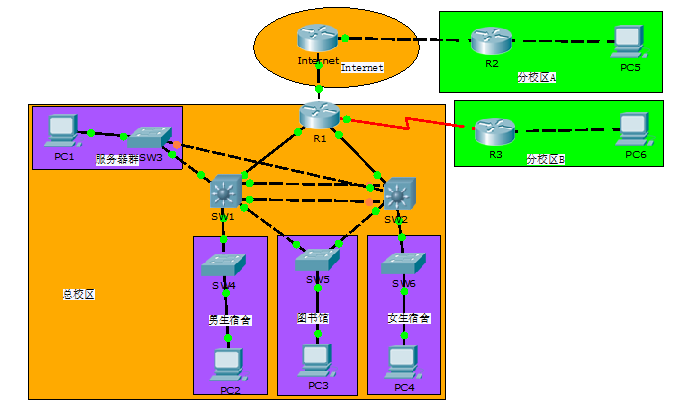
1. 实训任务：

项目：网络技术及企业中小型网络项目实战

1. 组网拓扑：



1. 组网需求：

如拓扑图所示为某校园网络简易拓扑， R1作为核心路由器，SW1, SW2作为汇聚层交换机，LSW4-6作为各自楼层的接入交换机，R2和R3是两个分校区的路由器，现按照要求实现如下配置：

2.1 IP地址规划：全网IP地址自行规划，遵循IP地址规划原则，内网使用私网地址，Internet使用公网地址，同时考虑后续网络扩展（IP地址使用详见《设备台账示例》）。

2.2 二层网络：全网VLAN自行规划，交换机群使用RSTP+HSRP实现环路避免及业务负载，要求所有的终端接入到网络中，能立即转发数据，服务器业务主走SW1，图书馆务主走SW2 。

2.3 SW1和SW2互联接口使用链路聚合，使用active模式。

2.4 男、女宿舍所有终端通过DHCP获取地址。

2.5 内部网络使用OSPF实现全网互联互通。

2.6 服务器不允许宿舍终端访问。

2.7 全网业务均可通过出口路由器访问Internet。

2.8 主校区和分校区A通过GRE互联互通，主校区和分校区B通过ppp互联互通并启用CHAP认证。

2.9校园网所有设备只允许图书馆所在网段进行telnet。

3、实训提交资料：

实训完成后以个人为单位输出以下资料：

3.1 全网设备配置脚本及Cisco Packet Tracer 拓扑文件；

3.2 全网设备台账，详见附件二：《设备台账示例》；

3.3 项目验收测试报告。

**设备基础配置**

**实验1 设备基础配置**

**学习目标**

* 掌握设备系统参数的配置方法，包括设备名称、系统时间及系统时区
* 掌握Console口空闲超时时长的配置方法
* 掌握登录信息的配置方法
* 掌握登录密码的配置方法
* 掌握保存配置文件的方法
* 掌握配置路由器接口IP地址的方法
* 掌握测试两台直连路由器连通性的方法
* 掌握重启设备的方法

**拓扑图**

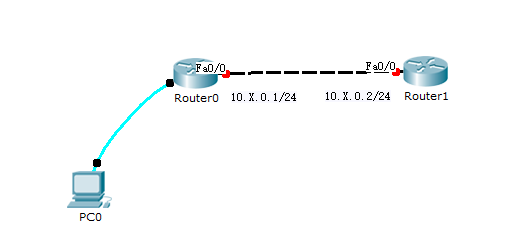


图1 设备基础配置拓扑图

**场景**

您是公司的网络管理员，现在公司购买了两台CISCO 2811系列路由器。路由器在使用之前，需要先配置路由器的设备名称、系统时间及登录密码等管理信息。

**操作步骤**

1. **进入特权模式**

CISCO IOS有三种模式即：用户模式（用“>”表示）；特权模式（用“#”表示）；配置模式（用“(config) #”表示）。

1.用户模式  
交换机启动完成后按下Enter键，首先进入的就是用户模式，在些用户模式下用户将受到极大的限制，只能用来查看一些统计信息。  
Switch>  
2.特权模式  
在用户模式下输入enable(可简写为en)命令就可以进入特权模式，用户在该模式下可以查看并修改Cisco设备的配置。  
Switch>en  
Switch#  
3.全局配置模式  
在特权模式下输入config terminal(可简写conf t)命令即可，用户在该模式下可修改交换机的全局配置。如修改主机名。  
Switch#conf t  
Switch(config)#

4.各模式退出命令，在任意模式下输入exit，将退出当前模式。

1. **查看系统信息**

执行**show version**命令，查看路由器的软件版本与硬件信息。

Router#show version

（截图）

命令回显信息中包含了IOS版本，设备型号等信息。

1. **修改系统时间**

执行**show clock**命令查看当前系统时间。

Router#show clock

（截图）

IOS系统会自动保存时间，但如果时间不正确，可以在特权模式下执行**clock set**命令修改系统时间。

Router#clock set 11:30:00 june 19 2018 //具体时间按照当时时间配置

执行**show clock**命令查看修改后系统时间。

Router#show clock

（截图）

1. **帮助功能和命令自动补全功能**

在系统中输入命令时，问号是通配符，Tab键是自动补全命令的快捷键。

Router#?

（截图）

在输入信息后输入“？”可查看以输入字母开头的命令。如输入“sh？”，设备将输出所有以sh开头的命令。

在输入的信息后增加空格，再输入“？”，这时设备将尝试识别输入的信息所对应的命令，然后输出该命令的其他参数。例如输入“sh？”，如果只有show命令是以sh开头的，那么设备将输出sh命令的参数；如果以sh开头的命令还有其他的，设备将报错。

另外可以使用键盘上Tab键补全命令，比如键入“sh”后，按键盘“Tab”键可以将命令补全为“show”。如有多个以“sh”开头的命令存在，则在多个命令之间循环切换。

命令在不发生歧义的情况下可以使用简写，如“show”可以简写为“sh”或“sho”等，“interface”可以简写为“int”或“inter”等。

1. **修改设备名称**

配置设备时，为了便于区分，往往给设备定义不同的名称。如下我们依照实验拓扑图，修改设备名称。

修改Router0路由器的设备名称为R0。

Router(config)#hostname R0

（截图）

修改Router1路由器的设备名称为R1。

Router(config)#hostname R0

（截图）

1. **配置Console口参数**

默认情况下，通过Console口登陆无密码，任何人都可以直接连接到设备，进行配置。

为避免由此带来的风险，可以将Console接口登录方式配置为密码认证方式，密码为“cisco”。

空闲时间指的是经过没有任何操作的一定时间后，会自动退出该配置界面，再次登陆会根据系统要求，提示输入密码进行验证。

设置空闲超时时间为20分钟。

R0(config)#

R0(config)#line console 0

R0(config-line)#password cisco

R0(config-line)#login

R0(config-line)#exec-timeout 20

执行do show run 命令查看配置结果。

R0(config-line)#do show run

（截图）

退出系统，并使用新配置的密码登录系统。

R0#exit

R0 con0 is now available

Press RETURN to get started.

User Access Verification

Password:

R0>

1. **配置接口IP地址和描述信息**

配置R0上F0/0接口的IP地址。

R0(config)#interface fastEthernet 0/0

R0(config-if)#no shutdown

R0(config-if)#ip add 10.X.0.1 255.255.255.0

R0(config-if)#description TO:R1-F0/0

在当前接口视图下，执行**do show run**命令查看配置结果。

R0(config-if)#do show run

（截图）

执行**do show int f0/0**命令查看接口信息。

R0(config-if)#do show int f0/0

（截图）

从命令回显信息中可以看到，接口的物理状态与协议状态均为Up，表示对应的物理层与数据链路层均可用。

配置R1上F0/0接口的IP地址。

R1(config)#interface fastEthernet 0/0

R1(config-if)#no shutdown

R1(config-if)#ip add 10.X.0.2 255.255.255.0

R1(config-if)#description TO:R0-F0/0

在当前接口视图下，执行**do show run**命令查看配置结果。

R1(config-if)#do show run

（截图）

执行**do show int f0/0**命令查看接口信息。

R1(config-if)#do show int f0/0

（截图）

从命令回显信息中可以看到，接口的物理状态与协议状态均为Up，表示对应的物理层与数据链路层均可用。

配置完成后，在R0上通过执行ping命令测试R0和R1间的连通性。

R0#ping 10.X.0.2

Router# （截图）

1. **配置远程登陆参数**

默认情况下，设备无法通过远程登陆设备，可以通过VTY接口实现远程登陆设备。

在R0上将VTY接口登录方式配置为密码认证方式，密码为 “cisco”。

R0(config)#

R0(config)#line vty 0 4

R0(config-line)#password cisco

R0(config-line)#login

执行do show run命令查看配置结果。

R0(config-line)#do show run

（截图）

在R1上将VTY接口登录方式配置为密码认证方式，密码为 “cisco”。

R1(config)#

R1(config)#line vty 0 4

R1(config-line)#password cisco

R1(config-line)#login

执行do show run命令查看配置结果。

R1(config-line)#do show run

（截图）

在R0上进入特权模式，使用telnet登录R1。

R0#telnet 10.X.0.2

Trying 10.X.0.1 ...Open

User Access Verification

Password:

（截图）

1. 查看当前设备上存储的文件列表

在特权视图下执行**dir**命令，查看当前目录下的文件列表。

R0#dir

（截图）

R1#dir

（截图）

1. **管理设备配置文件**

执行**show running-config**命令查看保存的配置文件。

R0#show running-config

（截图）

执行**show startup-config**命令查看保存的配置文件。

R0#show startup-config

startup-config is not present

R0#

系统中没有已保存的配置文件。执行**write**命令保存当前配置文件。

R0#write

Building configuration...

[OK]

R0#

重新执行**show startup-config**命令查看已保存的配置信息。

R0#show startup-config

（截图）

若要清除保存的配置文件，可删除闪存中的配置文件。

R0#erase startup-config

Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]

[OK]

Erase of nvram: complete

%SYS-7-NV\_BLOCK\_INIT: Initialized the geometry of nvram

重新执行**show startup-config**命令查看已保存的配置信息。

R0#show startup-config

（截图）

1. **重启设备**

执行**reboot**命令重启路由器。

R0#reload

Proceed with reload? [confirm]

**协议报文分析实验**

**实验2 协议报文分析**

**学习目标**

* 掌握以太网帧结构
* 掌握IP报文结构
* 掌握TCP/UDP报文结构
* 掌握ICMP报文结构，熟练使用ping 和tracert命令
* 掌握ARP协议原理及工作过程

**拓扑图**

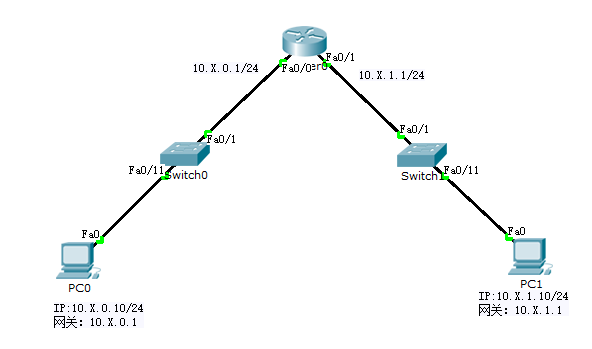


图1 协议报文分析拓扑

**操作步骤**

1. 配置各设备基础配置

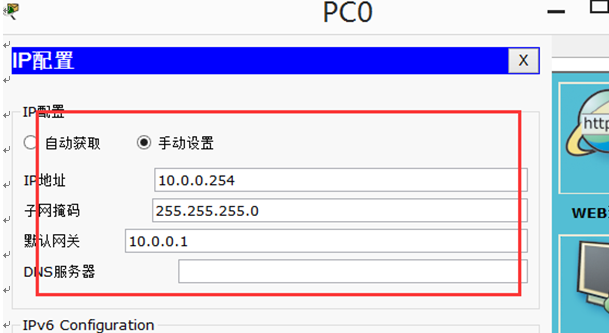
按照拓扑图组网，并完成基础配置：

R0:

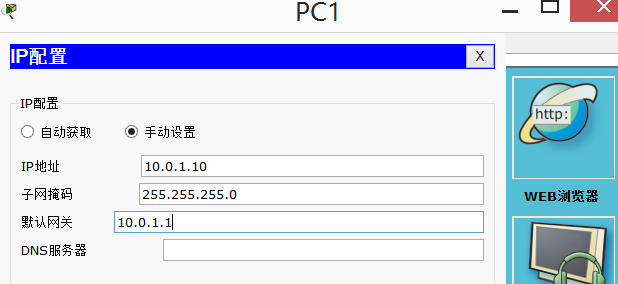
|  |
| --- |
| *Router>EN*  *Router#conf*  *Configuring from terminal, memory, or network [terminal]?*  *Enter configuration commands, one per line. End with CNTL/Z.*  *Router(config)#hostname R0 //设置设备名称*  *R0(config)#int f0/0 //进入F0/0接口*  *R0(config-if)#no shutdown //开启接口*  *R0(config-if)#ip add 10.X.0.1 255.255.255.0 //配置IP地址，注意X表示学号*  *R0(config-if)#description TO:SW0-F0/1 //接口描述*  *R0(config)#int f0/1*  *R0(config-if)#no shutdown*  *R0(config-if)#ip add 10.X.1.1 255.255.255.0 //配置IP地址，注意X表示学号*  *R0(config-if)#description TO:SW1-F0/1*  *R0(config-if)#exit*  *R0(config)#line vty 0 4*  *R0(config-line)#password cisco //配置telnet密码为cisco*  *R0(config-line)#login //配置密码认证*  *R0(config-line)#exit*  *R0(config)#exit*  *R0#*  *%SYS-5-CONFIG\_I: Configured from console by console*  *R0#wr*  *Building configuration...*  *[OK]*  *R0#* |

