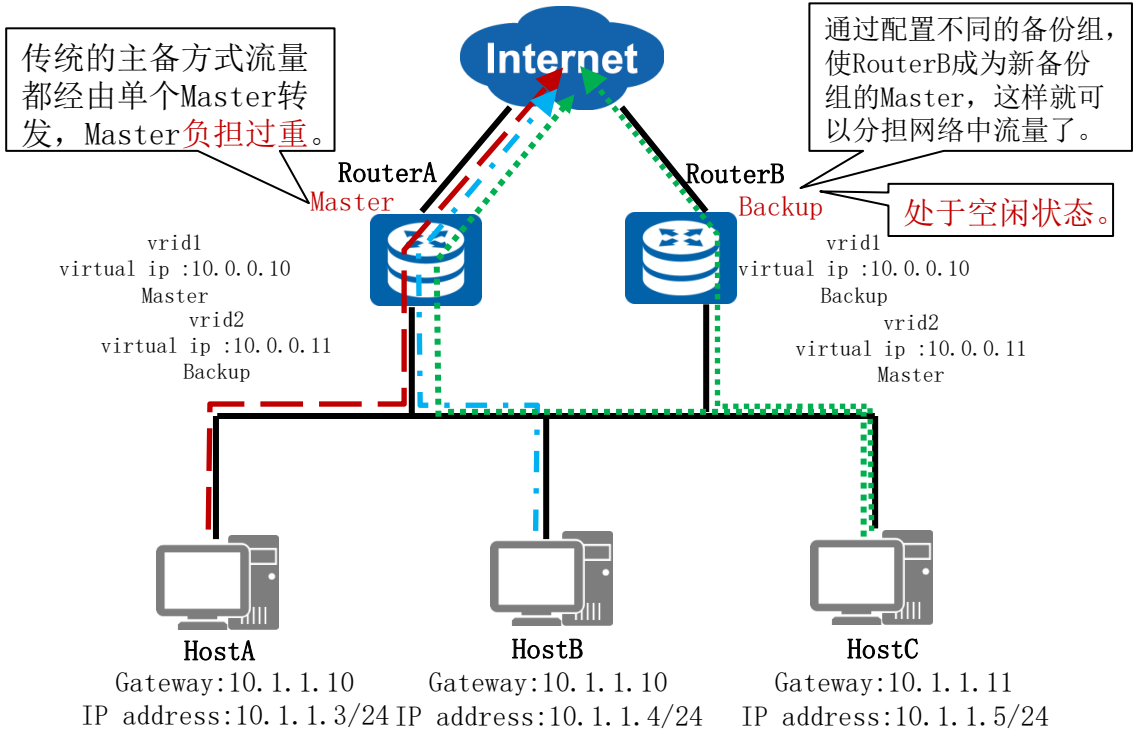


VRRP联动功能

- 解决方法：利用VRRP的联动功能监视上行接口或链路故障，主动进行主备切换。

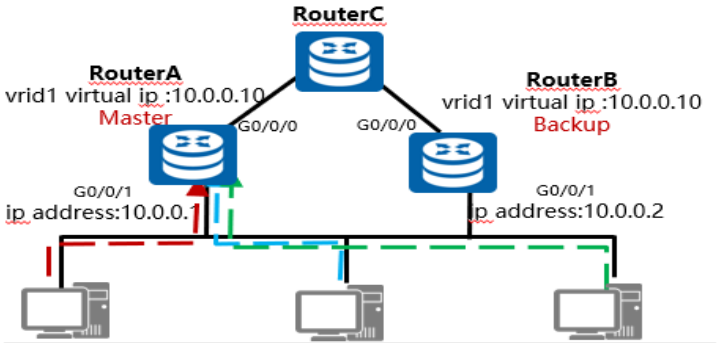


VRRP负载分担工作过程



VRRP配置实现

主备备份方式



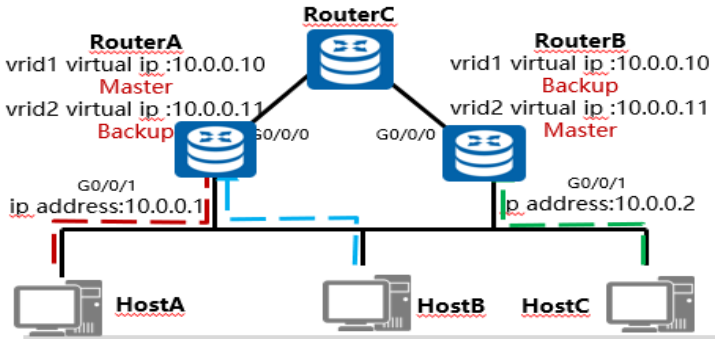
RouterA配置:

```
interface GigabitEthernet0/0/1
 ip address 10.0.0.1 255.255.255.0
 vrrp vrid 1 virtual-ip 10.0.0.10
 vrrp vrid 1 priority 120
 vrrp vrid 1 preempt-mode timer delay 20
 vrrp vrid 1 track interface GigabitEthernet0/0/0 reduce 30
```

RouterB配置:

```
interface GigabitEthernet0/0/1
 ip address 10.0.0.2 255.255.255.0
 vrrp vrid 1 virtual-ip 10.0.0.10
```

负载分担方式



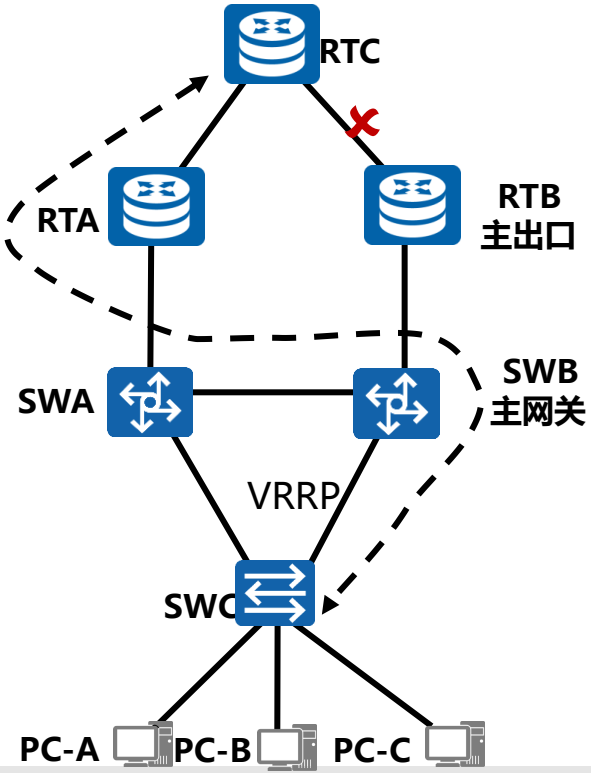
RouterA配置:

```
interface GigabitEthernet0/0/1
 ip address 10.0.0.1 255.255.255.0
 vrrp vrid 1 virtual-ip 10.0.0.10
 vrrp vrid 1 priority 120
 vrrp vrid 1 preempt-mode timer delay 20
 vrrp vrid 1 track interface GigabitEthernet0/0/0 reduce 30
 vrrp vrid 2 virtual-ip 10.0.0.11
```

RouterB配置:

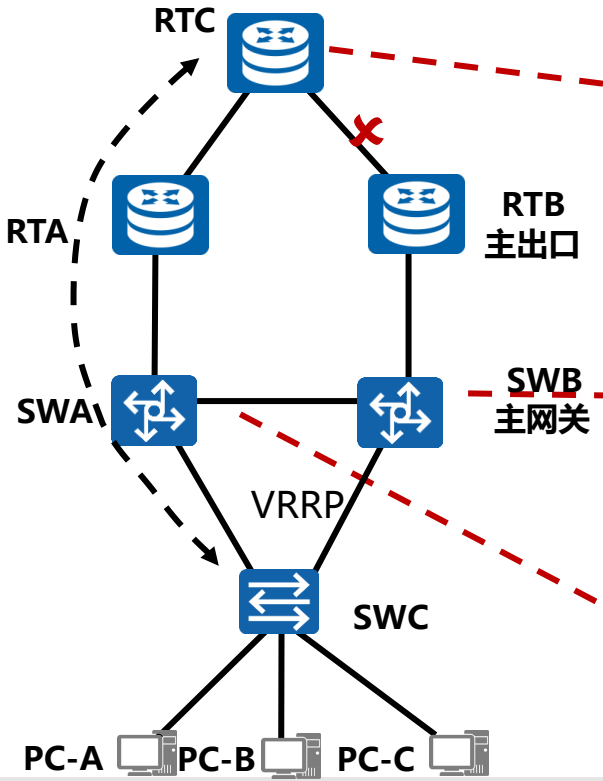
```
interface GigabitEthernet0/0/1
 ip address 10.0.0.2 255.255.255.0
 vrrp vrid 1 virtual-ip 10.0.0.10
 vrrp vrid 2 virtual-ip 10.0.0.11
 vrrp vrid 2 priority 120
 vrrp vrid 2 preempt-mode timer delay 20
 vrrp vrid 2 track interface GigabitEthernet0/0/0 reduce 30
```

BFD与VRRP联动配置需求



- 场景需求
  - 如图，SWA和SWB为VRRP备份组，SWB为主用。当RTB与RTC的互联链路出现故障时，SWB能够快速感知并切换为备用网关状态，且SWA成为主用网关。

BFD与VRRP联动配置实现



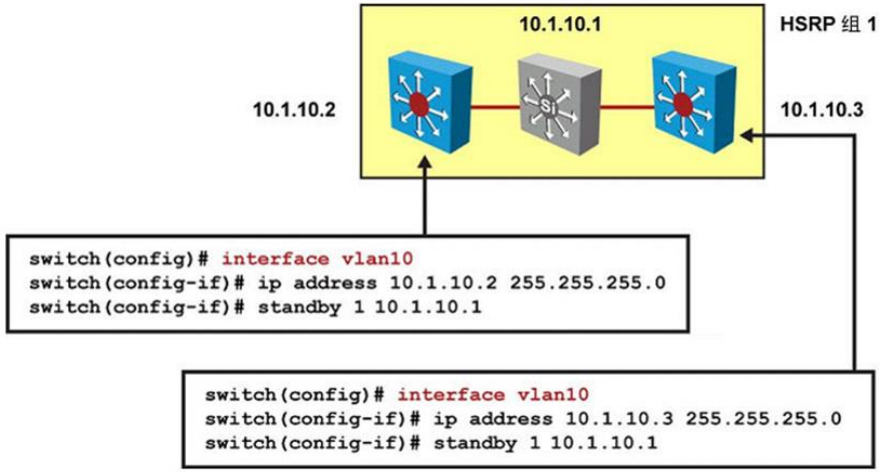

```
#
bfd
#
bfd 1 bind peer-ip 10.0.24.2 source-ip 10.0.45.5 auto
commit
```

```
#
bfd
#
bfd 1 bind peer-ip 10.0.45.5 source-ip 10.0.24.2 auto
commit
#
interface Vlanif100
 ip address 10.0.12.2 255.255.255.0
 vrrp vrid 1 virtual-ip 10.0.12.254
 vrrp vrid 1 priority 200
 vrrp vrid 1 track bfd-session session-   name 1 reduced 100
```

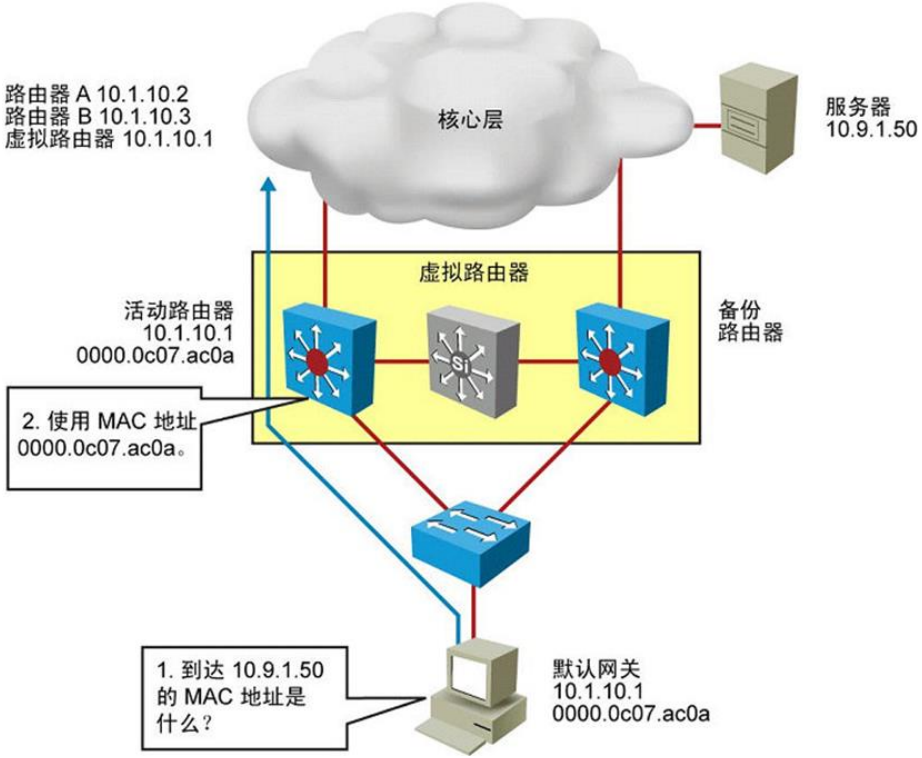
```
#
interface Vlanif100
 ip address 10.0.12.1 255.255.255.0
 vrrp vrid 1 virtual-ip 10.0.12.254
```

