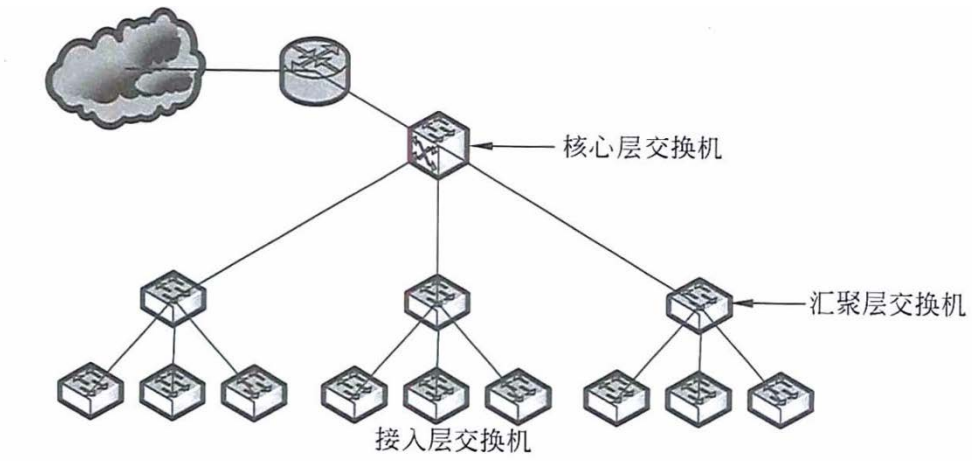
基本实验

1. 交换机和路由

1-1交换机基础

4-2-1 交换机的分类

- **根据交换方式划分**:
  - 存储转发式交换(Store and Forward)
  - 直通式交换(Cut-through)
  - 碎片过滤式交换(Fragment Free)
- **根据交换的协议层划分**:
  - 第二层交换：根据 MAC 地址进行交换
  - 第三层交换：根据网络层地址(IP 地址）进行交换
  - 多层交换：根据第四层端口号或应用协议进行交换
- **根据交换机结构划分**:
  - 固定端口交换机
  - 模块化交换机
- **根据配置方式划分**:
  - 堆叠型交换机
  - 非堆叠型交换机
- **根据管理类型划分**:
  - 网管型交换机
  - 非网管型交换机
  - 智能型交换机
- **根据层次型结构划分**:



  - 接入层交换机：接入层是工作站连接网络的入口，实现用户的**网络访问控制**
  - 汇聚层交换机：汇聚层将网络划分为多个广播 / 组播域，可以实现 VLAN 间的路由选择，并通过访问控制列表实现分组过滤，应提供第**三层交换功能**
  - 核心层交换机：核心层应采用可扩展的高性能交换机组成园区网的主干线路，提供链**路冗余、路由冗余、VLAN 中继和负载均衡**等功能，与汇聚层交换机具有兼容的技术支持相同的协议

4-2-2 交换机的性能参数

- **端口类型**:

- 双绞线端口：双绞线端口主要有 100Mbps 和 1000Mbps 两种
- 光纤端口：SC 端口(Subscriber Connector ）是一种光纤端口，可提供千兆位数据传输,，通常用于连接服务器的光纤网卡
- GBIC 端口：交换机上的 GBIC (Giga Bit-rate Interface Converter , GBIC ）插槽(Slot)用于安装千兆位端口光电转换器
- SFP 端口：小型机架可插拔设备(Sm all Form-factor Pluggable, SFP ）是 GBIC 的升级版本

➢ **传输模式**:

- 半双工(half-duplex)
- 全双工(full -duplex)
- 全双工 / 半双工自适应

➢ **包转发率**:

包转发率也称端口吞吐率，指交换机进行数据包转发的能力，单位为 pps(package per second)

包转发速率是以单位时间内发送 64 字节数据包的个数作为计算基准的，对千千兆以太网来说，计算方法如下:

$$1000\text{Mbps} \div 8\text{b} \div (64 + 8 + 12)\text{B} = 1488095\text{pps}$$

当以太网帧为 64 字节时，需考虑 8 字节的帧头和 12 字节的帧间隙开销，据此，一台千兆交换机的包转发速率的计算方法如下：(**1488)**

包转发率 = 千兆端口数 x 1.488Mpps+百兆端口数 x 0.1488Mpps+其余端口数 x 相应包转发数

➢ **背板带宽**:

交换机的背板带宽是指交换机端口处理器和数据总线之间单位时间内所能传输的最大数据量，背板带宽标志了一台交换机总的交换能力，单位 Gbps。

一般交换机的背板带宽从几个 Gbps 到上千个 Gbps 。交换机所有端口能提供的总带宽的计算公式为:

总带宽 = 端口数 x 端口速率 x2 (全双工模式）

➢ **MAC 地址数**:

MAC 地址数是指交换机的 MAC 地址表中可以存储的 MAC 地址数量。

➢ **VLAN 表项**:

目前，交换机 VLAN 表项数目在 1024 以上，可以满足一般企业的需要。

➢ **机架插槽数**:

机架插槽数是指机架式交换机所能安插的最大模块数，扩展槽数是指固定配置带扩展槽的交换机所能安插的最大模块数。

4-2-3　交换机支持的以太网协议

交换机支持的以太网协议		
标准	说明	规范
IEEE 802.3i	以太网10Base-T规范	两对UTP, RJ-45连接器，传输距离为100m
IEEE 802.3u	快速以太网物理层规范	100Base-TX: 2对5类UTP, 支持10Mbps 、100Mbps 自动协商; 100Base-T4: 4对3类UTP; 100Base-FX: 光纤。
IEEE 802.3z	千兆以太网物理层规范	1000Base-SX: 短波SMF; 1000Base-LX: 长波SMF或MMF。
IEEE 802.3ab	双绞线千兆以太网物理层规范	1000Base-TX
IEEE 802.3ad	Link Aggregation Control Protocol (LACP)	链路汇聚技术可以将多个链路绑定在一起，形成一条高速链路，以达到更高的带宽，并实现链路备份和负载均衡。
IEEE 802.3ae	万兆以太网物理层规范	10GBase-SR和10GBase-SW支持短波(850nm)多模光纤CMMF)，传输距离为2~300m; 10GBase-LR和l10GBase-LW支持长波(1310nm)单模光纤(SMF)，传输距离为2m~10km; 10GBase-ER和10GBase-EW支持超长波(1550nm)单模光纤(SMF)，传输距离为2m~40km。
IEEE 802.3af	Power over Ethernet（POE）	以太网供电，通过双绞线为以太网提供48V的直流电源。
IEEE 802.3x	Flow Control and Back pressure	为交换机提供全双工流控(full-duplex flow control) 和后压式半双工流控(back pressure half-duplex flow control)机制
IEEE 802.1d	Spanning Tree Protocol（STP）	利用生成树算法消除以太网中的循环路径，当网络发生故障时重新协商生成树，并起到链路备份的作用。
IEEE 802.1q	VLAN标记	定义了以太网MAC帧的VLAN标记。标记分两部分: VLANID(12位)和优先级(3位)
IEEE 802.1p	LAN第二层QoS/CoS协议	定义了交换机对MAC帧进行优先级分类，并对组播帧进行过滤的机制，可以根据优先级提供尽力而为(best-effort)的务质址，是IEEE 802.1q 的扩充协议。
IEEE 802.1s	Multiple Spanning Tree Protocol (MSTP)	这是802.1q的补充协议,为交换机增加了通过多重生成树进行VLAN通信的机制
IEEE 802.1v	基于协议和端口的VLAN划分	这是802.1q的补充协议，定义了基于数据链路层协议进行VLAN划分的机制
IEEE 802.1x	用户认证	在局域网中实现基千端口的访问控制
IEEE 802.1w	Rapid Spanning Tree Protocol (RSTP)	当局域网中由千交换机或其他网络元素失效而发生拓扑结构改变时，RSTP可以快速地重新配置生成树，恢复网络的连接。RSTP 对802 . Id 是向后兼容的。
GARP	通用属性注册协议 (GenencAttribute Registration Protocol,GARP)	提供了交换设备之间注册屈性的通用机制。属性信息(例如VLAN标识符)在整个局域网设备中传播开来，并且由相关设备形成一个“ 可达性”子集。GARP 是IEEE 802.1p 的扩充部分。
GVRP	GARP VLAN注册协议(GARP VLAN Registration Protocol,GVRP)	GVRP是GARP的应用，提供与802.lq兼容的VLAN裁剪(VLAN pruning)功能，以及在802.1q干线端口(trunk port)建立动态VLAN的机制。GVRP定义在IEEE 802.lp中。
GMRP	GARP 组播注册协议(GARP Multicast Registration protocol, GMRP)	为交换机提供了根据组播成员的动态信息进行组播树修剪的功能，使得交换机可以动态地管理组播过程。GMRP定义在IEEE 802.1p中。

1-2路由器基础

2-1-1　路由器的分类

- **从功能、性能和应用方面划分**:
  - 骨干路由器：骨干路由器是实现主干网络互连的关键设备，通常采用模块化结构，通过热备份、双电源和双数据通路等冗余技术提高可靠性，华为的 NE40E 系列以上路由器就属于骨干路由器。
  - 企业级路由器：企业级路由器连接许多终端系统，提供通信分类、优先级控制、用户认证、多协议路由和快速自愈等功能。
  - 接入级路由器：接入级路由器也叫边缘路由器，主要用于连接小型企业的客户群。

2-1-2　路由器的端口

- **RJ-45 端口**：这种端口通过双绞线连接以太网。
- **AUI 端口**：AUI 端口是一种 D 型 15 针连接器，用在令牌环网或总线型以太网中。
- **高速同步串口**：在路由器与广域网的连接中，高速同步串行口(Synchronous Serial Port)端口用于连接 DDN、帧中继、X.25 和 PSTN 等网络。
- **ISDN BRI 端口**：ISDN BRI 端口通过 ISDN 线路实现路由器与 Internet 或其他网络的远程连接，ISDN BRI 的 3 个通道(2B+D)的总带宽为 144kbps,端口采用 RJ-45 标准，与 ISDN NTI 的连接使用 RJ-45-to-RJ-45 直通线。
- **异步串口**：异步串口(ASYNC)主要应用于与 Modem 或 Modem 池的连接，以实现远程计算机通过 PSTN 拨号接入。
- **Console 端口**：Console 端口通过配置专用电缆连接至计算机串行口，利用终端仿真程序（如 Hyper Terminal）对路由器进行本地配置。路由器的 Console 端口为 RJ-45 口。
- **AUX 端口**：对路由器进行远程配置时要使用 AUX 端口(Auxiliary Prot)。AUX 端口在外观上 RJ-45 端口一样，只是内部电路不同，实现的功能也不一样。通过 AUX 端口与 Modem 进行连接必须借助 RJ-45 to DB9 或 RJ-45 to DB25 适配器进行电路转换。

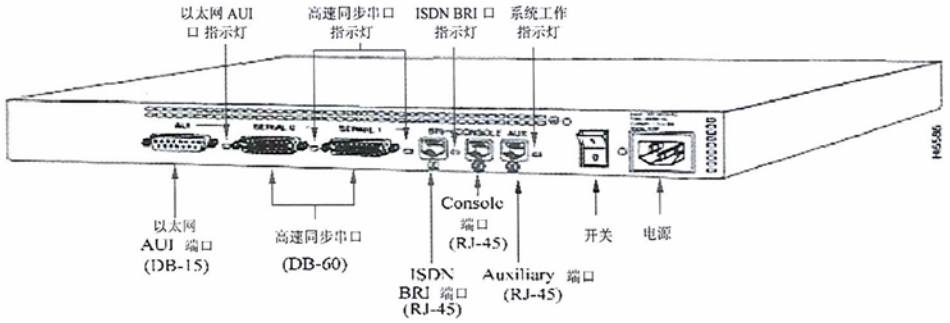


图 10-9　路由器背板示意图

2-1-3　路由器的操作系统

华为路由器、交换机等数据网络产品采用的是通用路由平台 VRP (Versatile Routing Platform)，常用的 VRP 有 VRP5 和 VRP8 两个版本。VRP5 是目前大多数华为设备使用的组件化设计、高可靠性网络操作系统，而 VRP8 支持分布式应用和虚拟化技术，可以适应企业快速扩展的业务需求。

IOS(Internetwork Operating System，互联网操作系统)软件系统包括"BootROM 软件"和"系统软件"两部分，是路由器、交换机等设备启动、运行的必要软件，为网络设备提供支撑、管理、业务等功能。

路由器或交换机的操作是由配置文件(configuration file 或 config)控制。

IOS 有 3 种命令级别，用户视图、系统视图和具体业务视图。

1-3访问路由和交换机

如果要对网络互连设备进行具体的配置，有效地访问一般来用以下几种方法访问路由器或交换机:

- 通过设备的 Console(控制台)端口接终端或运行终端仿真软件的计算机
- 通过设备的 AUX 端口接 Modem,通过电话线与远方的终端或运行终端仿真软件的计算机相连
- 通过 Telnet 程序访问
- 通过 web 浏览器访问
- 通过网管软件访问

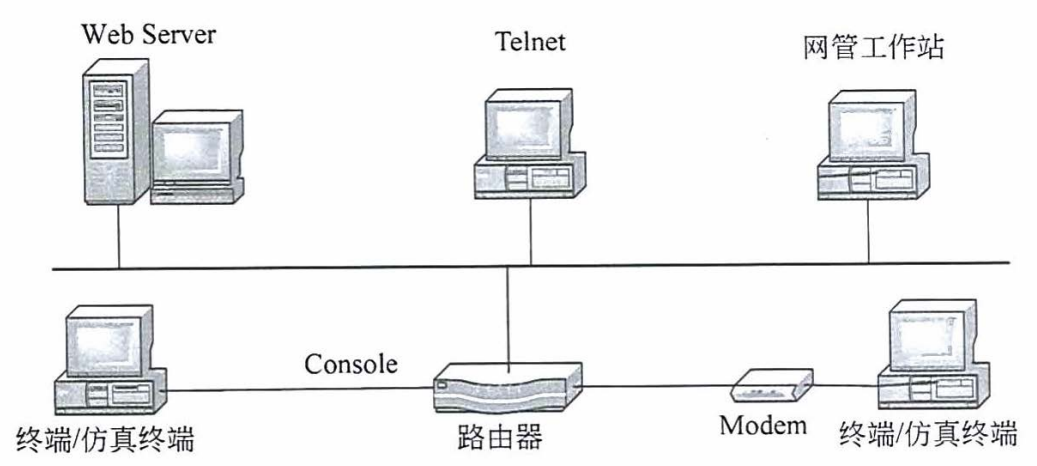


图 10-11　访问路由器的几种方法

2.　交换机配置

不同厂家生产的不同型号的交换机，其具体的配置命令和方法是有差别的，不过配置的原理基本上是相同的，本文档所有的实验均采用华为的 **eNSP** 模拟器及相关路由交换设备进行实验。

2-1交换机的基本配置

2-1-1　console 线路配置

- **电缆连接及终端配置**:

如图 10-13 所示，接好 PC 机和交换机各自的电源线，在关机状态下，把 PC 机的串口 1(COMI)通过控制台电缆与交换机的 Console 端口相连，即完成设备的连接工作。

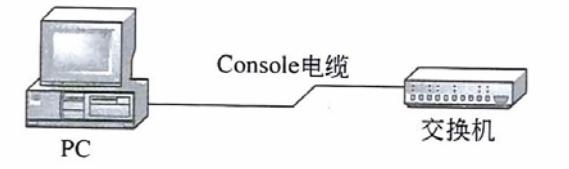


图 10-13　仿真终端与交换机的连接

交换机 Console 端口的默认参数如下:

- 端口速率:9600bps
- 数据位:8
- 奇偶校验:无
- 停止位:1
- 流控:无

在配置 PC 机的超级终端时只需保证端口属性的配置参数与上述参数相匹配即可。

- **交换机的启动**:

在配置好终端仿真软件后，终端窗口就会显示交换机的启动信息，显示交换机的版权信息和软件加载过程，直到出现提示用户设置登录密码(完成 Console 登录密码设置后)。

2-1-2　console 线路密码配置

由于华为设备在使用 console 配置时，路由和交换机几乎没有区别，本实验统一以华为路由器配置为主，交换机配置参考路由器配置。

1> 设备管理方式有几种?

两种：本地管理、远程管理

2> 这两种管理方式分别使用什么线路?

本地管理使用 console 线路

远程管理使用 vty 线路

- **配置 console 线路密码**

2-1-2.1　密码认证模式

```
<Huawei>system-view                    //进入系统试图
[Huawei]sysname R1                     //修改设备名称
[R1]user-interface console 0           //进入 console 线路
[R1-ui-console0]authentication-mode password      //选择密码认证模式
Please configure the login password (maximum length 16):huawei123   //设置密码
[R1-ui-console0]quit
[R1]quit
<R1>quit                               //退出设备登陆
  Configuration console exit, please press any key to log on
Login authentication
Password:                  //在此输入密码，进入设备
<R1>
```

2-1-2.2　aaa 认证模式

1> 配置 aaa 模式本地管理密码:

```
[R1]user-interface console 0                  //进入 console 线路
[R1-ui-console0]authentication-mode aaa       //选择 aaa 模式的认证
[R1-ui-console0]quit
[R1]aaa                                       //进入 aaa 认证模式
[R1-aaa]local-user user0 password cipher huawei123
[R1-aaa]local-user user1 password cipher huawei234
[R1-aaa]local-user user2 password cipher huawei345     //创建三个账号及对应密码
[R1-aaa]local-user user0 privilege level 0
[R1-aaa]local-user user1 privilege level 1
[R1-aaa]local-user user2 privilege level 2             //为三个账号分配不同的权限级别
[R1-aaa]quit
```

（退出设备登陆，然后通过不同的用户进入设备）

2> 设备上配置的用户有多少级权限?

0-15，一共 16 级权限

3> 不同级别的权限分别代表什么?

0 级：访问级权限，通过 0 级用户进入设备基本上什么都不能做，就像游客一样。

1 级：监控级权限，通过 1 级用户进入设备可以对设备的运行状态进行监控。

2 级：系统级权限，通过 2 级用户进入设备可以对设备进行业务配置。

3 级：管理级权限:

15 级：最高级权限（3-15 级暂不研究）

2-1-3　远程管理配置

1> 设备的远程管理线路是哪个？

vty 线路

2> vty 线路和 console 线路有什么不同？

vty 线路可以同时允许多个用户登录，而 console 线路只能允许一个用户同时访问。

3> 远程管理的方式有哪些？

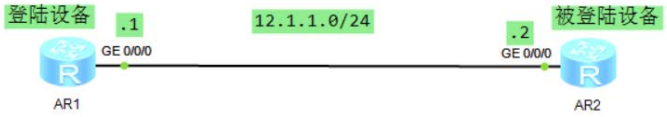
Telnet 协议和 SSH 协议

4> Telnet 和 SSH 有何不同？

Telnet 是明文协议，所有的数据都以明文的方式发送，不安全。

SSH 是密文协议，数据经过加密后再发送，安全性更高。

2-1-3.1 telnet 远程管理



- R1

配置接口 IP 确保和 R2 处于同一网段

```
<Huawei>system-view
Enter system view, return user view with Ctrl+Z.
[Huawei]sysname R1
[R1]interface GigabitEthernet 0/0/0                    //进入 R1 GE0 接口
[R1-GigabitEthernet0/0/0]ip address 12.1.1.1 24        //GE0 接口配置 IP
Apr 22 2018 14:46:49-08:00 R1 %%01IFNET/4/LINK_STATE(l)[0]:The line protocol IP
on the interface GigabitEthernet0/0/0 has entered the UP state.
```

- R2

1） 配置接口 IP 确保和 R1 处于同一网段

```
<Huawei>system-view
Enter system view, return user view with Ctrl+Z.
[Huawei]sysname R2
[R2]interface GigabitEthernet 0/0/0                    //进入 R2 GE0 接口
[R2-GigabitEthernet0/0/0]ip address 12.1.1.2 24        //GE0 接口配置 IP
Apr 22 2018 14:54:19-08:00 R2 %%01IFNET/4/LINK_STATE(l)[0]:The line protocol IP
on the interface GigabitEthernet0/0/0 has entered the UP state.
```

2） 配置 telnet 远程登陆

```
[R2]user-interface vty 0 4                             //进入远程线路 vty 0 4
[R2-ui-vty0-4]authentication-mode aaa                  //使用 aaa 认证模式
[R2-ui-vty0-4]quit
[R2]aaa                                                //进入 aaa 配置
[R2-aaa]local-user user-r1 password cipher huawei123   //创建账号及对应密码
[R2-aaa]local-user user-r1 privilege level 2           //给该账号分配 2 级权限
[R2-aaa]local-user user-r1 service-type telnet         //定义用户的服务类别（启动 telnet 服务）
[R2-aaa]quit
```

3） 进入 R1 验证

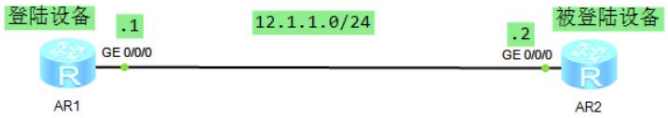
通过 telnet 登录 R2：

```
<R1>telnet 12.1.1.2
```

Username:user-r1
Password:
<R2>system-view
[R2]sysname R22
[R22]

（进入 R2，对 R2 的主机名做修改，telnet 远程管理实现）

2-1-3.2 SSH 远程管理



- R1

配置接口 IP 确保和 R2 处于同一网段

<Huawei>system-view
Enter system view, return user view with Ctrl+Z.
[Huawei]sysname R1
[R1]interface GigabitEthernet 0/0/0 //进入 R1 GE0 接口
[R1-GigabitEthernet0/0/0]ip address 12.1.1.1 24 //GE0 接口配置 IP
Apr 22 2018 14:46:49-08:00 R1 %%01IFNET/4/LINK_STATE(l)[0]:The line protocol IP on the interface GigabitEthernet0/0/0 has entered the UP state.