SW0 和SW1 不用进行配置

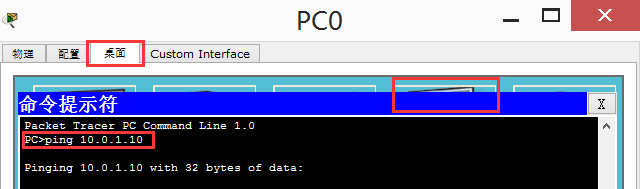
PC0 //注意根据个人学号配置IP地址和网关，此处以“0”为例。



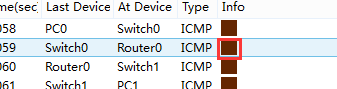
PC1 //注意根据个人学号配置IP地址和网关，此处以“0”为例。

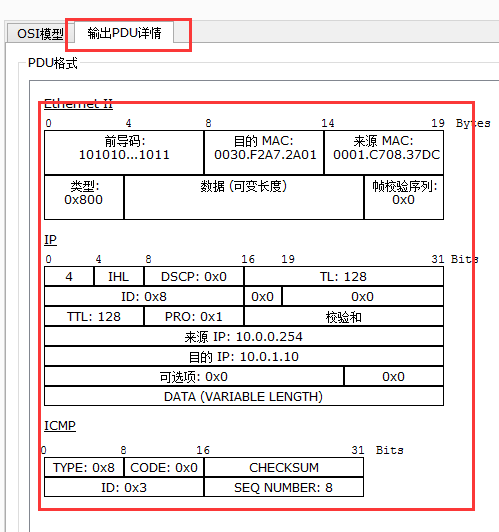


1. **Ping命令使用和报文分析**
2. 单击右下角“模拟”图标；
3. 单击“自动捕获/播放”；
4. 在PC0“命令提示符”中进行ping测试。

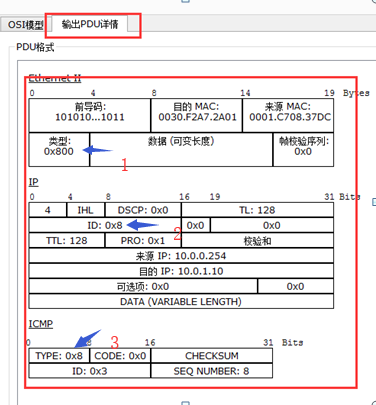


1. 查看“事件列表”中报文交互情况。
2. 选择“ICMP”报文，进行报文分析。

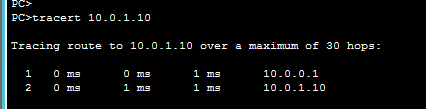




1. 请回答如下问题：
2. 请找出PC0发送至SW0设备的ICMP请求报文，将报文内容截图，并回答报文中源MAC 目的MAC，源IP，目的IP分别是多少？
3. 请找出SW0发送至R0设备的ICMP请求报文，将报文内容截图，并回答报文中源MAC 目的MAC，源IP，目的IP分别是多少？
4. 请找出R0发送至SW1设备的ICMP请求报文，将报文内容截图，并回答报文中源MAC 目的MAC，源IP，目的IP分别是多少？
5. 从PC0发出的报文的IP头部，在发送至PC1时哪些内容发生了变化？
6. 如下图所标注，各字段的含义是什么？



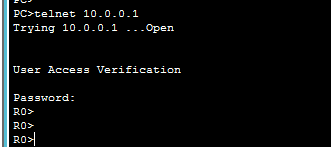
1. **Tracert 命令使用和报文分析**
2. 在PC0“命令提示符”中进行tracert测试。



1. 查看“事件列表”中报文交互情况。
2. 请回答如下问题：
3. tracert 有什么作用？
4. Tracert 的工作原理？
5. PC0发出的报文有何规律？
6. **telnet 协议交互过程**
7. 执行在PC0“命令提示符”中进行telnet R0。



1. 单击“模拟”，查看“事件列表”中报文交互情况。
2. 在PC0上输入密码“cisco”，后回车，登录R0成功。



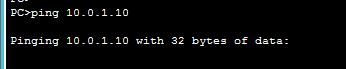
1. 查看“事件列表”中报文交互情况。
2. 交互完成后，在PC0上，退出R0。
3. 查看“事件列表”中报文交互情况。
4. 请回答如下问题：
5. 寻找到TCP建立过程中三次握手的报文并截图。
6. 为什么TCP建立连接使用三次握手，断开连接使用四次握手？
7. telnet协议有何作用，是由什么协议承载的，端口号是多少？
8. **ARP协议及交互过程。**
9. 在PC0上查看ARP表项，使用命令“arp -a”；



1. 如果PC0上有arp信息，可使用命令“arp -d”删除。



1. 单击“模拟”，在PC0上ping 10.0.1.10；



1. 在“事件列表中”查看ARP交互过程。
2. 请回答如下问题：
3. 什么情况下会进行ARP？
4. ARP协议的作用是什么？
5. ARP的请求和回应报文各是单播、组播还是广播报文？

**网络项目拓扑搭建实验**

**实验3 网络项目拓扑搭建**

**学习目标**

* 掌握企业网拓扑搭建技巧
* 利用Cisco Packet Tracer搭建实训拓扑
* 完成各设备初始配置
* 完成各路由器接口IP地址配置
* 完成出口静态缺省路由配置

**拓扑图**



图1拓扑

**操作步骤**

1. 网络拓扑搭建

1、按照拓扑图组网，完成网络搭建，建议各设备型号选择如下：

路由器选择2811，三层交换机选择 3560，二层交换机选择2950。

2、拓扑中R1和R3需添加串行口接口卡，具体添加步骤如下：

A.关闭R1和R3电源，单击下图所示：

B.在R1和R3上分别选择“WIC-1T”子卡拖动到设备区域；



C.在R1上再添加 “WIC-1T”子卡拖动到设备区域；

D．开启R1和R3电源。

3、完成设备互联

A．严格遵守“同种设备交叉线，异种设备直通线”的网线使用原则，及路由器与路由器之间互联使用交叉线，路由器与PC机互联使用交叉线，交换机与交换机互联使用交叉线，交换机与路由器或PC及互联使用直通线。

B． R1和R2之间使用串口线互联。

C．必须按照前期规划，按照附件《附件二：设备台账示例》中设备互联规划进行线缆连接。

1. **完成各设备基础配置**

各设备在入网时需配置基础配置，至少包括修改设备名称，配置telnet功能，接口描述。

1. 各设备按照附件《附件二：设备台账示例》中修改对应设备名称。

参考配置如下：

R1:

|  |
| --- |
| *Router>EN*  *Router#conf*  *Configuring from terminal, memory, or network [terminal]?*  *Enter configuration commands, one per line. End with CNTL/Z.*  *Router(config)#hostname R1 //设置设备名称* |

1. 配置除Internet路由器外所有设备telnet功能，采用密码认证，密码统一使用“cisco”，参考配置如下：

|  |
| --- |
| *R1(config)#line vty 0 4*  *R1(config-line)#password cisco //配置telnet密码为cisco*  *R1(config-line)#login //配置密码认证*  *R1(config-line)#exit* |

1. 各设备按照附件《附件二：设备台账示例》中完成各接口描述，参考配置如下：

R1:

|  |
| --- |
| *R1(config)#int f0/0*  *R1(config-if)#description TO：Internet-F0/1*  *R1(config-if)#exit* |

1. **配置各路由器接口IP，并进行链路连通性测试。**

需配置各路由器接口IP地址并进行连通性测试。

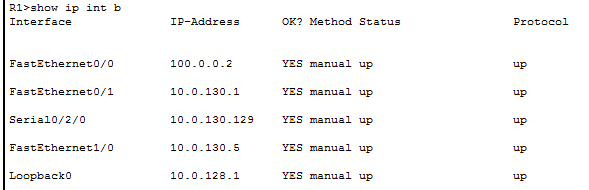
1. 各路由设备按照附件《附件二：设备台账示例》中接口IP规划进行接口IP地址配置，参考配置如下：

以R1 f0/0为例:

|  |
| --- |
| *R1(config)#int f0/0 //进入F0/0接口*  *R1(config-if)#no shutdown //开启接口*  *R1(config-if)#ip add 100.0.0.2 255.255.255.0 //配置IP地址，注意X表示学号*  *R1(config-if)#exit* |

1. 配置完成后可在各路由器设备上查看接口IP信息，检查与IP规划是否一致，且接口物理及协议是否UP，并截图。

命令如下：在特权视图下“show ip inter brief”



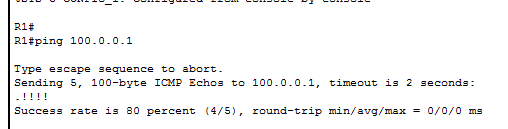
Internet接口IP信息（截图）

R1接口IP信息（截图）

R2接口IP信息（截图）

R3接口IP信息（截图）

1. 对于同一链路两端都配置了IP地址可进行连通性测试，如在R1上对接口F0/0连通性进行测试，并截图，如下：在特权模式ping X.X.X.X（对端接口IP）。



Internet—R1（截图）

Internet—R2（截图）

R1—R3（截图）

1. **设置路由器管理IP**

路由器可使用loopback 0地址配置32位IP地址作为管理IP；

按照《设备台账示例》中设备管理IP地址规划，进行网管地址配置。

|  |  |  |
| --- | --- | --- |
| R1 |  | 10.X.128.1/32 |
| R2 |  | 10.X.128.2/32 |
| R3 |  | 10.X.128.3/32 |

1. R1管理地址配置

|  |
| --- |
| *R1(config)#int loo 0*  *R1(config-if)#ip add 10.0.128.1 255.255.255.255*  *R1(config-if)#exit* |

1. R2管理地址配置

|  |
| --- |
| *R2(config)#int loo 0*  *R2(config-if)#ip add 10.0.128.2 255.255.255.255*  *R2(config-if)#exit* |

1. R3管理地址配置

|  |
| --- |
| *R3(config)#int loo 0*  *R3(config-if)#ip add 10.0.128.3 255.255.255.255*  *R3(config-if)#exit* |

1. **出口设备静态缺省路由配置**

企业内网使用私网IP，Inetnet使用公网IP，企业内网设备需拥有全网路由，使用缺省路由实现，Inetnet不能有私网路由，故出口路由器与运营商路由器不能采用动态路由进行路由学习。具体解决方案为出口路由器上使用静态路由做缺省路由指向运营商设备。

1. 在R1上进行如下配置:

*R1(config)#ip route 0.0.0.0 0.0.0.0 100.0.0.1*

1. 在R1上查看路由表，并截图：

R1(config)#do show ip rou

R1路由表（截图）

1. 在R2上进行如下配置:

*R2(config)#ip route 0.0.0.0 0.0.0.0 200.0.0.1*

1. 在R2上查看路由表，并截图：

*R2(config)#do show ip rou*

R2路由表（截图）

1. 在R1上对R2进行ping测：

*R1#ping 200.0.0.2*

R1 ping R2结果 （截图）

1. **保存配置并用U盘带走文件**

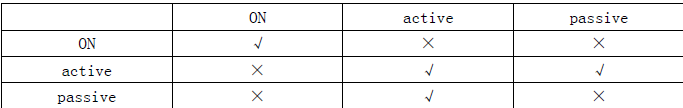
**链路聚合实验**

**实验4-1 链路聚合实验**

**学习目标**

* 掌握链路聚合原理
* 掌握链路聚合配置

**链路聚合技术分析**

* 随着网络规模不断扩大，用户对骨干链路的带宽和可靠性提出了越来越高的要求。在传统技术中，常用更换高速率的接口板或更换支持高速率接口板的设备的方式来增加带宽，但这种方案需要付出高额的费用，而且不够灵活。
* 采用链路聚合技术可以在不进行硬件升级的条件下，通过将多个物理接口捆绑为一个逻辑接口，来达到增加链路带宽的目的。在实现增大带宽目的的同时，链路聚合采用备份链路的机制，可以有效的提高设备之间链路的可靠性。
* CISCO 链路聚合模式匹配图
* 
* 本项目中汇聚交换机SW1和SW2之间需要进行链路聚合提高带宽及提升链路可靠性。

**拓扑图**

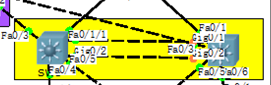


图1拓扑

**操作步骤**

1. 创建链路聚合端口

1、将《网络项目拓扑搭建实验》中保存的拓扑打开:拓扑中SW1和SW2之间各有两个端口互联，可将G0/1和G0/2加入同一链路聚合组中。



2、在SW1上创建port-channel：

|  |
| --- |
| *SW1>enable*  *SW1#conf*  *Configuring from terminal, memory, or network [terminal]?*  *Enter configuration commands, one per line. End with CNTL/Z.*  *SW1(config)#interface port-channel 12* |

3、在SW2上创建port-channel：

|  |
| --- |
| *SW2>enable*  *SW2#conf*  *Configuring from terminal, memory, or network [terminal]?*  *Enter configuration commands, one per line. End with CNTL/Z.*  *SW2(config)#interface port-channel 12* |

1. **物理接口关联port-channel**
2. 将SW1的G0/1和G0/2加入port-channel12中，参考命令如下：

|  |
| --- |
| *SW1(config-if)#int g0/1*  *SW1(config-if)#channel-group 12 mode active*  *SW1(config-if)#int g0/2*  *SW1(config-if)#channel-group 12 mode active* |