HSRP配置

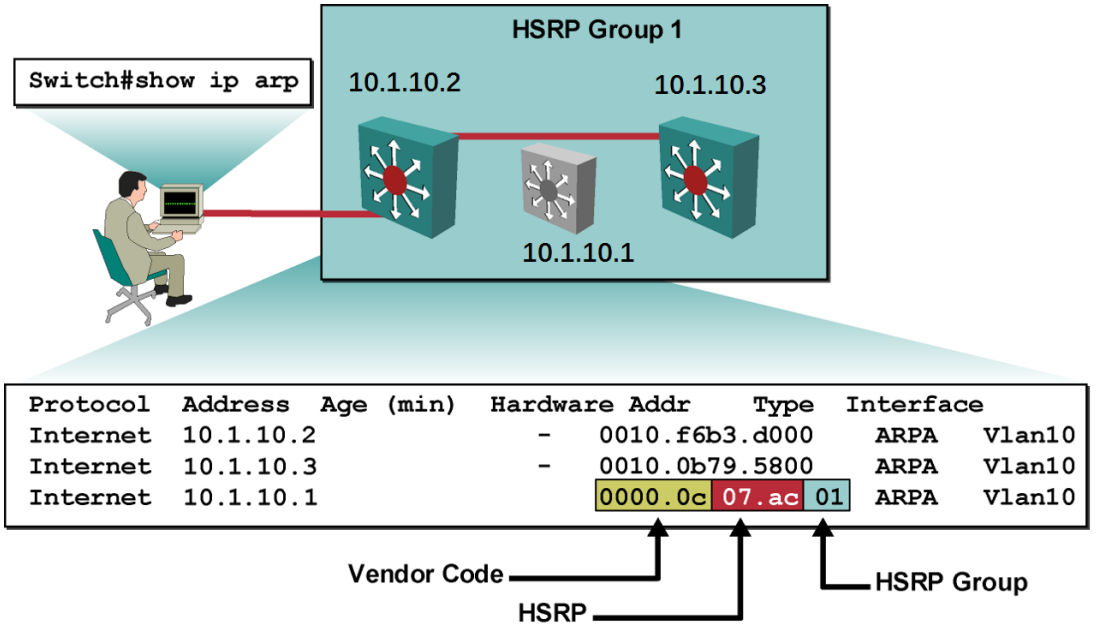
- 备份组(Standby Group)
  - 用于模拟一台虚拟路由器的一组HSRP设备
- 接口上启用HSRP后将自动禁用ICMP重定向



Active路由器转发数据

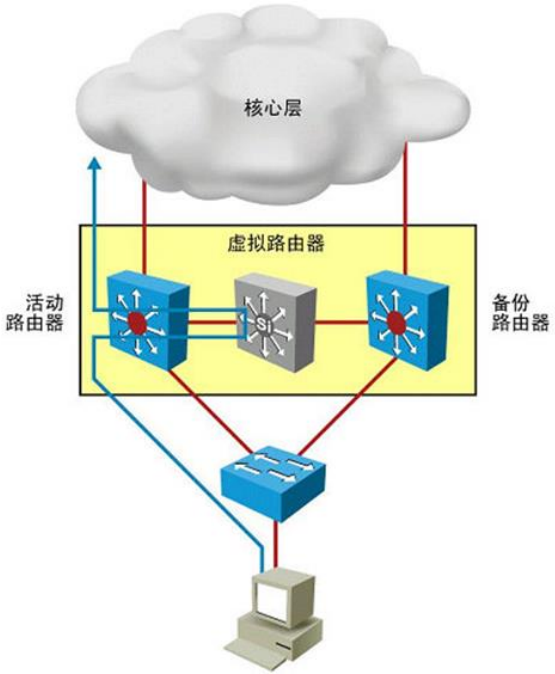


虚拟路由器的MAC地址



Active和Standby路由器

- Active路由器
  - 响应对虚拟路由器IP地址的ARP请求，使用虚拟路由器的MAC地址进行响应
  - 负责虚拟路由器的报文转发
  - 发送Hello消息
  - 知道虚拟路由器的IP地址
- Standby路由器
  - 监听周期性的Hello消息
  - 发送Hello消息
  - 若没有从Active路由器收到Hello消息则成为Active路由器

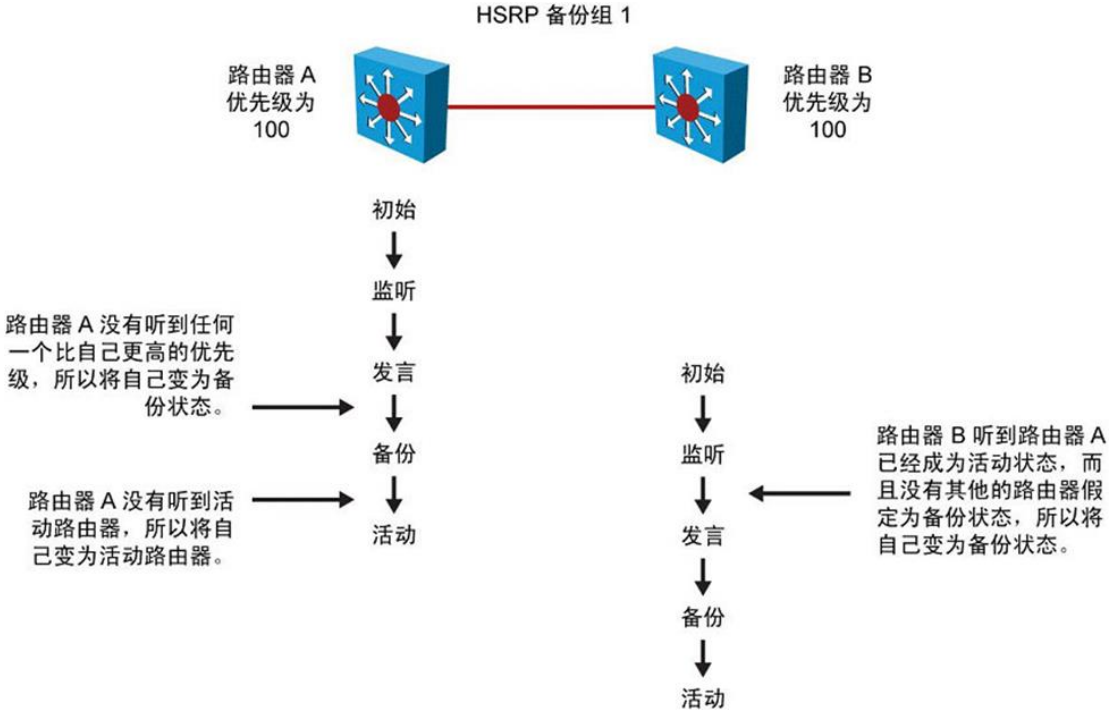


HSRP状态

- 一台HSRP路由器可以处于以下5个状态之一。

状态	描述
Initial	初始状态；配置变化时的状态或接口刚刚up时的状态
Listen	路由器知道虚拟IP地址；它正在监听来自其他路由器的Hello消息
Speak	路由器发送周期性的Hello消息，参与active或standby路由器的选举
Standby	路由器作为下一个active路由器的候选，路由器发送周期性的Hello消息
Active	路由器当前负责转发发送到该HSRP组虚拟MAC地址的报文，路由器发送周期性的Hello消息

HSRP状态迁移



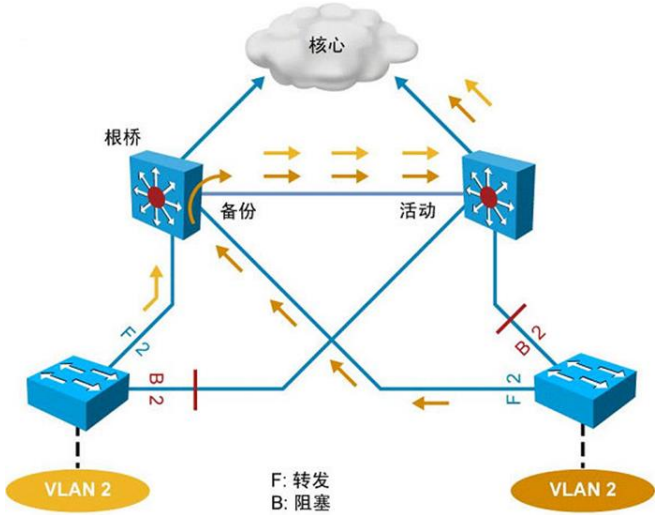
HSRP优先级和抢占模式

- 一个HSRP组中具有最高优先级的设备成为Active路由器
- 缺省优先级为100
- 若优先级相同，具有最高接口IP地址的路由器成为Active路由器
- 抢占(Preempt)使得具有更高优先级的设备成为Active。

```
switch(config)# interface vlan 10
switch(config-if)# ip address 10.1.1.2 255.255.255.0
switch(config-if)# standby 1 ip 10.1.1.1
switch(config-if)# standby 1 priority 110
switch(config-if)# standby 1 preempt
```

HSRP和STP

- 建议：HSRP的Active路由器应该和STP根桥配置在同一台设备。



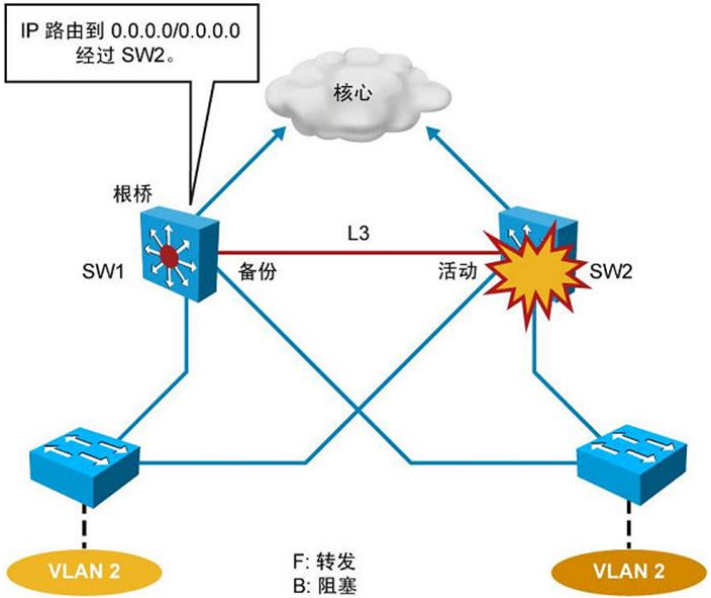
HSRP验证

- 为备份组配置验证字符串(最多八个字符，默认为 cisco)。

```
switch(config)# interface vlan 10
switch(config-if)# ip address 10.1.1.2 255.255.255.0
switch(config-if)# standby 1 ip 10.1.1.1
switch(config-if)# standby 1 priority 110
switch(config-if)# standby 1 preempt
switch(config-if)# standby 1 authentication xyz123
```

HSRP的计时器

- 当Active路由器故障时，计时器决定备份路由器什么时候成为Active路由器。
- 计算IGP收敛时间时应该考虑HSRP切换的延迟。



HSRP计时器配置

- 配置Hello和Hold计时器(可设置为毫秒级别)。
- Hold计时器应该至少3倍于Hello计时器。
- 配置抢占延迟，使得抢占在交换机完全启动并且网络连通性收敛后进行抢占。

```
switch(config)# interface vlan 10
switch(config-if)# ip address 10.1.1.2 255.255.255.0
switch(config-if)# standby 1 ip 10.1.1.1
switch(config-if)# standby 1 priority 110
switch(config-if)# standby 1 preempt
switch(config-if)# standby 1 timers msec 200 msec 750
switch(config-if)# standby 1 preempt delay minimum 300
```