- R2

1） 配置接口 IP 确保和 R1 处于同一网段

<Huawei>system-view
Enter system view, return user view with Ctrl+Z.
[Huawei]sysname R2
[R2]interface GigabitEthernet 0/0/0 //进入 R2 GE0 接口
[R2-GigabitEthernet0/0/0]ip address 12.1.1.2 24 //GE0 接口配置 IP
Apr 22 2018 14:54:19-08:00 R2 %%01IFNET/4/LINK_STATE(l)[0]:The line protocol IP on the interface GigabitEthernet0/0/0 has entered the UP state.

2） 配置 ssh 远程登陆

[R2]stelnet server enable //开启 SSH 协议
[R2]rsa local-key-pair create //创建加密报文的密钥对
Input the bits in the modulus[default = 512]:1024 //密钥长度
[R2]aaa //使用 aaa 认证模式
[R2-aaa]local-user user-ssh password cipher huawei123 //创建账号及对应密码
[R2-aaa]local-user user-ssh privilege level 2 //给该账号分配 2 级权限
[R2-aaa]local-user user-ssh service-type ssh 创建 ssh 用户
[R2-aaa]quit
[R2]user-interface vty 0 4 //进入 vty 线路
[R2-ui-vty0-4]authentication-mode aaa
[R2-ui-vty0-4]protocol inbound ssh //开启 vty 线路的 ssh 访问功能
[R2-ui-vty0-4]quit
[R2]ssh user user-ssh authentication-type all //定义 ssh 用户的认证模式

3） 进入 R1 验证

通过 ssh 登录 R2：
[R1]ssh client first-time enable

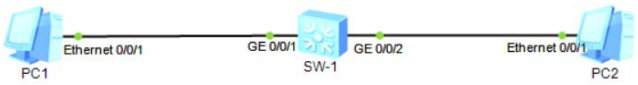
[R1]stelnet 12.1.1.2
Please input the username:user-ssh
Continue to access it? (y/n)[n]:y
Save the server's public key? (y/n)[n]:y
Enter password:
<R2>
（ssh 远程登录成功）

2-1-4　交换机端口配置

交换机的接口属性默认支待一般网络环境，一般情况下是不需要对其接口进行设置的。在某些情况下需要对其端口属性进行配置时，配置的对象主要有接口隔离、速率、双工等信息。

2-1-5.1 接口隔离设置

- **配置接口 GE0/0/1 和 GE0/0/2 的接口隔离功能，实现两个接口之间的二层数据隔离，三层数据互通**



<Switch1>system-view
Enter system view, return user view with Ctrl+Z.
[Switch1]port-isolate mode L2　　//端口隔离模式选择 L2
[Switch1]interface GigabitEthernet 0/0/1　　//进入 GE0 接口
[Switch1-GigabitEthernet0/0/1]port-isolate enable group 1　//接口隔离选择默认组 1
[Switch1-GigabitEthernet0/0/1]quit
[Switch1]interface GigabitEthernet 0/0/2　　//进入 GE2 接口
[Switch1-GigabitEthernet0/0/2]port-isolate enable group 1　//接口隔离选择默认组 1
[Switch1-GigabitEthernet0/0/2]quit
[Switch1]
端口隔离实验成功

2-1-5.2 接口速率设置

- **配置以太网接口 GE0/0/1 在自协商模式下协商速率为 100Mb/s**

<Switch1>system-view
Enter system view, return user view with Ctrl+Z.
[Switch1]interface GigabitEthernet 0/0/1　　//进入 GE1 端口
[Switch1-GigabitEthernet0/0/1]negotiation auto　//自动协商
[Switch1-GigabitEthernet0/0/1]auto speed 100　　//协商速率

2-1-5.3 接口模式设置

- **配置以太网接口 GE0/0/1 在自协商模式下双工模式为全双工模式**

<Switch1>system-view
Enter system view, return user view with Ctrl+Z.
[Switch1]interface GigabitEthernet 0/0/1　　//进入 GE1 端口
[Switch1-GigabitEthernet0/0/1]negotiation auto　//自动协商
[Switch1-GigabitEthernet0/0/1] auto duplex full　　//全双工模式

2-1-5.4 查看和配置 MAC 地址表

交换机通过学习网络中设备的 MAC 地址，并将学习得到的 MAC 地址存放在交换机的缓存中。在需要向目标地址发送数据时就从 MAC 表地址中查找相应地址，找到后才可以向目标快速发送数据。

MAC 表由多条 MAC 地址表项组成。MAC 地址表项由 MAC、VLAN 和端口组成，交换机在收到数据帧时，会解析出数据帧的源 MAC 地址和 VLAN ID 并与接收数据帧的端口组合成一条数据表项。MAC 地址表项的查看可以了解交换机运行的状态信息，排查故障。

- **执行命令 display mac-address，查看所有的 MAC 地址表项**

```
[WS-C2950G-48-EI-5-1]display mac-address
MAC ADDR        VLAN ID  STATE          PORT INDEX               AGING TIME(s)
0001-7a76-3d08  1        LEARNED        GigabitEthernet1/0/49    AGING
0001-7a76-3e5a  1        LEARNED        GigabitEthernet1/0/49    AGING
0[illegible]d-2[illegible]b-e5c1  1        LEARNED        GigabitEthernet1/0/49    AGING
0[illegible]f-e[illegible]9-fd6d  1        LEARNED        GigabitEthernet1/0/49    AGING
0[illegible]f-e[illegible]9-fd6e  1        LEARNED        GigabitEthernet1/0/49    AGING
0[illegible]f-e[illegible]9-dd57  1        LEARNED        GigabitEthernet1/0/49    AGING
0[illegible]-cb[illegible]d-06b8  1        LEARNED        GigabitEthernet1/0/49    AGING
[illegible]-0[illegible]f-0240  1        LEARNED        GigabitEthernet1/0/49    AGING
[illegible]-002d  1        LEARNED        GigabitEthernet1/0/49    AGING
[illegible]-9d77  1        LEARNED        GigabitEthernet1/0/49    AGING
[illegible]-e[illegible]8-4de8  1        LEARNED        GigabitEthernet1/0/49    AGING
[illegible]-6[illegible]-bbca  1        LEARNED        GigabitEthernet1/0/49    AGING
[illegible]-8982  1        LEARNED        GigabitEthernet1/0/49    AGING
[illegible]-6[illegible]-0c4c  1        LEARNED        GigabitEthernet1/0/49    AGING
[illegible]-0d7e  1        LEARNED        GigabitEthernet1/0/49    AGING
[illegible]5260  2        LEARNED        GigabitEthernet1/0/49    AGING
[illegible]2bb  2        LEARNED        GigabitEthernet1/0/49    AGING
[illegible]-1c  2        LEARNED        GigabitEthernet1/0/49    AGING
[illegible]b  2        LEARNED        GigabitEthernet1/0/49    AGING
[illegible]  2        LEARNED        GigabitEthernet1/0/49    AGING
[illegible]  2        LEARNED        GigabitEthernet1/0/49    AGING
[illegible]0  2        LEARNED        GigabitEthernet1/0/49    AGING
  ---- More ----
```

- **执行命令 display interface vlanif 10 显示 VLANIF 接口的 MAC 地址**

```
[Switch1-Ethernet0/0/2]display interface vlanif 10
Vlanif10 current state : UP
Line protocol current state : UP
Last line protocol up time : 2018-04-24 20:34:36 UTC-08:00
Description:
Route Port,The Maximum Transmit Unit is 1500
Internet Address is 10.1.1.100/24
IP Sending Frames' Format is PKTFMT_ETHNT_2, Hardware address is 4c1f-cc6b-75e6
Current system time: 2018-04-24 20:36:02-08:00
    Input bandwidth utilization  : --
    Output bandwidth utilization : --

[Switch1-Ethernet0/0/2]q
[Switch1]display interface vlanif 10
Vlanif10 current state : UP
Line protocol current state : UP
Last line protocol up time : 2018-04-24 20:34:36 UTC-08:00
Description:
Route Port,The Maximum Transmit Unit is 1500
Internet Address is 10.1.1.100/24
IP Sending Frames' Format is PKTFMT_ETHNT_2, Hardware address is 4c1f-cc6b-75e6
Current system time: 2018-04-24 20:36:07-08:00
    Input bandwidth utilization  : --
    Output bandwidth utilization : --
```

- **在 MAC 地址表中增加静态 MAC 地址表项，目的 MAC 地址为 0001-0002-0003,VLAN10 的报文从接 Ethernet0/0/5 转发出去**

[Switch1] mac-address static 0001-0002-0003 ethernet 0/0/5 vlan 10

2-2配置和管理 VLAN

1> 什么是 VLAN?

VLAN 是一种在交换机上划分逻辑网段的二层技术。

2> 为什么要通过交换机划分网段?

① 因为交换机的端口密度比路由器高，并且价格比路由器低，所以组网成本更低。

② 因为交换机划分网段比路由器组网更灵活。

③ 减少广播风暴。

3> VLAN 之间是如何通信的?

不同 VLAN 之间的通信要引入第三层交换技术（三层交换机、路由器）、网关等）才可以解决。

4> VLAN 的配置与管理

主要涉及链路和接口类型、GARP 协议和 VLAN 的配置。

① 链路类型：为了适应不同网络环境的组网需要，链路类型分为**接入链路(Access Link）**和**干道链路(Trunk Link)**两种链路类型。

- 接入链路只能承载 1 个 VLAN 的数据帧，用于连接交换机和用户终端
- 干道链路能承载多个不同 VLAN 的数据帧，用于交换机间互连或连接交换机与路由器

② 接口类型：根据接口连接对象以及对收发数据帧处理的不同，以太网接口分为

- Access 接口：连接终端用户
- Trunk 接口：交换机与交换机或交换机与路由器互联
- Hybrid 接口：交换机与交换机或交换机与路由器互联
- QinQ 接口：公网与私网的互联

③ GARP 协议主要用于建立一种属性传递扩散的机制，以保证协议实体能够注册和注销该属性。是为了简化网络中配置 VLAN 的操作，通过 GVRP 的 VLAN 自动注册功能将设备上的 VLAN 信息快速复制到整个交换网，达到减少手工配置量及保证 VLAN 配置正确的目的（思科 VTP）。

④ 交换机的初始状态是工作在透明模式，有一个默认的 VLAN1，所有端口属于 VLAN1。

2-5-1 划分 VLAN 的方法

虚拟局域网的实现形式有多种，分别是基于接口、MAC 地址、子网、网络层协议、匹配策略方式来划分 VLAN。

① 基于接口划分 VLAN:
交换机的每个接口配置不同的 PVID，当数据帧进入交换机时没有带 VLAN 标签，该数据帧就会被打上接口指定 PVID 的 Tag 并在指定 PVID 中传输。

② 基于源 MAC 地址来划分 VLAN:
建立 MAC 地址和 VLAN ID 映射关系表，当交换机收到的是 Untagged 帧时，就依据该表给数据帧添加指定 VLAN 的 Tag 并在指定 VLAN 中传输。

③ 基于 IP 子网划分 VLAN:
建立 IP 地址和 VLAN ID 映射关系表，当交换机收到的是 Untagged 帧，就依据该表给数据帧添加指定 VLAN 的 Tag 并在指定 VLAN 中传输。

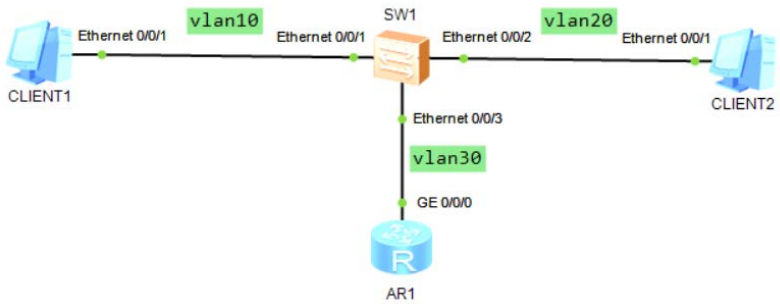
④ 基于网络层协议划分 VLAN:
建立以太网帧中的协议域和 VLAN ID 的映射关系表，当收到的是 Untagged 帧，就依据该表给数据帧添加指定 VLAN 的 Tag 并在指定 VLAN 中传输。

⑤ 基于策略匹配划分 VLAN:
实现多种组合的划分，包括接口、MAC 地址、IP 地址等。
建立配置策略，当收到的是 Untagged 帧，且匹配配置的策略时，给数据帧添加指定 VLAN 的 Tag 并在指定 VLAN 中传输。

2-5-2 配置 VLAN 举例

在网络中，用于终端与交换机、交换机与交换机、交换机与路由器连接时 VLAN 的划分方式多种多样，需要灵活运用。这里就**接入层交换机(二层交换机)的 VLAN 划分举例说明**。

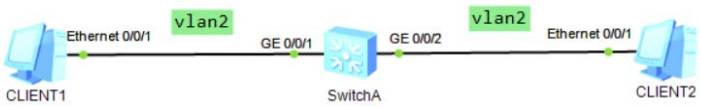
2-1-4.1 基于接口划分 VLAN




```
[SW1]vlan 10
[SW1-vlan10]quit
[SW1]vlan 20
[SW1-vlan20]quit        //创建 vlan10、vlan20(快速创建多个 vlan 使用 vlan batch 10 20 命令)
[SW1]display vlan summary        //查看设备的 vlan 信息
[SW1]int Ethernet0/0/1
[SW1-Ethernet0/0/1]port link-type access
[SW1-Ethernet0/0/1]port default vlan 10        //将接口 e0/0/1 划入对应的 vlan10
```

[SW1-Ethernet0/0/1]quit
[SW1]int e0/0/2
[SW1-Ethernet0/0/2]**port default vlan 20**　　//将接口 e0/0/2 划入对应的 vlan20
[SW1-Ethernet0/0/2]quit
[SW1]int Ethernet0/0/3
[SW1-Ethernet0/0/3]**port link-type trunk**
[SW1-Ethernet0/0/3]**port trunk allow-pass vlan 30**　　//将接口 e0/0/3 划入对应的 vlan30
[SW1-Ethernet0/0/3]quit
[SW1]display port vlan active　　//查看接口对应的 vlan 信息
[SW1]quit

2-1-4.2 基于 MAC 地址划分 VLAN



<Huawei>system-view
Enter system view, return user view with Ctrl+Z.
[Huawei]sysname SwitchA
[SwitchA]vlan batch 2
Info: This operation may take a few seconds. Please wait for a moment...done.
[SwitchA]interface gigabitethernet 0/0/1　　//在接口视图配置上联接口
[SwitchA-GigabitEthernet0/0/1]port link-type hybrid　　//配置上联接口类型
[SwitchA-GigabitEthernet0/0/1]port hybrid tagged vlan 2　　//通过 VLAN2
[SwitchA-GigabitEthernet0/0/1]quit
[SwitchA]interface gigabitethernet 0/0/2　　//进入交换机接口视图
[SwitchA-GigabitEthernet0/0/2]port link-type hybrid　　//配置接口类型
[SwitchA-GigabitEthernet0/0/2]port hybrid untagged vlan 2　　//将接口加入 VLAN2
[SwitchA-GigabitEthernet0/0/2]quit
[SwitchA]vlan 2　　//进入 vlan2 配置
[SwitchA-vlan2]mac-vlan mac-address 22-22-22-22　　//PC 的 MAC 地址与 VLAN2 关联
[SwitchA-vlan2]quit
[SwitchA]interface gigabitethernet 0/0/2
[SwitchA-GigabitEthernet0/0/2]mac-vlan enable　　//基于 MAC 地址启用接口
Info: This operation may take a few seconds. Please wait for a moment...done.
[SwitchA-GigabitEthernet0/0/2]quit

2-3配置 GVRP 协议

GARP(Generic Attribute Registration Protocol)是通用属性注册协议的应用，提供 802.1Q 兼容的 VLAN 裁剪 VLAN pruning 功能和在 802.1Q 干线端口 trunk port 上建立动态 VLAN 的功能。

GARP 作为一个属性注册协议的载体，可以用来传播属性，将 GARP 协议报文的内容映射成不同的属性即可支持不同上层协议应用。

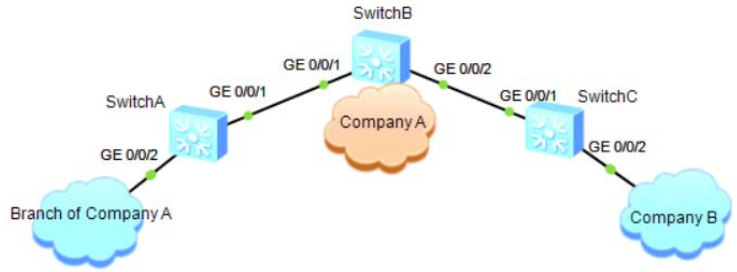
GVRP（GARP VLAN Registration Protocol）是 GARP 的一种应用，用于注册和注销 VLAN 属性。

GARP 协议通过目的 MAC 地址区分不同的应用。在 IEEE Std 802.1Q 中将 01-80-C2-00-00-21 分配给 VLAN 应用，即 GVRP。

- **配置 GVRP 示例**

1> 组网需求

如图所示，公司 A、公司 A 的分公司以及公司 B 之间有较多的交换设备相连，需要通过 GVRP 功能，实现 VLAN 的动态注册。公司 A 的分公司与总部通过 SwitchA 和 SwitchB 互通；公司 B 通过 SwitchB 和 SwitchC 与公司 A 互通，但只允许公司 B 配置的 VLAN 通过。



2> 配置思路

① 使能 GVRP 功能，实现 VLAN 的动态注册。

② 公司 A 的所有交换机配置 GVRP 功能并配置接口注册模式为 Normal，以简化配置。

③ 公司 B 的所有交换机配置 GVRP 功能并将与公司 A 相连的接口的注册模式配置为 Fixed，以控制只允许公司 B 配置的 VLAN 通过。

说明：

使能 GVRP 之前，必须先设置 VCMP 的角色为 Transparent 或 Silent。

3> 配置步骤

① 配置交换机 SwitchA

//全局使能 GVRP 功能

```
<Huawei>
<Huawei>system-view
Enter system view, return user view with Ctrl+Z.
[Huawei]sysname SwitchA
[SwitchA]vcmp role silent
```

//配置接口为 Trunk 类型，并允许所有 VLAN 通过

```
[SwitchA]interface gigabitethernet 0/0/1
[SwitchA-GigabitEthernet0/0/1]port link-type trunk
[SwitchA-GigabitEthernet0/0/1]port trunk allow-pass vlan all
[SwitchA-GigabitEthernet0/0/1]quit
[SwitchA]interface gigabitethernet 0/0/2
[SwitchA-GigabitEthernet0/0/2]port link-type trunk
[SwitchA-GigabitEthernet0/0/2]port trunk allow-pass vlan all
[SwitchA-GigabitEthernet0/0/2]quit
```

//使能接口的 GVRP 功能，并配置接口注册模式

```
[SwitchA]interface gigabitethernet 0/0/1
[SwitchA-GigabitEthernet0/0/1]gvrp
[SwitchA-GigabitEthernet0/0/1]gvrp registration normal
[SwitchA-GigabitEthernet0/0/1]quit
[SwitchA]interface gigabitethernet 0/0/2
[SwitchA-GigabitEthernet0/0/2]gvrp
[SwitchA-GigabitEthernet0/0/2]gvrp registration normal
[SwitchA-GigabitEthernet0/0/2]quit
```