1. 查看SW1上etherchannel状态：

|  |
| --- |
| *SW1#show int etherchannel*  *GigabitEthernet0/1:*  *Port state = 1*  *Channel group = 12 Mode = Active Gcchange = -*  *Port-channel = Po12 GC = - Pseudo port-channel = Po12*  *Port index = 0 Load = 0x00 Protocol = LACP*  *Flags: S - Device is sending Slow LACPDUs F - Device is sending fast LACPDUs*  *A - Device is in active mode. P - Device is in passive mode.*  *Local information:*  *LACP port Admin Oper Port Port*  *Port Flags State Priority Key Key Number State*  *Fa0/1 SA down 32768 0x0 0x0 0x25*  *Age of the port in the current state: 13244d:10h:55m:54s*  *GigabitEthernet0/2:*  *Port state = 1*  *Channel group = 12 Mode = Active Gcchange = -*  *Port-channel = Po12 GC = - Pseudo port-channel = Po12*  *Port index = 0 Load = 0x00 Protocol = LACP*  *Flags: S - Device is sending Slow LACPDUs F - Device is sending fast LACPDUs*  *A - Device is in active mode. P - Device is in passive mode.*  *Local information:*  *LACP port Admin Oper Port Port*  *Port Flags State Priority Key Key Number State*  *Fa0/2 SA down 32768 0x0 0x0 0x26*  *Age of the port in the current state: 13244d:10h:55m:54s*  *----*  *Port-channel12:Port-channel12 (Primary aggregator)*  *Age of the Port-channel = 00d:00h:00m:48s*  *Logical slot/port = 2/12 Number of ports = 0*  *HotStandBy port = null*  *Port state =*  *Protocol = 1*  *Port Security = Disabled* |

1. 将SW2的G0/1和G0/2加入port-channel12中，参考命令如下：

|  |
| --- |
| *SW2(config-if)#int g0/1*  *SW2(config-if)#channel-group 12 mode active*  *SW2(config-if)#int g0/2*  *SW2(config-if)#channel-group 12 mode active* |

1. 查看SW2上etherchannel状态：

|  |
| --- |
| *SW2#show interfaces etherchannel*  *GigabitEthernet0/1:*  *Port state = 1*  *Channel group = 12 Mode = Active Gcchange = -*  *Port-channel = Po12 GC = - Pseudo port-channel = Po12*  *Port index = 0 Load = 0x00 Protocol = LACP*  *Flags: S - Device is sending Slow LACPDUs F - Device is sending fast LACPDUs*  *A - Device is in active mode. P - Device is in passive mode.*  *Local information:*  *LACP port Admin Oper Port Port*  *Port Flags State Priority Key Key Number State*  *Fa0/1 SA down 32768 0x0 0x0 0x25*  *Partner's information:*  *LACP port Admin Oper Port Port*  *Port Flags Priority Dev ID Age key Key Number State*  *Fa0/1 SA 32768 0003.E436.CA98 0x0 0x0 0x25*  *Age of the port in the current state: 00d:00h:00m:08s*  *GigabitEthernet0/2:*  *Port state = 1*  *Channel group = 12 Mode = Active Gcchange = -*  *Port-channel = Po12 GC = - Pseudo port-channel = Po12*  *Port index = 0 Load = 0x00 Protocol = LACP*  *Flags: S - Device is sending Slow LACPDUs F - Device is sending fast LACPDUs*  *A - Device is in active mode. P - Device is in passive mode.*  *Local information:*  *LACP port Admin Oper Port Port*  *Port Flags State Priority Key Key Number State*  *Fa0/2 SA down 32768 0x0 0x0 0x26*  *Partner's information:*  *LACP port Admin Oper Port Port*  *Port Flags Priority Dev ID Age key Key Number State*  *Fa0/2 SA 32768 0003.E436.CA98 0x0 0x0 0x26*  *Age of the port in the current state: 00d:00h:00m:08s*  *----*  *Port-channel12:Port-channel12 (Primary aggregator)*  *Age of the Port-channel = 00d:00h:13m:37s*  *Logical slot/port = 2/12 Number of ports = 2*  *HotStandBy port = null*  *Port state =*  *Protocol = 1*  *Port Security = Disabled*  *Ports in the Port-channel:*  *Index Load Port EC state No of bits*  *------+------+------+------------------+-----------*  *0 00 Gig0/1 Active 0*  *0 00 Gig0/2 Active 0*  *Time since last port bundled: 00d:00h:00m:08s Gig0/2* |

1. **保存配置并用U盘带走文件**

**VLAN实验**

**实验4-2 VLAN**

**学习目标**

* 掌握交换机工作原理
* 掌握VLAN技术，理解业务VLAN、互联VLAN、管理VLAN的含义
* 掌握Access和Trunk类型接口的配置方法

**拓扑图**



图1拓扑

**操作步骤**

1. 创建VLAN
2. 将《链路聚合实验》中保存的拓扑打开:拓扑中交换机SW1-6在使用VLAN前需创建VLAN各交换机所需创建VLAN 列表如下：

|  |  |
| --- | --- |
| 交换机名称 | 所需创建vlan-ID |
| SW1 | 2,11,13,101-104 |
| SW2 | 2,12,13,101-104 |
| SW3 | 2,101 |
| SW4 | 2,102 |
| SW5 | 2,103 |
| SW6 | 2,104 |

2、在各设备上创建VLAN，以SW1为例：

|  |
| --- |
| *SW1>enable*  *SW1#configure terminal*  *Enter configuration commands, one per line. End with CNTL/Z.*  *SW1(config)#*  *SW1(config)#vlan 2*  *SW1(config-vlan)#name guanli*  *SW1(config-vlan)#vlan 11*  *SW1(config-vlan)#name hulian-R1*  *SW1(config-vlan)#vlan 13*  *SW1(config-vlan)#name hulian-SW2*  *SW1(config-vlan)#vlan 101*  *SW1(config-vlan)#name PC1*  *SW1(config-vlan)#vlan 102*  *SW1(config-vlan)#name PC2*  *SW1(config-vlan)#vlan 103*  *SW1(config-vlan)#name PC3*  *SW1(config-vlan)#vlan 104*  *SW1(config-vlan)#name PC4*  *SW1(config-vlan)#exit* |

3、查看各交换VLAN信息，以SW1为例：

|  |
| --- |
| *SW1#show vlan brief*  *VLAN Name Status Ports*  *---- -------------------------------- --------- -------------------------------*  *1 default active Fa0/1, Fa0/2, Fa0/3, Fa0/4*  *Fa0/5, Fa0/6, Fa0/7, Fa0/8*  *Fa0/9, Fa0/10, Fa0/11, Fa0/12*  *Fa0/13, Fa0/14, Fa0/15, Fa0/16*  *Fa0/17, Fa0/18, Fa0/19, Fa0/20*  *Fa0/21, Fa0/22, Fa0/23, Fa0/24*  *Gig0/1, Gig0/2, Po12*  *2 guanli active*  *11 hulian active*  *13 hulian-SW2 active*  *101 PC1 active*  *102 PC2 active*  *103 PC3 active*  *104 PC4 active* |

1. **修改交换机端口类型及透传VLAN**
2. 按照《设备台账示例》中对各交换机规划的接口类型及透传VLAN进行配置。
3. Access接口类型配置参考命令：

|  |
| --- |
| 以SW1的F0/1接口为例：  *SW1(config)#int f0/1*  *SW1(config-if)#switchport mode access*  *SW1(config-if)#switchport access vlan 11* |

查看VLAN信息， F0/1接口添加到vlan11。

|  |
| --- |
| *SW1#show vlan brief*  *VLAN Name Status Ports*  *---- -------------------------------- --------- -------------------------------*  *1 default active Fa0/2, Fa0/3, Fa0/4, Fa0/5*  *Fa0/6, Fa0/7, Fa0/8, Fa0/9*  *Fa0/10, Fa0/11, Fa0/12, Fa0/13*  *Fa0/14, Fa0/15, Fa0/16, Fa0/17*  *Fa0/18, Fa0/19, Fa0/20, Fa0/21*  *Fa0/22, Fa0/23, Fa0/24, Gig0/1*  *Gig0/2, Po12*  *2 guanli active*  *11 hulian active Fa0/1*  *13 hulian-SW2 active*  *101 PC1 active*  *102 PC2 active*  *103 PC3 active*  *104 PC4 active*  *1002 fddi-default active*  *1003 token-ring-default active*  *1004 fddinet-default active*  *1005 trnet-default active*  *SW1#* |

1. Trunk接口类型配置参考命令：

|  |
| --- |
| 汇聚交换机（SW1/SW2）以SW1的F0/3接口为例：  *SW1(config)#int f0/3*  *SW1(config-if)#switchport mode trunk*  *SW1(config-if)#switchport trunk encapsulation dot1q*  *SW1(config-if)#switchport trunk allowed vlan 2,101*  接入交换机（SW3--6）以SW3的F0/1接口为例：  *SW3(config)#int f0/1*  *SW3config-if)#switchport mode trunk*  *SW3(config-if)#switchport trunk allowed vlan 2,101* |

1. 链路聚合端口接口类型及透传VLAN

|  |
| --- |
| 以SW1的*Port-channel 12*接口为例：  *SW1(config)#* *interface Port-channel 12*  *SW1(config-if)#switchport mode trunk*  *SW1(config-if)#switchport trunk encapsulation dot1q*  *SW1(config-if)#switchport trunk allowed vlan 2,13,101,103* |

1. **保存配置并用U盘带走文件**

**RSTP实验**

**实验5-1RSTP**

**学习目标**

* 了解二层环路产生的原因，影响。
* 理解STP、PVST、RSTP原理
* 掌握RSTP部署方式和配置

**原理**

STP 简介

1 基本STP

为了增加局域网的冗余性，我们常常会在网络中引入冗余链路，然而这样却会引起交换环路。交换环路会带来三个问题：广播风暴、同一帧的多个拷贝、交换机CAM 表不稳定。STP(STP，Spanning Tree Protocol)可以解决这些问题，STP 基本思路是阻断一些交换机接口，构建一棵没有环路的转发树。STP 利用BPDU(Bridge Protocol Data Unit)和其他交换机进行通信，从而确定哪个交换机该阻断哪个接口。在BPDU 中有几个关键的字段，例如：根桥ID、路径代价、端口ID 等。

为了在网络中形成一个没有环路的拓扑，网络中的交换机要进行以下三个步骤：（1）选举根桥、（2）选取根口、（3）选取指定口。这些步骤中，哪个交换机能获胜将取决于以因

素（按顺序进行）：

（1） 最低的根桥ID；

（2） 最低的根路径代价；

（3） 最低发送者桥ID；

（4） 最低发送者端口ID。

每个交换机都具有一个唯一的桥ID，这个ID 由两部分组成：网桥优先级+MAC 地址。网桥优先级是一个2 个字节的数，交换机的默认优先级为32768；MAC 地址就是交换机的MAC地址。具有最低桥ID 的交换机就是根桥。根桥上的接口都是指定口，会转发数据包。选举了根桥后，其他的交换机就成为非根桥了。每台非根桥要选举一条到根桥的根路径。STP 使用路径Cost 来决定到达根桥的最佳路径（Cost 是累加的，带宽大的链路Cost 低），最低Cost 值的路径就是根路径，该接口就是根口；如果Cost 职一样，就根据选举顺序选举

根口。根口是转发数据包的。

交换机的其他接口还要决定是指定口还是阻断口，交换机之间将进一步根据上面的四个因素来竞争。指定口是转发数据帧的。剩下的其它的接口将被阻断，不转发数据包。这样网络就构建出一棵没有环路的转发树。

当网络的拓扑发生变化时，网络会从一个状态向另一个状态过渡，重新打开或阻断某些接口。交换机的端口要经过几种状态： 禁用（Disable）、阻塞（Blocking）、监听状态(Listening)、学习状态（Learning）、最后是转发状态(Forwarding)。

2 PVST

当网络上有多个VLAN 时，PVST(Per Vlan STP)会为每个VLAN 构建一棵STP 树。这样的好处是可以独立地为每个VLAN 控制哪些接口要转发数据，从而实现负载平衡。缺点是如果VLAN 数量很多，会给交换机带来沉重的负担。Cisco 交换机默认的模式就是PVST。

3 RSTP

RSTP 实际上是把减少STP 收敛时间的一些措施融合在STP 协议中形成新的协议

RSTP中，接口的角色有：根接口、指定接口、备份接口(Backup Interface)、替代接口（Alternate Interface）。接口的状态有：丢弃（Discarding）、学习状态（Learning）、转发状态(Forwarding)。

4 portfast

STP 的收敛时间通常需要30—50 秒。为了减少收敛时间，有一些改善措施。Portfast特性使得以太网接口一旦有设备接入，就立即进入转发状态，如果接口上连接的只是计算机或者其他不运行STP 的设备，这是非常合适的。

**拓扑图**



图1拓扑

**操作步骤**

1. 设置交换机STP模式为RSTP（rapid-pvst）
2. 将《VLAN实验》中保存的拓扑打开，SW1-SW6需部署RSTP。
3. 检查现网交换机生成树模式，cisco交换机默认为STP模式，需修改为RSTP。

|  |
| --- |
| *SW1#show spanning-tree*  *VLAN0001*  *Spanning tree enabled protocol ieee*  *Root ID Priority 32769*  *Address 0003.E436.CA98*  *This bridge is the root*  *Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec*  *Bridge ID Priority 32769 (priority 32768 sys-id-ext 1)*  *Address 0003.E436.CA98*  *Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec*  *Aging Time 20*  *Interface Role Sts Cost Prio.Nbr Type*  *---------------- ---- --- --------- -------- --------------------------------*  *Po12 Desg LSN 3 128.28 Shr* |