HSRP版本

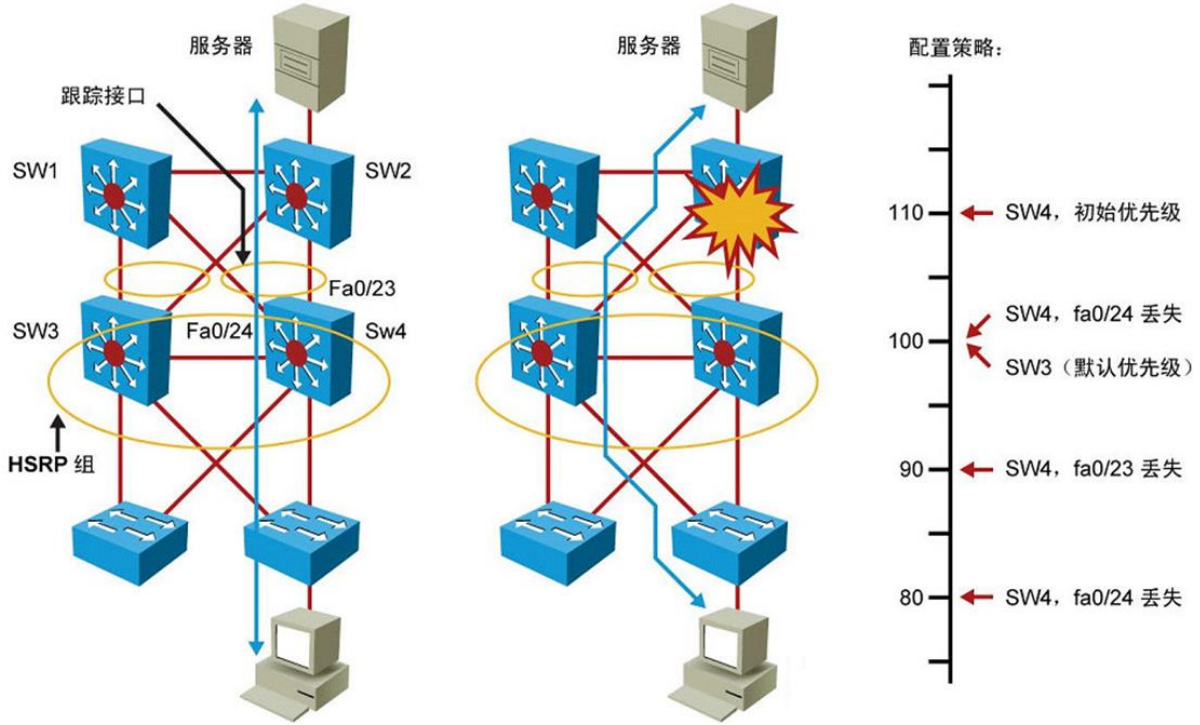
- HSRPv1（默认）
  - 组号从0到255
  - 虚拟MAC地址为0000.0C07.ACXX （XX为HSRP组号）
  - Hello报文发送到组播地址224.0.0.2
- HSRPv2
  - 组号从0到4095
  - 虚拟MAC地址为0000.0C9F.FXXX （XXX为HSRP组号）
  - Hello报文发送到组播地址224.0.0.102
  - HSRPv2和HSRPv1具有不同的报文格式
- 同一个HSRP组中的所有设备应该配置相同的版本。

```
switch(config-if)# standby 1 version 2
```

查看备份组状态

```
switch#show standby brief
Interface Grp  Pri   P State   Active          Standby         Virtual IP
Vl10        1    110 P Active  local           10.1.1.3        10.1.1.1
-------------------------------------------------------------------------------------------
 switch#show standby
Vlan10 - Group 1 (version 2)
  State is Active
    7 state changes, last state change 00:04:52
  Virtual IP address is 10.1.1.1
  Active virtual MAC address is 0000.0c9f.f00a
    Local virtual MAC address is 0000.0c9f.f00a (v2 default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 1.768 secs
  Authentication MD5, key-string
  Preemption enabled
  Active router is local
  Standby router is 10.1.1.3, priority 100 (expires in 9.520 sec)
  Priority 110 (configured 110)
  IP redundancy name is "hsrp-Vl10-1" (default)
```

HSRP接口跟踪



HSRP接口跟踪配置

- 配置备份组
- 配置优先级(缺省为100)
- 配置同一个HSRP组中所有设备的抢占
- 配置跟踪接口及其优先级减少值(缺省为10)

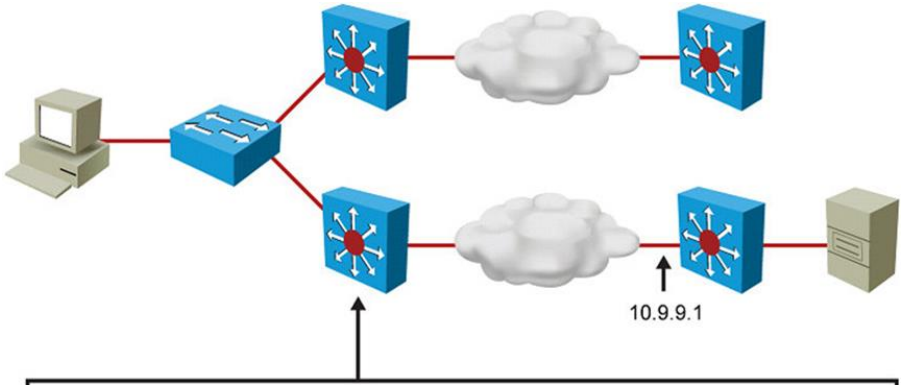
```
switch(config)# interface vlan 10
switch(config-if)# ip address 10.1.1.2 255.255.255.0
switch(config-if)# standby 1 ip 10.1.1.1
switch(config-if)# standby 1 priority 110
switch(config-if)# standby 1 preempt
switch(config-if)# standby 1 track fastethernet0/23 20
switch(config-if)# standby 1 track fastethernet0/24
```

跟踪对象

```
switch(config)# track 1 ?
  interface  Select an interface to track
  ip         IP protocol
  list       Group objects in a list
```

- Standby命令可以跟踪接口或对象。
- 跟踪对象使用track命令定义。
  - Track 编号 interface检查线路协议。
  - Track 编号 ip 检查网络可达性(比如路由或者IP SLA)。
  - Track 编号 list定义更复杂的条件。

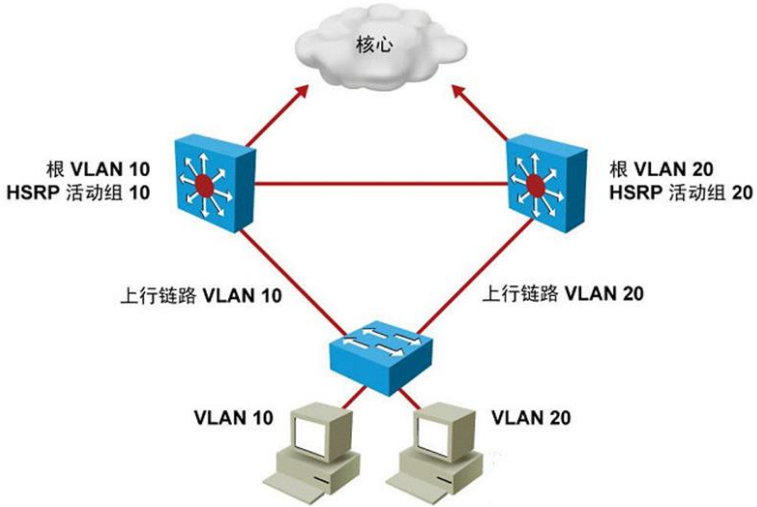
HSRP和IP SLA跟踪



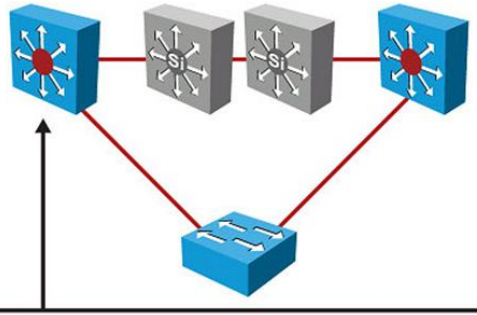

```
sw(config)# ip sla 18
sw(config-sla)# icmp-echo 10.9.9.1
sw(config)# ip sla schedule 18 start-time now life forever
sw(config)# track 90 ip sla 18 state
sw(config)# interface vlan10
sw(config-if)# ip address 10.1.1.2 255.255.255.0
sw(config-if)# standby 1 ip 10.1.1.1
sw(config-if)# standby 1 priority 110
sw(config-if)# standby 1 preempt
sw(config-if)# standby 1 track 90 decrement 20
```

多个HSRP组

- 为了在接入/汇聚层链路上进行负载分担，在同一台多层交换机上为每个VLAN配置HSRP Active路由器和生成树的根桥。



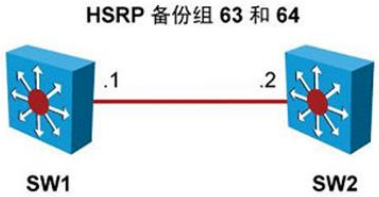
多个HSRP组的配置



```
switch(config)# spanning-tree vlan 10 root primary
switch(config)# spanning-tree vlan 20 root secondary
switch(config)# interface vlan 10
switch(config-if)# ip address 10.1.10.2 255.255.255.0
switch(config-if)# standby 10 ip 10.1.10.1
switch(config-if)# standby 10 priority 110
switch(config-if)# standby 10 preempt
switch(config)# interface vlan 20
switch(config-if)# ip address 10.1.20.2 255.255.255.0
switch(config-if)# standby 20 ip 10.1.20.1
switch(config-if)# standby 20 priority 90
switch(config-if)# standby 20 preempt
```

查看HSRP

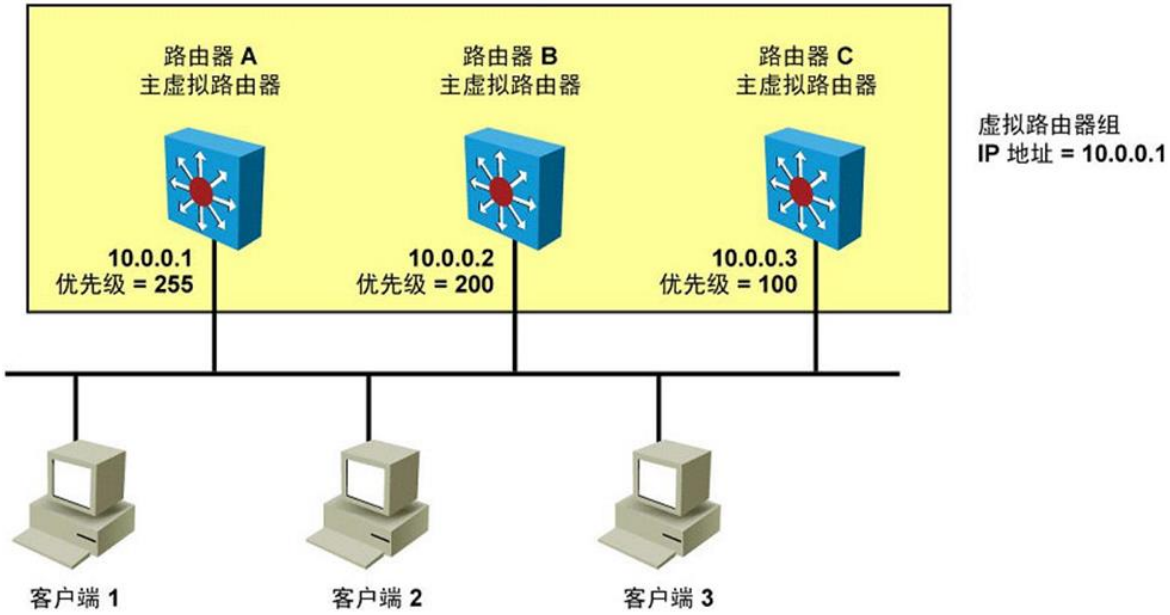
```
SW1#show standby brief
                     P indicates configured to preempt.
                     |
Interface   Grp  Pri P State   Active     Standby    Virtual IP
V163        63   120 P Active  local      10.1.63.2  10.1.63.254
V164        64   90  P Standby 10.1.64.1  local      10.1.64.254

SW1#show standby neighbor vlan64
HSRP neighbors on Vlan64
  10.1.64.1
    Active groups: 64
    No standby groups
```



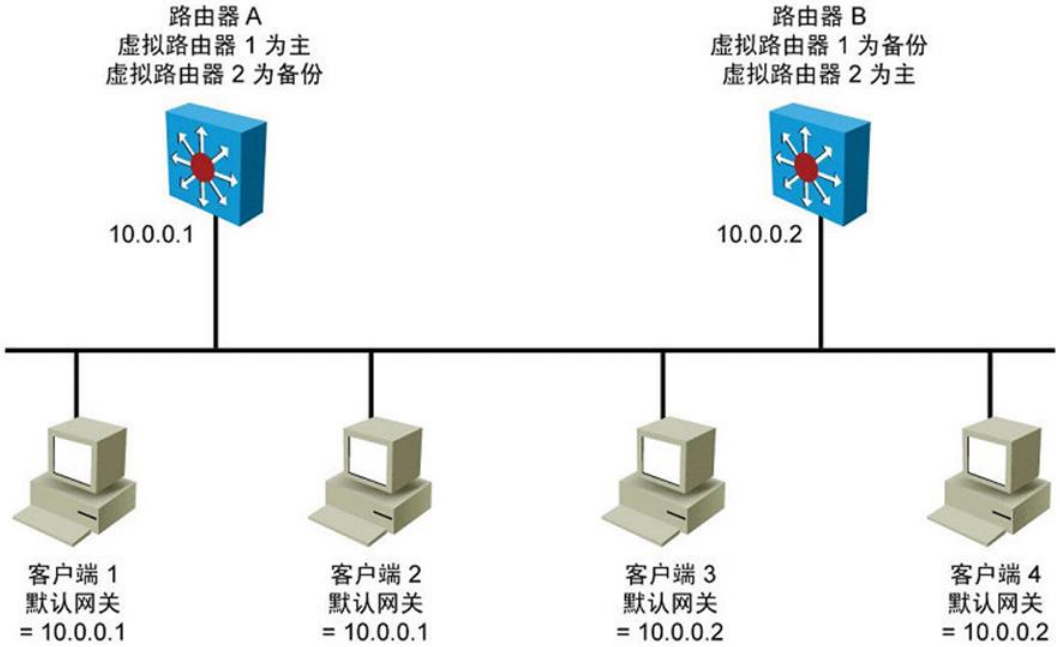
HSRP vs. VRRP

HSRP	VRRP
思科私有，1994	IETF 1998-2005，RFC 3768
v1最多255个组 v2 4096	最多255个组
1个Active、1个Standby、多个候选	1个Master、多个Backup
虚拟IP不能等于Active/Standby设备真实IP地址	虚拟IP地址可以与组成员真实IP地址相同
使用224.0.0.2	使用224.0.0.18
可以跟踪接口或对象	只能跟踪对象
缺省计时器：Hello为3秒、Hold为10秒	缺省计时器：Hello为1秒、Hold为3秒
支持验证	早期版本支持，现在不再支持