② 配置交换机 SwitchB

//全局使能 GVRP 功能

```
<Huawei>
<Huawei>system-view
Enter system view, return user view with Ctrl+Z.
[Huawei]sysname SwitchB
[SwitchB]vcmp role silent
//配置接口为 Trunk 类型，并允许所有 VLAN 通过
[SwitchB]interface gigabitethernet 0/0/1
[SwitchB-GigabitEthernet0/0/1]port link-type trunk
[SwitchB-GigabitEthernet0/0/1]port trunk allow-pass vlan all
[SwitchB-GigabitEthernet0/0/1]quit
[SwitchB]interface gigabitethernet 0/0/2
[SwitchB-GigabitEthernet0/0/2]port link-type trunk
[SwitchB-GigabitEthernet0/0/2]port trunk allow-pass vlan all
[SwitchB-GigabitEthernet0/0/2]quit
//使能接口的 GVRP 功能，并配置接口注册模式
[SwitchB]interface gigabitethernet 0/0/1
[SwitchB-GigabitEthernet0/0/1]gvrp
[SwitchB-GigabitEthernet0/0/1]gvrp registration normal
[SwitchB-GigabitEthernet0/0/1]quit
[SwitchB]interface gigabitethernet 0/0/2
[SwitchB-GigabitEthernet0/0/2]gvrp
[SwitchB-GigabitEthernet0/0/2]gvrp registration normal
[SwitchB-GigabitEthernet0/0/2]quit
```

③ 配置交换机 SwitchC

```
//创建 VLAN101 ~ VLAN200
<HUAWEI>system-view
[HUAWEI]sysname SwitchC
[SwitchC]vlan batch 101 to 200
//全局使能 GVRP 功能
[SwitchC]vcmp role silent
[SwitchC]gvrp
//配置接口为 Trunk 类型，并允许所有 VLAN 通过
[SwitchC]interface gigabitethernet 0/0/1
[SwitchC-GigabitEthernet0/0/1]port link-type trunk
[SwitchC-GigabitEthernet0/0/1]port trunk allow-pass vlan all
[SwitchC-GigabitEthernet0/0/1]quit
[SwitchC]interface gigabitethernet 0/0/2
[SwitchC-GigabitEthernet0/0/2]port link-type trunk
[SwitchC-GigabitEthernet0/0/2]port trunk allow-pass vlan all
[SwitchC-GigabitEthernet0/0/2]quit
//使能接口的 GVRP 功能，并配置接口注册模式
[SwitchC]interface gigabitethernet 0/0/1
[SwitchC-GigabitEthernet0/0/1]gvrp
[SwitchC-GigabitEthernet0/0/1]gvrp registration fixed
[SwitchC-GigabitEthernet0/0/1]quit
[SwitchC]interface gigabitethernet 0/0/2
```

```
[SwitchC-GigabitEthernet0/0/2]gvrp
[SwitchC-GigabitEthernet0/0/2]gvrp registration normal
[SwitchC-GigabitEthernet0/0/2]quit
```

④ 验证配置结果

配置完成后，公司 A 的分公司用户可以与总部互通，公司 A 属于 VLAN101 ~ VLAN200 的用户可以与公司 B 用户互通。

在 SwitchA 上使用命令 **display gvrp statistics**，查看接口的 GVRP 统计信息，

其中包括：

GVRP 状态、GVRP 注册失败次数、上一个 GVRP 数据单元源 MAC 地址和接口 GVRP 注册类型，结果如下：

```
[SwitchA]display gvrp statistics

  GVRP statistics on port GigabitEthernet0/0/1
    GVRP status                     : Enabled
    GVRP registrations failed       : 0
    GVRP last PDU origin            : 4c1f-cca0-368b
    GVRP registration type          : Normal

  GVRP statistics on port GigabitEthernet0/0/2
    GVRP status                     : Enabled
    GVRP registrations failed       : 0
    GVRP last PDU origin            : 0000-0000-0000
    GVRP registration type          : Normal
```

SwitchB 和 SwitchC 的查看方法与 SwitchA 类似，这里不再赘述。

2-4 配置 STP 协议

以太网交换网络中为了进行链路备份，提高网络可靠性，通常会使用冗余链路。但是使用冗余链路会在交换网络上产生环路，引发广播风暴以及 MAC 地址表不稳定等故障现象，从而导致用户通信质量较差，甚至通信中断。

为解决交换网络中的环路问题，提出了生成树协议 STP（Spanning Tree Protocol）。运行 STP 协议的设备通过彼此交互信息发现网络中的环路，并有选择的对某个端口进行阻塞，最终将环形网络结构修剪成无环路的树形网络结构，从而防止报文在环形网络中不断循环，避免设备由于重复接收相同的报文造成处理能力下降。

生成树协议也是随着网络的发展而不断更新的，从最初的 IEEE 802.1D 中定义的 STP 到 IEEE 802.1W 中定义的快速生成树协议 RSTP（Rapid Spanning Tree Protocol），再到最新的 IEEE 802.1S 中定义的多生成树协议 MSTP（Multiple Spanning Tree Protocol）。

生成树协议中，MSTP 兼容 RSTP、STP，RSTP 兼容 STP。三种生成树协议的比较如表 1-1 所示

➢ 表 1 三种生成树协议的比较

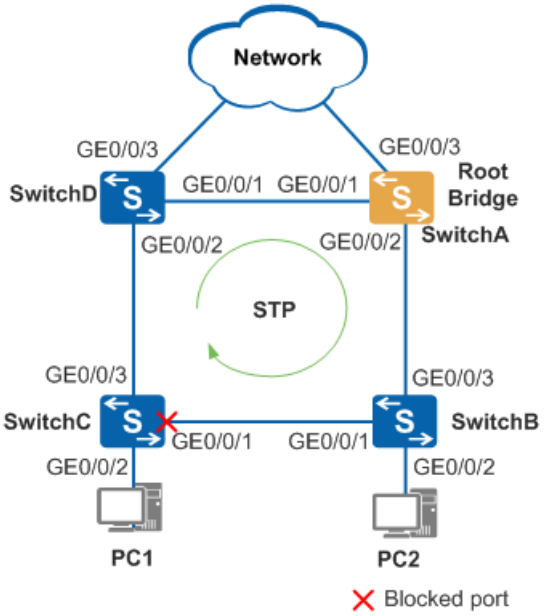
生成树协议	特点	应用场景
STP	•形成一棵无环路的树，解决广播风暴并实现冗余备份。 •收敛速度较慢。	无需区分用户或业务流量，所有VLAN共享一棵生成树。
RSTP	•形成一棵无环路的树，解决广播风暴并实现冗余备份。 •收敛速度快。	
MSTP	•形成多棵无环路的树，解决广播风暴并实现冗余备份。 •收敛速度快。 •多棵生成树在VLAN间实现负载均衡，不同VLAN的流量按照不同的路径转发。	需要区分用户或业务流量，并实现负载分担。不同的VLAN通过不同的生成树转发流量，每棵生成树之间相互独立。

配置 STP 示例

- 配之前注意事项
  - 本举例适用于 S 系列交换机所有产品的所有版本。
  - 与终端相连的端口不用参与 STP 计算，建议将其设置为边缘端口或去使能 STP。

1> 组网需求

图1 配置STP功能组网图



如图 1 所示，当前网络中存在环路，SwitchA、SwitchB、SwitchC 和 SwitchD 都运行 STP，通过彼此交互信息发现网络中的环路，并有选择的对某个端口进行阻塞，最终将环形网络结构修剪成无环路的树形网络结构，从而防止报文在环形网络中不断循环，避免设备由于重复接收相同的报文造成处理能力下降。

2> 配置思路

在处于环形网络中的交换设备上配置 STP 基本功能，包括:

① 配置环网中的设备生成树协议工作在 STP 模式。

② 配置根桥和备份根桥设备。

③ 配置端口的路径开销值，实现将该端口阻塞。

④ 使能 STP，实现破除环路。

3> 配置步骤

① 配置 STP 基本功能

a) 配置环网中的设备生成树协议工作在 STP 模式

```
//配置交换设备 SwitchA 的 STP 工作模式。
<HUAWEI>system-view
[HUAWEI]sysname SwitchA
[SwitchA]stp mode stp
//配置交换设备 SwitchB 的 STP 工作模式。
<HUAWEI>system-view
[HUAWEI]sysname SwitchB
[SwitchB]stp mode stp
//配置交换设备 SwitchC 的 STP 工作模式。
<HUAWEI>system-view
[HUAWEI]sysname SwitchC
[SwitchC]stp mode stp
```

//配置交换设备 SwitchD 的 STP 工作模式。

```
<HUAWEI>system-view
[HUAWEI]sysname SwitchD
[SwitchD]stp mode stp
```

b) 配置根桥和备份根桥设备

//配置 SwitchA 为根桥。

```
[SwitchA] stp root primary
```

//配置 SwitchD 为备份根桥。

```
[SwitchD] stp root secondary
```

c) 配置端口的路径开销值，实现将该端口阻塞

说明：

•端口路径开销值取值范围由路径开销计算方法决定，这里选择使用华为计算方法为例，配置将被阻塞端口的路径开销值为 20000。

•同一网络内所有交换设备的端口路径开销应使用相同的计算方法。

//配置 SwitchA 的端口路径开销计算方法为华为计算方法。

```
[SwitchA]stp pathcost-standard legacy
```

//配置 SwitchB 的端口路径开销计算方法为华为计算方法。

```
[SwitchB]stp pathcost-standard legacy
```

//配置 SwitchC 的端口路径开销计算方法为华为计算方法。

```
[SwitchC]stp pathcost-standard legacy
```

//配置 SwitchC 端口 GigabitEthernet0/0/1 端口路径开销值为 20000。

```
[SwitchC]interface gigabitethernet 0/0/1
[SwitchC-GigabitEthernet0/0/1]stp cost 20000
[SwitchC-GigabitEthernet0/0/1]quit
```

//配置 SwitchD 的端口路径开销计算方法为华为计算方法。

```
[SwitchD]stp pathcost-standard legacy
```

d) 使能 STP，实现破除环路

•将与 PC 机相连的端口设置为边缘端口并使能端口的 BPDU 报文过滤功能

//配置 SwitchB 端口 GigabitEthernet0/0/2 设置为边缘端口并使能端口的 BPDU 报文过滤功能。

```
[SwitchB]interface gigabitethernet 0/0/2
[SwitchB-GigabitEthernet0/0/2]stp edged-port enable
[SwitchB-GigabitEthernet0/0/2]stp bpdu-filter enable
[SwitchB-GigabitEthernet0/0/2]quit
```

//配置 SwitchC 端口 GigabitEthernet0/0/2 设置为边缘端口并使能端口的 BPDU 报文过滤功能。

```
[SwitchC]interface gigabitethernet 0/0/2
[SwitchC-GigabitEthernet0/0/2]stp edged-port enable
[SwitchC-GigabitEthernet0/0/2]stp bpdu-filter enable
[SwitchC-GigabitEthernet0/0/2]quit
```

•设备全局使能 STP

//设备 SwitchA 全局使能 STP。

```
[SwitchA]stp enable
```

//设备 SwitchB 全局使能 STP。

```
[SwitchB]stp enable
```

//设备 SwitchC 全局使能 STP。

```
[SwitchC]stp enable
```

//设备 SwitchD 全局使能 STP。

[SwitchD]stp enable

② 验证配置

经过以上配置，在网络计算稳定后，执行以下操作，验证配置结果。

//在 SwitchA 上执行 **display stp brief** 命令，查看端口状态和端口的保护类型，结果如下：

```
[SwitchA]DIS STP BRIEF
 MSTID  Port                        Role  STP State     Protection
   0    GigabitEthernet0/0/1        DESI  FORWARDING      NONE
   0    GigabitEthernet0/0/2        DESI  FORWARDING      NONE
```

将 SwitchA 配置为根桥后，与 SwitchB、SwitchD 相连的端口 GigabitEthernet0/0/2 和 GigabitEthernet0/0/1 在生成树计算中被选举为指定端口。

//在 SwitchD 上执行 **display stp brief** 命令，查看端口状态和端口的保护类型，结果如下：

```
[SwitchD]dis stp brief
 MSTID  Port                        Role  STP State     Protection
   0    GigabitEthernet0/0/1        ROOT  FORWARDING      NONE
   0    GigabitEthernet0/0/2        DESI  FORWARDING      NONE
```

将 SwitchD 配置为备根桥后，与 SwitchA、SwitchC 相连的端口 GigabitEthernet0/0/1 被选举为根端口、GigabitEthernet0/0/2 在生成树计算中被选举为指定端口。

//在 SwitchB 上执行 **display stp interface gigabitethernet 0/0/1 brief** 命令，查看端口 GigabitEthernet0/0/1 状态，结果如下：

```
[SwitchB]display stp interface GigabitEthernet 0/0/1 brief
 MSTID  Port                        Role  STP State     Protection
   0    GigabitEthernet0/0/1        DESI  FORWARDING      NONE
```

端口 GigabitEthernet0/0/1 在生成树选举中成为指定端口，处于 FORWARDING 状态。

在 SwitchC 上执行 **display stp brief** 命令，查看端口状态，结果如下：

```
[SwitchC]dis stp brief
 MSTID  Port                        Role  STP State     Protection
   0    GigabitEthernet0/0/1        ALTE  DISCARDING      NONE
   0    GigabitEthernet0/0/3        ROOT  FORWARDING      NONE
```

端口 GigabitEthernet0/0/3 在生成树选举中成为根端口，处于 FORWARDING 状态。

端口 GigabitEthernet0/0/1 在生成树选举中成为 Alternate 端口，处于 DISCARDING 状态。

2-5 配置 MSTP+VRRP 组合组网示例

2-5-1 MSTP+VRRP 组合简介

VRRP:

虚拟路由冗余协议(Virtual Router Redundancy Protocol，简称 VRRP)是由 IETF 提出的解决局域网中配置静态网关出现单点失效现象的路由协议。

网络中部署 VRRP 负载分担时，多台设备同时承担业务，每个虚拟设备都包括一个 Master 设备和若干个 Backup 设备。如果为了接入备份需要同时部署冗余链路，则需要部署 MSTP 消除网络中的环路，保证流量的负载分担。

MSTP:

以太网交换网络中为了进行链路备份，提高网络可靠性，通常会使用冗余链路。但是使用冗余链路会在交换网络上产生环路，引发广播风暴以及 MAC 地址表不稳定等故障现象，从而导致用户通信质量较差，甚至通信中断。为解决交换网络中的环路问题，提出了生成树协议 STP（Spanning Tree Protocol）。

STP（Spanning Tree Protocol）是用来解决网络中环路问题的协议。运行该协议的设备通过彼此交互

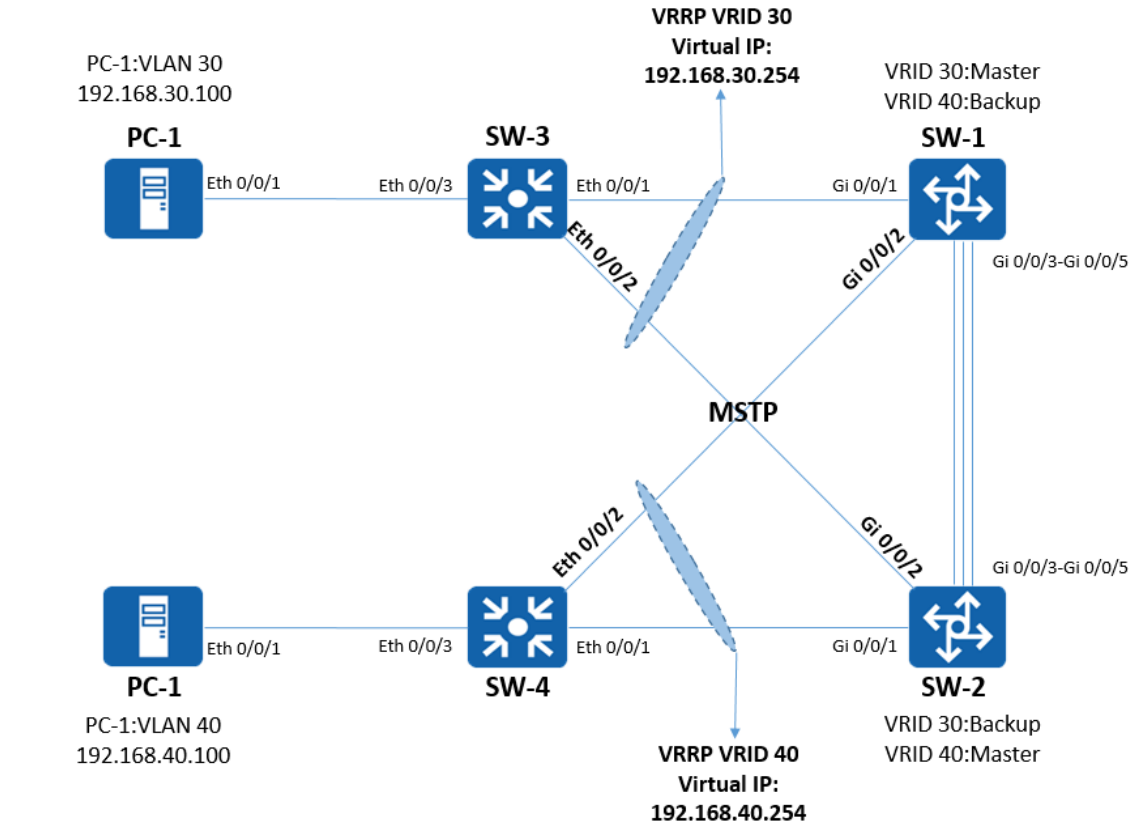
信息而发现网络中的环路，并对某些端口进行阻塞以消除环路。

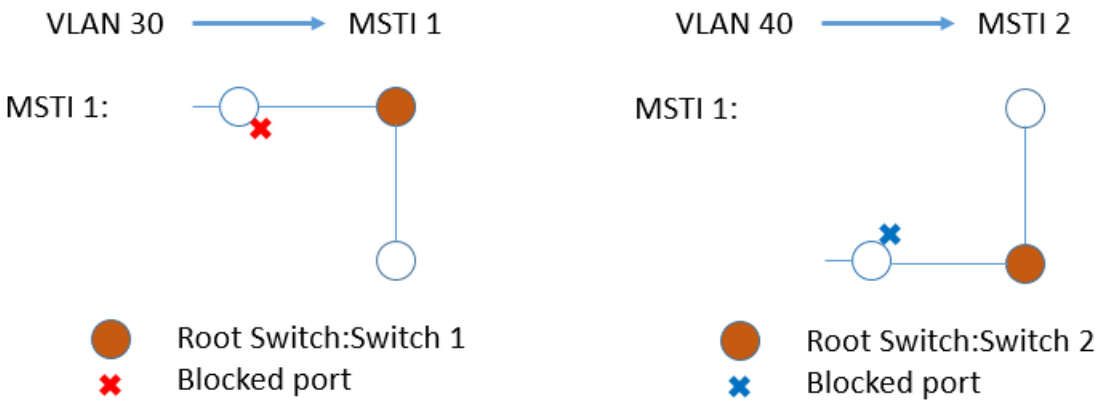
生成树协议中，MSTP 兼容 RSTP、STP，RSTP 兼容 STP。三种生成树协议的比较如表 1-1 所示

表 1-1 三种生成树协议的比较

生成树协议	特点	应用场景
STP	● 形成一棵无环路的树，解决广播风暴并实现冗余备份。 ● 收敛速度较慢。	无需区分用户或业务流量，所有 VLAN 共享一棵生成树。
RSTP	● 形成一棵无环路的树，解决广播风暴并实现冗余备份。 ● 收敛速度快。	
MSTP	● 形成多棵无环路的树，解决广播风暴并实现冗余备份。 ● 收敛速度快。 ● 多棵生成树在 VLAN 间实现负载均衡，不同 VLAN 的流量按照不同的路径转发。	需要区分用户或业务流量，并实现负载分担。不同的 VLAN 通过不同。 的生成树转发流量，每棵生成树间相互独立。

2-5-2　组网需求


VRRP VRID 30
Virtual IP:
192.168.30.254
PC-1:VLAN 30
192.168.30.100
VRID 30:Master
VRID 40:Backup
PC-1
SW-3
SW-1
Eth 0/0/1
Eth 0/0/3
Eth 0/0/1
Gi 0/0/1
Eth 0/0/2
Gi 0/0/2
Gi 0/0/3-Gi 0/0/5
MSTP
Eth 0/0/2
Gi 0/0/2
Gi 0/0/3-Gi 0/0/5
Eth 0/0/1
Eth 0/0/3
Eth 0/0/1
Gi 0/0/1
PC-1
SW-4
SW-2
PC-1:VLAN 40
192.168.40.100
VRRP VRID 40
Virtual IP:
192.168.40.254
VRID 30:Backup
VRID 40:Master


VLAN 30
MSTI 1
MSTI 1:
Root Switch:Switch 1
Blocked port
VLAN 40
MSTI 2
MSTI 1:
Root Switch:Switch 2
Blocked port