1. 将SW1—6生成树模式改为RSTP。

参考配置如下：

|  |
| --- |
| *以SW1为例*  *SW1>enable*  *SW1#configure terminal*  *Enter configuration commands, one per line. End with CNTL/Z.*  *SW1(config)#spanning-tree mode rapid-pvst* |

4、查看各交换生成树模式，以SW1为例：

|  |
| --- |
| *SW1#show spanning-tree*  *VLAN0001*  *Spanning tree enabled protocol rstp*  *Root ID Priority 32769*  *Address 0003.E436.CA98*  *This bridge is the root*  *Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec*  *Bridge ID Priority 32769 (priority 32768 sys-id-ext 1)*  *Address 0003.E436.CA98*  *Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec*  *Aging Time 20*  *Interface Role Sts Cost Prio.Nbr Type*  *---------------- ---- --- --------- -------- --------------------------------*  *Po12 Desg FWD 3 128.28 Shr* |

1. **设置根桥及备份根桥**
2. 在汇聚交换机SW1和SW2上为各VLAN设置根桥和备份根桥；

SW1为VLAN 2,11,13,101,102的根桥优先级设为0，为VLAN103的备份根桥，优先级设为4096；配置如下：

|  |
| --- |
| *SW1(config)#spanning-tree vlan 2 root primary*  *SW1(config)#spanning-tree vlan 11 root primary*  *SW1(config)#spanning-tree vlan 13 root primary*  *SW1(config)#spanning-tree vlan 101 root primary*  *SW1(config)#spanning-tree vlan 102 root primary*  *SW1(config)#spanning-tree vlan 103 root secondary* |

SW2为VLAN 12, 103,104的根桥优先级设为0，为VLAN2,13,101的备份根桥，优先级设为4096；配置如下：

|  |
| --- |
| *SW2(config)#spanning-tree vlan 12 root primary*  *SW2(config)#spanning-tree vlan 103 root primary*  *SW2(config)#spanning-tree vlan 104 root primary*  *SW2(config)#spanning-tree vlan 2 root secondary*  *SW2(config)#spanning-tree vlan 13 root secondary*  *SW2(config)#spanning-tree vlan 101 root secondary* |

1. 在各交换机上查看所属VLAN的生成树状态，并截图；

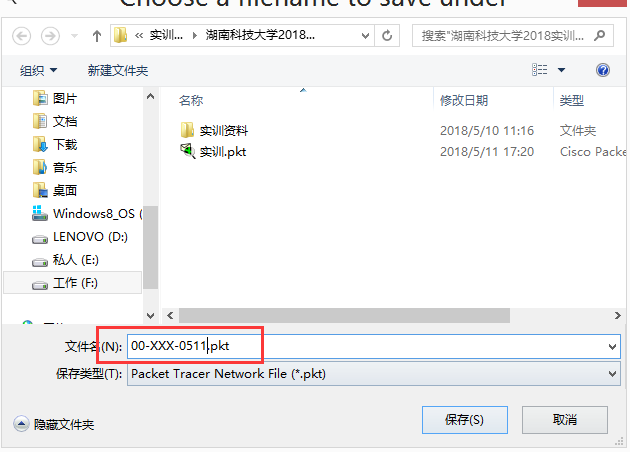
|  |
| --- |
| 以SW1为例，关注各VLAN端口角色和端口状态。  *SW1# show spanning-tree active*  *VLAN0002*  *Spanning tree enabled protocol rstp*  *Root ID Priority 24578*  *Address 0003.E436.CA98*  *This bridge is the root*  *Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec*  *Bridge ID Priority 24578 (priority 24576 sys-id-ext 2)*  *Address 0003.E436.CA98*  *Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec*  *Aging Time 20*  *Interface Role Sts Cost Prio.Nbr Type*  *---------------- ---- --- --------- -------- --------------------------------*  *Fa0/4 Desg FWD 19 128.4 P2p*  *Fa0/3 Desg FWD 19 128.3 P2p*  *Fa0/5 Desg FWD 19 128.5 P2p*  *Po12 Desg FWD 3 128.28 Shr*  *VLAN0011*  *Spanning tree enabled protocol rstp*  *Root ID Priority 24587*  *Address 0003.E436.CA98*  *This bridge is the root*  *Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec*  *Bridge ID Priority 24587 (priority 24576 sys-id-ext 11)*  *Address 0003.E436.CA98*  *Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec*  *Aging Time 20*  *Interface Role Sts Cost Prio.Nbr Type*  *---------------- ---- --- --------- -------- --------------------------------*  *Fa0/1 Desg FWD 19 128.1 P2p*  *VLAN0013*  *Spanning tree enabled protocol rstp*  *Root ID Priority 24589*  *Address 0003.E436.CA98*  *This bridge is the root*  *Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec*  *Bridge ID Priority 24589 (priority 24576 sys-id-ext 13)*  *Address 0003.E436.CA98*  *Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec*  *Aging Time 20*  *Interface Role Sts Cost Prio.Nbr Type*  *---------------- ---- --- --------- -------- --------------------------------*  *Po12 Desg FWD 3 128.28 Shr*  *VLAN0101*  *Spanning tree enabled protocol rstp*  *Root ID Priority 24677*  *Address 0003.E436.CA98*  *This bridge is the root*  *Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec*  *Bridge ID Priority 24677 (priority 24576 sys-id-ext 101)*  *Address 0003.E436.CA98*  *Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec*  *Aging Time 20*  *Interface Role Sts Cost Prio.Nbr Type*  *---------------- ---- --- --------- -------- --------------------------------*  *Fa0/3 Desg FWD 19 128.3 P2p*  *Po12 Desg FWD 3 128.28 Shr*  *VLAN0102*  *Spanning tree enabled protocol rstp*  *Root ID Priority 24678*  *Address 0003.E436.CA98*  *This bridge is the root*  *Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec*  *Bridge ID Priority 24678 (priority 24576 sys-id-ext 102)*  *Address 0003.E436.CA98*  *Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec*  *Aging Time 20*  *Interface Role Sts Cost Prio.Nbr Type*  *---------------- ---- --- --------- -------- --------------------------------*  *Fa0/4 Desg BLK 19 128.4 P2p*  *VLAN0103*  *Spanning tree enabled protocol rstp*  *Root ID Priority 24679*  *Address 0005.5EA7.B684*  *Cost 3*  *Port 28(Port-channel 12)*  *Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec*  *Bridge ID Priority 28775 (priority 28672 sys-id-ext 103)*  *Address 0003.E436.CA98*  *Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec*  *Aging Time 20*  *Interface Role Sts Cost Prio.Nbr Type*  *---------------- ---- --- --------- -------- --------------------------------*  *Fa0/5 Desg FWD 19 128.5 P2p*  *Po12 Root FWD 3 128.28 Shr* |

SW1---SW6生成树状态截图。

1. **设置portfast**
2. 将所有连接PC的交换机端口都设成portfast端口，这样可以不用等到30S的转发时延，端口UP后可立即进行数据转发。
3. SW3-SW6的F0/11接口设置为portfast。

|  |
| --- |
| 以SW3为例，  *SW3(config)#interface fastEthernet 0/11*  *SW3(config-if)#spanning-tree portfast* |

1. **保存配置并用U盘带走文件**



**VLAN间路由实验**

**实验5-2VLAN间路由**

**学习目标**

* 了解三层交换机的工作原理。
* 配置三层交换机
* 理解理解业务VLAN、互联VLAN、管理VLAN的含义

**原理**

在交换机上划分VLAN 后，VLAN 间的计算机就无法通信了。VLAN 间的通信需要借助第三层设备，我们可以使用路由器来实现这个功能，如果使用路由器通常会采用单臂路由模式。实践上，VLAN 间的路由大多是通过三层交换机实现的，三层交换机可以看成是路由器加交换机，然而因为采用了特殊的技术，其数据处理能力比路由器要大得多。

从使用者的角度可以把三层交换机看成是二层交换机和路由器的组合，这

个虚拟的路由器和每个VLAN 都有一个接口进行连接，不过这个接口是VLAN1 或VLAN2 接口。Cisco 早些年采用的基于NetFlow 的三层交换技术；现在Cisco 主要采用CEF 技术。CEF 技术中，交换机利用路由表形成转发信息库（FIB），FIB 和路由表是同步的，关键的是它的查询是硬件化，查询速度快得多。除了FIB，还有邻接表(Adjacency Table)，该表和ARP 表有些类似，主要放置了第二层的封装信息。FIB 和邻接表都是在数据转发之前就已经建立准备好了，这样一有数据要转发，交换机就能直接利用它们进行数据转发和封装，不需要查询路由表和发送ARP 请求，所以VLAN 间的路由速率大大提高。

**拓扑图**



图1拓扑

**操作步骤**

1. 配置汇聚交换机业务VLAN地址
2. 将《RSTP实验》中保存的拓扑打开，汇聚交换机SW1与SW2需为互联VLAN设置IP地址。
3. SW1按照《设备台账示例》中分配好的IP地址进行配置。

Int vlan 11 10.X.130.2/30

Int vlan 13 10.X.130.9/30

|  |
| --- |
| *SW1(config)#ip routing //开启三层转发*  *SW1(config)#int vlan 11*  *SW1(config-if)#ip add 10.0.130.2 255.255.255.252*  *SW1(config)#int vlan 13*  *SW1(config-if)#ip add 10.0.130.9 255.255.255.252* |

1. SW2按照《设备台账示例》中分配好的IP地址进行配置。

Int vlan 12 10.X.130.6/30

Int vlan 13 10.X.130.10/30

|  |
| --- |
| *SW2(config)#ip routing //开启三层转发*  *SW2(config)#int vlan 12*  *SW2(config-if)#ip add 10.0.130.6 255.255.255.252*  *SW2(config)#int vlan 13*  *SW2(config-if)#ip add 10.0.130.10 255.255.255.252* |

1. 测试SW1互联地址连通性

|  |
| --- |
| *SW1(config)#do ping 10.0.130.1*  *Type escape sequence to abort.*  *Sending 5, 100-byte ICMP Echos to 10.0.130.1, timeout is 2 seconds:*  *.!!!!!!*  *Success rate is 120 percent (6/5), round-trip min/avg/max = 0/0/1 ms*  *SW1(config)#do ping 10.0.130.10*  *Type escape sequence to abort.*  *Sending 5, 100-byte ICMP Echos to 10.0.130.10, timeout is 2 seconds:*  *.!!!!*  *Success rate is 80 percent (4/5), round-trip min/avg/max = 0/0/1 ms* |

1. 测试SW2互联地址连通性

|  |
| --- |
| *SW2(config)#do ping 10.0.130.5*  *Type escape sequence to abort.*  *Sending 5, 100-byte ICMP Echos to 10.0.130.5, timeout is 2 seconds:*  *.!!!!!!*  *Success rate is 120 percent (6/5), round-trip min/avg/max = 0/0/1 ms*  *SW2(config)#do ping 10.0.130.9*  *Type escape sequence to abort.*  *Sending 5, 100-byte ICMP Echos to 10.0.130.9, timeout is 2 seconds:*  *.!!!!*  *Success rate is 80 percent (4/5), round-trip min/avg/max = 0/0/1 ms* |

1. 配置汇聚交换机业务VLAN地址

SW1和SW2作为各业务网关需为各业务VLAN配置IP地址。

1. SW1按照《设备台账示例》中分配好的IP地址进行配置。

int vlan 101 10.X.0.251/24

int vlan 102 10.X.1.1/24

int vlan 103 10.X.2.251/24

|  |
| --- |
| *SW1>enable*  *SW1#configure terminal*  *SW1(config)#int vlan 101*  *SW1(config-if)#ip add 10.0.0.251 255.255.255.0*  *SW1(config-if)#int vlan 102*  *SW1(config-if)#ip add 10.0.1.1 255.255.255.0*  *SW1(config-if)#int vlan 103*  *SW1(config-if)#ip add 10.0.2.251 255.255.255.0* |

1. 配置完成后，验证配置，

|  |
| --- |
| *SW1#show ip int b*  *Interface IP-Address OK? Method Status Protocol*  *Vlan101 10.0.0.251 YES manual up up*  *Vlan102 10.0.1.1 YES manual up up*  *Vlan103 10.0.2.251 YES manual up up* |

1. SW2按照《设备台账示例》中分配好的IP地址进行配置。

int vlan 101 10.X.0.252/24

int vlan 103 10.X.2.252/24

int vlan 104 10.X.3.1/24

|  |
| --- |
| *SW2>enable*  *SW2#configure terminal*  *SW2(config)#int vlan 101*  *SW2(config-if)#ip add 10.0.0.252 255.255.255.0*  *SW2(config-if)#int vlan 103*  *SW2config-if)#ip add 10.0.2.251 255.255.255.0*  *SW2(config-if)#int vlan 104*  *SW2(config-if)#ip add 10.0.3.1 255.255.255.0* |

1. 配置完成后，验证配置，

|  |
| --- |
| *SW1#show ip int b*  *Interface IP-Address OK? Method Status Protocol*  *Vlan101 10.0.0.251 YES manual up up*  *Vlan103 10.0. 2.252 YES manual up up*  *Vlan104 10.0.3.1 YES manual up up* |

1. **设置管理VLAN地址**

按照《设备台账示例》网管地址规划，为交换机设置管理VLAN IP地址。

|  |  |  |
| --- | --- | --- |
| SW1 | 2 | 10.X.129.1/24 |
| SW2 | 2 | 10.X.129.2/24 |
| SW3 | 2 | 10.X.129.3/24 |
| SW4 | 2 | 10.X.129.4/24 |
| SW5 | 2 | 10.X.129.5/24 |
| SW6 | 2 | 10.X.129.6/24 |