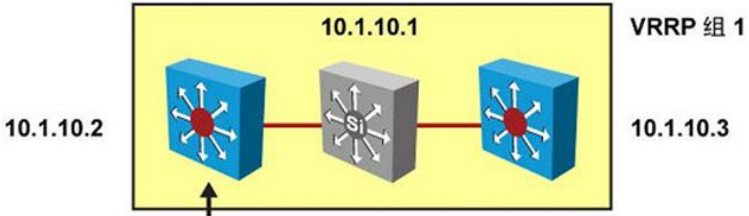
关于VRRP



VRRP运作流程



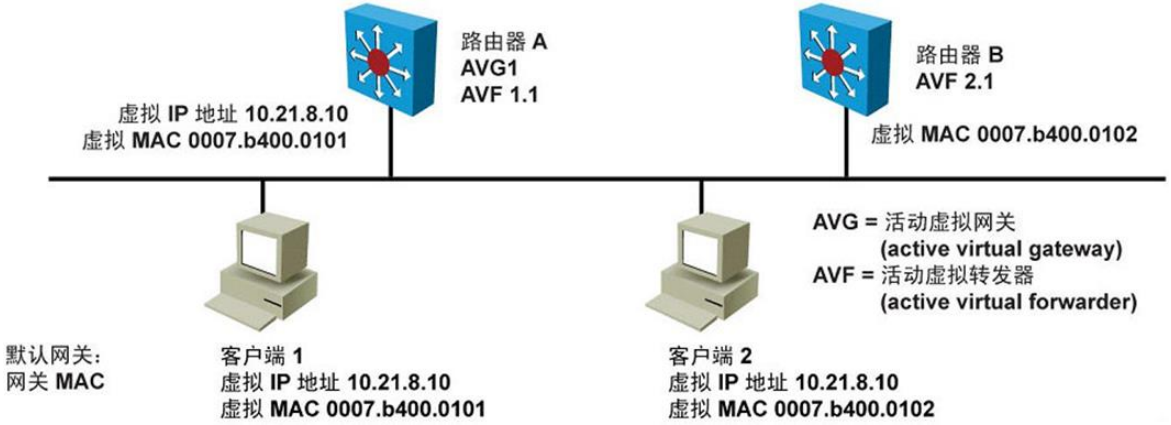
VRRP配置




```
sw(config)# track 90 interface fa0/24 line-protocol
sw(config)# interface vlan10
sw(config-if)# ip address 10.1.10.2 255.255.255.0
sw(config-if)# vrrp 1 10.1.10.1
sw(config-if)# vrrp 1 priority 110
sw(config-if)# vrrp 1 timers advertise msec 500
sw(config-if)# vrrp 1 authentication md5 keystring xyz123
sw(config-if)# vrrp 1 track 90 decrement 20
```

关于GLBP

- 多台设备都能够转发数据，无需配置多个备份组
- 提供一个虚拟IP地址和多个虚拟MAC地址
- 发往同一个虚拟IP地址的流量被分担到多台路由器
- 故障时提供自动的切换

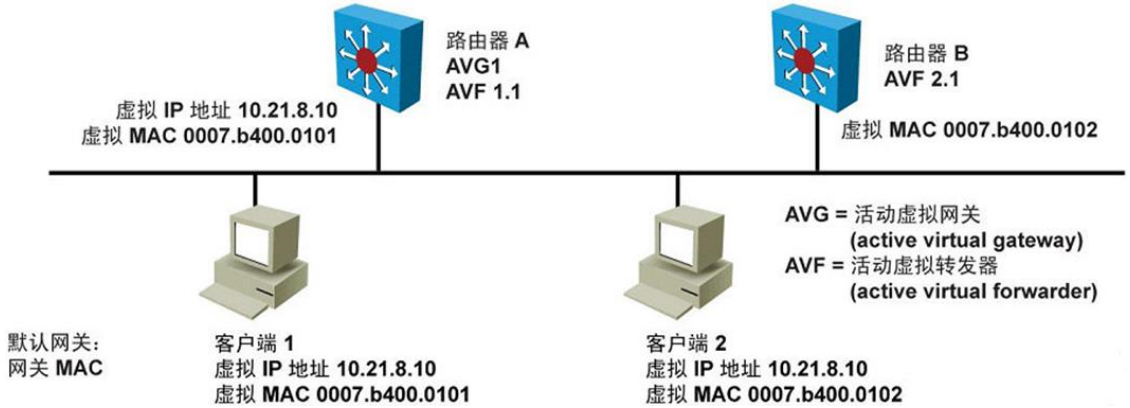


GLBP vs. HSRP

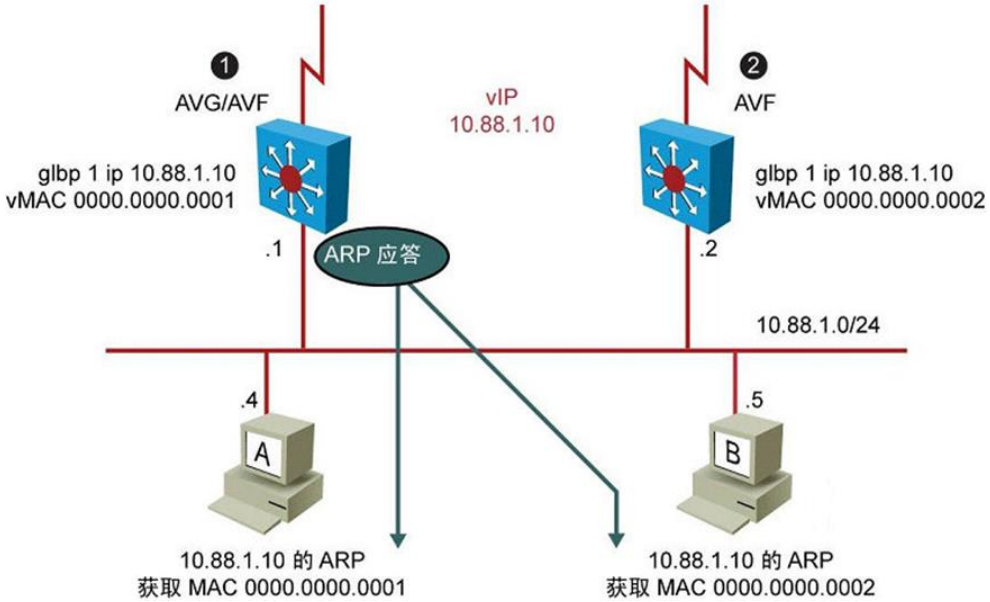
HSRP	GLBP
思科私有，1994	思科私有，2005
v1最多255个组 v2 4096	最多1024个组
1个Active、1个Standby、多个候选	1个AVG、多个AVF(AVG将流量在多个AVF间分担)
虚拟IP不能等于Active/Standby设备真实IP地址	虚拟IP不能等于Active/Standby设备真实IP地址
一个备份组有一个虚拟MAC	一个备份组中每个AVF都有一个虚拟MAC
使用224.0.0.2	使用224.0.0.102
可以跟踪接口或对象	只能跟踪对象
缺省计时器：Hello为3秒、Hold为10秒	缺省计时器：Hello为3秒、Hold为10秒
支持验证	支持验证

GLBP运作

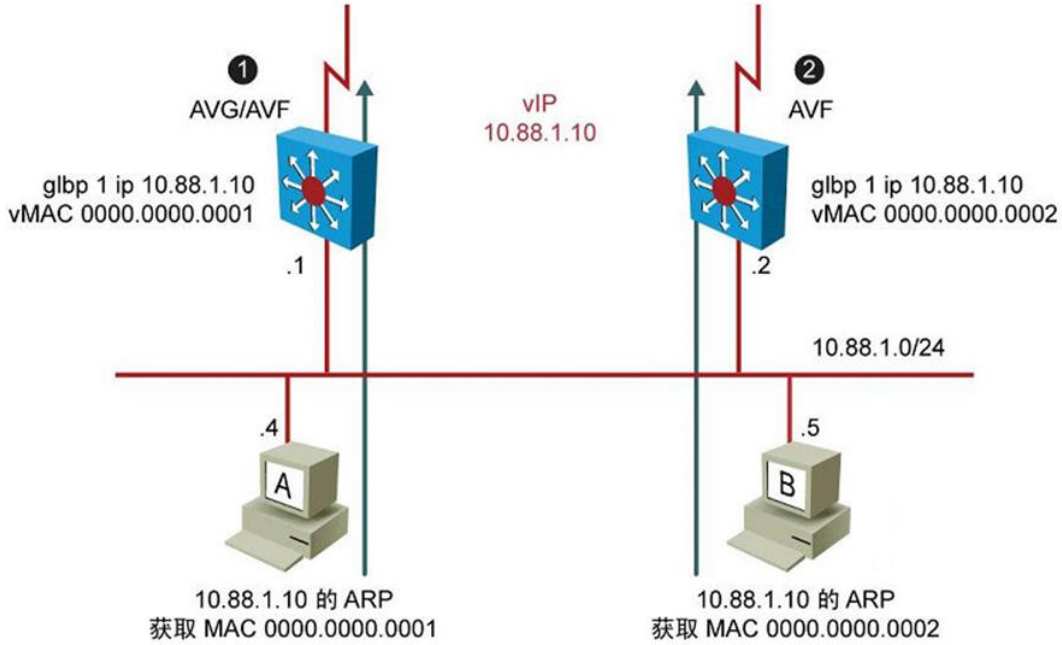
- 一个GLBP组中的成员选举出一个AVG。
- AVG为该组中的每个成员分配一个虚拟MAC。
- AVG负责应答来自不同客户端对虚拟IP地址的ARP请求，并且使用不同的虚拟MAC地址应答，从而实现负载分担。
- 每台路由器作为一个AVF，将分配到一个虚拟MAC



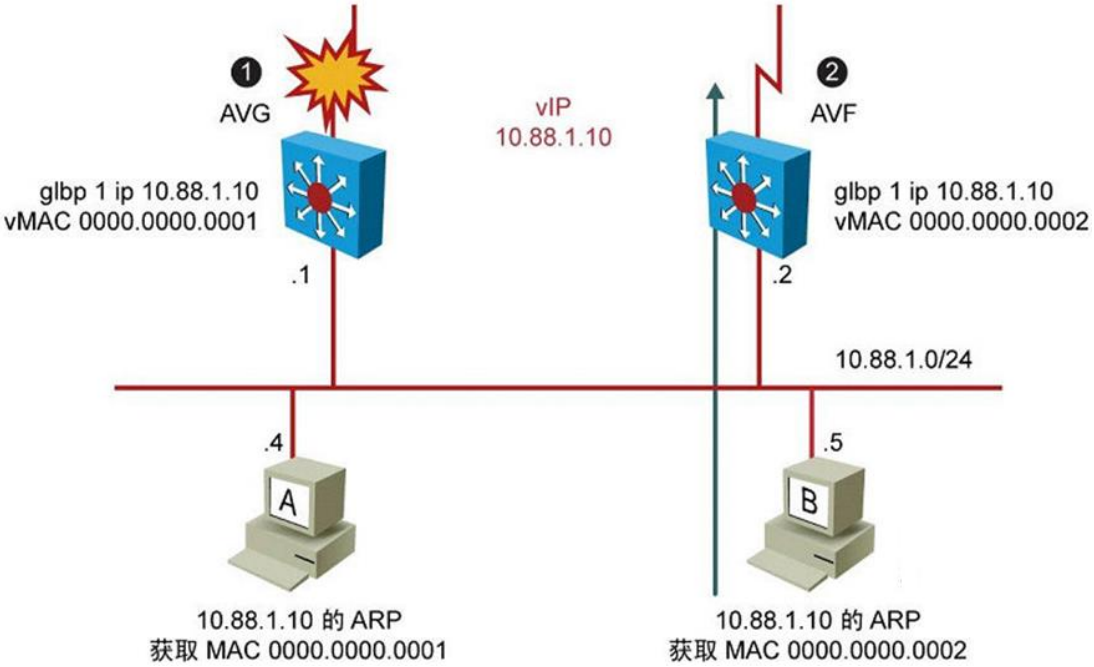
GLBP运作



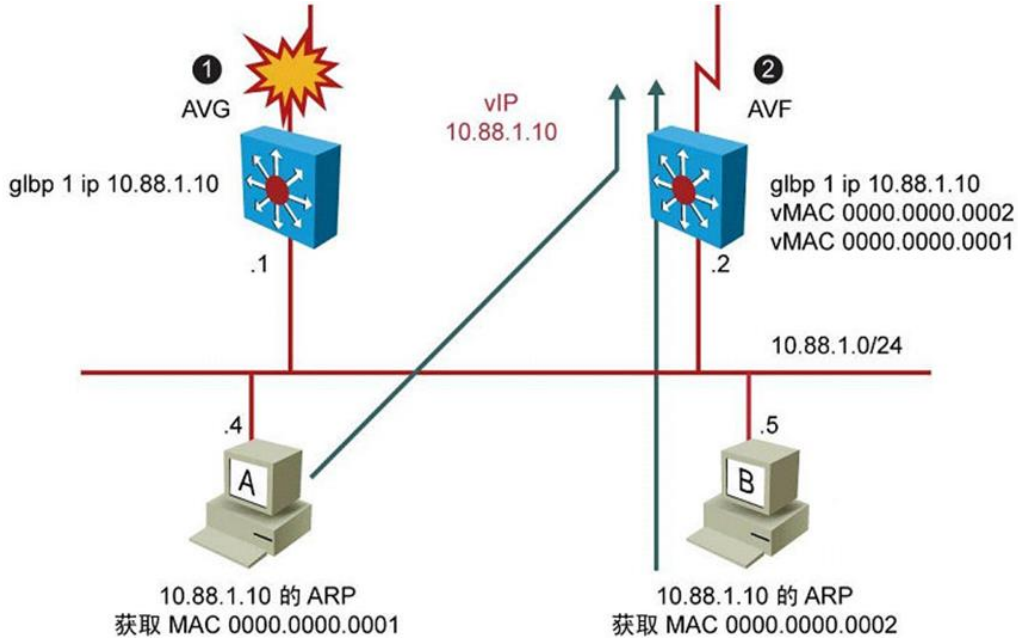
GLBP运作(续)