设备	接口	对应 VLANIF	IP 地址
SW-1	Gi 0/0/1	VLANIF30 VLANIF40	VLAN30:192.168.30.254/24 VLAN40:192.168.40.254/24
	Gi 0/0/2	VLANIF30 VLANIF40	
SW-1/2	Gi 0/0/3-Gi 0/0/5	VLANIF30 VLANIF40	
SW-2	Gi 0/0/1	VLANIF30 VLANIF40	
	Gi 0/0/2	VLANIF30 VLANIF40	
SW-3	Eth 0/0/1	VLANIF30 VLANIF40	
	Eth 0/0/2	VLANIF30 VLANIF40	
	Eth 0/0/3	**VLANIF30**	
SW-4	Eth 0/0/1	VLANIF30 VLANIF40	
	Eth 0/0/2	VLANIF30 VLANIF40	
	Eth 0/0/3	**VLANIF40**	

2-5-3 配置思路

2-5-3.1 VLAN 划分

二层交换设备无法直接配置接口，需先配置 VLAN 再配置接口

- SW-1/2/3/4 配置 VLAN 30 VLAN 40

2-5-3.2 VRRP 配置

2-5-3.1 在 Switch1 和 Switch2 上创建 VRRP 备份组 VRID30，配置 Switch1 的优先级为 120，作为 Master 设备；Switch2 的优先级为缺省值，作为 Backup 设备。

2-5-3.2 在 Switch1 和 Switch2 上创建 VRRP 备份组 VRID40，配置 Switch2 的优先级为 120，作为 Master 设备；Switch1 的优先级为缺省值，作为 Backup 设备。

2-5-3.3 MSTP 配置

1> 在处于环形网络中的交换设备上配置 MSTP 基本功能

- SW-1/2/3/4 配置启用 MSTP 基本功能

2> 配置保护功能，实现对设备或链路的保护

- 主根桥和备份根桥之间的链路绑定 Eth-Trunk

3> 配置设备的二层转发功能

2-5-3.4 链路聚合配置

LACP（Link Aggregation Control Protocol，链路汇聚控制协议）是一种实现链路动态汇聚的协议。

1) 在带宽比较紧张的情况下，可以通过逻辑聚合扩展带宽到原链路的 N 倍。

2) 在需要对链路进行动态备份的情况下，可以通过配置链路聚合实现同一聚合组各个成员端口之间彼此动态备份。

- Eth-Trunk 设置 lacp 链路聚合、带宽、备份

2-5-4 操作步骤

2-5-4.1 VLAN 划分

- SW-1/2/3/4 均划分 VLAN30 VLAN40

  [SW-1/2/3/4]VLAN batch 30 40

- SW-1/2 VLAN 接口配置

```
[SW-1/2]interface Vlanif30
[SW-1/2-Vlanif30] ip address 192.168.30.253 255.255.255.0  //配置 SW-1/2 VLAN30 的 ip 地址
[SW-1/2-Vlanif30]quit
[SW-1/2]Interface Vlanif40
[SW-1/2-Vlanif40] ip address 192.168.40.253 255.255.255.0  //配置 SW-1/2 VLAN30 的 ip 地址
[SW-1/2-Vlanif40]quit
```

2-5-4.2 VRRP 配置

- **SW-1**:

```
[SW-1]interface Vlanif30
[SW-1-Vlanif30] vrrp vrid 30 virtual-ip 192.168.30.254  //创建组号为 30 的 VRRP 备份组并为备份组指定虚拟 IP 地址 192.168.30.254.
[SW-1-Vlanif30] vrrp vrid 30 priority 120  //配置 VRRP 备份组 30 的优先级为 120.
[SW-1-Vlanif30]quit
[SW-1]Interface Vlanif40
[SW-1-Vlanif40] vrrp vrid 40 virtual-ip 192.168.40.254  //创建组号为 40 的 VRRP 备份组并为备份组指定虚拟 IP 地址 192.168.40.254.
[SW-1-Vlanif40] vrrp vrid 40 priority 100  //配置 VRRP 备份组 40 的优先级为 100(缺省值).
[SW-1-Vlanif40]quit
```

- **SW-2**:

```
[SW-2]interface Vlanif30
[SW-2-Vlanif30] vrrp vrid 30 virtual-ip 192.168.30.254  //创建组号为 30 的 VRRP 备份组并为备份组指定虚拟 IP 地址 192.168.30.254.
[SW-2-Vlanif30] vrrp vrid 30 priority 100  //配置 VRRP 备份组 30 的优先级为 100(缺省值).
[SW-2-Vlanif30]quit
[SW-2]interface Vlanif40
[SW-2-Vlanif40] vrrp vrid 40 virtual-ip 192.168.40.254  //创建组号为 40 的 VRRP 备份组并为备份组指定虚拟 IP 地址 192.168.40.254.
[SW-2-Vlanif40] vrrp vrid 40 priority 120  //配置 VRRP 备份组 40 的优先级为 120.
[SW-2-Vlanif40]quit
```

2-5-4.3 MSTP 配置

1> 配置 Switch1、Switch2、Switch3 和 Switch4 到域名为 R34 的域内，创建实例 MSTI1 和实例 MSTI2

说明:

当两台交换设备的以下配置都相同时，这两台交换设备属于同一个 MST 域.

- MST 域的域名.
- 多生成树实例和 VLAN 的映射关系.
- MST 域的修订级别.

#SW-1/2/3/4 的 STP 配置。

```
[SW-1/2/3/4]stp region-configuration     //STP 域配置.
[SW-1/2/3/4-mst-region]region-name R34     //配置域名为 R34
[SW-1/2/3/4-mst-region] instance 1 vlan 30     //将 VLAN 30 映射到实例 1 上.
[SW-1/2/3/4-mst-region] instance 2 vlan 40     //将 VLAN 40 映射到实例 2 上.
[SW-1/2/3/4-mst-region] active region-configuration     //激活 MST 域的配置.
[SW-1/2/3/4-mst-region]quit
```

2> 在域 R34 内，配置 MSTI1 与 MSTI2 的根桥与备份根桥

- SW-1:

```
[SW-1]stp instance 1 root primary     //配置 Switch1 为 MSTI1 的根桥.
[SW-1]stp instance 2 root secondary     //配置 Switch1 为 MSTI2 的备份根桥.
[SW-1]quit
```

- SW-2:

```
[SW-2]stp instance 1 root secondary     //配置 Switch2 为 MSTI1 的备份根桥.
[SW-2]stp instance 2 root primary     //配置 Switch2 为 MSTI2 的根桥.
[SW-2]quit
```

3> 主根桥和备份根桥之间的链路绑定 Eth-Trunk

- SW-1:

```
[SW-1]interface Eth-Trunk1    //配置及接口 Eth-Trunk1.
[SW-1-Eth-Trunk1] port link-type trunk    //端口链路类型 Trunk.
[SW-1-Eth-Trunk1] port trunk allow-pass vlan 30 40    //端口 Trunk 允许 VLAN30 VLAN40 通过.
[SW-1-Eth-Trunk1] mode lacp-static    //Eth-Trunk1 使用 lacp 静态链路聚合协议.
[SW-1-Eth-Trunk1] max active-linknumber 2    //最大活跃链路为 2 条.
[SW-1-Eth-Trunk1]quit
```

- SW-2:

```
[SW-2]interface Eth-Trunk1    //配置及接口 Eth-Trunk1.
[SW-2-Eth-Trunk1] port link-type trunk    //端口链路类型 Trunk.
[SW-2-Eth-Trunk1] port trunk allow-pass vlan 30 40    //端口 Trunk 允许 VLAN30 VLAN40 通过.
[SW-2-Eth-Trunk1] mode lacp-static    //Eth-Trunk1 使用 lacp 静态链路聚合协议.
[SW-2-Eth-Trunk1] lacp preempt enable     //启用 lacp 抢占模式
[SW-2-Eth-Trunk1]quit
```

4> 配置处于环网中的设备的二层转发功能

- SW-1/2 中 GE 0/0/3-GE 0/0/5 端口配置
  - SW-1/2:

```
[SW-1/2]interface Eth-Trunk 1
[SW-1/2-Eth-Trunk1]trunkport gigabitethernet 0/0/3 to 0/0/5     //将 SW-1/2 的
```

GE0/0/3-GE0/0/5 加入 Eth-Trunk 1 中

- 由于 SW-1 和 SW-2 中 GE0/0/3-GE0/0/5 三个接口形成链路聚合，其中 GE0/0/5 接口作为聚合链路的备份链路、SW-1 为**主动端**，因此需要在 Switch-1 交换机中设置 GE 0/0/3 和 GE 0/0/4 接口的 lacp 优先级.
  - SW-1:

```
[SW-1]interface GigabitEthernet 0/0/3
[SW-1-GigabitEthernet0/0/3]lacp priority 100     //设置 lacp 优先级.
[SW-1-GigabitEthernet0/0/3]quit
[SW-1]interface GigabitEthernet 0/0/4
[SW-1-GigabitEthernet0/0/4]lacp priority 100     //设置 lacp 优先级.
[SW-1-GigabitEthernet0/0/4]quit
```

- SW-1/2 中 GE 0/0/1 和 GE 0/0/2 接口配置
  - SW-1/2:

```
[SW-1/2]interface GigabitEthernet 0/0/1
[SW-1/2-GigabitEthernet0/0/1]port link-type trunk
[SW-1/2-GigabitEthernet0/0/1]port trunk allow-pass vlan 30 40
[SW-1/2-GigabitEthernet0/0/1]quit
[SW-1/2]interface GigabitEthernet 0/0/2
[SW-1/2-GigabitEthernet0/0/2]port link-type trunk
[SW-1/2-GigabitEthernet0/0/2]port trunk allow-pass vlan 30 40
[SW-1/2-GigabitEthernet0/0/2]quit
```

- SW-3/4 中 GE 0/0/1 和 GE 0/0/2 接口配置
  - SW-3/4:

```
[SW-3/4]interface GigabitEthernet 0/0/1
[SW-3/4-GigabitEthernet0/0/1]port link-type trunk
[SW-3/4-GigabitEthernet0/0/1]port trunk allow-pass vlan 30 40
[SW-3/4-GigabitEthernet0/0/1]quit
[SW-3/4]interface GigabitEthernet 0/0/2
[SW-3/4-GigabitEthernet0/0/2]port link-type trunk
[SW-3/4-GigabitEthernet0/0/2]port trunk allow-pass vlan 30 40
[SW-3/4-GigabitEthernet0/0/2]quit
```

- SW-3/4 中 GE0/0/3 接口配置(直连到 PC 端)
  - SW-3/4:

```
[SW-3/4]interface GigabitEthernet 0/0/3
[SW-3/4-GigabitEthernet0/0/3]port link-type access
[SW-3-GigabitEthernet0/0/3]port default vlan 30     // SW-3 GE 0/0/3 接口对应 VLAN30.
[SW-4-GigabitEthernet0/0/3]port default vlan 40     // SW-4 GE 0/0/3 接口对应 VLAN40.
[SW-3/4-GigabitEthernet0/0/3]quit
```

2-5-5　验证配置

2-5-5.1 VRRP 配置验证

- 在 Switch1 上执行 display vrrp/display vrrp brief 命令，可以看到 Switch1 在备份组 30 中作为 Master 设备，在备份组 40 中作为 Backup 设备（配置有问题，建议自行寻找原因）

```
[SW-1]display  vrrp brief
VRID  State        Interface                Type     Virtual IP
------------------------------------------------------------------
30    Master       Vlanif30                 Normal   192.168.30.254
40    Master       Vlanif40                 Normal   192.168.40.254
------------------------------------------------------------------
Total:2     Master:2     Backup:0     Non-active:0
```

- 在 Switch2 上执行 display vrrp/display vrrp brief 命令，可以看到 Switch2 在备份组 30 中作为 Backup 设备，在备份组 40 中作为 Master 设备

```
[SW-2]display vrrp brief
VRID  State        Interface                Type     Virtual IP
------------------------------------------------------------------
30    Backup       Vlanif30                 Normal   192.168.30.254
40    Master       Vlanif40                 Normal   192.168.40.254
------------------------------------------------------------------
Total:2     Master:1     Backup:1     Non-active:0
```

2-5-5.2 MSTP 配置验证

说明：**本配置举例以实例 1 和实例 2 为例，因此不用关注实例 0 中端口的状态**

- 在实例 1 的根桥 Switch1 上执行 display stp brief 命令，查看端口状态，结果如下:

```
[SW-1]dis stp brief
 MSTID  Port                        Role  STP State     Protection
   0    GigabitEthernet0/0/1        DESI  FORWARDING      NONE
   0    GigabitEthernet0/0/2        ROOT  FORWARDING      NONE
   0    Eth-Trunk1                  ALTE  DISCARDING      NONE
   1    GigabitEthernet0/0/1        DESI  FORWARDING      NONE
   1    GigabitEthernet0/0/2        DESI  FORWARDING      NONE
   1    Eth-Trunk1                  DESI  FORWARDING      NONE
   2    GigabitEthernet0/0/1        DESI  FORWARDING      NONE
   2    GigabitEthernet0/0/2        DESI  FORWARDING      NONE
   2    Eth-Trunk1                  ROOT  FORWARDING      NONE
```

在 MSTI1 中，由于 Switch1 根桥，Switch1 的端口 Eth-Trunk1、GE 0/0/1 和 GE 0/0/2 成为指定端口.

在 MSTI2 中，Switch1 的端口 GE 0/0/1 和 GE 0/0/2 成为指定端口，端口 Eth-Trunk1 成为根端口.

- 在实例 2 的根桥 Switch2 上执行 display stp brief 命令，查看端口状态，结果如下:

```
[SW-2]dis stp brief
 MSTID  Port                        Role  STP State     Protection
   0    GigabitEthernet0/0/1        ROOT  FORWARDING      NONE
   0    GigabitEthernet0/0/2        DESI  FORWARDING      NONE
   0    Eth-Trunk1                  DESI  FORWARDING      NONE
   1    GigabitEthernet0/0/1        DESI  FORWARDING      NONE
   1    GigabitEthernet0/0/2        DESI  FORWARDING      NONE
   1    Eth-Trunk1                  ROOT  FORWARDING      NONE
   2    GigabitEthernet0/0/1        DESI  FORWARDING      NONE
   2    GigabitEthernet0/0/2        DESI  FORWARDING      NONE
   2    Eth-Trunk1                  DESI  FORWARDING      NONE
```

在 MSTI2 中，由于 Switch2 根桥，Switch2 的端口 Eth-Trunk1、GE 0/0/1 和 GE 0/0/2 成为指定端口.

在 MSTI1 中，Switch2 的端口 GE 0/0/1 和 GE 0/0/2 成为指定端口，端口 Eth-Trunk1 成为根端口.

- 在接入交换机 Switch3 上执行 display stp brief 命令，结果如下：

```
[SW-3]dis stp brief
 MSTID  Port                        Role  STP State     Protection
   0    GigabitEthernet0/0/1        ALTE  DISCARDING      NONE
   0    GigabitEthernet0/0/2        ROOT  FORWARDING      NONE
   0    GigabitEthernet0/0/3        DESI  FORWARDING      NONE
   1    GigabitEthernet0/0/1        ROOT  FORWARDING      NONE
   1    GigabitEthernet0/0/2        ALTE  DISCARDING      NONE
   1    GigabitEthernet0/0/3        DESI  FORWARDING      NONE
   2    GigabitEthernet0/0/1        ALTE  DISCARDING      NONE
   2    GigabitEthernet0/0/2        ROOT  FORWARDING      NONE
```

Switch3 的端口：

GE 0/0/1 在 MSTI1 中为根端口、在 MSTI2 中被阻塞；

GE 0/0/2 在 MSTI2 中为根端口、在 MSTI1 中被阻塞；

GE 0/0/3 在 MSTI1 中被计算为指定端口。

- 在接入交换机 Switch4 上执行 display stp brief 命令，结果如下：

```
[SW-4]dis stp brief
 MSTID  Port                        Role  STP State     Protection
   0    GigabitEthernet0/0/1        DESI  FORWARDING      NONE
   0    GigabitEthernet0/0/2        DESI  FORWARDING      NONE
   0    GigabitEthernet0/0/3        DESI  FORWARDING      NONE
   1    GigabitEthernet0/0/1        ALTE  DISCARDING      NONE
   1    GigabitEthernet0/0/2        ROOT  FORWARDING      NONE
   2    GigabitEthernet0/0/1        ROOT  FORWARDING      NONE
   2    GigabitEthernet0/0/2        ALTE  DISCARDING      NONE
   2    GigabitEthernet0/0/3        DESI  FORWARDING      NONE
```

Switch4 的端口：

GE 0/0/1 在 MSTI2 中为根端口、在 MSTI1 中被阻塞；

GE 0/0/2 在 MSTI1 中为根端口、在 MSTI2 中被阻塞；；

GE 0/0/2 在 MSTI1 中被计算为指定端口。

2-5-5.3 PC 端配置验证

- PC-1:IP:192.268.30.100/24
- PC-2:IP:192.268.40.100/24

PC-1/PC-2 互 ping 通即可

3. 路由器配置

路由器(Router)是一种典型的网络层设备，在 OSI 参考模型中被称为中介系统，用于完成网络层中继或第三层中继的任务。路由器负责在两个局域网的网络层间接传输数据分组，并确定网络上数据传送的最佳路径。

异种网络互联与多个子网互联都应采用路由器来完成。

路由器的主要工作就是为经过的每个数据包寻找一条最佳的传输路径，并将该数据有效地传送到目的站点。由此可见，选择最佳路径的策略（路由算法）是路由器的关键所在。为了完成这项工作，在路由器中保存着各种传输路径的相关数据—路由表(RoutingTable)供路由选择时使用。路由表中保存着子网的标志信息、下一跳地址和将数据转发出去的接口等信息。

路由表分为静态路由表和动态路由表

静态路由：手工指定（默认路由、静态路由）

动态路由：

距离矢量（Distance-Vector）路由协议：**RIP**（Routing information Protocol）

链路状态（Link-State）路由协议：**OSPF、IS-IS、IGP**

平衡混合（Balanced-Hybrid）路由协议：**BGP**

4-1路由器的基本配置

本实验以华为模拟器 eNSP 中 AR3260 为例

3-1-1 路由器管理配置

#设置系统的日期、时间和时区

<Huawei>clock timezone BJ add 08:00:00 //设置时区

<Huawei>clock datetime 20:10:00 2018-05-23 //设置时间

<Huawei>dis clock //查看时间

2018-05-23 20:10:05+08:00

Wednesday

Time Zone(BJ) : UTC+08:00

#设置设备名称和管理 IP

<Huawei>system-view //进入系统视图

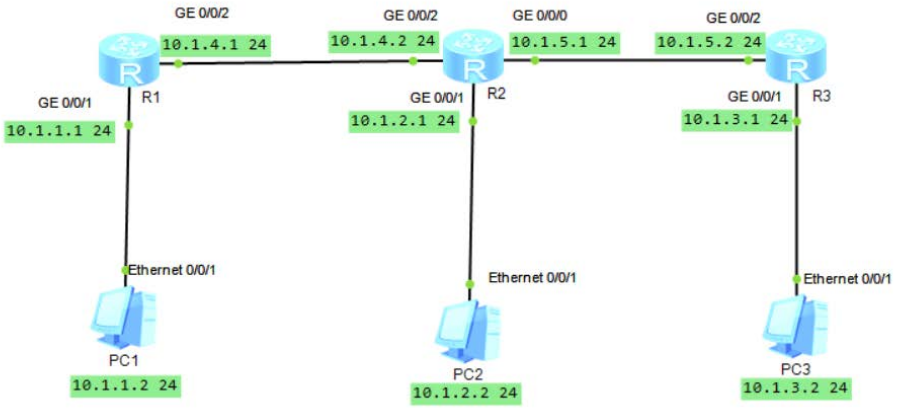
Enter system view, return user view with Ctrl+Z.