1. 设置SW1管理地址

|  |
| --- |
| *SW1>enable*  *SW1#configure terminal*  *Enter configuration commands, one per line. End with CNTL/Z.*  *SW1(config)#interface vlan 2*  *SW1(config-if)#ip add 10.0.129.1 255.255.255.0*  *SW1(config-if)#exit* |

1. 设置SW2管理地址

|  |
| --- |
| *SW2>enable*  *SW2#configure terminal*  *Enter configuration commands, one per line. End with CNTL/Z.*  *SW2(config)#interface vlan 2*  *SW2(config-if)#ip add 10.0.129.2 255.255.255.0*  *SW2(config-if)#exit* |

1. 设置SW3管理地址

|  |
| --- |
| *SW3>enable*  *SW3#configure terminal*  *Enter configuration commands, one per line. End with CNTL/Z.*  *SW3(config)#interface vlan 2*  *SW3(config-if)#ip add 10.0.129.3 255.255.255.0*  *SW3(config-if)#exit* |

1. 设置SW4管理地址

|  |
| --- |
| *SW4>enable*  *SW4#configure terminal*  *Enter configuration commands, one per line. End with CNTL/Z.*  *SW4(config)#interface vlan 2*  *SW4(config-if)#ip add 10.0.129.4 255.255.255.0*  *SW4(config-if)#exit* |

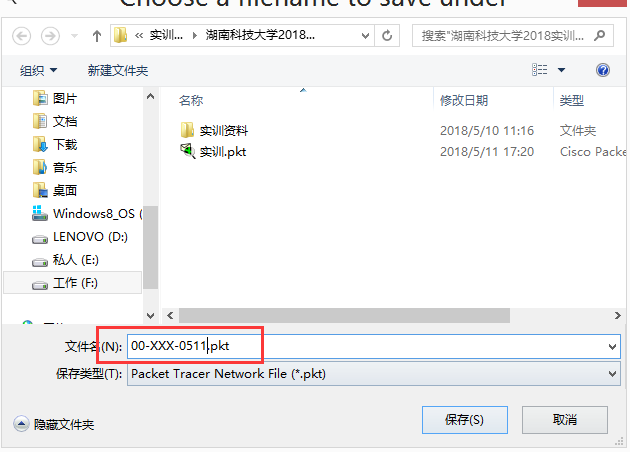
1. 设置SW5管理地址

|  |
| --- |
| *SW5>enable*  *SW5#configure terminal*  *Enter configuration commands, one per line. End with CNTL/Z.*  *SW5(config)#interface vlan 2*  *SW5(config-if)#ip add 10.0.129.5 255.255.255.0*  *SW5(config-if)#exit* |

1. 设置SW6管理地址

|  |
| --- |
| *SW6>enable*  *SW6#configure terminal*  *Enter configuration commands, one per line. End with CNTL/Z.*  *SW6(config)#interface vlan 2*  *SW6(config-if)#ip add 10.0.129.6 255.255.255.0*  *SW6(config-if)#exit* |

1. **保存配置并用U盘带走文件**



**HSRP实验**

**实验6-1HSRP实验**

**学习目标**

* 了解网关冗余技术。
* 配置HSRP实现对业务网关的冗余

**原理**

HSRP 是Cisco 的专有协议。HSRP（Hot Standby Router Protocol）把多台路由器组成一个“热备份组”，形成一个虚拟路由器。这个组内只有一个路由器是活动的（Active），并由它来转发数据包，如果活动路由器发生了故障，备份路由器将成为活动路由器。从网络内的主机来看，网关并没有改变。HSRP 路由器利用HELLO 包来互相监听各自的存在。当路由器长时间没有接收到HELLO包，就认为活动路由器故障，备份路由器就会成为活动路由器。HSRP 协议利用优先级决定哪个路由器成为活动路由器。如果一个路由器的优先级比其它路由器的优先级高，则该路由器成为活动路由器。路由器的缺省优先级是100。 一个组中，最多有一个活动路由器和一个备份路由器。

**拓扑图**



图1拓扑

**操作步骤**

1. 配置汇聚交换机HSRP

1、将《VLAN间路由实验》中保存的拓扑打开， 要求服务器区设备访问网络主走SW1，图书馆区设备访问网络主走SW2，交换机管理网段主走SW1。

1. 配置服务器区域VLAN101 HSRP。

1、VLAN101 standby 10.X.0.1

|  |
| --- |
| *SW1配置（主设备）：*  *SW1#conf t*  *Enter configuration commands, one per line. End with CNTL/Z.*  *SW1(config)#int vlan 101*  *SW1(config-if)#standby 101 ip 10.0.0.1 //设置虚拟IP*  *SW1(config-if)#standby 101 priority 105 //设置优先级105，使SW1为主*  *SW1(config-if)#standby 101 preempt //开启抢占功能*  *SW1(config-if)#standby 101 track fastEthernet 0/1 //追踪上行接口*  *SW2配置（备设备）*  *SW2#conf t*  *Enter configuration commands, one per line. End with CNTL/Z.*  *SW2(config)#int vlan 101*  *SW2(config-if)#standby 101 ip 10.0.0.1 //设置虚拟IP*  *SW2(config-if)#standby 101 preempt //开启抢占功能* |

2、查看HSRP状态

|  |
| --- |
| *在SW1查看HSRP状态：*  *SW1#show standby brief*  *P indicates configured to preempt.*  *|*  *Interface Grp Pri P State Active Standby Virtual IP*  *Vl1 101 105 P Active local 10.0.0.252 10.0.0.1*  *在SW2查看HSRP状态：*  *SW2#show standby brief*  *P indicates configured to preempt.*  *|*  *Interface Grp Pri P State Active Standby Virtual IP*  *Vl1 101 100 P Standby 10.0.0.251 local 10.0.0.1* |

3、在SW1上关闭F0/1接口验证HSRP切换过程

|  |
| --- |
| *SW1(config)#int f0/1*  *SW1(config-if)#shutdown*  *%HSRP-6-STATECHANGE: Vlan101 Grp 101 state Speak -> Standby*  *在SW1查看HSRP状态：*  *SW1(config-if)#do show stand b*  *P indicates configured to preempt.*  *|*  *Interface Grp Pri P State Active Standby Virtual IP*  *Vl1 101 95 P Standby 10.0.0.252 local 10.0.0.1*  *在SW2查看HSRP状态：*  SW2#show standby brief  P indicates configured to preempt.  |  *Interface Grp Pri P State Active Standby Virtual IP*  *Vl1 101 100 P Active local 10.0.0.251 10.0.0.1* |

4、在SW1上开启F0/1接口验证HSRP回切过程

|  |
| --- |
| *SW1(config)#int f0/1*  *SW1(config-if)#no shutdown*  *%* *HSRP-6-STATECHANGE: Vlan101 Grp 101 state Standby -> Active*  *在SW1查看HSRP状态：*  *SW1#show standby brief*  *P indicates configured to preempt.*  *|*  *Interface Grp Pri P State Active Standby Virtual IP*  *Vl1 101 105 P Active local 10.0.0.252 10.0.0.1*  *在SW2查看HSRP状态：*  *SW2#show standby brief*  *P indicates configured to preempt.*  *|*  *Interface Grp Pri P State Active Standby Virtual IP*  *Vl1 101 100 P Standby 10.0.0.251 local 10.0.0.1* |

1. 配置图书馆区域VLAN103 HSRP

1、VLAN103 standby 10.X.2.1

|  |
| --- |
| *SW2配置（主设备）：*  *SW2#conf t*  *Enter configuration commands, one per line. End with CNTL/Z.*  *SW2(config)#int vlan 103*  *SW2(config-if)#standby 103 ip 10.0.2.1 //设置虚拟IP*  *SW2(config-if)#standby 103 priority 105 //设置优先级105，使SW1为主*  *SW2(config-if)#standby 103 preempt //开启抢占功能*  *SW2(config-if)#standby 103 track fastEthernet 0/1 //追踪上行接口*  *SW1配置（备设备）*  *SW1#conf t*  *Enter configuration commands, one per line. End with CNTL/Z.*  *SW1(config)#int vlan 103*  *SW1(config-if)#standby 103 ip 10.0.2.1 //设置虚拟IP*  *SW1(config-if)#standby 103 preempt //开启抢占功能* |

2、查看HSRP状态

|  |
| --- |
| *在SW2查看HSRP状态：*  *SW2#show standby brief*  *P indicates configured to preempt.*  *|*  *Interface Grp Pri P State Active Standby Virtual IP*  *Vl1 103 105 P Active local 10.0.2.252 10.0.2.1*  *在SW1查看HSRP状态：*  *SW1#show standby brief*  *P indicates configured to preempt.*  *|*  *Interface Grp Pri P State Active Standby Virtual IP*  *Vl1 103 100 P Standby 10.0.2.251 local 10.0.2.1* |

1. 配置管理VLAN2 HSRP
2. VLAN2 standby 10.X.129.254

|  |
| --- |
| *SW1配置（主设备）：*  *SW1#conf t*  *Enter configuration commands, one per line. End with CNTL/Z.*  *SW1(config)#int vlan 2*  *SW1(config-if)#standby 2 ip 10.0.129.254//设置虚拟IP*  *SW1(config-if)#standby 2 priority 105 //设置优先级105，使SW1为主*  *SW1(config-if)#standby 2 preempt //开启抢占功能*  *SW1(config-if)#standby 2 track fastEthernet 0/1 //追踪上行接口*  *SW2配置（备设备）*  *SW2#conf t*  *Enter configuration commands, one per line. End with CNTL/Z.*  *SW2(config)#int vlan 2*  *SW2(config-if)#standby 2 ip 10.0.129.254//设置虚拟IP*  *SW2(config-if)#standby 2 preempt //开启抢占功能* |

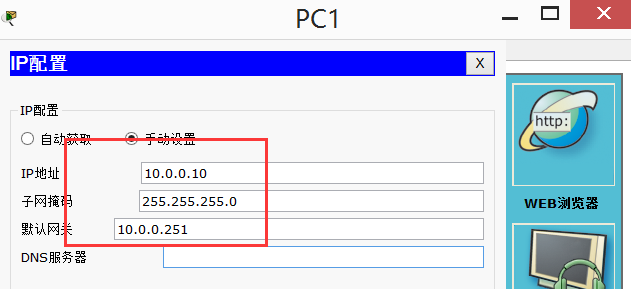
1. 2、查看HSRP状态

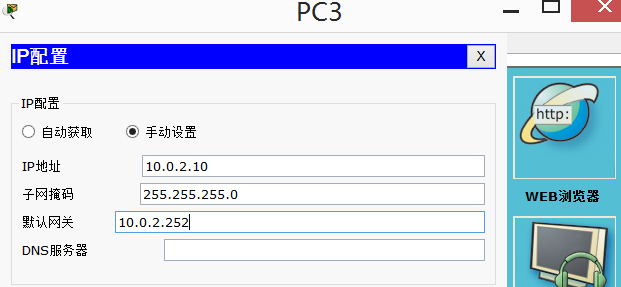
|  |
| --- |
| *在SW1查看HSRP状态：*  *SW1#show standby brief*  *P indicates configured to preempt.*  *|*  *Interface Grp Pri P State Active Standby Virtual IP*  *Vl1 2 105 P Active local 10.0.129.2 10.0.129.254*  *在SW2查看HSRP状态：*  *SW2#show standby brief*  *P indicates configured to preempt.*  *|*  *Interface Grp Pri P State Active Standby Virtual IP*  *Vl1 2 100 P Standby 10.0.129.1 local 10.0.129.254* |

1. **设置二层交换机缺省网关及PC机IP参数**
2. 设置SW3-SW6缺省网关（由于模拟器只支持HSRP配置，不支持具体功能，所以接入交换机网关配置为10.0.129.1，本应为standby IP）

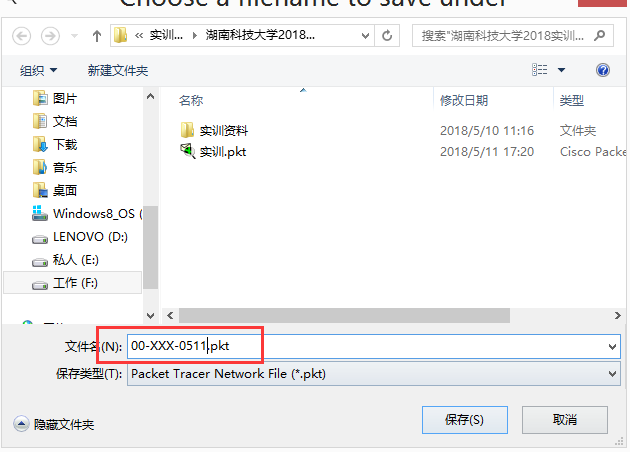
|  |
| --- |
| *SW3(config)#ip default-gateway 10.0.129.1 //配置缺省网关*  *SW4(config)#ip default-gateway 10.0.129.1*  *SW5(config)#ip default-gateway 10.0.129.1*  *SW6(config)#ip default-gateway 10.0.129.1* |

1. 设置PC1 和PC3的IP地址等参数（由于模拟器只支持HSRP配置，不支持具体功能，所以PC1网关配置为10.0.0.251，所以PC3网关配置为10.0.2.252，本应为standby IP）





1. **保存配置并用U盘带走文件**



**DHCP实验**

**实验6-1 DHCP实验**

**学习目标**

* 了解DHCP协议。
* 配置DHCP，为PC分配IP地址等参数

**原理**

IP 地址已是每台计算机必定配置的参数了，手工设置每一台计算机的IP 地址成为管理员最不愿意做的一件事，于是自动配置IP 地址的方法出现了，这就是DHCP（Dynamic HostConfiguration Protocol，动态主机配置协议）。DHCP 服务器能够从预先设置的IP 地址池里自动给主机分配IP 地址，它不仅能够保证IP 地址不重复分配，也能及时回收IP 地址以提高IP 地址的利用率。