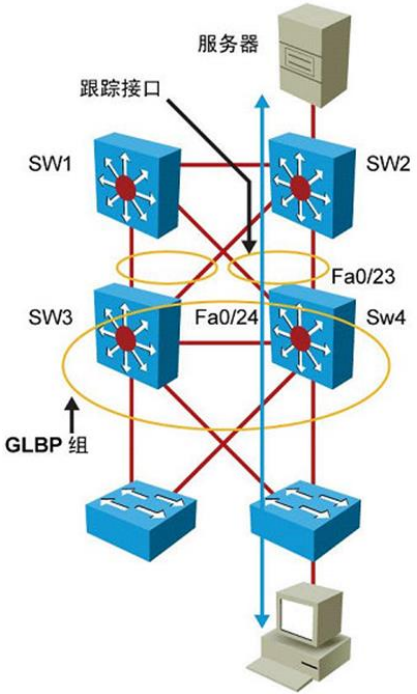
GLBP接口跟踪

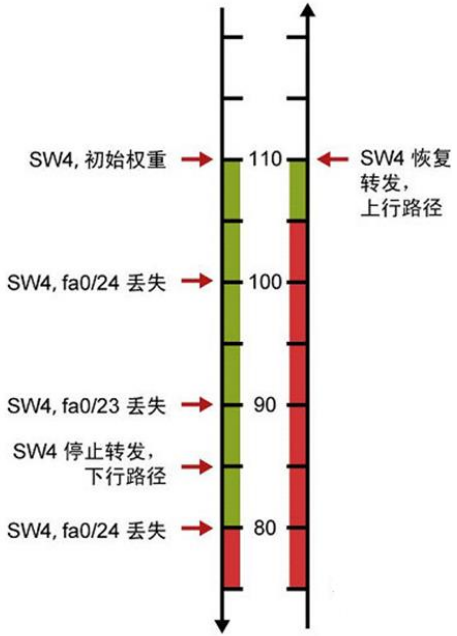


GLBP接口跟踪(续)

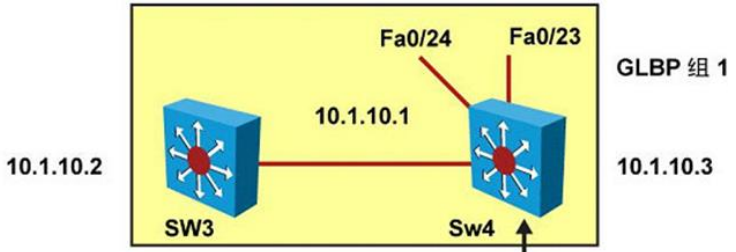


GLBP权重和优先级减少值





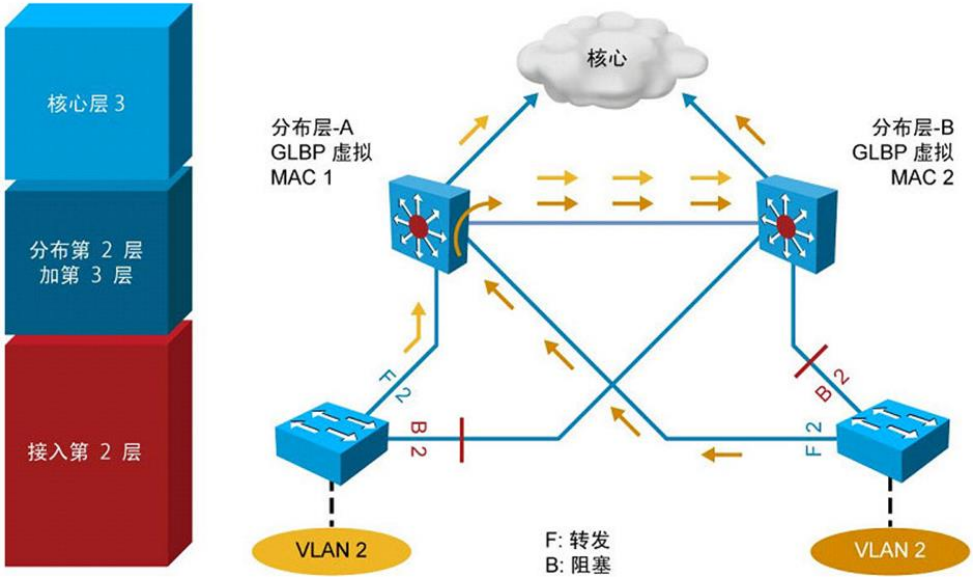
GLBP配置




```
SW4(config)# track 90 interface fa0/24 line-protocol
SW4(config)# track 91 interface fa0/23 line-protocol
SW4(config)# interface vlan10
SW4(config-if)# ip address 10.1.10.2 255.255.255.0
SW4(config-if)# glbp 1 10.1.10.1
SW4(config-if)# glbp 1 weighting 110 lower 85 upper 105
SW4(config-if)# glbp 1 timers msec 200 msec 700
SW4(config-if)# glbp 1 preempt delay minimum 300
SW4(config-if)# glbp 1 authentication md5 keystring xyz123
SW4(config-if)# glbp 1 weighting track 90 decrement 10
SW4(config-if)# glbp 1 weighting track 91 decrement 20
```

GLBP和生成树

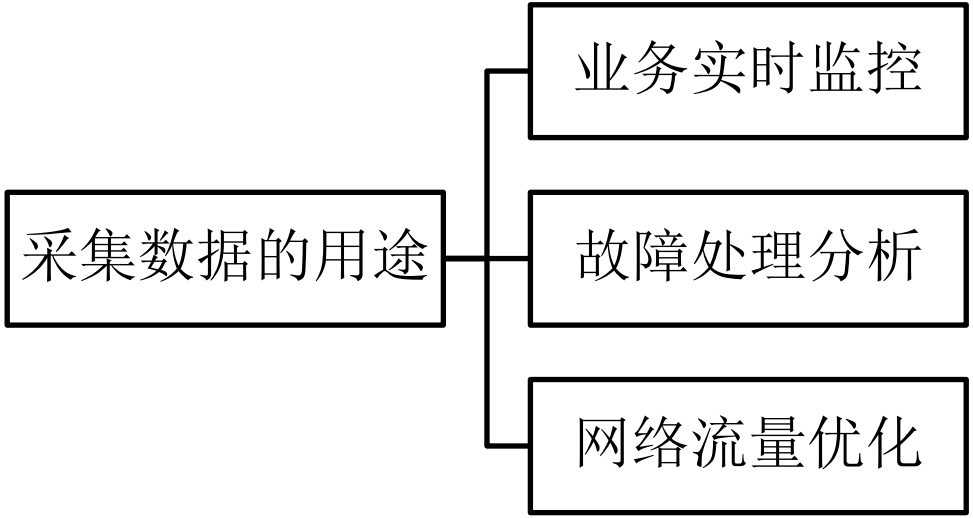
- 两个分布交换机均用作默认网关。
- 阻塞的上行链路导致流量选择的不是最优路径。



小结

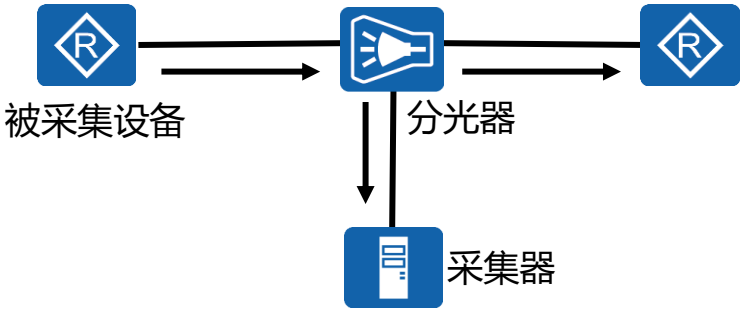
- 单个默认网关或Proxy ARP无法为园区网络提供冗余。
- HSRP为终端设备提供路由器冗余。
- 在接口上使用standby命令配置HSRP。
- 配置抢占、计时器和接口跟踪可以优化HSRP并减少切换时间。
- 使用debug命令检查HSRP状态变化。
- VRRP提供与HSRP类似的路由器冗余。
- VRRP支持一个Master路由器和一个或多个Backup路由器。
- VRRP是基于每接口进行配置。
- GLBP提供路由器冗余和负载分担。
- GLBP为每个AVF分配一个虚拟MAC地址，从而实现负载分担。
- GLBP配置步骤与HSRP和VRRP类似。