[Huawei]interface GigabitEthernet 0/0/0 进入配置接口（区别交换机的 vlan if）

[Huawei-GigabitEthernet0/0/0]ip address 100.100.100.100 24 //配置接口 ip/掩码

[Huawei-GigabitEthernet0/0/0]quit

3-1-2　静态路由配置



① 配置各路由的接口 IP

a)　R1

```
<Huawei>sys
<Huawei>system-view
Enter system view, return user view with Ctrl+Z.
[Huawei]un in en
Info: Information center is disabled.
[Huawei]sysname R1
[R1]interface GigabitEthernet 0/0/1
[R1-GigabitEthernet0/0/1]ip address 10.1.1.1 24              //配置接口 IP
[R1-GigabitEthernet0/0/1]quit
[R1]interface GigabitEthernet 0/0/2
[R1-GigabitEthernet0/0/2]ip address 10.1.4.1 24              //配置接口 IP
[R1-GigabitEthernet0/0/2]quit
```

b)　R2

```
<Huawei>system-view
Enter system view, return user view with Ctrl+Z.
[Huawei]un in en
Info: Information center is disabled.
[Huawei]sysname R2
[R2]interface GigabitEthernet 0/0/1
[R2-GigabitEthernet0/0/1]ip address 10.1.2.1 24      //配置接口 IP
[R2-GigabitEthernet0/0/1]interface GigabitEthernet 0/0/2
[R2-GigabitEthernet0/0/2]ip address 10.1.4.2 24     //配置接口 IP
[R2]interface GigabitEthernet 0/0/0
[R2-GigabitEthernet0/0/0]ip address 10.1.5.1 24     //配置接口 IP
[R2-GigabitEthernet0/0/0]quit
```

c)　R3

```
<Huawei>system-view
Enter system view, return user view with Ctrl+Z.
[Huawei]sysn
[R3]UN IN EN
Info: Information center is disabled.
[Huawei]sysname R3
```

```
[R3]interface GigabitEthernet 0/0/2
[R3-GigabitEthernet0/0/2]ip address 10.1.5.2 24   //配置接口 IP
[R3-GigabitEthernet0/0/2]quit
[R3]interface GigabitEthernet 0/0/1
[R3-GigabitEthernet0/0/1]ip address 10.1.3.1 24   //配置接口 IP
[R3-GigabitEthernet0/0/1]quit
```

② 配置各路由器的静态 IP

a) R1

```
[R1]ip route-static 10.1.2.0 255.255.255.0 10.1.4.2      //R1 到 PC2 的静态路由
[R1]ip route-static 10.1.3.0 255.255.255.0 10.1.4.2      //R1 到 PC3 的静态路由
[R1]ip route-static 10.1.5.0 255.255.255.0 10.1.4.2      //R1 到 R3 的静态路由
```

b) R2

```
[R2]ip route-static 10.1.1.0 255.255.255.0 10.1.4.1      //R2 到 PC1 的静态路由
[R2]ip route-static 10.1.3.0 255.255.255.0 10.1.5.2      //R2 到 PC3 的静态路由
```

c) R3

```
[R3]ip route-static 10.1.1.0 255.255.255.0 10.1.5.1      //R3 到 PC1 的静态路由
[R3]ip route-static 10.1.2.0 255.255.255.0 10.1.5.1      //R3 到 PC2 的静态路由
[R3]ip route-static 10.1.4.0 255.255.255.0 10.1.5.1      //R3 到 R1 的静态路由
```

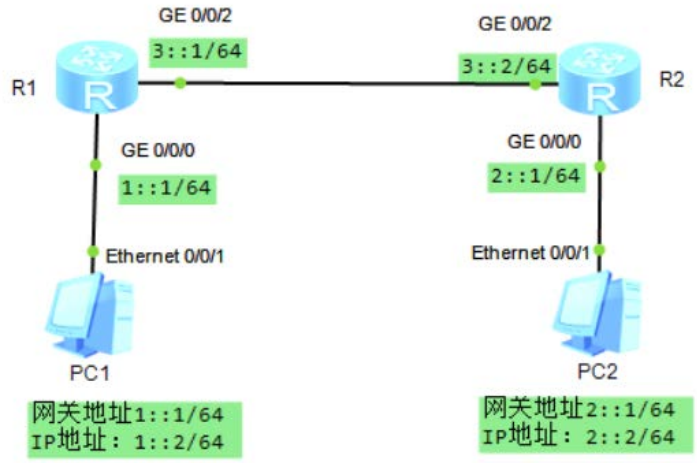
③ 在各个路由器上执行 display ip routing-table 查看路由表

```
[R1]dis ip routing-table
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
Routing Tables: Public
         Destinations : 9        Routes : 9

Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface

        10.1.1.0/24  Direct  0    0           D   10.1.1.1        GigabitEthernet
0/0/1
        10.1.1.1/32  Direct  0    0           D   127.0.0.1       GigabitEthernet
0/0/1
        10.1.2.0/24  Static  60   0          RD   10.1.4.2        GigabitEthernet
0/0/2
        10.1.3.0/24  Static  60   0          RD   10.1.4.2        GigabitEthernet
0/0/2
        10.1.4.0/24  Direct  0    0           D   10.1.4.1        GigabitEthernet
0/0/2
        10.1.4.1/32  Direct  0    0           D   127.0.0.1       GigabitEthernet
0/0/2
        10.1.5.0/24  Static  60   0          RD   10.1.4.2        GigabitEthernet
0/0/2
       127.0.0.0/8   Direct  0    0           D   127.0.0.1       InLoopBack0
       127.0.0.1/32  Direct  0    0           D   127.0.0.1       InLoopBack0
```

```
[R2] dis ip routing-table
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
Routing Tables: Public
         Destinations : 10       Routes : 10

Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface

        10.1.1.0/24  Static  60   0          RD   10.1.4.1        GigabitEthernet
0/0/2
        10.1.2.0/24  Direct  0    0           D   10.1.2.1        GigabitEthernet
0/0/1
        10.1.2.1/32  Direct  0    0           D   127.0.0.1       GigabitEthernet
0/0/1
        10.1.3.0/24  Static  60   0          RD   10.1.5.2        GigabitEthernet
0/0/0
        10.1.4.0/24  Direct  0    0           D   10.1.4.2        GigabitEthernet
0/0/2
        10.1.4.2/32  Direct  0    0           D   127.0.0.1       GigabitEthernet
0/0/2
        10.1.5.0/24  Direct  0    0           D   10.1.5.1        GigabitEthernet
0/0/0
        10.1.5.1/32  Direct  0    0           D   127.0.0.1       GigabitEthernet
0/0/0
       127.0.0.0/8   Direct  0    0           D   127.0.0.1       InLoopBack0
       127.0.0.1/32  Direct  0    0           D   127.0.0.1       InLoopBack0

[R3]dis ip routing-table
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
Routing Tables: Public
         Destinations : 9        Routes : 9

Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface

        10.1.1.0/24  Static  60   0          RD   10.1.5.1        GigabitEthernet
0/0/2
        10.1.2.0/24  Static  60   0          RD   10.1.5.1        GigabitEthernet
0/0/2
        10.1.3.0/24  Direct  0    0           D   10.1.3.1        GigabitEthernet
0/0/1
        10.1.3.1/32  Direct  0    0           D   127.0.0.1       GigabitEthernet
0/0/1
        10.1.4.0/24  Static  60   0          RD   10.1.5.1        GigabitEthernet
0/0/2
        10.1.5.0/24  Direct  0    0           D   10.1.5.2        GigabitEthernet
0/0/2
        10.1.5.2/32  Direct  0    0           D   127.0.0.1       GigabitEthernet
0/0/2
       127.0.0.0/8   Direct  0    0           D   127.0.0.1       InLoopBack0
       127.0.0.1/32  Direct  0    0           D   127.0.0.1       InLoopBack0
```

④ 在 PC 上互 ping，可以通信

3-1-3　静态路由 IPv6 配置



① 配置各路由的接口 IP（类似 IPv4 配置，IPv6 功能默认关闭，使用时需开启全局使能 IPv6）

a)　R1

```
<Huawei>system-view
Enter system view, return user view with Ctrl+Z.
[Huawei]un in en
Info: Information center is disabled.
[Huawei]sysname R1
[R1]ipv6                                    //全局使能 IPV6（启用路由器 IPv6 报文转发能力）
[R1]interface GigabitEthernet 0/0/0         //进入对应接口
[R1-GigabitEthernet0/0/0]ipv6 enable        //接口开启 IPv6 功能
[R1-GigabitEthernet0/0/0]ipv6 address 1::1 64   //接口配置对应的 IPv6 地址
[R1-GigabitEthernet0/0/0]quit
[R1]interface GigabitEthernet 0/0/2         //进入对应接口
[R1-GigabitEthernet0/0/2]ipv6 enable        //接口开启 IPv6 功能
[R1-GigabitEthernet0/0/2]ipv6 address 3::1 64   //接口配置对应的 IPv6 地址
[R1-GigabitEthernet0/0/2]quit
```

b)　R2

```
<Huawei>system-view
Enter system view, return user view with Ctrl+Z.
[Huawei]sysn R2
[R2]ipv6
[R2]interface GigabitEthernet 0/0/2
[R2-GigabitEthernet0/0/2]ipv6 enable
[R2-GigabitEthernet0/0/2]ipv6 address 3::2 64
[R2-GigabitEthernet0/0/2]quit
[R2]interface GigabitEthernet 0/0/0
[R2-GigabitEthernet0/0/0]ipv6 enable
[R2-GigabitEthernet0/0/0]ipv6 address 2::1 64
[R2-GigabitEthernet0/0/0]quit
```

R2 接口设置步骤同 R1

② 配置到各路由器的静态路由

a)　R1

```
[R1]ipv6 route-static 2:: 64 3::2          //R1 到 PC2 的静态 IPv6 路由
```

b) R2

[R2]**ipv6 route-static 1:: 64 3::1** //R2 到 PC1 的静态 IPv6 路由

③ 检查配置结果

使用 **display ipv6 routing-table** 命令查看路由器的 IP 路由表

使用 **Ping ipv6** 命令验证连通性，要求从 PC1 可以 ping 通 PC2

4-2 RIP 路由配置

距离矢量路由协议（D-V）

RIPv2 支持 CIDR/VLSM

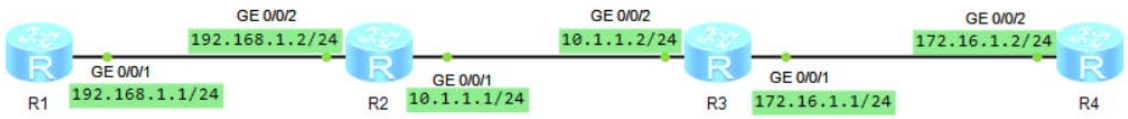
使用组播地址（224.0.0.x）发送路由信息

适用于小型网络（最大跳 15）

30s 广播一次路由信息

工作于网络层

优先级（AD）默认 100



① 配置各路由器的接口 IP

a) 配置 R1

```
<Huawei>system-view
Enter system view, return user view with Ctrl+Z.
[Huawei]un in en
Info: Information center is disabled.
[Huawei]sysn R1
[R1]int gig 0/0/1
[R1-GigabitEthernet0/0/1]ip address 192.168.1.1 24
[R1-GigabitEthernet0/0/1]
```

b) 配置 R2

```
<Huawei>system-view
Enter system view, return user view with Ctrl+Z.
[Huawei]Un in en
Info: Information center is disabled.
[Huawei]sysn R2
[R2]int gig 0/0/2
[R2-GigabitEthernet0/0/2]ip add 192.168.1.2 24
[R2-GigabitEthernet0/0/2]int gig 0/0/1
[R2-GigabitEthernet0/0/1]ip add 10.1.1.1 24
[R2-GigabitEthernet0/0/1]quit
```

c) 配置 R3

```
<Huawei>system-view
Enter system view, return user view with Ctrl+Z.
[Huawei]Un in en
Info: Information center is disabled.
[Huawei]sysn R3
```

[R3]int gig 0/0/2
[R3-GigabitEthernet0/0/2]ip add 10.1.1.2 24
[R3-GigabitEthernet0/0/2]int gig 0/0/1
[R3-GigabitEthernet0/0/1]ip add 172.16.1.1 24
[R3-GigabitEthernet0/0/1]quit

d) 配置 R4

<Huawei>system-view
Enter system view, return user view with Ctrl+Z.
[Huawei]Un in en
Info: Information center is disabled.
[Huawei]sysn R4
[R4]int gig 0/0/2
[R4-GigabitEthernet0/0/2]ip add 172.16.1.2 24
[R4-GigabitEthernet0/0/2]quit

② 配置各个路由器的 RIP 功能

a) 配置 R1

[R1]**rip** //进入 RIP 配置
[R1-rip-1]**network 192.168.1.0** //宣告网络
[R1-rip-1]quit

b) 配置 R2

[R2]**rip**
[R2-rip-1]**network 192.168.1.0**
[R2-rip-1]**network 10.0.0.0**
[R2-rip-1]quit

c) 配置 R3

[R3]**rip**
[R3-rip-1]**network 10.0.0.0**
[R3-rip-1]**network 172.16.0.0**
[R3-rip-1]quit

d) 配置 R4

[R4]**rip**
[R4-rip-1]**network 172.16.0.0**
[R4-rip-1]quit
[R4]

③ 查看各路由器上 RIP 信息

使用 display rip 1 route

```
[R1]dis rip 1 route
 Route Flags : R - RIP
               A - Aging, G - Garbage-collect
 ------------------------------------------------------------------------------
 Peer 192.168.1.2 on GigabitEthernet0/0/1
      Destination/Mask        Nexthop      Cost   Tag      Flags   Sec
         10.0.0.0/8        192.168.1.2       1    0         RA      12
       172.16.0.0/16       192.168.1.2       2    0         RA      12
[R2]dis rip 1 route
 Route Flags : R - RIP
               A - Aging, G - Garbage-collect
 ------------------------------------------------------------------------------
 Peer 10.1.1.2 on GigabitEthernet0/0/1
      Destination/Mask        Nexthop      Cost   Tag      Flags   Sec
       172.16.0.0/16          10.1.1.2       1    0         RA      11
```

```
[R3]dis rip 1 route
 Route Flags : R - RIP
               A - Aging, G - Garbage-collect
 ------------------------------------------------------------------------------
 Peer 10.1.1.1 on GigabitEthernet0/0/2
      Destination/Mask        Nexthop      Cost   Tag      Flags   Sec
      192.168.1.0/24          10.1.1.1        1    0         RA      22
[R4]dis rip 1 route
 Route Flags : R - RIP
               A - Aging, G - Garbage-collect
 ------------------------------------------------------------------------------
 Peer 172.16.1.1 on GigabitEthernet0/0/2
      Destination/Mask        Nexthop      Cost   Tag      Flags   Sec
      192.168.1.0/24        172.16.1.1        2    0         RA      14
         10.0.0.0/8         172.16.1.1        1    0         RA      14
```

④ 将 RIP 路由协议升级为 RIPv2 版本

分别在路由器 R1、R2、R3、R4 配置 RIP-2,在路由器 R1 上配置如下，其他路由器上配置方法相同。

[R1/R2/R3/R4]**rip** //进入 rip 配置

[R1/R2/R3/R4-rip-1]**version 2** //设置 RIPv2 版本

[R1/R2/R3/R4-rip-1]quit

使用 display rip 1 route 查看版本变更效果

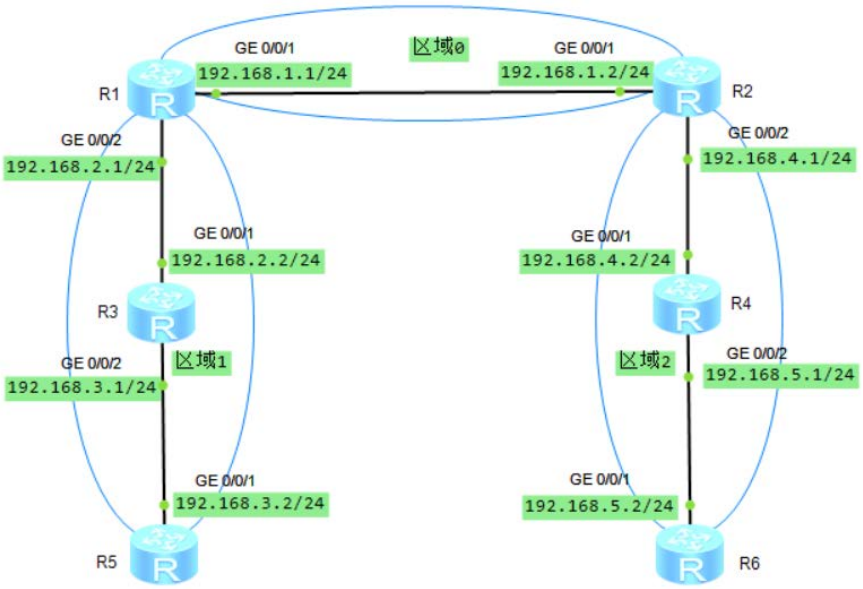
4-3 OSPF 路由配置

OSPF(Open Shortest Path First 开放式最短路径优先)

- 自治系统（AS）:
  自治系统包括一个单独管理实体下所控制的一组路由器（OSPF 是内部网关路由协议，工作于自治系统内部）
- 链路状态（LS）:
  指路由器接口的状态（如 Up 、Down 、IP 地址、网络类型、链路开销以及路由器和它邻接路由器间的关系）
  链路状态信息通过链路状态通告(Link State Advertisement, LSA) 扩散到网络上的每台路由器，每台路由器根据 LSA 信息建立一个于千网络的拓扑数据库（邻居表）
- 最短路径优先算法(SPF)=迪克斯加算法(Dijkstra)
  利用从 LSA 通告得来的信息计算到达每一个目标网络的最短路径，以自身为根生成一棵树，包含了到达每个目的网络的完整路径
- 路由器标识
  OSPF 的路由标识是一个 32 位的数字，它在自治系统中被用来唯一地识别路由器。
  默认使用最高回环地址（loopback），若回环地址没有被配置，则使用物理接口上最高的 IP 地址作为路由器标识
- 邻居和邻接
  OSPF 在相邻路由器间建立邻接关系，使它们交换路由信息。
  邻居是指共享同一网络的路由器，并使用 Hello 包来建立和维护邻居路由器间的邻接关系。
- 区域
  在 OSPF 网络中使用区域(Area)为自治系统分段。
  OSPF 是一种层次化的路由选择协议，**区域 0** 是一个 OSPF 网络中**必须具有**的区域，也称为**主干区域**，其他所有区域要求通过区域 0 互连到一起。

简化原理:

发送 Hello 报文建立邻间关系（邻居表）→形成链路状态数据库（拓扑表）→SPF（Dijkstra）算法形成路由表（路由表）



① 配置各个路由器的接口 IP

② 配置各路由器的区域

a) 区域 0

➢ 配置 R1

```
[R1]ospf                    //进入 ospf 配置
[R1-ospf-1]area 0    //进入区域 0
[R1-ospf-1-area-0.0.0.0]network 192.168.1.0 0.0.0.255    //宣告网络（通配符掩码）
```

➢ 配置 R2

```
[R2]ospf
[R2-ospf-1]area 0
[R2-ospf-1-area-0.0.0.0]network 192.168.1.0 0.0.0.255
```

b) 区域 1

➢ 配置 R1

```
[R1]ospf                    //进入 ospf 配置
[R1-ospf-1]area 1    //进入区域 1
[R1-ospf-1-area-0.0.0.1]network 192.168.2.0 0.0.0.255    //宣告网络（通配符掩码）
```

➢ 配置 R3

```
[R3]ospf
[R3-ospf-1]area 1
[R3-ospf-1-area-0.0.0.1]network 192.168.2.0 0.0.0.255
[R3-ospf-1-area-0.0.0.1]network 192.168.3.0 0.0.0.255
```

➢ 配置 R5

```
[R5]ospf
[R5-ospf-1]area 1
[R5-ospf-1-area-0.0.0.1]network 192.168.3.0 0.0.0.255
```

c) 区域 2

➢ 配置 R2

```
[R2-ospf-1]ospf                //进入 ospf 配置
[R2-ospf-1]area 2    //进入区域 2
[R2-ospf-1-area-0.0.0.2]network 192.168.4.0 0.0.0.255    //宣告网络（通配符掩码）
```

- 配置 R4

```
[R4]ospf
[R4-ospf-1]area 2
[R4-ospf-1-area-0.0.0.2]network 192.168.4.0 0.0.0.255
[R4-ospf-1-area-0.0.0.2]network 192.168.5.0 0.0.0.255
```

- 配置 R6

```
[R6]ospf
[R6-ospf-1]area 2
[R6-ospf-1-area-0.0.0.2]network 192.168.5.0 0.0.0.255
```