在动态IP 地址的方案中，每台计算机并不设定固定的IP 地址，而是在计算机开机时才被分配一个IP 地址，这台计算机被称为DHCP 客户端。而负责给DHCP 客户端分配IP 地址的计算机称为DHCP 服务器。也就是说DHCP 是采用客户/服务器(Client/Server)模式，有明确的客户端和服务器角色的划分。

DHCP 的工作过程如下：

1．DHCP 客户机启动时，客户机在当前的子网中广播DHCPDISCOVER 报文向DHCP服务器申请一个IP 地址。

2．DHCP 服务器收到DHCPDISCOVER 报文后，它将从针对那台主机的地址区间中为它提供一个尚未被分配出去的IP 地址，并把提供的IP 地址暂时标记为不可用。服务器以DHCPOFFER 报文送回给主机。如果网络里包含有不止一个的DHCP 服务器，则客户机可能收到好几个DHCPOFFER 报文，客户机通常只承认第一个DHCPOFFER。

3．客户端收到DHCPOFFER 后，向服务器发送一个含有有关DHCP 服务器提供的IP地址的DHCPREQUEST 报文。如果客户端没有收到DHCPOFFER 报文并且还记得以前的网络配置，此时使用以前的网络配置（如果该配置仍然在有效期限内）。

4．DHCP 服务器向客户机发回一个含有原先被发出的IP 地址及其分配方案的一个应答报文(DHCPACK)。

5．客户端接受到包含了配置参数的DHCPACK 报文，利用ARP 检查网络上是否有相同的IP 地址。如果检查通过，则客户机接受这个IP 地址及其参数，如果发现有问题，客户机向服务器发送DHCPDECLINE 信息， 并重新开始新的配置过程。服务器收到DHCPDECLINE 信息，将该地址标为不可用。

6．DHCP 服务器只能将那个IP 地址分配给DHCP 客户一定时间，DHCP 客户必须在该次租用过期前对它进行更新。客户机在50%租借时间过去以后，每隔一段时间就开始请求DHCP 服务器更新当前租借，如果DHCP 服务器应答则租用延期。如果DHCP 服务器始终没有应答，在有效租借期的87.5%，客户应该与任何一个其他的DHCP 服务器通信，并请求更新它的配置信息。如果客户机不能和所有的DHCP 服务器取得联系，租借时间到后，它必须放弃当前的IP 地址并重新发送一个DHCPDISCOVER 报文开始上述的IP 地址获得过程。

7．客户端可以主动向服务器发出DHCPRELEASE 报文，将当前的IP 地址释放。

**拓扑图**



图1拓扑

**操作步骤**

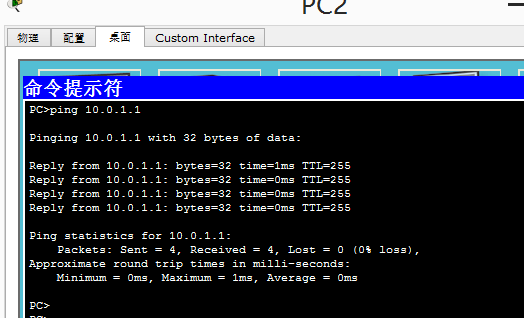
1. 在SW1上为vlan102配置DHCP 服务器
2. 将《HSRP实验》中保存的拓扑打开，PC2为DHCP客户端，需在SW1上配置DHCP服务器，为PC2分配IP地址等参数。
3. 在SW1上配置DHCP地址池，配置DHCP服务器

|  |
| --- |
| *SW1(config)#ip dhcp pool PC2 //定义地址池*  *SW1(dhcp-config)#network 10.0.1.0 255.255.255.0*  *//DHCP 服务器要分配的网络和掩码*  *SW1(dhcp-config)#default-router 10.0.1.1*  *//默认网关，这个地址要和相应网络所连接的路由器的以太口地址相同*  *SW1(dhcp-config)#dns-server 8.8.8.8 //DNS 服务器*  *SW1(dhcp-config)#exit*  *SW1(config)#exit* |

1. 在PC2上通过DHCP获取IP地址



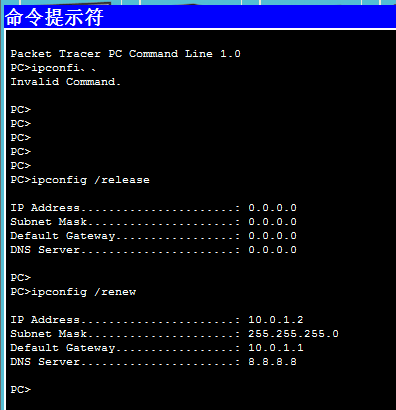
1. 在PC2上对网关进行PING测。



1. 在PC2上对DHCP 客户端进行调试，

使用命令 ipconfig/release 释放IP地址

使用命令 ipconfig/renew 重新获取IP地址

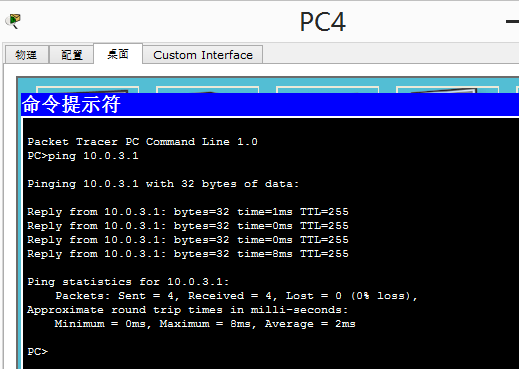


1. 在SW2上为vlan104配置DHCP 服务器
2. PC4为DHCP客户端，需在SW2上配置DHCP服务器，为PC4分配IP地址等参数。
3. 在SW2上配置DHCP地址池，配置DHCP服务器

|  |
| --- |
| *SW2(config)#ip dhcp pool PC4 //定义地址池*  *SW2(dhcp-config)#network 10.0.3.0 255.255.255.0*  *//DHCP 服务器要分配的网络和掩码*  *SW2(dhcp-config)#default-router 10.0.3.1*  *//默认网关，这个地址要和相应网络所连接的路由器的以太口地址相同*  *SW2(dhcp-config)#dns-server 8.8.8.8 //DNS 服务器*  *SW2(dhcp-config)#exit*  *SW2(config)#exit* |

1. 在PC4上通过DHCP获取IP地址



1. 在PC4上对网关进行PING测。
2. **保存配置并用U盘带走文件**

**RIP实验（选做）**

**实验7-1 RIP实验**

**学习目标**

* 了解RIP协议。
* 配置RIP，使总校区全网互联互通
* 在路由器上启动RIPv2 路由进程
* 启用参与路由协议的接口，并且通告网络

**原理**

动态路由协议包括距离向量路由协议和链路状态路由协议。RIP（Routing InformationProtocols，路由信息协议）是使用最广泛的距离向量路由协议。RIP 是为小网络环境设计的，因为这类协议的路由学习及路由更新将产生较大的流量，占用过多的带宽。

RIP 是由Xerox 在70 年代开发的，最初定义在RFC1058 中。RIP 用两种数据包传输更新：更新和请求，每个有RIP 功能的路由器默认情况下每隔30 秒利用UDP 520 端口向与它直连的网络邻居广播（RIP v1）或组播（RIP v2）路由更新。因此路由器不知道网络的全局情况，如果路由更新在网络上传播慢，将会导致网络收敛较慢，造成路由环路。为了避免路由环路，RIP 采用水平分割、毒性逆转、定义最大跳数、闪式更新、抑制计时5 个机制避免路由环路。

RIP 协议分为版本1 和版本2。不论是版本1 或版本2，都具备下面的特征：

1. 是距离向量路由协议；

2. 使用跳数（Hop Count）作为度量值；

3．默认路由更新周期为30 秒；

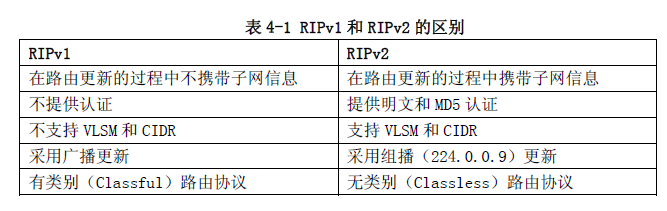
4. 管理距离（AD）为120；

5. 支持触发更新；

6. 最大跳数为15 跳；

7. 支持等价路径,默认4 条,最大6 条；

8. 使用UDP520 端口进行路由更新。



**拓扑图**



图1拓扑

**操作步骤**

将《DHCP实验》中保存的拓扑打开， 总校区中出口路由器R1，汇聚交换机SW1和SW2需要部署RIP，动态学习路由条目。

1. 在R1上配置RIP
2. 查看R1各接口IP地址

|  |
| --- |
| *R1#show ip int b*  *Interface IP-Address OK? Method Status Protocol*  *FastEthernet0/0 100.0.0.2 YES manual up up*  *FastEthernet0/1 10.0.130.1 YES manual up up*  *Serial0/2/0 10.0.130.129 YES unset up up*  *FastEthernet1/0 10.0.130.5 YES manual up up*  *FastEthernet1/1 unassigned YES unset administratively down down*  *Loopback0 10.0.128.1 YES manual up up*  *R1#* |

1. R1上配置RIP协议

|  |
| --- |
| *R1(config)#router rip //进入RIP模式*  *R1(config-router)#version 2 //设置RIP版本2*  *R1(config-router)#network 10.0.0.0 //开启各接口RIP，连Inetnet的接口不开启RIP*  *R1(config-router)#default-information originate //下发缺省路由，只在R1上配置* |

在R1上查看RIP 的datebase。

|  |
| --- |
| *R1#show ip rip database*  *R1#show ip rip database*  *0.0.0.0/0 auto-summary*  *0.0.0.0/0*  *[0] via 0.0.0.0, 01:18:07*  *10.0.0.0/24 is possibly down*  *10.0.0.0/24 is possibly down is possibly down*  *10.0.1.0/24 is possibly down*  *10.0.1.0/24 is possibly down*  *10.0.2.0/24 is possibly down*  *10.0.2.0/24 is possibly down is possibly down*  *10.0.3.0/24 is possibly down*  *10.0.3.0/24 is possibly down*  *10.0.128.1/32 auto-summary*  *10.0.128.1/32 directly connected, Loopback0*  *10.0.129.0/24 is possibly down*  *10.0.129.0/24 is possibly down is possibly down*  *10.0.130.0/30 auto-summary*  *10.0.130.0/30 directly connected, FastEthernet0/1*  *10.0.130.4/30 auto-summary*  *10.0.130.4/30 directly connected, FastEthernet1/0*  *10.0.130.8/30 is possibly down*  *10.0.130.8/30 is possibly down is possibly down*  *10.0.130.128/30 auto-summary*  *10.0.130.128/30 directly connected, Serial0/0* |

1. 在SW1和SW2上配置RIP
2. 查看SW1各接口IP地址

|  |
| --- |
| *SW1#show ip int b*  *Interface IP-Address OK? Method Status Protocol*  *Vlan2 10.0.129.1 YES manual up up*  *Vlan11 10.0.130.2 YES manual up up*  *Vlan13 10.0.130.9 YES manual up up*  *Vlan101 10.0.0.251 YES manual up up*  *Vlan102 10.0.1.1 YES manual up up*  *Vlan103 10.0.2.251 YES manual up up* |

1. SW1上配置RIP协议

|  |
| --- |
| *SW1(config)#router rip //进入RIP模式*  *SW1(config-router)#version 2 //设置RIP版本2*  *SW1(config-router)#network 10.0.0.0 //开启各接口RIP，连Inetnet的接口不开启RIP* |

1. 查看SW2各接口IP地址

|  |
| --- |
| *SW2#show ip int b*  *Interface IP-Address OK? Method Status Protocol*  *Vlan2 10.0.129.2 YES manual up up*  *Vlan11 10.0.130.6 YES manual up up*  *Vlan13 10.0.130.10 YES manual up up*  *Vlan101 10.0.0.252 YES manual up up*  *Vlan103 10.0.2.252 YES manual up up*  *Vlan104 10.0.3.1 YES manual up up* |

1. SW2上配置RIP协议

|  |
| --- |
| *SW2(config)#router rip //进入RIP模式*  *SW2(config-router)#version 2 //设置RIP版本2*  *SW2(config-router)#network 10.0.0.0 //开启各接口RIP，连Inetnet的接口不开启RIP* |

1. 在各设备上查看IP路由表
2. 在R1上查看IP路由表

|  |
| --- |
| *R1#show ip route*  *Gateway of last resort is 100.0.0.1 to network 0.0.0.0*  *10.0.0.0/8 is variably subnetted, 10 subnets, 3 masks*  *R 10.0.0.0/24 [120/1] via 10.0.130.2, 00:00:04, FastEthernet0/1*  *[120/1] via 10.0.130.6, 00:00:01, FastEthernet1/0*  *R 10.0.1.0/24 [120/1] via 10.0.130.2, 00:00:04, FastEthernet0/1*  *R 10.0.2.0/24 [120/1] via 10.0.130.2, 00:00:04, FastEthernet0/1*  *[120/1] via 10.0.130.6, 00:00:01, FastEthernet1/0*  *R 10.0.3.0/24 [120/1] via 10.0.130.6, 00:00:01, FastEthernet1/0*  *C 10.0.128.1/32 is directly connected, Loopback0*  *R 10.0.129.0/24 [120/1] via 10.0.130.2, 00:00:04, FastEthernet0/1*  *[120/1] via 10.0.130.6, 00:00:01, FastEthernet1/0*  *C 10.0.130.0/30 is directly connected, FastEthernet0/1*  *C 10.0.130.4/30 is directly connected, FastEthernet1/0*  *R 10.0.130.8/30 [120/1] via 10.0.130.2, 00:00:04, FastEthernet0/1*  *[120/1] via 10.0.130.6, 00:00:01, FastEthernet1/0*  *C 10.0.130.128/30 is directly connected, Serial0/0*  *100.0.0.0/24 is subnetted, 1 subnets*  *C 100.0.0.0 is directly connected, FastEthernet0/0*  *S\* 0.0.0.0/0 [1/0] via 100.0.0.1* |