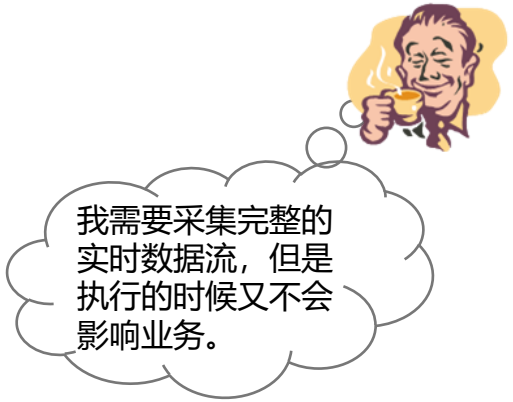
数据采集的作用



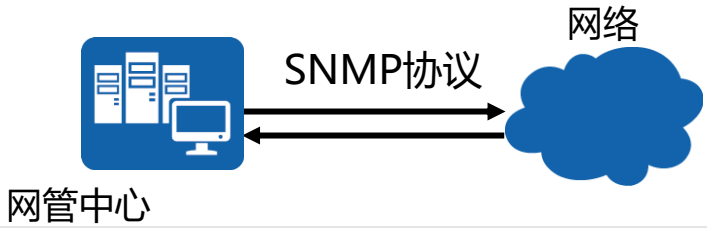
数据采集的方法

- 分光器物理采集





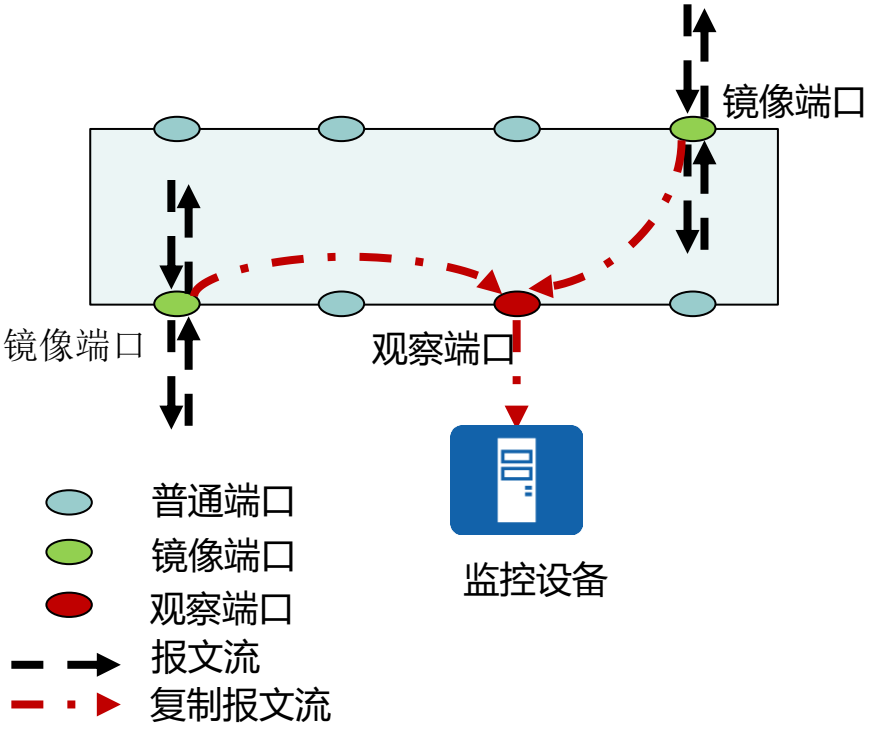
- NMS集中采集



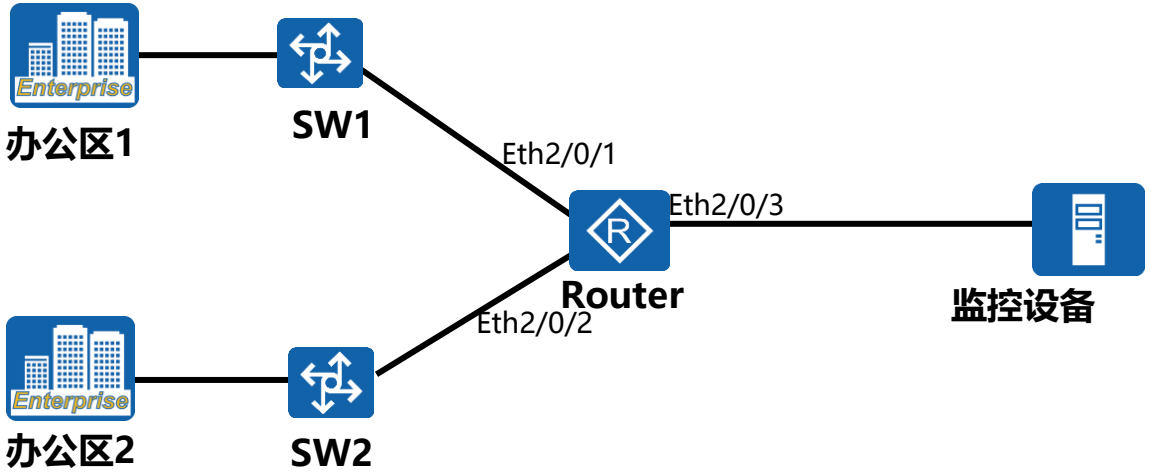
镜像概述

- 镜像定义
  - 将镜像端口（源端口）的报文复制一份到观察端口（目的端口）。
- 镜像作用
  - 获取完整报文用于分析网络状况。
- 镜像优点
  - 不影响原有网络，快捷方便。
  - 采集的是实时数据流，真实可靠。

镜像的角色

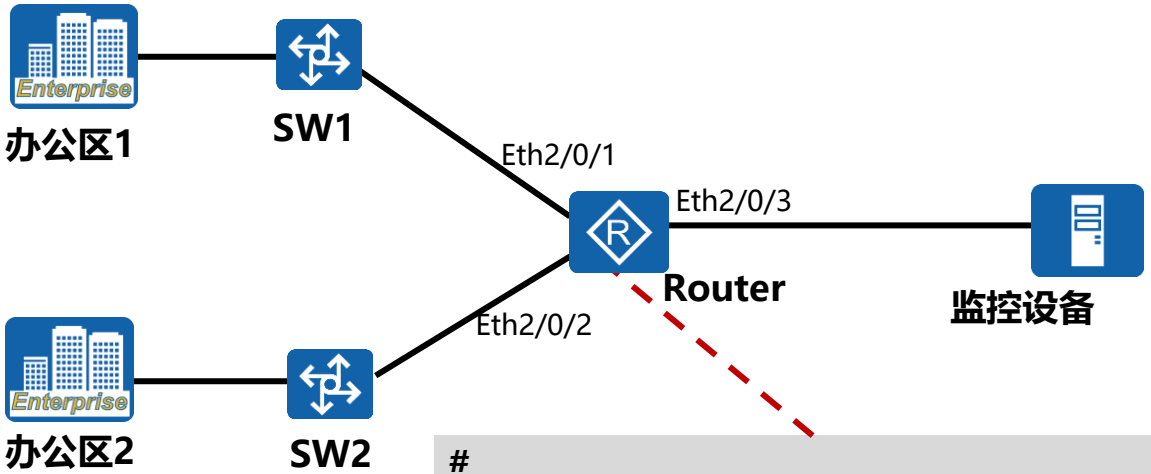


本地端口镜像配置需求



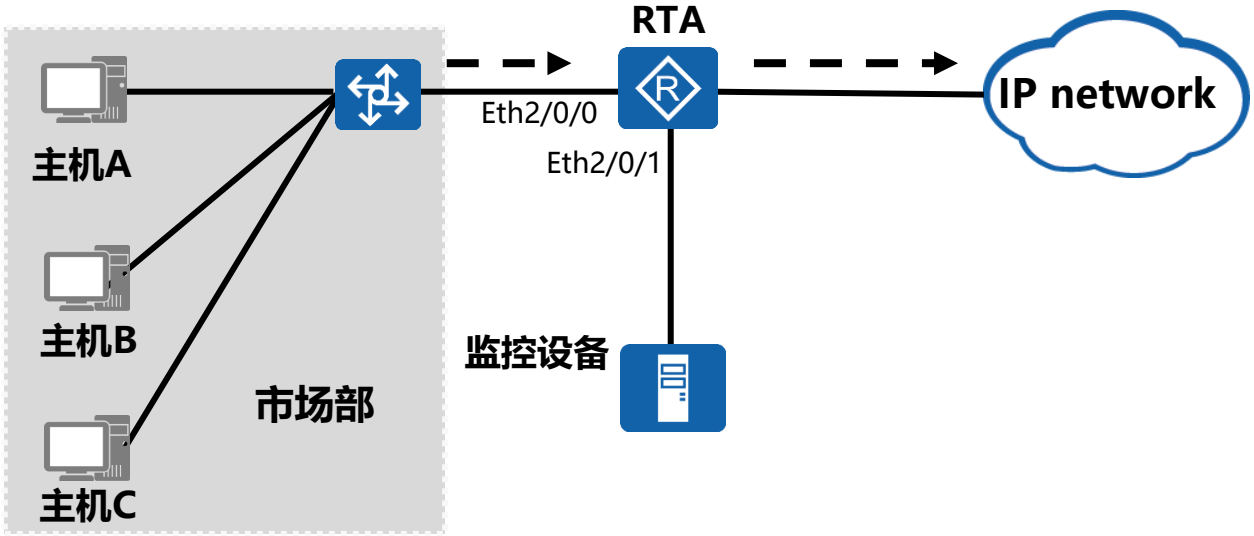
– 某企业中，办公区1和办公区2用户分别通过接口Eth2/0/1、Eth2/0/2接入Router。一台监控设备接在Router的接口Eth2/0/3上，用于数据分析监控。为保证企业的信息安全，用户希望通过监控设备对办公区1和办公区2发送的所有报文进行监控。

本地端口镜像配置实现



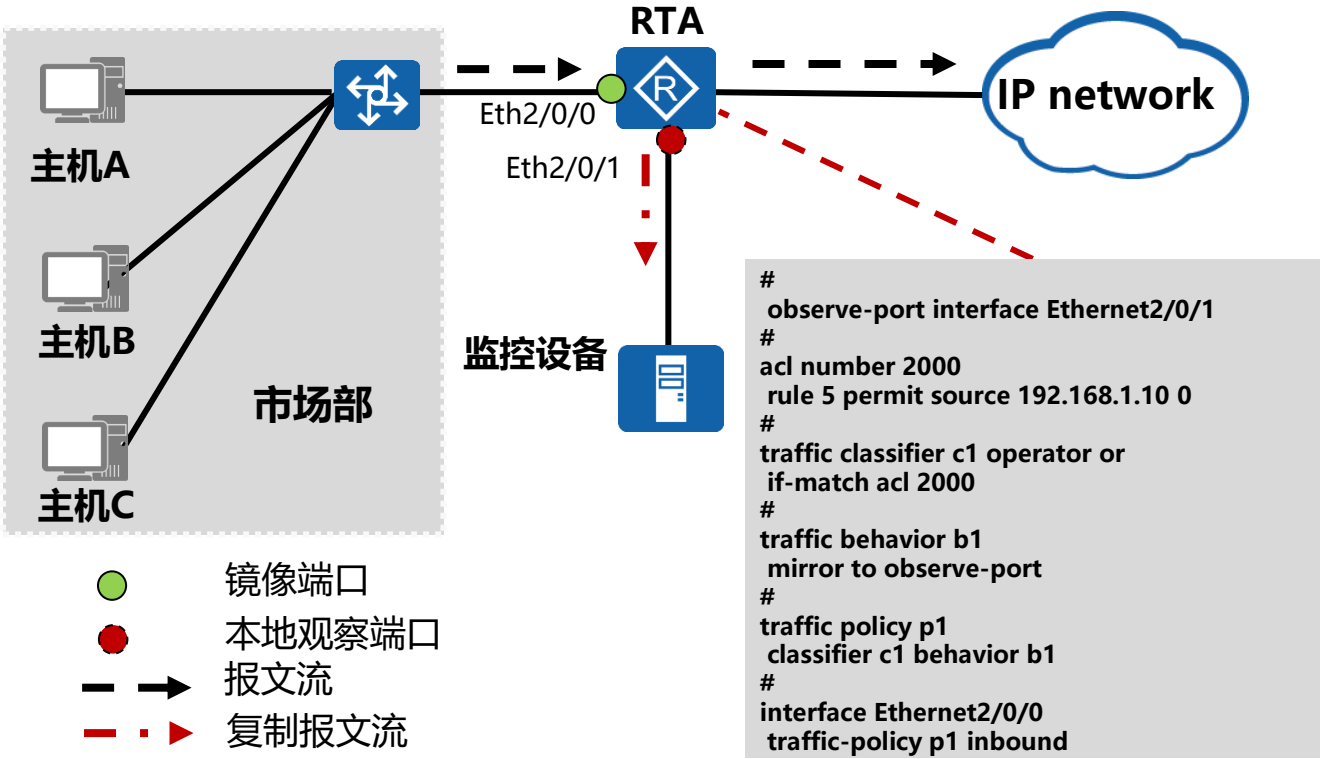

```
#
 observe-port interface Ethernet2/0/3
#
interface Ethernet2/0/1
 mirror to observe-port inbound
#
interface Ethernet2/0/2
 mirror to observe-port inbound
```

流镜像配置需求



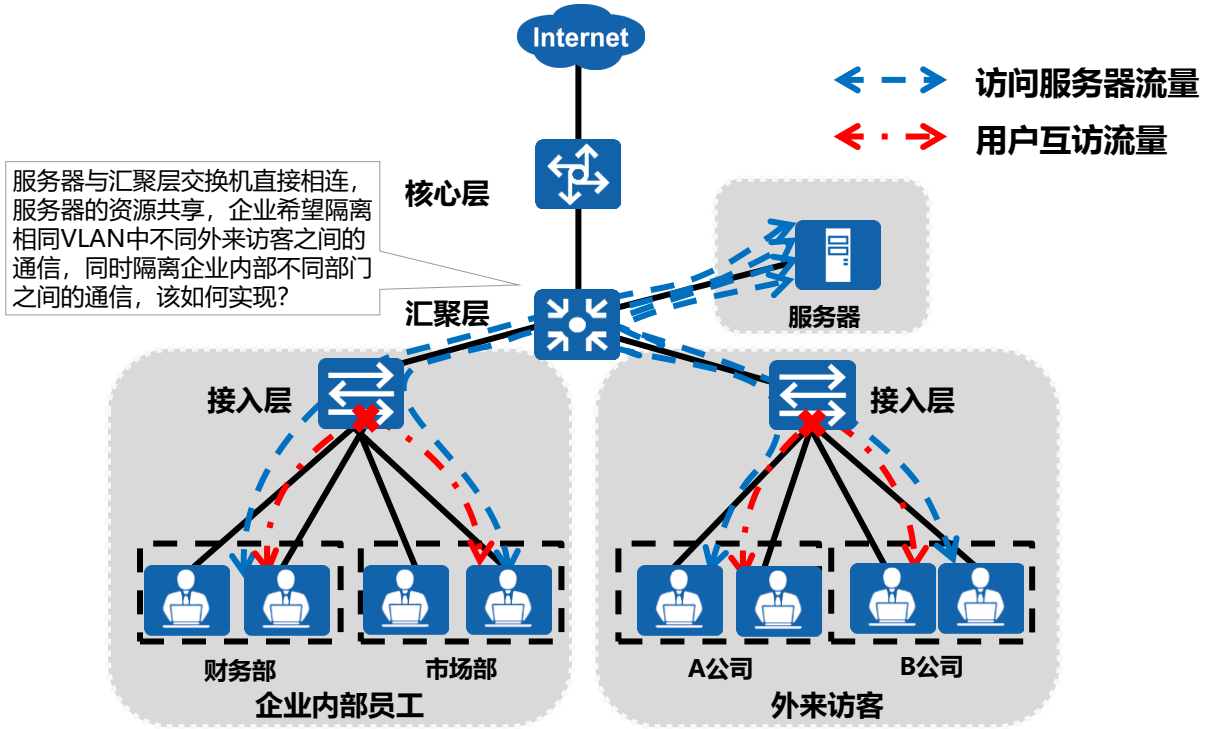
– 某企业中，市场部用户通过接口Eth2/0/0接入路由器RTA。一台监控设备接在RTA的接口Eth2/0/1上，用于数据分析监控。用户希望监控市场部IP地址为192.168.1.10的主机发出的所有报文。