③ 查看各路由器的路由表(dis ip routing-table/dis ospf peer)

```
[R1]dis ip routing-table
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
Routing Tables: Public
         Destinations : 9        Routes : 9

Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface

      127.0.0.0/8   Direct  0    0           D   127.0.0.1       InLoopBack0
      127.0.0.1/32  Direct  0    0           D   127.0.0.1       InLoopBack0
    192.168.1.0/24  Direct  0    0           D   192.168.1.1     GigabitEthernet
0/0/1
    192.168.1.1/32  Direct  0    0           D   127.0.0.1       GigabitEthernet
0/0/1
    192.168.2.0/24  Direct  0    0           D   192.168.2.1     GigabitEthernet
0/0/2
    192.168.2.1/32  Direct  0    0           D   127.0.0.1       GigabitEthernet
0/0/2
    192.168.3.0/24  OSPF    10   2           D   192.168.2.2     GigabitEthernet
0/0/2
    192.168.4.0/24  OSPF    10   2           D   192.168.1.2     GigabitEthernet
0/0/1
    192.168.5.0/24  OSPF    10   3           D   192.168.1.2     GigabitEthernet
0/0/1
```

```
[R2]dis ip routing-table
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
Routing Tables: Public
         Destinations : 9        Routes : 9

Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface

      127.0.0.0/8   Direct  0    0           D   127.0.0.1       InLoopBack0
      127.0.0.1/32  Direct  0    0           D   127.0.0.1       InLoopBack0
    192.168.1.0/24  Direct  0    0           D   192.168.1.2     GigabitEthernet
0/0/1
    192.168.1.2/32  Direct  0    0           D   127.0.0.1       GigabitEthernet
0/0/1
    192.168.2.0/24  OSPF    10   2           D   192.168.1.1     GigabitEthernet
0/0/1
    192.168.3.0/24  OSPF    10   3           D   192.168.1.1     GigabitEthernet
0/0/1
    192.168.4.0/24  Direct  0    0           D   192.168.4.1     GigabitEthernet
0/0/2
    192.168.4.1/32  Direct  0    0           D   127.0.0.1       GigabitEthernet
0/0/2
    192.168.5.0/24  OSPF    10   2           D   192.168.4.2     GigabitEthernet
0/0/2
```

```
[R3]dis ip routing-table
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
Routing Tables: Public
         Destinations : 9        Routes : 9

Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface

      127.0.0.0/8   Direct  0    0           D   127.0.0.1       InLoopBack0
      127.0.0.1/32  Direct  0    0           D   127.0.0.1       InLoopBack0
    192.168.1.0/24  OSPF    10   2           D   192.168.2.1     GigabitEthernet
0/0/1
    192.168.2.0/24  Direct  0    0           D   192.168.2.2     GigabitEthernet
0/0/1
    192.168.2.2/32  Direct  0    0           D   127.0.0.1       GigabitEthernet
0/0/1
    192.168.3.0/24  Direct  0    0           D   192.168.3.1     GigabitEthernet
0/0/2
    192.168.3.1/32  Direct  0    0           D   127.0.0.1       GigabitEthernet
0/0/2
    192.168.4.0/24  OSPF    10   3           D   192.168.2.1     GigabitEthernet
0/0/1
    192.168.5.0/24  OSPF    10   4           D   192.168.2.1     GigabitEthernet
0/0/1
```

```
[R4]dis ip routing-table
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
Routing Tables: Public
         Destinations : 9        Routes : 9

Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface

      127.0.0.0/8   Direct  0    0           D   127.0.0.1       InLoopBack0
      127.0.0.1/32  Direct  0    0           D   127.0.0.1       InLoopBack0
    192.168.1.0/24  OSPF    10   2           D   192.168.4.1     GigabitEthernet
0/0/1
    192.168.2.0/24  OSPF    10   3           D   192.168.4.1     GigabitEthernet
0/0/1
    192.168.3.0/24  OSPF    10   4           D   192.168.4.1     GigabitEthernet
0/0/1
    192.168.4.0/24  Direct  0    0           D   192.168.4.2     GigabitEthernet
0/0/1
    192.168.4.2/32  Direct  0    0           D   127.0.0.1       GigabitEthernet
0/0/1
    192.168.5.0/24  Direct  0    0           D   192.168.5.1     GigabitEthernet
0/0/2
    192.168.5.1/32  Direct  0    0           D   127.0.0.1       GigabitEthernet
0/0/2
```

```
[R5]dis ip routing-table
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
Routing Tables: Public
         Destinations : 8        Routes : 8

Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface

      127.0.0.0/8   Direct  0    0           D   127.0.0.1       InLoopBack0
      127.0.0.1/32  Direct  0    0           D   127.0.0.1       InLoopBack0
    192.168.1.0/24  OSPF    10   3           D   192.168.3.1     GigabitEthernet
0/0/1
    192.168.2.0/24  OSPF    10   2           D   192.168.3.1     GigabitEthernet
0/0/1
    192.168.3.0/24  Direct  0    0           D   192.168.3.2     GigabitEthernet
0/0/1
    192.168.3.2/32  Direct  0    0           D   127.0.0.1       GigabitEthernet
0/0/1
    192.168.4.0/24  OSPF    10   4           D   192.168.3.1     GigabitEthernet
0/0/1
    192.168.5.0/24  OSPF    10   5           D   192.168.3.1     GigabitEthernet
0/0/1
```

```
[R6]dis ip routing-table
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
Routing Tables: Public
         Destinations : 8        Routes : 8

Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface

      127.0.0.0/8   Direct  0    0           D   127.0.0.1       InLoopBack0
      127.0.0.1/32  Direct  0    0           D   127.0.0.1       InLoopBack0
    192.168.1.0/24  OSPF    10   3           D   192.168.5.1     GigabitEthernet
0/0/1
    192.168.2.0/24  OSPF    10   4           D   192.168.5.1     GigabitEthernet
0/0/1
    192.168.3.0/24  OSPF    10   5           D   192.168.5.1     GigabitEthernet
0/0/1
    192.168.4.0/24  OSPF    10   2           D   192.168.5.1     GigabitEthernet
0/0/1
    192.168.5.0/24  Direct  0    0           D   192.168.5.2     GigabitEthernet
0/0/1
    192.168.5.2/32  Direct  0    0           D   127.0.0.1       GigabitEthernet
0/0/1
```

使用 dis ospf routing 查看 R1 R3 R5 R6

```
[R1]dis ospf routing

      OSPF Process 1 with Router ID 192.168.1.1
            Routing Tables

 Routing for Network
 Destination        Cost  Type       NextHop         AdvRouter       Area
 192.168.1.0/24     1     Transit    192.168.1.1     192.168.1.1     0.0.0.0
 192.168.2.0/24     1     Transit    192.168.2.1     192.168.1.1     0.0.0.1
 192.168.3.0/24     2     Transit    192.168.2.2     192.168.3.2     0.0.0.1
 192.168.4.0/24     2     Inter-area 192.168.1.2     192.168.1.2     0.0.0.0
 192.168.5.0/24     3     Inter-area 192.168.1.2     192.168.1.2     0.0.0.0

 Total Nets: 5
 Intra Area: 3  Inter Area: 2  ASE: 0  NSSA: 0
```

```
[R3]dis ospf routing

      OSPF Process 1 with Router ID 192.168.2.2
            Routing Tables

 Routing for Network
 Destination        Cost  Type       NextHop         AdvRouter       Area
 192.168.2.0/24     1     Transit    192.168.2.2     192.168.2.2     0.0.0.1
 192.168.3.0/24     1     Transit    192.168.3.1     192.168.2.2     0.0.0.1
 192.168.1.0/24     2     Inter-area 192.168.2.1     192.168.1.1     0.0.0.1
 192.168.4.0/24     3     Inter-area 192.168.2.1     192.168.1.1     0.0.0.1
 192.168.5.0/24     4     Inter-area 192.168.2.1     192.168.1.1     0.0.0.1

 Total Nets: 5
 Intra Area: 2  Inter Area: 3  ASE: 0  NSSA: 0
```

```
[R5]dis ospf routing

      OSPF Process 1 with Router ID 192.168.3.2
            Routing Tables

 Routing for Network
 Destination        Cost  Type       NextHop         AdvRouter       Area
 192.168.3.0/24     1     Transit    192.168.3.2     192.168.3.2     0.0.0.1
 192.168.1.0/24     3     Inter-area 192.168.3.1     192.168.1.1     0.0.0.1
 192.168.2.0/24     2     Transit    192.168.3.1     192.168.2.2     0.0.0.1
 192.168.4.0/24     4     Inter-area 192.168.3.1     192.168.1.1     0.0.0.1
 192.168.5.0/24     5     Inter-area 192.168.3.1     192.168.1.1     0.0.0.1

 Total Nets: 5
 Intra Area: 2  Inter Area: 3  ASE: 0  NSSA: 0
```

```
[R6]dis ospf routing

      OSPF Process 1 with Router ID 192.168.5.2
            Routing Tables

 Routing for Network
 Destination        Cost  Type       NextHop         AdvRouter       Area
 192.168.5.0/24     1     Transit    192.168.5.2     192.168.5.2     0.0.0.2
 192.168.1.0/24     3     Inter-area 192.168.5.1     192.168.1.2     0.0.0.2
 192.168.2.0/24     4     Inter-area 192.168.5.1     192.168.1.2     0.0.0.2
 192.168.3.0/24     5     Inter-area 192.168.5.1     192.168.1.2     0.0.0.2
 192.168.4.0/24     2     Transit    192.168.5.1     192.168.4.2     0.0.0.2

 Total Nets: 5
 Intra Area: 2  Inter Area: 3  ASE: 0  NSSA: 0
```

4-4 IS-IS 路由配置

中间系统到中间系统（Intermediate System to Intermediate System, IS-IS)属于内部网关协议(Interior Gateway Protocol,IGP)，用于自治系统内部。

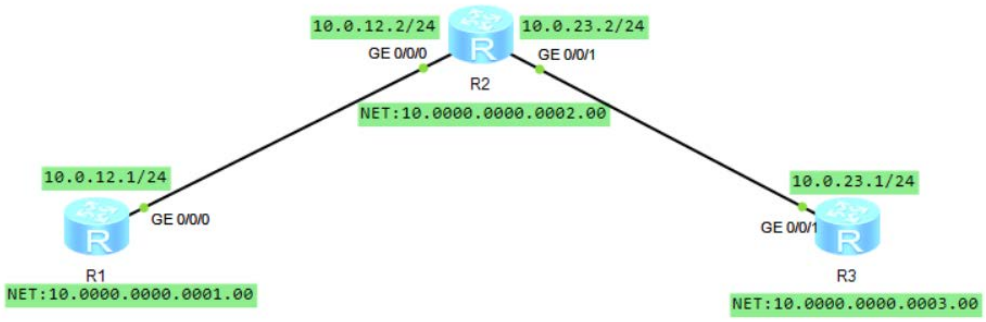
为了支持大规模的路由网络，IS-IS 在自治系统内采用骨干区域与非骨干区域两级的分层结构。一般来说，将 Level-1 路由器部署在非骨干区域，Level-2 路由器和 Level-1-2 路由器部署在骨干区域。每一个非骨干区域都通过 Level-1-2 路由器与骨干区域相连。

链路状态路由协议（L-S）

Net-Entity：网络实体，运行 IS-IS 的路由器必须配置一个网络实体，格式为：SEL 服务访问点

区域 ID	系统 ID	SEL
1 字节	16 字节	1 字节

例如：4A.2000.00E0.008C.00 十六进制表示



① 配置各路由器的接口 IP

② 配置各路由器的 IS-IS 功能

a) 配置 R1

```
[R1]isis        //进入 isis 配置
[R1-isis-1]network-entity 10.0000.0000.0001.00        //宣告本路由(R1)的网络实体
[R1-isis-1]quit
[R1]int gig 0/0/0                    //进入出口链路端口
[R1-GigabitEthernet0/0/0]isis enable        //端口使能 isis
[R1-GigabitEthernet0/0/0]quit
```

b) 配置 R2

```
[R2]isis        //进入 isis 配置
[R2-isis-1]network-entity 10.0000.0000.0002.00        //宣告本路由(R2)的网络实体
[R2-isis-1]quit
[R2]int gig 0/0/0                    //进入出口链路端口
[R2-GigabitEthernet0/0/0]isis enable        //端口使能 isis
[R2-GigabitEthernet0/0/0]int gig 0/0/1
[R2-GigabitEthernet0/0/1]isis enable
```

c) 配置 R3

```
[R3]isis
[R3-isis-1]network-entity 10.0000.0000.0003.00
[R3-isis-1]quit
[R3]int gig 0/0/0
[R3-GigabitEthernet0/0/0]isis enable
```

与 R1 类似

③ 查看各路由器的路由表(dis ip routing/dis isis peer/dis isis route/dis isis lsdb)

4-5 BGP 路由配置

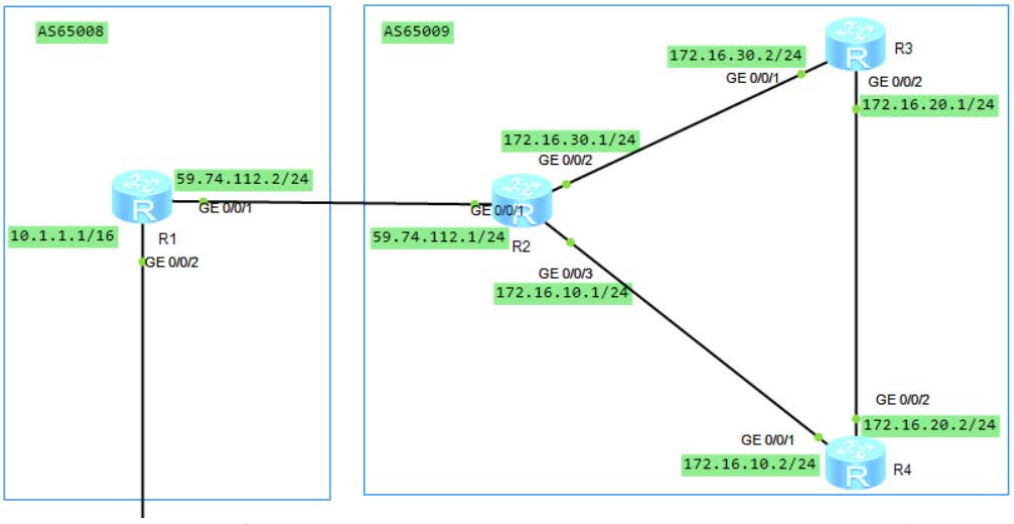
边界网关协议(Border Gateway Protocol,BGP)是一种实现自治系统(Autonomous System,AS)之间的路由可达并选择最佳路由的距离矢量路由协议(D-V)

支持多出口大型网络；路由采用增量更新；除了下一跳还有经过 AS 列表通过信息；允许 CIDR、VLSM、支持鉴别、验证等；分为 EBGP（外部）、IBGP（内部）

- 实现自治系统间通信网络的信息可达
- 多个 BGP 路由器之间的协调
- BGP 支持基千策略的路径选择，可以为域内和域间的网络可达性配置不同的策略
- BGP 只需要在启动时交换一次完整信息，不需要在所有路由更新报文中传送完整的路由数据库信息，后续的路由更新报文只通告网络的变化信息，避免网络变化使得信息黛大幅增加
- 在 BGP 通告目的网络的可达性信息时，除了处理指定目的网络的下一跳信息之外，通告中还包括了通路向量，即去往该目的网络时需要经过的 AS 的列表，使接受者能够清楚了解去往目的网络的通路信息
- BGP 在不同自治系统(AS)之间进行路由转发，分为 EBGP 和 IBGP 两种情况。EBGP 外部边界网关协议，用于在不同的自治系统间交换路由信息。IBGP 内部边界网关协议，用于向内部路由器提供更多信息

配置 BGP 示例

1> 组网需求



如图所示，需要在所有路由器间运行 BGP 协议，R1、R2 之间建立 EBGP 连接，R2、R3 和 R4 之间建立 IBGP 全连接。

2> 配置思路

采用如下的思路配置 BGP 的基本功能：

① 在 R2、R3 和 R4 间配置 IBGP 连接。

② 在 R1 和 R2 之间配置 EBGP 连接。

3> 配置步骤

① 配置各路由器的接口 IP

//配置 R2；R1、R3 和 R4 的配置与 R1 类似。

```
<Huawei>sys
Enter system view, return user view with Ctrl+Z.
[Huawei]un in en
Info: Information center is disabled.
```

[Huawei]sysn R1
[R1]sysn R2
[R2]int gig 0/0/1
[R2-GigabitEthernet0/0/1]ip add 59.74.112.1 24
[R2-GigabitEthernet0/0/1]quit
[R2]int gig 0/0/2
[R2-GigabitEthernet0/0/2]ip add 172.16.30.1 24
[R2-GigabitEthernet0/0/2]quit
[R2]int gig 0/0/3
[R2-GigabitEthernet0/0/3]ip add 172.16.10.1 24
[R2-GigabitEthernet0/0/3]quit

② 配置 IBGP

a) 配置 R2

[R2]bgp 65009 //启动 BGP 及 AS 号
[R2-bgp]router-id 2.2.2.2 //配置 BGP 的 router-id（自定义）
[R2-bgp]peer 172.16.10.2 as-number 65009 //配置 BGP 的对等实体
[R2-bgp]peer 172.16.30.2 as-number 65009
[R2-bgp]quit

b) 配置 R3

[R3]bgp 65009
[R3-bgp]router-id 3.3.3.3
[R3-bgp]peer 172.16.30.1 as-number 65009
[R3-bgp]peer 172.16.20.2 as-number 65009
[R3-bgp]quit

c) 配置 R4

[R4]bgp 65009
[R4-bgp]router-id 4.4.4.4
[R4-bgp]peer 172.16.20.1 as-number 65009
[R4-bgp]peer 172.16.10.1 as-number 65009
[R4-bgp]quit

③ 配置 EBGP

a) 配置 R1

[R1]bgp 65008
[R1-bgp]router-id 1.1.1.1
[R1-bgp]peer 59.74.112.1 as-number 65009 //配置 BGP 的对等实体
[R1-bgp]quit

b) 配置 R2

[R2]bgp 65009
[R2-bgp]peer 59.74.112.2 as-number 65008 //配置 BGP 的对等实体
[R2-bgp]quit

//在 R2 查看 BGP 对等实体的连接状态。

```
[R2]dis bgp peer

 BGP local router ID : 2.2.2.2
 Local AS number : 65009
 Total number of peers : 3              Peers in established state : 3

  Peer            V          AS  MsgRcvd  MsgSent  OutQ  Up/Down       State Pre
fRcv
  59.74.112.2     4       65008        2        2     0 00:00:09 Established
    0
  172.16.10.2     4       65009        4        5     0 00:02:24 Established
    0
  172.16.30.2     4       65009        5        5     0 00:03:07 Established
    0
```

可以看出，R2 其它路由器的 BGP 连接均已建立。

④ 配置 R1 的发布路由 10.1.0.0/16

```
[R1]bgp 65008
[R1-bgp]ipv4-family unicast
[R1-bgp-af-ipv4]network 10.1.0.0 255.255.0.0
[R1-bgp-af-ipv4]quit
```

//查看 R1、R2、R3、R4 的路由表信息（display bgp routing-table）

```
[R1]display bgp routing-table

 BGP Local router ID is 1.1.1.1
 Status codes: * - valid, > - best, d - damped,
               h - history,  i - internal, s - suppressed, S - Stale
               Origin : i - IGP, e - EGP, ? - incomplete


 Total Number of Routes: 1
      Network            NextHop        MED        LocPrf    PrefVal Path/Ogn

 *>   10.1.0.0/16        0.0.0.0         0                      0      i
[R2]display bgp routing-table

 BGP Local router ID is 2.2.2.2
 Status codes: * - valid, > - best, d - damped,
               h - history,  i - internal, s - suppressed, S - Stale
               Origin : i - IGP, e - EGP, ? - incomplete


 Total Number of Routes: 1
      Network            NextHop        MED        LocPrf    PrefVal Path/Ogn

 *>   10.1.0.0/16        59.74.112.2     0                      0      65008i
[R3]display bgp routing-table

 BGP Local router ID is 3.3.3.3
 Status codes: * - valid, > - best, d - damped,
               h - history,  i - internal, s - suppressed, S - Stale
               Origin : i - IGP, e - EGP, ? - incomplete


 Total Number of Routes: 1
      Network            NextHop        MED        LocPrf    PrefVal Path/Ogn

   i  10.1.0.0/16        59.74.112.2     0          100        0      65008i
[R4] display bgp routing-table

 BGP Local router ID is 4.4.4.4
 Status codes: * - valid, > - best, d - damped,
               h - history,  i - internal, s - suppressed, S - Stale
               Origin : i - IGP, e - EGP, ? - incomplete


 Total Number of Routes: 1
      Network            NextHop        MED        LocPrf    PrefVal Path/Ogn

   i  10.1.0.0/16        59.74.112.2     0          100        0      65008i
```

从路由表可以看出，R3/R4 学到了 AS65008 中的 10.1.0.0 的路由，但因为下一跳 192.168.1.2 不可达，所以也不是有效路由。

⑤ 配置 BGP 引入直连路由

//配置 R2

```
[R2]bgp 65009
[R2-bgp]ipv4-family unicast
[R2-bgp-af-ipv4]import-route direct          //引入直连路由
[R2-bgp-af-ipv4]quit
```

//查看 R1 的 BGP 路由表

```
[R1]display bgp routing-table

 BGP Local router ID is 1.1.1.1
 Status codes: * - valid, > - best, d - damped,
               h - history,  i - internal, s - suppressed, S - Stale
               Origin : i - IGP, e - EGP, ? - incomplete


 Total Number of Routes: 4
      Network            NextHop        MED        LocPrf    PrefVal Path/Ogn

 *>   10.1.0.0/16        0.0.0.0         0                      0      i
      59.74.112.0/24     59.74.112.1     0                      0      65009?
 *>   172.16.10.0/24     59.74.112.1     0                      0      65009?
 *>   172.16.30.0/24     59.74.112.1     0                      0      65009?
```