1. 在SW1上查看IP路由表

|  |
| --- |
| *SW1#show ip route*  *Gateway of last resort is 10.0.130.1 to network 0.0.0.0*  *10.0.0.0/8 is variably subnetted, 10 subnets, 3 masks*  *C 10.0.0.0/24 is directly connected, Vlan101*  *C 10.0.1.0/24 is directly connected, Vlan102*  *C 10.0.2.0/24 is directly connected, Vlan103*  *R 10.0.3.0/24 [120/1] via 10.0.129.2, 00:00:15, Vlan2*  *[120/1] via 10.0.130.10, 00:00:15, Vlan13*  *[120/1] via 10.0.0.252, 00:00:15, Vlan101*  *[120/1] via 10.0.2.252, 00:00:15, Vlan103*  *R 10.0.128.1/32 [120/1] via 10.0.130.1, 00:00:20, Vlan11*  *C 10.0.129.0/24 is directly connected, Vlan2*  *C 10.0.130.0/30 is directly connected, Vlan11*  *R 10.0.130.4/30 [120/1] via 10.0.130.1, 00:00:20, Vlan11*  *[120/1] via 10.0.129.2, 00:00:15, Vlan2*  *[120/1] via 10.0.130.10, 00:00:15, Vlan13*  *[120/1] via 10.0.0.252, 00:00:15, Vlan101*  *C 10.0.130.8/30 is directly connected, Vlan13*  *R 10.0.130.128/30 [120/1] via 10.0.130.1, 00:00:20, Vlan11*  *R\* 0.0.0.0/0 [120/1] via 10.0.130.1, 00:00:20, Vlan11* |

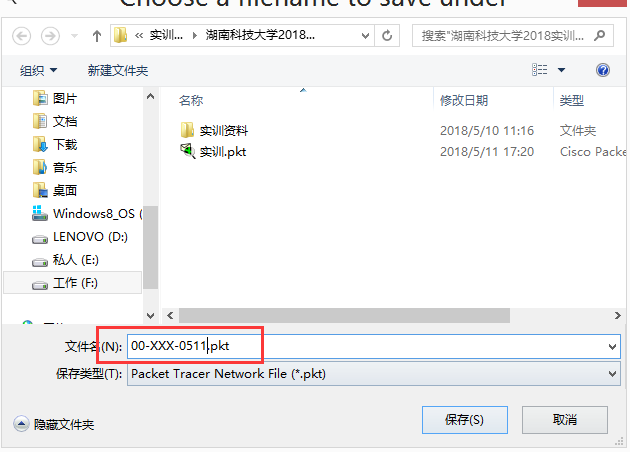
1. 在SW2上查看IP路由表

|  |
| --- |
| *SW2#show ip route*  *Gateway of last resort is 10.0.130.5 to network 0.0.0.0*  *10.0.0.0/8 is variably subnetted, 10 subnets, 3 masks*  *C 10.0.0.0/24 is directly connected, Vlan101*  *R 10.0.1.0/24 [120/1] via 10.0.129.1, 00:00:06, Vlan2*  *[120/1] via 10.0.130.9, 00:00:06, Vlan13*  *[120/1] via 10.0.0.251, 00:00:06, Vlan101*  *[120/1] via 10.0.2.251, 00:00:06, Vlan103*  *C 10.0.2.0/24 is directly connected, Vlan103*  *C 10.0.3.0/24 is directly connected, Vlan104*  *R 10.0.128.1/32 [120/1] via 10.0.130.5, 00:00:03, Vlan12*  *C 10.0.129.0/24 is directly connected, Vlan2*  *R 10.0.130.0/30 [120/1] via 10.0.129.1, 00:00:06, Vlan2*  *[120/1] via 10.0.130.9, 00:00:06, Vlan13*  *[120/1] via 10.0.0.251, 00:00:06, Vlan101*  *[120/1] via 10.0.2.251, 00:00:06, Vlan103*  *C 10.0.130.4/30 is directly connected, Vlan12*  *C 10.0.130.8/30 is directly connected, Vlan13*  *R 10.0.130.128/30 [120/1] via 10.0.130.5, 00:00:03, Vlan12*  *R\* 0.0.0.0/0 [120/1] via 10.0.130.5, 00:00:03, Vlan12* |

1. **路由业务测试**
2. 在PC2上对全网地址进行ping测。

|  |
| --- |
|  |

1. **保存配置并用U盘带走文件**



**OSPF实验**

**实验7-2 OSPF实验**

**学习目标**

* 了解OSPF协议。
* 配置OSPF，使总校区全网互联互通
* 在路由器上启动OSPF 路由进程
* 启用参与路由协议的接口，并且通告网络

**原理**

OSPF（Open Shortest Path First,开放最短链路优先）路由协议是典型的链路状态路由协议。本实验只讨论单区域的OSPF。OSPF 作为一种内部网关协议（Interior Gateway Protocol，IGP），用于在同一个自治系统（AS）中的路由器之间交换路由信息。OSPF 的特性如下:

1. 可适应大规模网络；

2. 收敛速度快；

3. 无路由环路；

4. 支持VLSM 和CIDR；

5. 支持等价路由；

6. 支持区域划分, 构成结构化的网络；

7. 提供路由分级管理；

8. 支持简单口令和MD5 认证；

9. 以组播方式传送协议报文；

10. OSPF 路由协议的管理距离是110；

11. OSPF 路由协议采用cost 作为度量标准；

12. OSPF 维护邻居表、拓扑表和路由表。

另外，OSPF 将网络划分为四种类型：广播多路访问型（BMA）、非广播多路访问型（NBMA）、点到点型（Point-to-Point）、点到多点型（Point-to-MultiPoint）。不同的二层链路的类型需要OSPF 不同的网络类型来适应。

下面的几个术语是学习OSPF 要掌握的：

1. 链路：链路就是路由器用来连接网络的接口；

2. 链路状态：用来描述路由器接口及其与邻居路由器的关系。所有链路状态信息构成

链路状态数据库；

3. 区域：有相同的区域标志的一组路由器和网络的集合。在同一个区域内的路由器有

相同的链路状态数据库；

4. 自治系统：采用同一种路由协议交换路由信息的路由器及其网络构成一个自治系统；

5. 链路状态通告（LSA）：LSA 用来描述路由器的本地状态，LSA 包括的信息有关于路由

器接口的状态和所形成的邻接状态；

6. 最短路经优先（SPF）算法：是OSPF 路由协议的基础。SPF 算法有时也被称为Dijkstra

算法，这是因为最短路径优先算法(SPF)是Dijkstra 发明的。OSPF 路由器利用 SPF，独立

地计算出到达任意目的地的最佳路由。

**拓扑图**



图1拓扑

**操作步骤**

将《DHCP实验》中保存的拓扑打开， 总校区中出口路由器R1，汇聚交换机SW1和SW2需要部署OSPF，动态学习路由条目。

1. 在R1上配置OSPF
2. 查看R1各接口IP地址

|  |
| --- |
| *R1#show ip int b*  *Interface IP-Address OK? Method Status Protocol*  *FastEthernet0/0 100.0.0.2 YES manual up up*  *FastEthernet0/1 10.0.130.1 YES manual up up*  *Serial0/2/0 10.0.130.129 YES unset up up*  *FastEthernet1/0 10.0.130.5 YES manual up up*  *FastEthernet1/1 unassigned YES unset administratively down down*  *Loopback0 10.0.128.1 YES manual up up*  *R1#* |

1. R1上配置OSPF协议

|  |
| --- |
| *R1(config)#router ospf 1 //进入OSPF进程视图*  *R1(config-router)#router-id 10.0.128.1 //设置router-id为loopback0地址*  *R1(config-router)#network 10.0.130.1 0.0.0.0 area 0*  *//开启接口OSPF功能并归属区域0*  *R1(config-router)#network 10.0.130.5 0.0.0.0 area 0*  *R1(config-router)#network 10.0.128.1 0.0.0.0 area 0*  *R1(config-router)#default-information originate //下发缺省路由* |

1. 在SW1和SW2上配置OSPF
2. 查看SW1各接口IP地址

|  |
| --- |
| *SW1#show ip int b*  *Interface IP-Address OK? Method Status Protocol*  *Vlan2 10.0.129.1 YES manual up up*  *Vlan11 10.0.130.2 YES manual up up*  *Vlan13 10.0.130.9 YES manual up up*  *Vlan101 10.0.0.251 YES manual up up*  *Vlan102 10.0.1.1 YES manual up up*  *Vlan103 10.0.2.251 YES manual up up* |

1. SW1上配置OSPF协议

|  |
| --- |
| *SW1(config)#router ospf 1 //进入OSPF进程视图*  *SW1(config-router)#router-id 10.0.129.1 //设置router-id为loopback0地址*  *SW1(config-router)#network 10.0.130.2 0.0.0.0 area 0*  *//开启接口OSPF功能并归属区域0*  *SW1(config-router)#network 10.0.130.9 0.0.0.0 area 0*  *SW1(config-router)# network 10.0.129.1 0.0.0.0 area 0*  *SW1(config-router)# network 10.0.0.251 0.0.0.0 area 0*  *SW1(config-router)# network 10.0.1.1 0.0.0.0 area 0*  *SW1(config-router)# network 10.0.2.251 0.0.0.0 area 0*  *SW1(config-router)#passive-interface vlan 2 //设置非互联vlan为passive接口*  *SW1(config-router)#passive-interface vlan 101*  *SW1(config-router)#passive-interface vlan 102*  *SW1(config-router)#passive-interface vlan 103* |

1. 查看SW2各接口IP地址

|  |
| --- |
| *SW2#show ip int b*  *Interface IP-Address OK? Method Status Protocol*  *Vlan2 10.0.129.2 YES manual up up*  *Vlan11 10.0.130.6 YES manual up up*  *Vlan13 10.0.130.10 YES manual up up*  *Vlan101 10.0.0.252 YES manual up up*  *Vlan103 10.0.2.252 YES manual up up*  *Vlan104 10.0.3.1 YES manual up up* |

1. SW2上配置OSPF协议

|  |
| --- |
| *SW2(config)#router ospf 1 //进入OSPF进程视图*  *SW2(config-router)#router-id 10.0.129.2 //设置router-id为loopback0地址*  *SW2(config-router)#network 10.0.130.6 0.0.0.0 area 0*  *//开启接口OSPF功能并归属区域0*  *SW2(config-router)#network 10.0.130.10 0.0.0.0 area 0*  *SW2(config-router)#network 10.0.129.2 0.0.0.0 area 0*  *SW2(config-router)#network 10.0.0.252 0.0.0.0 area 0*  *SW2(config-router)#network 10.0.2.252 0.0.0.0 area 0*  *SW2(config-router)#network 10.0.3.1 0.0.0.0 area 0*  *SW1(config-router)#passive-interface vlan 2 //设置非互联vlan为passive接口*  *SW1(config-router)#passive-interface vlan 101*  *SW1(config-router)#passive-interface vlan 103*  *SW1(config-router)#passive-interface vlan 104* |

1. 在各设备上查看OSPF邻居关系
2. 在R1上查看OSPF 邻居关系

|  |
| --- |
| *R1#show ip ospf neighbor*  *Neighbor ID Pri State Dead Time Address Interface*  *10.0.129.1 1 FULL/BDR 00:00:37 10.0.130.2 FastEthernet0/1*  *10.0.129.2 1 FULL/BDR 00:00:36 10.0.130.6 FastEthernet1/0* |

R1和SW1及SW2形成邻接关系。

1. 在SW1上查看OSPF 邻居关系

|  |
| --- |
| *SW1#show ip ospf neighbor*  *Neighbor ID Pri State Dead Time Address Interface*  *10.0.128.1 1 FULL/DR 00:00:36 10.0.130.1 Vlan11*  *10.0.129.2 1 FULL/BDR 00:00:31 10.0.130.10 Vlan13* |

SW1和R1及SW2形成邻接关系。

1. 在SW2上查看OSPF 邻居关系

|  |
| --- |
| *SW2#show ip ospf neighbor*  *Neighbor ID Pri State Dead Time Address Interface*  *10.0.128.1 1 FULL/DR 00:00:36 10.0.130.5 Vlan12*  *10.0.129.1 1 FULL/BDR 00:00:31 10.0.130.9 Vlan13* |