流镜像配置实现

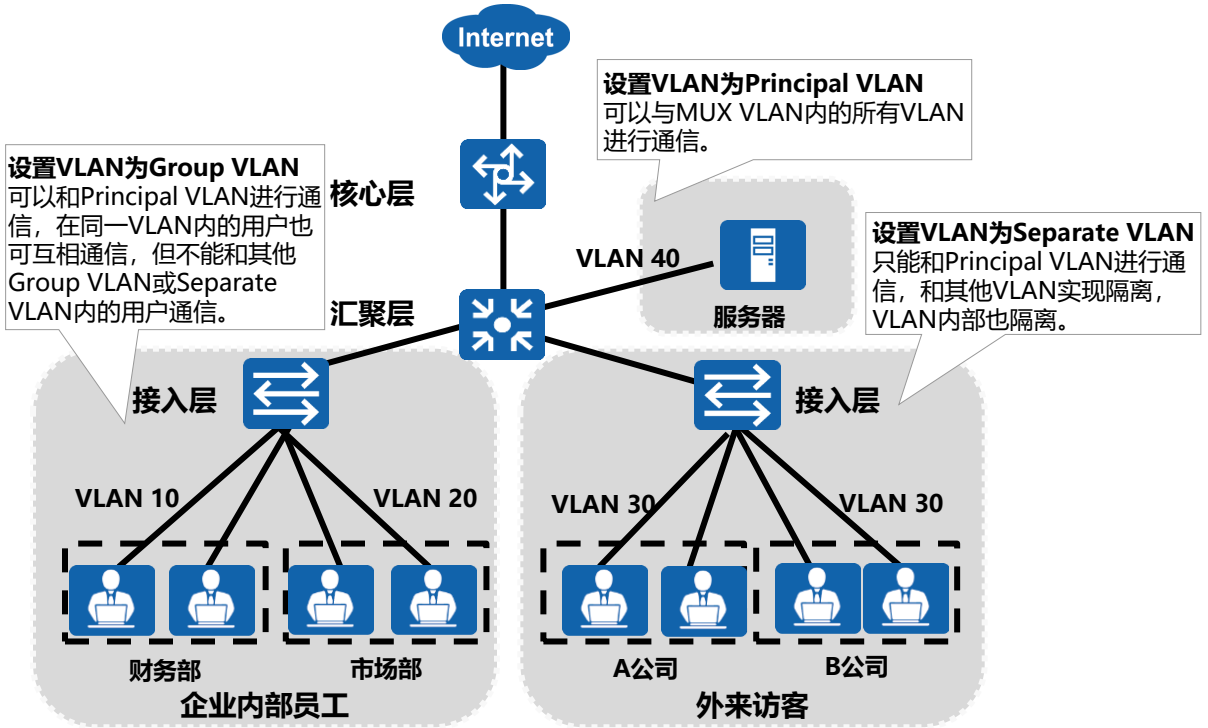



```
#
 observe-port interface Ethernet2/0/1
#
acl number 2000
 rule 5 permit source 192.168.1.10 0
#
traffic classifier c1 operator or
 if-match acl 2000
#
traffic behavior b1
 mirror to observe-port
#
traffic policy p1
 classifier c1 behavior b1
#
interface Ethernet2/0/0
 traffic-policy p1 inbound
```