//查看 R4 的 BGP 路由表

```
[R4]display bgp routing-table

 BGP Local router ID is 4.4.4.4
 Status codes: * - valid, > - best, d - damped,
               h - history,  i - internal, s - suppressed, S - Stale
               Origin : i - IGP, e - EGP, ? - incomplete


 Total Number of Routes: 4
      Network            NextHop        MED        LocPrf    PrefVal Path/Ogn

 *>i  10.1.0.0/16        59.74.112.2     0          100         0      65008i
 *>i  59.74.112.0/24     172.16.10.1     0          100         0      ?
  i   172.16.10.0/24     172.16.10.1     0          100         0      ?
 *>i  172.16.30.0/24     172.16.10.1     0          100         0      ?
```

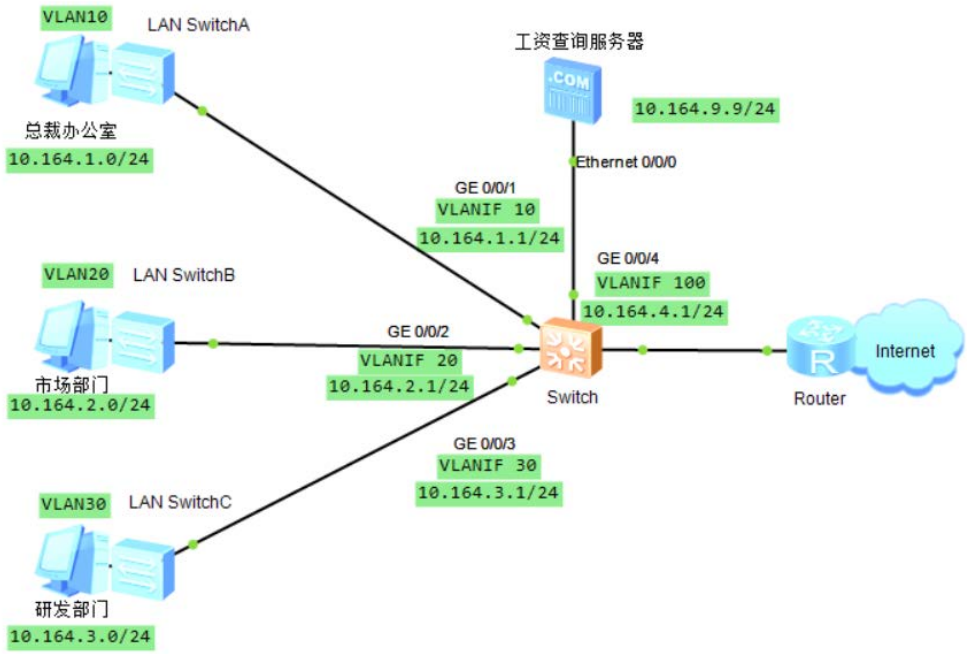
可以看出，到 10.1.0.0 的路由变为有效路由，下一跳为 R1 的地址。

//在 R4 使用 Ping 进行验证

```
[R4]ping 10.1.1.1
  PING 10.1.1.1: 56  data bytes, press CTRL_C to break
    Reply from 10.1.1.1: bytes=56 Sequence=1 ttl=254 time=70 ms
    Reply from 10.1.1.1: bytes=56 Sequence=2 ttl=254 time=60 ms
    Reply from 10.1.1.1: bytes=56 Sequence=3 ttl=254 time=90 ms
    Reply from 10.1.1.1: bytes=56 Sequence=4 ttl=254 time=30 ms
    Reply from 10.1.1.1: bytes=56 Sequence=5 ttl=254 time=80 ms

  --- 10.1.1.1 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 30/66/90 ms
```

4-6 ACL 综合应用

1> 组网需要



如图所示，某公司通过 Switch 实现各部门之间的互连。

公司要求禁止研发部门和市场部门在上班时间（8:00 至 17:30）访问工资查询服务器（IP 地址为 10.164.9.9），总裁办公室不受限制，可以随时访问。

2> 配置思路

采用如下的思路在 Switch 上进行配置：

① 配置时间段、高级 ACL 和基于 ACL 的流分类，使设备可以基于时间的 ACL，对用户访问服务器的报文进行过滤，从而限制不同用户在特定时间访问特定服务器的权限。

② 配置流行为，拒绝匹配上 ACL 的报文通过。

③ 配置并应用流策略，使 ACL 和流行为生效。

3> 配置步骤

① 配置接口加入 VLAN，并配置 VLANIF 接口的 IP 地址

//将 GE0/0/1 ~ GE0/0/3 分别加入 VLAN10、20、30，GE0/0/4 加入 VLAN100，并配置各 VLANIF 接口的 IP 地址。

```
<Huawei>sys
Enter system view, return user view with Ctrl+Z.
[Huawei]un in en
Info: Information center is disabled.
[Huawei]sysn Swtich
[Swtich]vlan batch 10 20 30 100
Info: This operation may take a few seconds. Please wait for a moment...done.
[Swtich]int gig 0/0/1
[Swtich-GigabitEthernet0/0/1]port link-type trunk
[Swtich-GigabitEthernet0/0/1]port trunk allow-pass vlan 10
[Swtich-GigabitEthernet0/0/1]quit
[Swtich]int gig 0/0/2
[Swtich-GigabitEthernet0/0/2]port link-type trunk
[Swtich-GigabitEthernet0/0/2]port trunk allow-pass vlan 20
[Swtich-GigabitEthernet0/0/2]quit
[Swtich]int gig 0/0/3
[Swtich-GigabitEthernet0/0/3]port link-type trunk
[Swtich-GigabitEthernet0/0/3]port trunk allow-pass vlan 30
[Swtich-GigabitEthernet0/0/3]quit
[Swtich]int gig 0/0/4
[Swtich-GigabitEthernet0/0/4]port link-type trunk
[Swtich-GigabitEthernet0/0/4]port trunk allow-pass vlan 100
[Swtich-GigabitEthernet0/0/4]quit
[Swtich]int vlan 10
[Swtich-Vlanif10]ip address 10.164.1.1 255.255.255.0
[Swtich-Vlanif10]quit
[Swtich]int vlan 20
[Swtich-Vlanif20]ip address 10.164.2.1 255.255.255.0
[Swtich-Vlanif20]quit
[Swtich]int vlan 30
[Swtich-Vlanif30]ip address 10.164.3.1 255.255.255.0
[Swtich-Vlanif30]quit
[Swtich]int vlan 100
[Swtich-Vlanif100]ip address 10.164.9.1 255.255.255.0
[Swtich-Vlanif100]quit
```

② 配置时间段

//配置 8:00 至 17:30 的周期时间段。

```
[Swtich]time-range satime 8:00 to 17:30 working-day          //设置时间段
```

③ 配置 ACL

//配置市场部门到工资查询服务器的访问规则。

```
[Swtich]acl 3002
[Swtich-acl-adv-3002] rule deny ip source 10.164.2.0 0.0.0.255 destination 10.164.9.9 0.0.0.0 time-
```

```
range satime
[Swtich-acl-adv-3002]quit
```

//配置研发部门到工资查询服务器的访问规则。

```
[Swtich]acl 3003
[Swtich-acl-adv-3003]rule deny ip source 10.164.3.0 0.0.0.255 destination 10.164.9.9 0.0.0.0 time-range satime
[Swtich-acl-adv-3003]quit
```

④ 配置基于 ACL 的流分类

//配置流分类 c_market，对匹配 ACL 3002 的报文进行分类。

```
[Swtich]traffic classifier c_market
[Swtich-classifier-c_market]if-match acl 3002
[Swtich-classifier-c_market]quit
```

//配置流分类 c_rd，对匹配 ACL 3003 的报文进行分类。

```
[Swtich]traffic classifier c_rd
[Swtich-classifier-c_rd]if-match acl 3003
[Swtich-classifier-c_rd]quit
```

⑤ 配置流行为

//配置流行为 b_market，动作为拒绝报文通过。

```
[Swtich]traffic behavior b_market
[Swtich-behavior-b_market]deny
[Swtich-behavior-b_market]quit
```

//配置流行为 b_rd，动作为拒绝报文通过。

```
[Swtich]traffic behavior b_rd
[Swtich-behavior-b_rd]deny
[Swtich-behavior-b_rd]quit
```

⑥ 配置流策略

//配置流策略 p_market，将流分类 c_market 与流行为 b_market 关联。

```
[Swtich]traffic policy p_market
[Swtich-trafficpolicy-p_market]classifier c_market behavior b_market
[Swtich-trafficpolicy-p_market]quit
```

//配置流策略 p_rd，将流分类 c_rd 与流行为 b_rd 关联。

```
[Swtich]traffic policy p_rd
[Swtich-trafficpolicy-p_rd]classifier c_rd behavior b_rd
[Swtich-trafficpolicy-p_rd]quit
```

⑦ 应用流策略

//由于市场部访问服务器的流量从接口 GE0/0/2 进入 Switch，所以可以在 GE0/0/2 接口的入方向应用流策略 p_market。

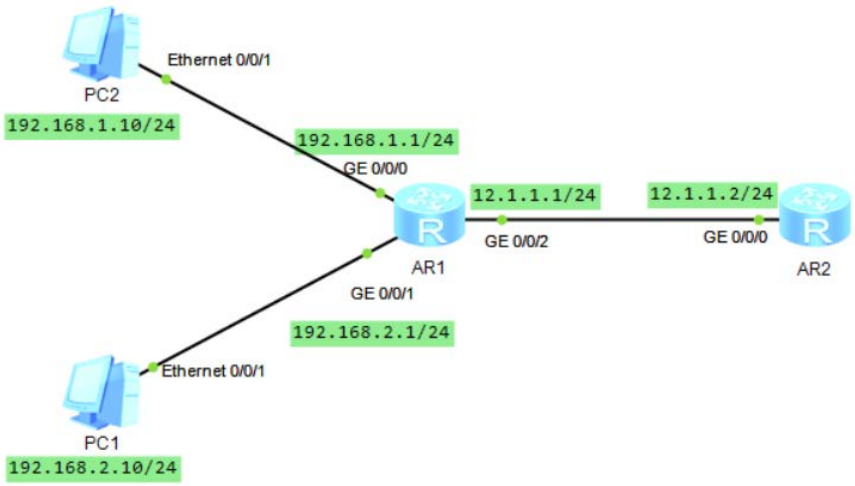
```
[Swtich]int gig 0/0/2
[Swtich-GigabitEthernet0/0/2] traffic-policy p_market inbound
[Swtich-GigabitEthernet0/0/2]quit
```

//由于研发部访问服务器的流量从接口 GE0/0/3 进入 Switch，所以可以在 GE0/0/3 接口的入方向应用流策略 p_rd。

```
[Swtich]int gig 0/0/3
[Swtich-GigabitEthernet0/0/3]traffic-policy p_rd inbound
[Swtich-GigabitEthernet0/0/3]quit
```

⑧ 验证配置结果

4-7 NAT 实例配置



（本实验未完成，但配置思路类似）

◆ 配置各路由、PC 的接口 IP

1> 静态 NAT 转换

[AR1-GigabitEthernet0/0/1]int gig 0/0/2

[AR1-GigabitEthernet0/0/2]nat server global 12.1.1.100 inside 192.168.2.10 //地址转换

[AR1-GigabitEthernet0/0/2]nat static enable //使能 NAT

[AR1-GigabitEthernet0/0/2]quit

#全局模式或者接口都可以配置 NAT

[AR1]nat static global 12.1.1.10 inside 192.168.1.10 netmask 255.255.255.255

2> 动态 NAT 转换

[AR1]acl number 2000 //使用 ACL 规则

[AR1-acl-basic-2000]rule 1 permit source 192.168.1.0 0.0.0.3 //定义内网范围

[AR1-acl-basic-2000]quit

[AR1]nat address-group 1 12.1.1.11 12.1.1.18 //配置 NAT 转换的公网地址池

[AR1]int gig 0/0/2

[AR1-GigabitEthernet0/0/2]nat outbound 2000 address-group 1 no-pat

//在接口出方向使用动态 NAT

[AR1-GigabitEthernet0/0/2]quit

AR2 配置

interface GigabitEthernet0/0/0

ip address 12.1.1.2 255.255.255.0

nat static enable

4-8 IPsec 实例配置

某公司由总部和分支机构构成，通过 IPSec 实现网络安全，具体网络拓扑结构和主路由器及分支路由器上的配置如下。

路由器地址分配表		
	总部	分部
内部网段网号	172.22.1.0	172.22.2.0
英特网段网号	168.1.1.0	167.1.1.0
路由器内部端口IP地址	172.22.1.100	172.22.2.100
路由器Internet端口IP地址	168.1.1.1	167.1.1.1
隧道端口IP地址	192.168.1.1	192.168.1.2

① 配置各路由器的接口 IP

② 分别在总部路由器 R1 和分支机构路由器 R2 配置接口地址和静态路由

```
[R1]ip route-static 167.1.1.0 255.255.255.0 168.1.1.2
[R1]ip route-static 172.22.2.0 255.255.255.0 168.1.1.2
[R2]ip route-static 168.1.1.0 255.255.255.0 167.1.1.2
[R2]ip route-static 172.22.1.0 255.255.255.0 167.1.1.2
```

③ 分别在 R1 和 R2 上配置 ACL.定义各自要保护的数据流

//在 RI 上配置 ACL,定义由子网 172.22.1.0/24 去子网 72.22.2.0/24 的数据流

```
[R1]acl number 3101
[R1-acl-adv-3101]rule permit ip source 172.22.1.0 0.0.0.255 destination 172.22.2.0 0.0.0.255
[R1-acl-adv-3101]quit
```

//在 R2 上配置 ACL,定义由子网 172.22.2.0/24 去子网 172.22.1.0/24 的数据流

```
[R2]acl number 3101
[R2-acl-adv-3101]rule permit ip source 172.22.2.0 0.0.0.255 destination 172.22.1.0 0.0.0.255
[R2-acl-adv-3101]quit
```

④ 分别在 RI 和 R2 上创建 IPSec 安全提议

//R1 上配置 IPSec 安全提议

```
[R1]ipsec proposal tran1        //创建名为 tran1 的安全提议
[R1-ipsec-proposal-tran1]esp authentication-algorithm sha2-256      //采用 sha2 算法认证
[R1-ipsec-proposal-tran1]esp encryption-algorithm aes-128           //采用 aes 算法加密
[R1-ipsec-proposal-tran1]quit
```

//R1 上配置 IPSec 安全提议

```
[R2]ipsec proposal tran1
[R2-ipsec-proposal-tran1]esp authentication-algorithm sha2-256
```

```
[R2-ipsec-proposal-tran1]esp encryption-algorithm aes-128
[R2-ipsec-proposal-tran1]quit
```

分别在 R1 和 R2 上执行 display ipsec proposal 会显示所配置的信息

```
[R1]display ipsec proposal

Number of proposals: 1

IPSec proposal name: tran1
 Encapsulation mode: Tunnel
 Transform         : esp-new
 ESP protocol      : Authentication SHA2-HMAC-256
                     Encryption     AES-128
```

```
[R2]display ipsec proposal

Number of proposals: 1

IPSec proposal name: tran1
 Encapsulation mode: Tunnel
 Transform         : esp-new
 ESP protocol      : Authentication SHA2-HMAC-256
                     Encryption     AES-128
```

⑤ 分别在 R1 和 R2 上配置 IKE 对等体

//在 R1 上配置 IKE 安全提议

```
[R1]ike proposal 5          //创建 IKE 安全提议 5
[R1-ike-proposal-5]encryption-algorithm aes-cbc-128      //采用 aes-cbc 加密（默认）
[R1-ike-proposal-5]authentication-algorithm sha2-256     //采用 sha1 算法认证（默认）
[R1-ike-proposal-5]dh group14
[R1-ike-proposal-5]quit
```

//在 R1 上配置 IKE 对等体，并根据默认配置，配置预共享密钥和对端 ID

```
[R1]ike peer spub       //创建 IKE 对等实体
[R1-ike-peer-spub] undo version 2     //使用 v2 版本
[R1-ike-peer-spub] ike-proposal 5     //使用安全提议 5
[R1-ike-peer-spub] pre-shared-key cipher Huawei    //与共享密钥
[R1-ike-peer-spub] remote-address 167.1.1.1          //远程地址
[R1-ike-peer-spub] quit
```

//在 R2 上配置 IKE 安全提议

```
[R2]ike proposal 5
[R2-ike-proposal-5]encryption-algorithm aes-cbc-128
[R2-ike-proposal-5]authentication-algorithm sha2-256
[R2-ike-proposal-5]dh group14
[R2-ike-proposal-5]quit
```

//在 R2 上配置 IKE 对等体，并根据默认配置，配置预共享密钥和对端 ID

```
[R1]ike peer spua
[R1-ike-peer-spub] undo version 2
[R1-ike-peer-spub] ike-proposal 5
[R1-ike-peer-spub] pre-shared-key cipher Huawei
[R1-ike-peer-spub] remote-address 168.1.1.1
[R1-ike-peer-spub] quit
```

⑥ 分别在 R1 和 R2 上创建安全策略。

```
//在 R1 上配置 IKE 动态协商方式安全策略
[R1]ipsec policy map1 10 isakmp
[R1-ipsec-policy-isakmp-map1-10]ike-peer spub
[R1-ipsec-policy-isakmp-map1-10]proposal tran1
[R1-ipsec-policy-isakmp-map1-10]security acl 3101
[R1-ipsec-policy-isakmp-map1-10]quit
//在 R2 上配置 IKE 动态协商方式安全策略
[R1]ipsec policy map1 10 isakmp
[R1-ipsec-policy-isakmp-map1-10]ike-peer spua
[R1-ipsec-policy-isakmp-map1-10]proposal tran1
[R1-ipsec-policy-isakmp-map1-10]security acl 3101
```

[R1-ipsec-policy-isakmp-map1-10]quit

⑦ 分别在 R1 和 R2 的接口上应用各自的安全策略组，使接口具有 IPSec 的保护功能

//在 R1 的接口上引用安全策略组

[R1]int gig 0/0/1

[R1-GigabitEthernet0/0/1]ipsec policy map1

[R1-GigabitEthernet0/0/1]quit

//在 R2 的接口上引用安全策略组

[R2]int gig 0/0/1

[R2-GigabitEthernet0/0/1]ipsec policy map1

[R2-GigabitEthernet0/0/1]quit

⑧ 配置验证

配置成功后，总部和分支机构的 PC 执行 ping 操作正常，它们之间的数据传输将被加密，执行命令 display ipsec statistics 可以查看数据包的统计信息

4-9 IPv6-over-IPv4 GRE 隧道配置

由于从 IPv4 向 IPv6 过渡是大势所趋，所以目前有许多从 IPv4 向 IPv6 过渡的技术。本节通过实例介绍采用隧道策略实现从 IPv4 向 IPv6 过渡的技术。

1、双栈策略

双栈策略是指在网络节点中同时具有 IPv4 和 IPv6 两个协议栈，这样，它既可以接收、处理、收发 IPv4 的分组，也可以接收、处理、收发 IPv6 的分组。

缺点：对网元设备的要求较高，涉及网络中的所有网元设备都支持双协议栈，投资大、建设周期比较长。

2、隧道策略

利用一种协议来传输另一种协议的数据的技术

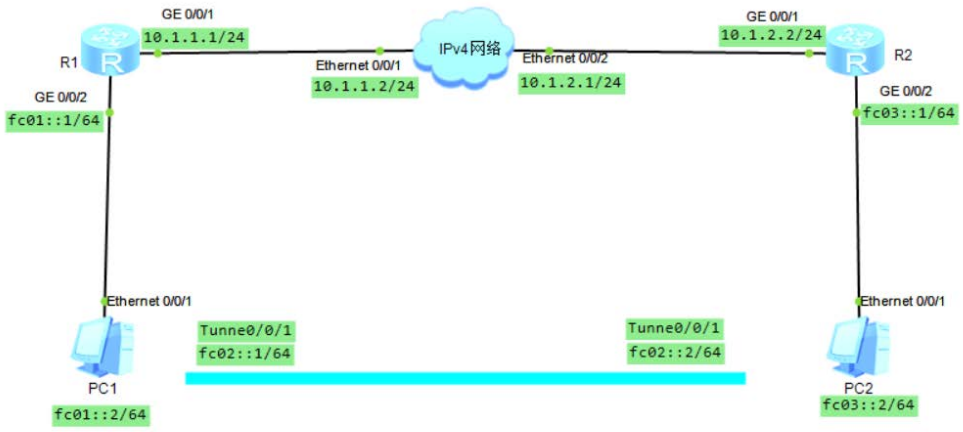
主流隧道技术：构造隧道、6to4 隧道以及 MPLS 隧道

目前的隧道技术主要实现了在 IPv4 数据包中封装 IPv6 数据包。

本实验采用 IPv6-over-IPv4 隧道技术：

是将 IPv6 报文封装在 IPv4 报文中，让 IPv6 数据包穿过 IPv4 网络进行通信，隧道技术只要求在隧道的入口和出口处进行修改，对其他部分没有要求，容易实现。但是，隧道技术不能实现 IPv4 主机与 1Pv6 主机的直接通信。