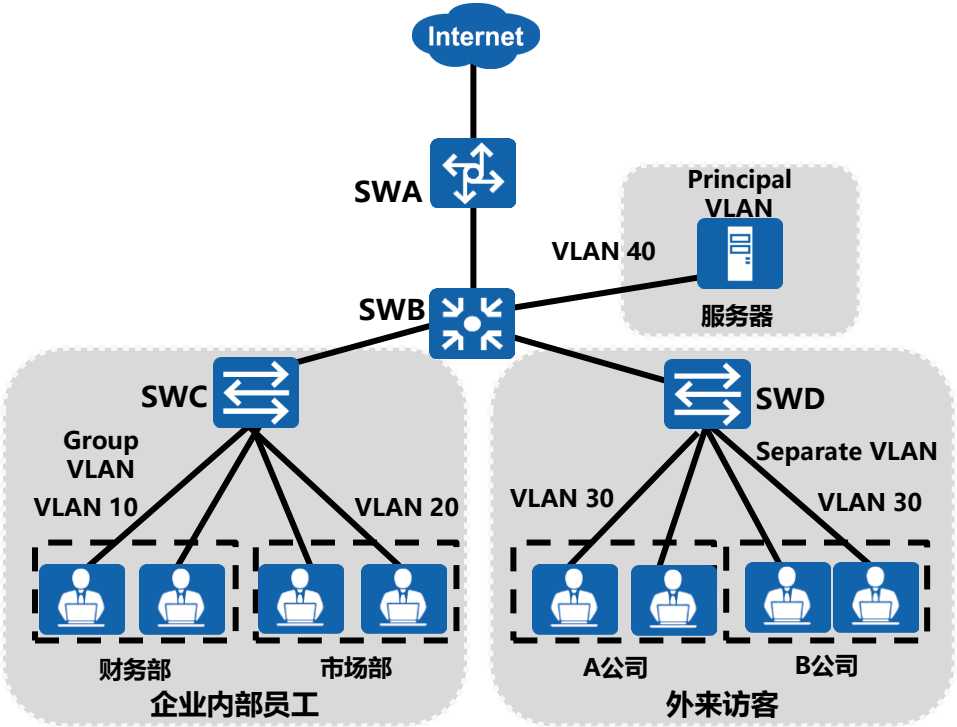
MUX VLAN应用场景



MUX VLAN基本概念

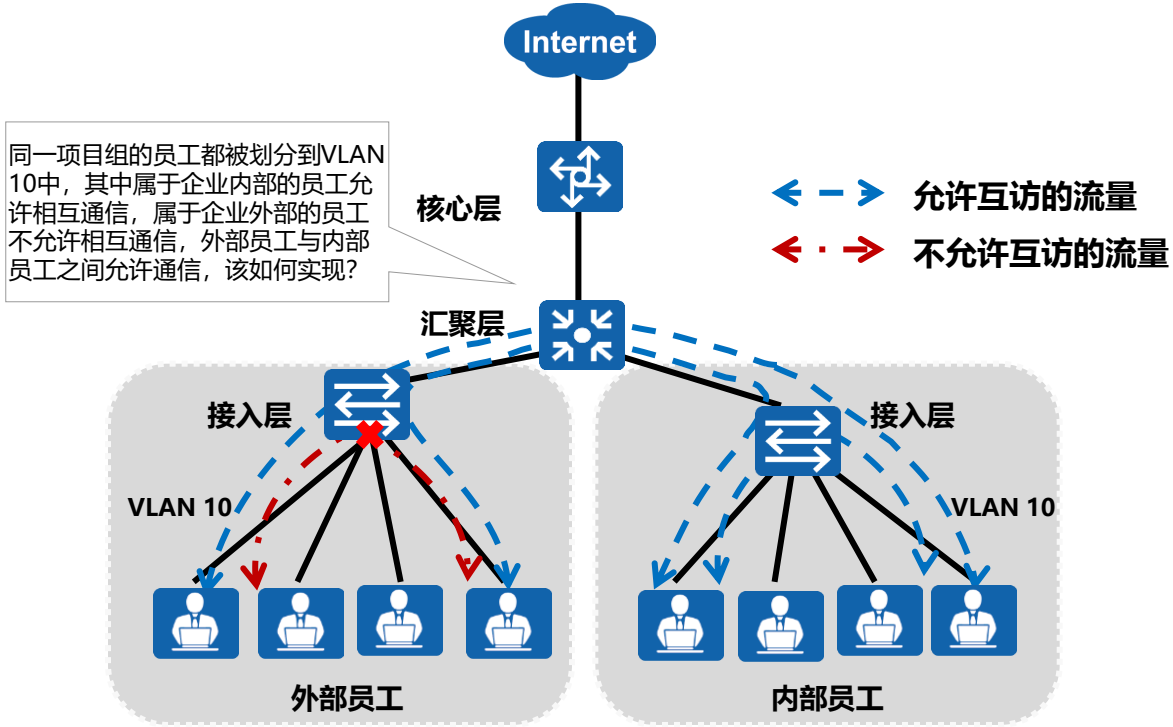


MUX VLAN配置实现

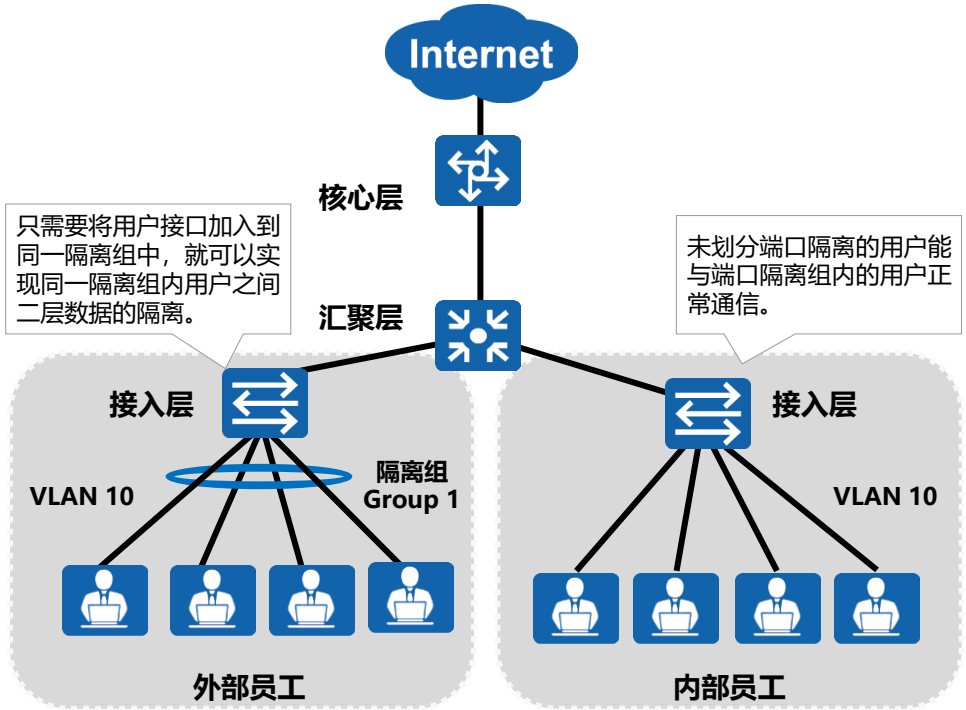


MUX VLAN

端口隔离应用场景

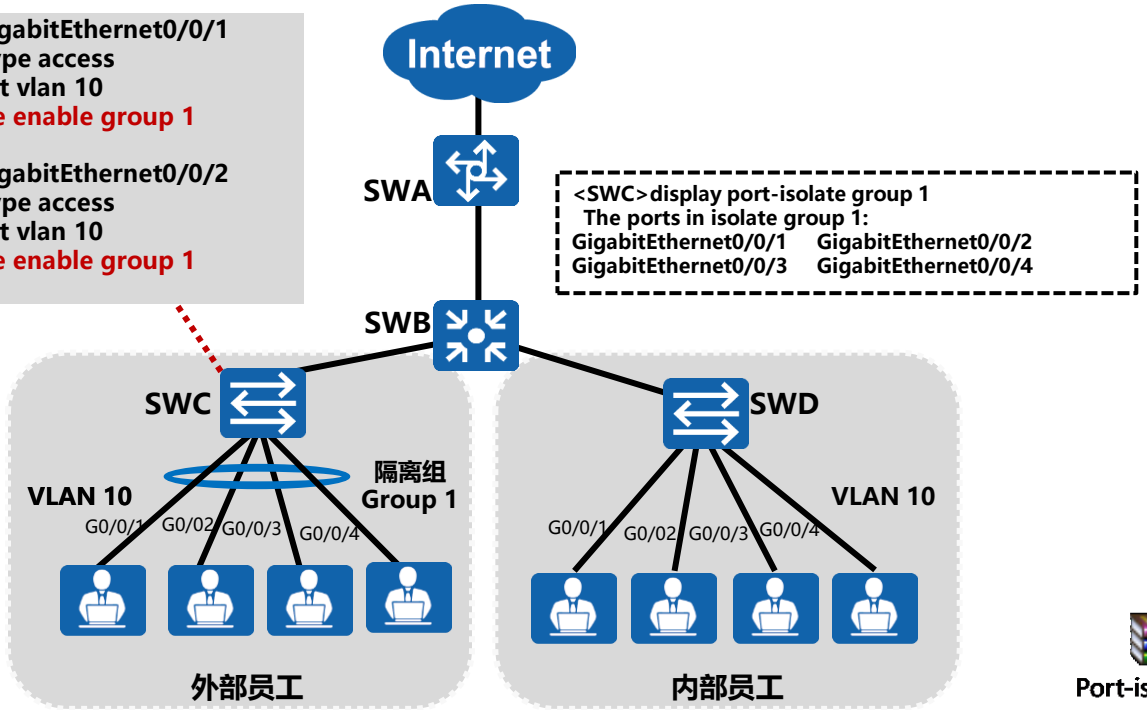


端口隔离基本概念



端口隔离配置实现

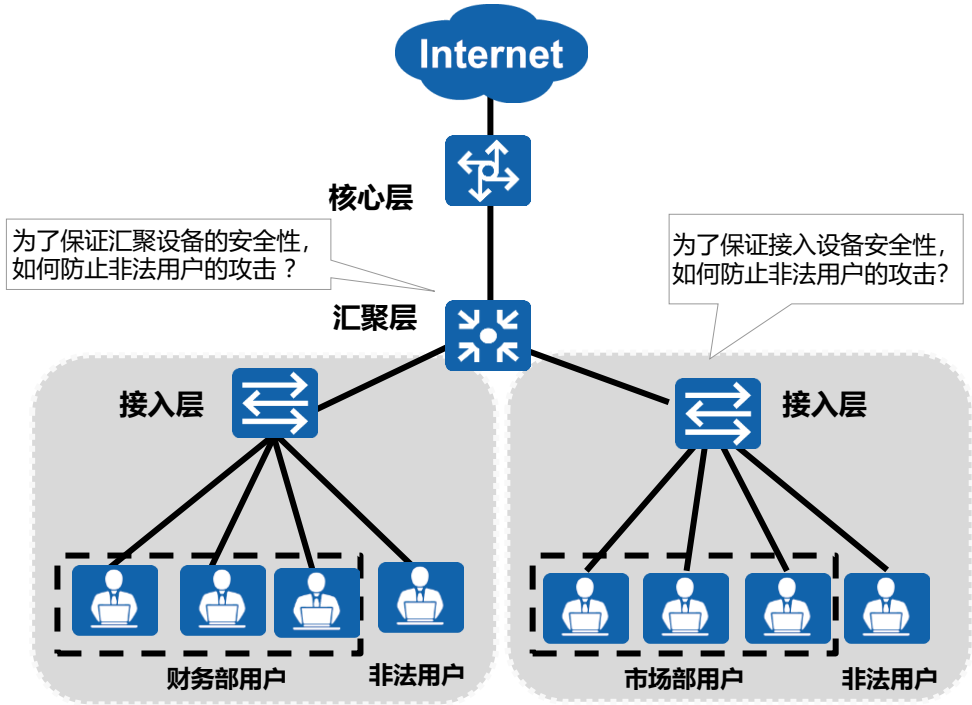
```
interface GigabitEthernet0/0/1
 port link-type access
 port default vlan 10
 port-isolate enable group 1
#
interface GigabitEthernet0/0/2
 port link-type access
 port default vlan 10
 port-isolate enable group 1
.....
```




```
<SWC>display port-isolate group 1
  The ports in isolate group 1:
GigabitEthernet0/0/1    GigabitEthernet0/0/2
GigabitEthernet0/0/3    GigabitEthernet0/0/4
```

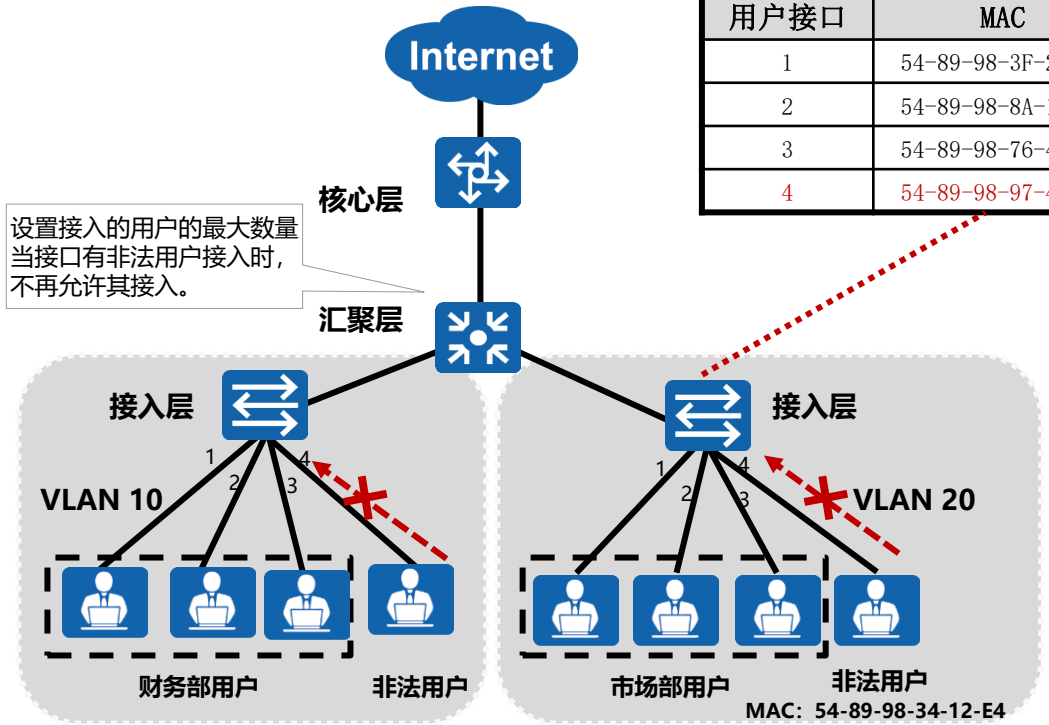
Port-isolate.rar

端口安全应用场景



端口安全解决方案

用户接口	MAC	VLAN
1	54-89-98-3F-24-E5	20
2	54-89-98-8A-13-EE	20
3	54-89-98-76-42-C4	20
4	54-89-98-97-45-20	20



端口安全类型

- 端口安全（Port Security）通过将接口学习到的动态MAC地址转换为安全MAC地址（包括安全动态MAC、安全静态MAC和Sticky MAC）阻止非法用户通过本接口和交换机通信，从而增强设备的安全性。

类型	定义	特点
安全动态MAC地址	使能端口安全而未使能Sticky MAC功能时转换的MAC地址。	设备重启后表项会丢失，需要重新学习。缺省情况下不会被老化，只有在配置安全MAC的老化时间后才可以被老化。
安全静态MAC地址	使能端口安全时手工配置的静态MAC地址。	不会被老化，手动保存配置后重启设备不会丢失。
Sticky MAC地址	使能端口安全后又同时使能Sticky MAC功能后转换得到的MAC地址。	不会被老化，手动保存配置后重启设备不会丢失。

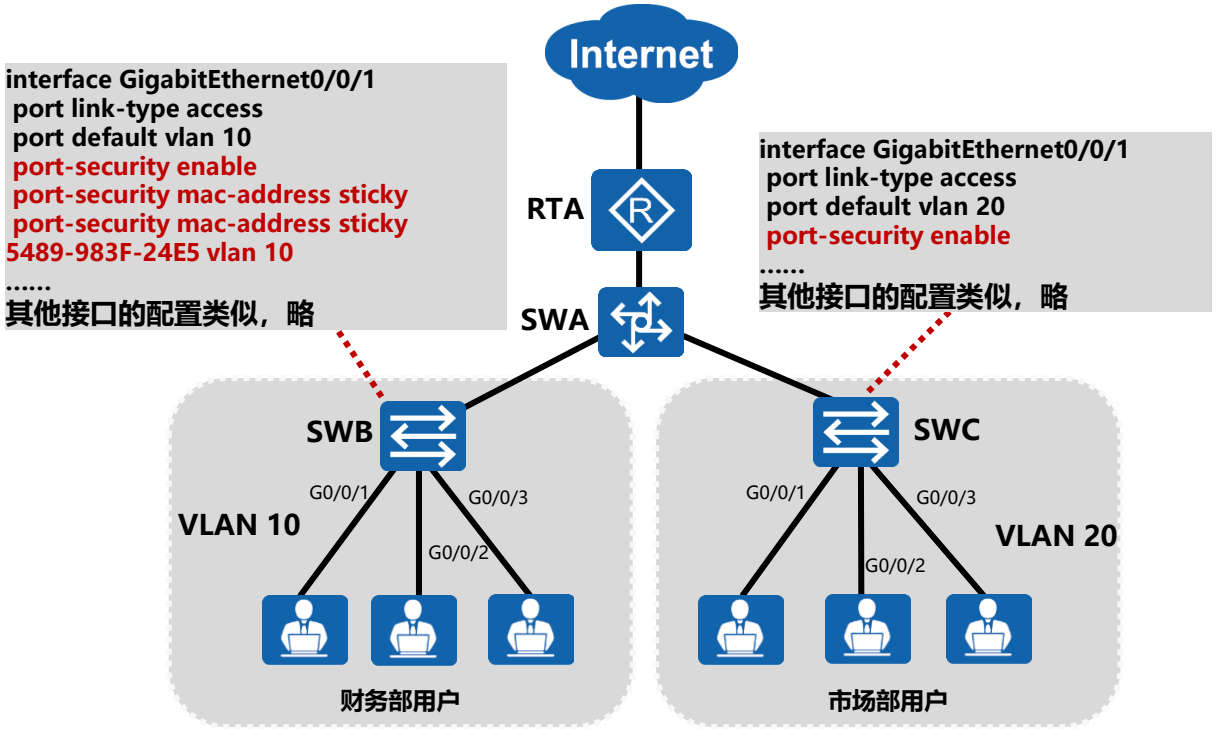
端口安全限制动作

- 超过安全MAC地址限制数后的动作：

动作	实现说明
restrict	丢弃源MAC地址不存在的报文并上报告警。推荐使用restrict动作。
protect	只丢弃源MAC地址不存在的报文，不上报告警。
shutdown	接口状态被置为error-down，并上报告警。默认情况下，接口关闭后不会自动恢复，只能由网络管理人员在接口视图下使用restart命令重启接口进行恢复。

- 接口上安全MAC地址数达到限制后，如果收到源MAC地址不存在的报文，端口安全则认为有非法用户攻击，就会根据配置的动作对接口做保护处理。缺省情况下，保护动作是restrict。

端口安全配置实现



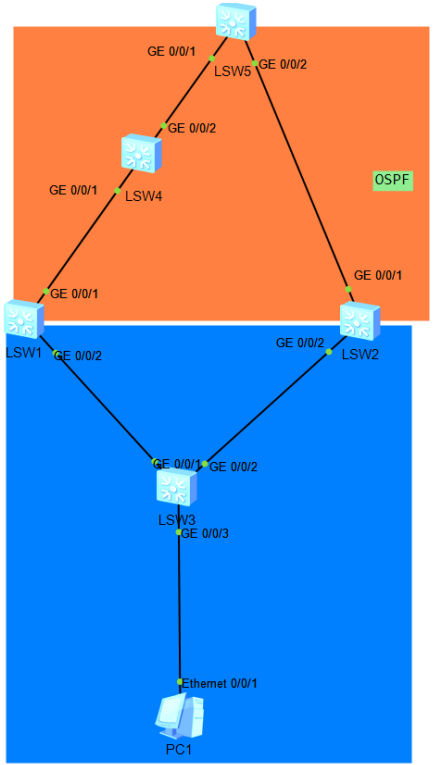
Port Security.rar

华为VRRP实验

实验需求：

1. 按照拓扑搭建，全交换机，不准有路由器
2. 橙色部分是三层，蓝色部分是二层
3. 路由跑OSPF
4. 网关冗余协议使用VRRP
5. 四个VLAN的GW实现冗余和负载
6. Ping 8.8.8.8（SW5的环回口）

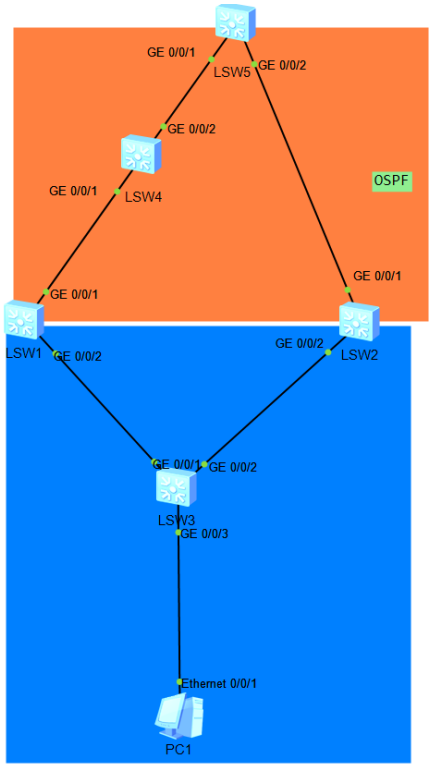
注意：自己解决可能的环路问题



思科HSRP实验

实验需求：

1. 按照拓扑搭建，全交换机，不准有路由器
2. 橙色部分是三层，蓝色部分是二层
3. 路由跑OSPF
4. 网关冗余协议使用HSRP
5. 四个VLAN的GW实现冗余和负载
6. Ping 8.8.8.8（SW5的环回口）



THANK YOU

Ping 通您的梦想～

腾讯课堂交流群：17942636

ADD：苏州市干将东路666号和基广场401-402；Tel：0512-8188 8288；

课程咨询QQ：2853771087 ； 官网 :www.51glab.com