路由器 R1 和 R2 经 IPv4 网络连接，路由器以太口分别连接两个 IPv6 网段。通过 Tunnel 将 IPv6 的数据包封装到 IPv4 的数据包中，实现点到点的数据传输。网络拓扑图如图所示。



① 配置 R1、R2 接口 IP

a) R1

```
[R1]int gig 0/0/1
[R1-GigabitEthernet0/0/1]ip add 10.1.1.1 24
[R1-GigabitEthernet0/0/1]quit
[R1]ipv6                    //全局使能 IPv6
[R1]int gig 0/0/2
[R1-GigabitEthernet0/0/2]ipv6 enable        //对应接口启动 IPv6 功能
[R1-GigabitEthernet0/0/2]ipv6 add fc01::1 64        //接口配置 IPv6 地址
[R1-GigabitEthernet0/0/2]quit
```

b) R2

```
[R2]int gig 0/0/1
[R2-GigabitEthernet0/0/1]ip add 10.1.2.2 24
[R2-GigabitEthernet0/0/1]quit
[R2]ipv6
[R2]int gig 0/0/2
[R2-GigabitEthernet0/0/2]ipv6 enable
[R2-GigabitEthernet0/0/2]ipv6 add fc03::1 64
[R2-GigabitEthernet0/0/2]quit
```

② 配置 R1 和 R2 的 IPV4 静态路由

```
[R1]ip route-static 10.1.2.2 255.255.255.0 10.1.1.2
[R2]ip route-static 10.1.1.1 255.255.255.0 10.1.2.1
```

③ 配置 R1 和 R2 的 Tunnel 接口

a) R1

```
[R1]int Tunnel 0/0/1            //进入隧道 Tunnel 0/0/1
[R1-Tunnel0/0/1]tunnel-protocol gre    //启用隧道协议 GRE
[R1-Tunnel0/0/1]ipv6 enable            //隧道端口使能 IPv6
[R1-Tunnel0/0/1]ipv6 add fc02::1 64     //配置 IPv6 地址
[R1-Tunnel0/0/1]source 10.1.1.1         //源端地址
[R1-Tunnel0/0/1]destination 10.1.2.2    //目的地址
[R1-Tunnel0/0/1]quit
```

b) R2

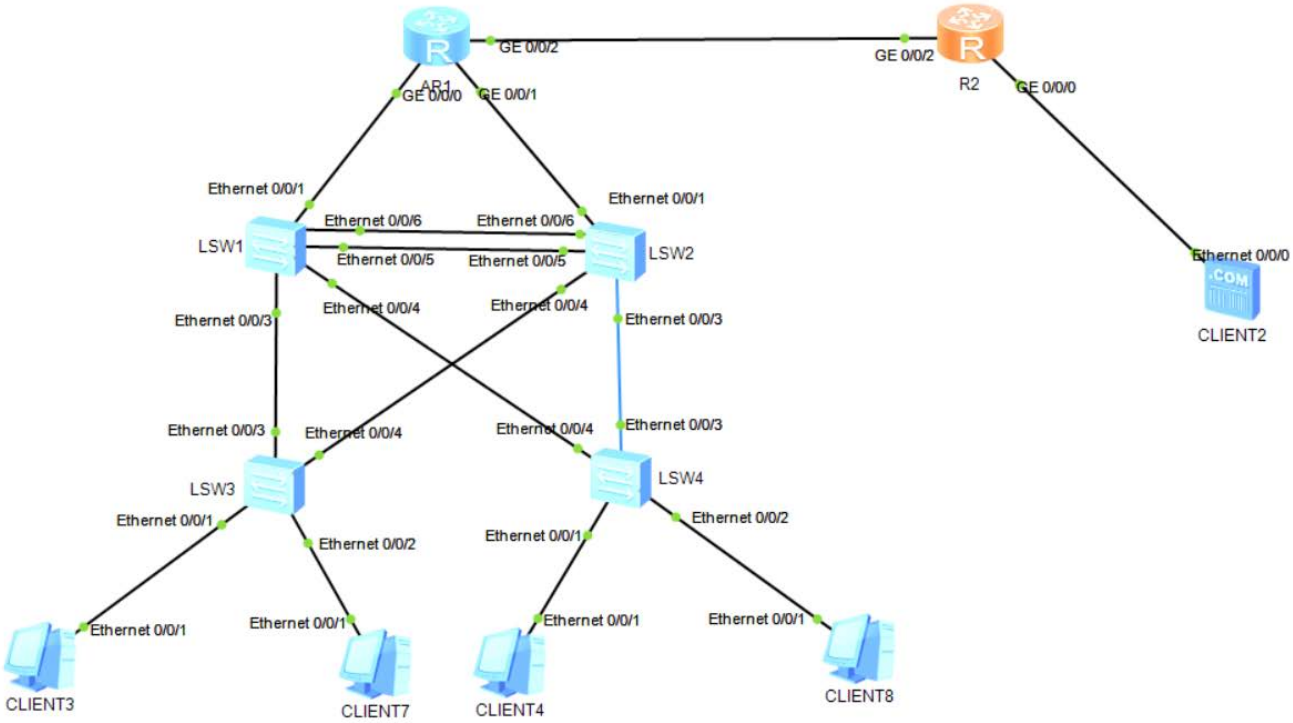
```
[R2]int tunnel 0/0/1
[R2-Tunnel0/0/1]tunnel-protocol gre
[R2-Tunnel0/0/1]ipv6 enable
[R2-Tunnel0/0/1]ipv6 add fc02::2 64
[R2-Tunnel0/0/1]source 10.1.2.2
[R2-Tunnel0/0/1]destination 10.1.1.1
[R2-Tunnel0/0/1]quit
```

④ 配置 R1 和 R2 的 Tunnel 静态路由

```
[R1]ipv6 route-static fc03::1 64 Tunnel 0/0/1
[R2]ipv6 route-static fc01::1 64 Tunnel 0/0/1
```

⑤ 检查配置结果

4. 交换路由综合实验



4-1 需求分析

- 交换部分：

1> 将 SW1-SW2 间的 e0/0/5、e0/0/6 配置为手工方式的 eth-trunk，链路编号为 eth-trunk 12

2> 将 SW1、SW2、SW3、SW4 间的所有链路配置为 trunk

3> 在 SW1、SW2、SW3、SW4 上创建 vlan10、vlan20、vlan11、vlan12:

4> 在 SW1、SW2、SW3、SW4 上开启 STP 协议

5> 将 SW1 设置为所有 VLAN 的根交换机，将 SW2 设置为所有 VLAN 的备份根交换机

6> 将 PC3、PC4 划入 vlan10、将 PC7、PC8 划入 vlan20

- 路由部分：

1> IP 地址规划如下：

vlan10 ---------- 10.1.10.0/24
vlan20 ---------- 10.1.20.0/24
vlan11 ---------- 10.1.11.0/24
vlan12 ---------- 10.1.12.0/24
R1-R2 ---------- 12.1.1.0/24
R2-Client2 ---------- 20.1.1.0/24

2> 将 SW1 设置为 vlan10、vlan20 的网关，IP 地址为 vlan 对应网段的最后一个可用 IP

3> 将 SW2 设置为 vlan10、vlan20 的备份网关，IP 地址为 vlan 对应网段的倒数第二个可用 IP:

4> 将 SW1 的 e0/0/1 接口划入 vlan11，并为 vlan11 配置对应网段的第一个可用 IP:

5> 将 SW2 的 e0/0/1 接口划入 vlan12，并为 vlan12 配置对应网段的第一个可用 IP:

6> 将 R1 的 g0/0/0 接口 IP 配置为 10.1.11.0/24 网段的最后一个可用 IP:

7> 将 R1 的 g0/0/1 接口 IP 配置为 10.1.12.0/24 网段的最后一个可用 IP:

8> 配置 R1-R2 相连接口的 IP 地址，R1 配置网段第一个可用 IP，R2 配置网段第二个可用 IP:

9> 配置 R2-Client2 相连接口的 IP 地址，Client2 配置网段第一个可用 IP，R2 配置网段最后一个可用 IP

10> 在 SW1、SW2、R1 间运行 OSPF 100，将 vlan10、vlan20、vlan11、vlan12 对应网段宣告进 area0

11> 在 R1 上添加缺省静态路由，将下一跳指向 R2

12> 在 R1 上将缺省静态路由发布进 OSPF 100

13> 在 R1-R2 间运行 OSPF 200，将 R1-R2 间网段以及 R2-Client2 间网段宣告进 area0

- 访问控制部分：

1> 在 R1 上配置 PAT，让 vlan10、vlan20 内的所有主机共用 12.1.1.10/24 这个 IP 访问 Client2

2> 要求 vlan10 内的主机可以访问 Client2 的 web 服务，但不能访问 Client2 的 ftp 服务；vlan20 内的主机可以访问 Client2 的 ftp 服务，但不能访问 Client2 的 web 服务

其余流量不做限制:

4-2操作步骤

4-2-1 交换部分

1> 将 SW1-SW2 间的 e0/0/5、e0/0/6 配置为手工方式的 eth-trunk，链路编号为 eth-trunk 12

SW-1

```
[SW-1]int Eth-Trunk 12
[SW-1-Eth-Trunk12]trunkport Ethernet 0/0/5 to 0/0/6
[SW-1-Eth-Trunk12]quit
```

SW-2

```
[SW-2]int Eth-Trunk 12
[SW-2-Eth-Trunk12]trunkport Ethernet 0/0/5 to 0/0/6
[SW-2-Eth-Trunk12]quit
```

2> 将 SW1、SW2、SW3、SW4 间的所有链路配置为 trunk

SW-1

```
[SW-1]int Eth-Trunk 12
[SW-1-Eth-Trunk12]port link-type trunk
[SW-1-Eth-Trunk12]port trunk allow-pass vlan all
[SW-1-Eth-Trunk12]dis th
#
interface Eth-Trunk12
 port link-type trunk
 port trunk allow-pass vlan 2 to 4094
#
return
[SW-1-Eth-Trunk12]int e0/0/3
[SW-1-Ethernet0/0/3] port link-type trunk
[SW-1-Ethernet0/0/3] port trunk allow-pass vlan 2 to 4094
[SW-1-Ethernet0/0/3]int e0/0/4
[SW-1-Ethernet0/0/4] port link-type trunk
[SW-1-Ethernet0/0/4] port trunk allow-pass vlan 2 to 4094
[SW-1-Ethernet0/0/4]quit
```

SW-2

```
[SW-2]int Eth-Trunk 12
[SW-2-Eth-Trunk12]port link-type trunk
[SW-2-Eth-Trunk12]port trunk allow-pass vlan all
[SW-2-Eth-Trunk12]dis th
#
```

```
interface Eth-Trunk12
 port link-type trunk
 port trunk allow-pass vlan 2 to 4094
#
return
[SW-2-Eth-Trunk12]int e0/0/3
[SW-2-Ethernet0/0/3]port link-type trunk
[SW-2-Ethernet0/0/3] port trunk allow-pass vlan 2 to 4094
[SW-2-Ethernet0/0/3]int e0/0/4
[SW-2-Ethernet0/0/4]port link-type trunk
[SW-2-Ethernet0/0/4] port trunk allow-pass vlan 2 to 4094
[SW-2-Ethernet0/0/4]quit
```

- SW-3

```
[SW-3]int e0/0/3
[SW-3-Ethernet0/0/3] port link-type trunk
[SW-3-Ethernet0/0/3] port trunk allow-pass vlan 2 to 4094
[SW-3-Ethernet0/0/3]int e0/0/4
[SW-3-Ethernet0/0/4] port link-type trunk
[SW-3-Ethernet0/0/4] port trunk allow-pass vlan 2 to 4094
```

- SW-4

```
[SW-4]int e0/0/3
[SW-4-Ethernet0/0/3] port link-type trunk
[SW-4-Ethernet0/0/3] port trunk allow-pass vlan 2 to 4094
[SW-4-Ethernet0/0/3]int e0/0/4
[SW-4-Ethernet0/0/4] port link-type trunk
[SW-4-Ethernet0/0/4] port trunk allow-pass vlan 2 to 4094
```

3> 在 SW1、SW2、SW3、SW4 上创建 vlan10、vlan20、vlan11、vlan12

```
[SW-1/2/3/4]vlan batch 10 11 12 20
```

4> 在 SW1、SW2、SW3、SW4 上开启 STP 协议

```
[SW-1/2/3/4]stp mode stp
```

5> 将 SW1 设置为所有 VLAN 的根交换机，将 SW2 设置为所有 VLAN 的备份根交换机

- SW-1

```
[SW-1]stp priority 0
```

- SW-2

```
[SW-2]stp priority 4096
```

6> 将 PC3、PC4 划入 vlan10、将 PC7、PC8 划入 vlan20

- SW-3

```
[SW-3]int e0/0/1
[SW-3-Ethernet0/0/1]port link-type access
[SW-3-Ethernet0/0/1]port default vlan 10
[SW-3-Ethernet0/0/1]int e0/0/2
[SW-3-Ethernet0/0/2] port link-type access
[SW-3-Ethernet0/0/2] port default vlan 20
```

- SW-4

```
[SW-4]int e0/0/1
[SW-4-Ethernet0/0/1] port link-type access
```

```
[SW-4-Ethernet0/0/1] port default vlan 10
[SW-4-Ethernet0/0/1]int e0/0/2
[SW-4-Ethernet0/0/2] port link-type access
[SW-4-Ethernet0/0/2] port default vlan 20
```

4-2-2　路由部分

1>　将 SW1 设置为 vlan10、vlan20 的网关，IP 地址为 vlan 对应网段的最后一个可用 IP

```
[SW-1]int vlan 10
[SW-1-Vlanif10]ip add 10.1.10.254 24
[SW-1-Vlanif10]quit
[SW-1]int vlan 20
[SW-1-Vlanif20]ip add 10.1.20.254 24
[SW-1-Vlanif20]quit
```

2>　将 SW2 设置为 vlan10、vlan20 的备份网关，IP 地址为 vlan 对应网段的倒数第二个可用 IP

```
[SW-2]int vlan 10
[SW-2-Vlanif10]ip add 10.1.10.253 24
[SW-2-Vlanif10]quit
[SW-2]int vlan 20
[SW-2-Vlanif20]ip add 10.1.20.253 24
[SW-2-Vlanif20]quit
```

3>　将 SW1 的 e0/0/1 接口划入 vlan11，并为 vlan11 配置对应网段的第一个可用 IP

```
[SW-1]int e0/0/1
[SW-1-Ethernet0/0/1]port link-type access
[SW-1-Ethernet0/0/1]port default vlan 11
[SW-1-Ethernet0/0/1]quit
[SW-1]int vlan 11
[SW-1-Vlanif11]ip add 10.1.11.1 24
[SW-1-Vlanif11]quit
```

4>　将 SW2 的 e0/0/1 接口划入 vlan12，并为 vlan12 配置对应网段的第一个可用 IP

```
[SW-2]int e0/0/1
[SW-2-Ethernet0/0/1]port link-type access
[SW-2-Ethernet0/0/1]port default vlan 12
[SW-2-Ethernet0/0/1]quit
[SW-2]int vlan 12
[SW-2-Vlanif12]ip add 10.1.12.1 24
```

5>　将 R1 的 g0/0/0 接口 IP 配置为 10.1.11.0/24 网段的最后一个可用 IP

```
[R1]int gig 0/0/0
[R1-GigabitEthernet0/0/0]ip add 10.1.11.254 24
[R1-GigabitEthernet0/0/0]quit
```

6>　将 R1 的 g0/0/1 接口 IP 配置为 10.1.12.0/24 网段的最后一个可用 IP

```
[R1]int gig 0/0/1
[R1-GigabitEthernet0/0/1]ip add 10.1.12.254 24
[R1-GigabitEthernet0/0/1]quit
```

7>　配置 R1-R2 相连接口的 IP 地址，R1 配置网段第一个可用 IP，R2 配置网段第二个可用 IP

```
[R1]int g0/0/2
[R1-GigabitEthernet0/0/2]ip add 12.1.1.1 24
[R1-GigabitEthernet0/0/2]quit
```

```
[R2]int g0/0/2
[R2-GigabitEthernet0/0/2]ip add 12.1.1.2 24
[R2-GigabitEthernet0/0/2]quit
```

8> 配置 R2-Client2 相连接口的 IP 地址，Client2 配置网段第一个可用 IP，R2 配置网段最后一个可用 IP

Client2 为服务器，配置方法参考 PC，IP:20.1.1.1/24

```
[R2]int g0/0/0
[R2-GigabitEthernet0/0/0]ip add 20.1.1.254 24
[R2-GigabitEthernet0/0/0]quit
```

9> 在 SW1、SW2、R1 间运行 OSPF 100，将 vlan10、vlan20、vlan11、vlan12 对应网段宣告进 area0

- SW-1

```
[SW-1]ospf 100
[SW-1-ospf-100]area 0
[SW-1-ospf-100-area-0.0.0.0]network 10.1.11.0 0.0.0.255
[SW-1-ospf-100-area-0.0.0.0]network 10.1.10.0 0.0.0.255
[SW-1-ospf-100-area-0.0.0.0]network 10.1.20.0 0.0.0.255
[SW-1-ospf-100-area-0.0.0.0]quit
```

- SW-2

```
[SW-2]ospf 100
[SW-2-ospf-100]area 0
[SW-2-ospf-100-area-0.0.0.0]network 10.1.12.0 0.0.0.255
[SW-2-ospf-100-area-0.0.0.0]network 10.1.10.0 0.0.0.255
[SW-2-ospf-100-area-0.0.0.0]network 10.1.20.0 0.0.0.255
[SW-2-ospf-100-area-0.0.0.0]quit
```

- R1

```
[R1]ospf 100
[R1-ospf-100]area 0
[R1-ospf-100-area-0.0.0.0]network 10.1.11.0 0.0.0.255
[R1-ospf-100-area-0.0.0.0]network 10.1.12.0 0.0.0.255
[R1-ospf-100-area-0.0.0.0]quit
```

10> 在 R1 上添加缺省静态路由，将下一跳指向 R2

```
[R1]ip route-static 0.0.0.0 0 12.1.1.2
```

11> 在 R1 上将缺省静态路由发布进 OSPF 100

```
[R1]ospf 100
[R1-ospf-100]default-route-advertise
[R1-ospf-100]quit
```

12> 在 R1-R2 间运行 OSPF 200，将 R1-R2 间网段以及 R2-Client2 间网段宣告进 area0

```
[R1]ospf 200
[R1-ospf-200]area 0
[R1-ospf-200-area-0.0.0.0]network 12.1.1.0 0.0.0.255
[R1-ospf-200-area-0.0.0.0]quit

[R2]ospf 200
[R2-ospf-200]area 0
[R2-ospf-200-area-0.0.0.0]network 12.1.1.0 0.0.0.255
[R2-ospf-200-area-0.0.0.0]network 20.1.1.0 0.0.0.255
[R2-ospf-200-area-0.0.0.0]quit
```

4-2-3　访问控制部分

1>　在 R1 上配置 PAT，让 vlan10、vlan20 内的所有主机共用 12.1.1.10/24 这个 IP 访问 Client2

```
[R1]nat address-group 0 12.1.1.10 12.1.1.10                    //配置公网地址池
[R1]acl 2000
[R1-acl-basic-2000]rule permit source 10.1.10.0 0.0.0.255
[R1-acl-basic-2000]rule permit source 10.1.20.0 0.0.0.255        //ACL 定义私网地址
[R1]int g0/0/2
[R1-GigabitEthernet0/0/2]nat outbound 2000 address-group 0                    //外网接口调用 ACL 规则
[R1-GigabitEthernet0/0/2]quit
```

2>　要求 vlan10 内的主机可以访问 Client2 的 web 服务，但不能访问 Client2 的 ftp 服务；vlan20 内的主机可以访问 Client2 的 ftp 服务，但不能访问 Client2 的 web 服务

其余流量不做限制:

```
[R1]acl 3000
[R1-acl-adv-3000]rule permit tcp source 10.1.10.0 0.0.0.255 destination 20.1.1.1 0 destination-port eq 80
[R1-acl-adv-3000]rule deny tcp source 10.1.20.0 0.0.0.255 destination 20.1.1.1 0 destination-port eq 21
[R1-acl-adv-3000]rule permit tcp source 10.1.20.0 0.0.0.255 destination 20.1.1.1 0 destination-port eq 21
[R1-acl-adv-3000]rule deny tcp source 10.1.20.0 0.0.0.255 destination 20.1.1.1 0 destination-port eq 80
[R1]int g0/0/2
[R1-GigabitEthernet0/0/2]traffic-filter outbound acl 3000
```