SW2和R1及SW1形成邻接关系。

1. 在各设备上查看IP路由表
2. 在R1上查看IP路由表

|  |
| --- |
| *R1#show ip route*  *Gateway of last resort is 100.0.0.1 to network 0.0.0.0*  *10.0.0.0/8 is variably subnetted, 9 subnets, 3 masks*  *O 10.0.0.0/24 [110/2] via 10.0.130.2, 00:00:32, FastEthernet0/1*  *O 10.0.1.0/24 [110/2] via 10.0.130.2, 00:00:32, FastEthernet0/1*  *O 10.0.2.0/24 [110/2] via 10.0.130.2, 00:00:32, FastEthernet0/1*  *C 10.0.128.1/32 is directly connected, Loopback0*  *O 10.0.129.0/24 [110/2] via 10.0.130.2, 00:00:42, FastEthernet0/1*  *O 10.0.130.8/30 [110/2] via 10.0.130.2, 00:05:11, FastEthernet0/1*  *[110/2] via 10.0.130.6, 00:05:11, FastEthernet1/0*  *C 10.0.130.128/30 is directly connected, Serial0/0*  *100.0.0.0/24 is subnetted, 1 subnets*  *C 100.0.0.0 is directly connected, FastEthernet0/0*  *S\* 0.0.0.0/0 [1/0] via 100.0.0.1* |

1. 在SW1上查看IP路由表

|  |
| --- |
| *SW1#show ip route*  *Gateway of last resort is 10.0.130.1 to network 0.0.0.0*  *10.0.0.0/8 is variably subnetted, 10 subnets, 3 masks*  *C 10.0.0.0/24 is directly connected, Vlan101*  *C 10.0.1.0/24 is directly connected, Vlan102*  *C 10.0.2.0/24 is directly connected, Vlan103*  *O 10.0.3.0/24 [110/2] via 10.0.130.10, 00:00:28, Vlan13*  *[110/2] via 10.0.129.2, 00:00:28, Vlan2*  *[110/2] via 10.0.0.252, 00:00:28, Vlan101*  *[110/2] via 10.0.2.252, 00:00:28, Vlan103*  *O 10.0.128.1/32 [110/2] via 10.0.130.1, 00:10:01, Vlan11*  *C 10.0.129.0/24 is directly connected, Vlan2*  *C 10.0.130.0/30 is directly connected, Vlan11*  *O 10.0.130.4/30 [110/2] via 10.0.130.1, 00:00:28, Vlan11*  *[110/2] via 10.0.130.10, 00:00:28, Vlan13*  *[110/2] via 10.0.129.2, 00:00:28, Vlan2*  *[110/2] via 10.0.0.252, 00:00:28, Vlan101*  *[110/2] via 10.0.2.252, 00:00:28, Vlan103*  *C 10.0.130.8/30 is directly connected, Vlan13*  *O 10.0.130.128/30 [110/65] via 10.0.130.1, 00:10:01, Vlan11*  *O\*E2 0.0.0.0/0 [110/1] via 10.0.130.1, 00:10:01, Vlan11* |

1. 在SW2上查看IP路由表

|  |
| --- |
| *SW2#show ip route*  *Gateway of last resort is 10.0.130.5 to network 0.0.0.0*  *10.0.0.0/8 is variably subnetted, 10 subnets, 3 masks*  *C 10.0.0.0/24 is directly connected, Vlan101*  *O 10.0.1.0/24 [110/2] via 10.0.130.9, 00:01:15, Vlan13*  *[110/2] via 10.0.129.1, 00:01:15, Vlan2*  *[110/2] via 10.0.0.251, 00:01:15, Vlan101*  *[110/2] via 10.0.2.251, 00:01:15, Vlan103*  *C 10.0.2.0/24 is directly connected, Vlan103*  *C 10.0.3.0/24 is directly connected, Vlan104*  *O 10.0.128.1/32 [110/2] via 10.0.130.5, 00:06:29, Vlan12*  *C 10.0.129.0/24 is directly connected, Vlan2*  *O 10.0.130.0/30 [110/2] via 10.0.130.5, 00:01:15, Vlan12*  *[110/2] via 10.0.130.9, 00:01:15, Vlan13*  *[110/2] via 10.0.129.1, 00:01:15, Vlan2*  *[110/2] via 10.0.0.251, 00:01:15, Vlan101*  *[110/2] via 10.0.2.251, 00:01:15, Vlan103*  *C 10.0.130.4/30 is directly connected, Vlan12*  *C 10.0.130.8/30 is directly connected, Vlan13*  *O 10.0.130.128/30 [110/65] via 10.0.130.5, 00:06:29, Vlan12*  *O\*E2 0.0.0.0/0 [110/1] via 10.0.130.5, 00:06:29, Vlan12* |

1. **路由业务测试**
2. 在PC2上对全网地址进行ping测。

|  |
| --- |
|  |

1. **保存配置并用U盘带走文件**

**PPP实验**

**实验8-1 PPP实验**

**学习目标**

* 了解PPP协议原理。
* 了解CHAP认证过程
* 配置PPP及CHAP认证

**原理**

1. PPP 是串行线路上（同步电路或者异步电路）的一种帧封装格式，但是PPP 可以提供对多种网络层协议的支持。PPP 支持认证、多链路捆绑等功能。

PPP 经过4 个过程在一个点到点的链路上建立通信连接：

• 链路的建立和配置协调：通信的发起方发送LCP 帧来配置和检测数据链路

• 认证：对链路建立时对端身份进行验证，这一阶段是可选的。

• 网络层协议配置协调：通信的发起方发送NCP 帧以选择并配置网络层协议

• 关闭链路：通信链路将一直保持到LCP 或NCP 帧关闭链路或发生一些外部事件

2. PPP 认证：PAP 和CHAP

（1）PAP——密码验证协议

PAP（Password Authentication Protocol）利用2 次握手的简单方法进行认证。在PPP 链路建立完毕后，源节点不停地在链路上反复发送用户名和密码，直到验证通过。PAP的验证中，密码在链路上是以明文传输的，而且由于是源节点控制验证重试频率和次数，因此PAP 不能防范再生攻击和重复的尝试攻击。

（2）CHAP——询问握手验证协议

CHAP(Challenge Handshake Authentication Protocol)利用3 次握手周期地验证源端节点的身份。CHAP 验证过程在链路建立之后进行，而且在以后的任何时候都可以再次进行。这使得链路更为安全；CHAP 不允许连接发起方在没有收到询问消息的情况下进行验证尝试。CHAP 每次使用不同的询问消息，每个消息都是不可预测的唯一的值，CHAP 不直接传送密码，只传送一个不可预测的询问消息，以及该询问消息与密码经过MD5 加密运算后的加密值。所以CHAP 可以防止再生攻击，CHAP 的安全性比PAP 要高。

**拓扑图**



图1拓扑

**操作步骤**

将《OSPF实验》中保存的拓扑打开， 总校区中出口路由器R1和分校区B的路由器R3之间通过串行链路连接，运行PPP协议，为了提高安全性要求进行chap认证。

1. 在R1上配置PPP
2. 在R1上配置PPP协议

|  |
| --- |
| *R1>enable*  *R1#conf t*  *R1(config)#int s0/2/0*  *R1(config-if)#encapsulation ppp //设置封装协议为PPP*  *R1(config-if)#ip add 10.0.130.129 255.255.255.252 //配置接口IP* |

1. R3上配置PPP协议

|  |
| --- |
| *R3>enable*  *R3#conf t*  *R3(config)#int s0/2/0*  *R3(config-if)#encapsulation ppp //设置封装协议为PPP*  *R3(config-if)#ip add 10.0.130.130 255.255.255.252 //配置接口IP* |

1. 在R3上对PPP链路对端地址进行ping测

|  |
| --- |
| *R3(config-if)#do ping 10.0.130.129*  *Type escape sequence to abort.*  *Sending 5, 100-byte ICMP Echos to 10.0.130.129, timeout is 2 seconds:*  *!!!!!*  *Success rate is 100 percent (5/5), round-trip min/avg/max = 1/3/5 ms* |

1. 配置CHAP认证
2. 配置R1为认证方

|  |
| --- |
| *R1(config)#interface s0/2/0*  *R1(config-if)#ppp authentication chap //配置chap认证认证方*  *R1(config-if)#exit*  *R1(config)#username R3 password 0 cisco //设置chap认证用户名密码* |

1. 配置R3为被认证方

|  |
| --- |
| *R3(config)#username R1 password 0 cisco //设置chap认证用户名密码* |

1. 关闭R1的S0/2/0接口，然后在打开，使PPP链路重新协商

|  |
| --- |
| *R1(config)#int s0/2/0*  *R1(config-if)#shutdown //关闭端口*  *%LINK-5-CHANGED: Interface Serial0/2/0, changed state to administratively down*  *%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/2/0, changed state to down*  *R1(config-if)#no shutdown //打开端口*  *%LINK-5-CHANGED: Interface Serial0/2/0, changed state to up*  *%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/2/0, changed state to up //ppp链路重新协商建立* |

1. 查看R1和R3路由表，寻找R1和R3上由PPP协议建立的主机路由

|  |
| --- |
| *R1#show ip route*  *10.0.0.0/8 is variably subnetted, 11 subnets, 3 masks*  *O 10.0.0.0/24 [110/2] via 10.0.130.6, 00:30:06, FastEthernet1/0*  *[110/2] via 10.0.130.2, 00:30:06, FastEthernet0/1*  *O 10.0.1.0/24 [110/2] via 10.0.130.2, 00:30:06, FastEthernet0/1*  *O 10.0.2.0/24 [110/2] via 10.0.130.6, 00:30:06, FastEthernet1/0*  *[110/2] via 10.0.130.2, 00:30:06, FastEthernet0/1*  *O 10.0.3.0/24 [110/2] via 10.0.130.6, 00:30:06, FastEthernet1/0*  *C 10.0.128.1/32 is directly connected, Loopback0*  *O 10.0.129.0/24 [110/2] via 10.0.130.6, 00:30:06, FastEthernet1/0*  *[110/2] via 10.0.130.2, 00:30:06, FastEthernet0/1*  *C 10.0.130.0/30 is directly connected, FastEthernet0/1*  *C 10.0.130.4/30 is directly connected, FastEthernet1/0*  *O 10.0.130.8/30 [110/2] via 10.0.130.6, 00:30:06, FastEthernet1/0*  *[110/2] via 10.0.130.2, 00:30:06, FastEthernet0/1*  *C 10.0.130.128/30 is directly connected, Serial0/2/0*  *C 10.0.130.130/32 is directly connected, Serial0/2/0 //32位主机直连路由*  *100.0.0.0/24 is subnetted, 1 subnets*  *C 100.0.0.0 is directly connected, FastEthernet0/0*  *S\* 0.0.0.0/0 [1/0] via 100.0.0.1*  *R3#show ip route*  *C 10.0.130.128/30 is directly connected, Serial0/2/0*  *C 10.0.130.129/32 is directly connected, Serial0/2/0 //32位主机直连路由* |

1. 在R1和R3之间部署OSPF，实现总部和分校区B互联互通
2. 在R1上配置OSPF

|  |
| --- |
| *R1(config)#router ospf 1*  *R1(config-router)#network 10.0.130.129 0.0.0.0 area 0 //使能S0/2/0接口ospf*  *R1(config-router)#exit* |

1. 在R3上配置OSPF

|  |
| --- |
| *R3(config)#router ospf 1*  *R3(config-router)#router-id 10.0.128.3*  *R3(config-router)#network 10.0.128.3 0.0.0.0 area 0 //使能接口ospf*  *R3(config-router)#network 10.0.130.130 0.0.0.0 area 0 //使能接口ospf*  *R3(config-router)#network 10.0.5.1 0.0.0.0 area 0 //使能接口ospf* |

1. 在R3上查看OSPF 邻居关系

|  |
| --- |
| *R3#show ip ospf neighbor*  *Neighbor ID Pri State Dead Time Address Interface*  *10.0.128.1 0 FULL/ - 00:00:31 10.0.130.129 Serial0/2/0* |

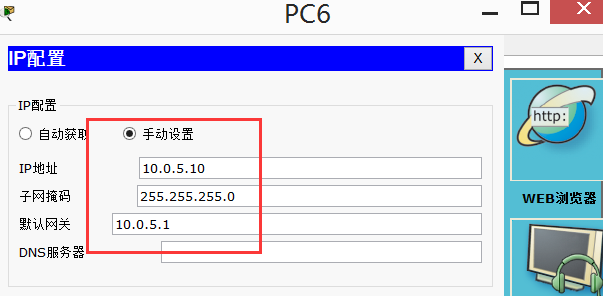
1. 在各设备上查看IP路由表
2. 在R1上查看IP路由表，关注分校区B路由

|  |
| --- |
| *R1#show ip route*  *Gateway of last resort is 100.0.0.1 to network 0.0.0.0*  *Gateway of last resort is 100.0.0.1 to network 0.0.0.0*  *10.0.0.0/8 is variably subnetted, 13 subnets, 3 masks*  *O 10.0.0.0/24 [110/2] via 10.0.130.6, 00:43:12, FastEthernet1/0*  *[110/2] via 10.0.130.2, 00:43:12, FastEthernet0/1*  *O 10.0.1.0/24 [110/2] via 10.0.130.2, 00:43:12, FastEthernet0/1*  *O 10.0.2.0/24 [110/2] via 10.0.130.6, 00:43:12, FastEthernet1/0*  *[110/2] via 10.0.130.2, 00:43:12, FastEthernet0/1*  *O 10.0.3.0/24 [110/2] via 10.0.130.6, 00:43:12, FastEthernet1/0*  *O 10.0.5.0/24 [110/65] via 10.0.130.130, 00:00:00, Serial0/2/0*  *C 10.0.128.1/32 is directly connected, Loopback0*  *O 10.0.128.3/32 [110/65] via 10.0.130.130, 00:00:11, Serial0/2/0*  *O 10.0.129.0/24 [110/2] via 10.0.130.6, 00:43:12, FastEthernet1/0*  *[110/2] via 10.0.130.2, 00:43:12, FastEthernet0/1*  *C 10.0.130.0/30 is directly connected, FastEthernet0/1*  *C 10.0.130.4/30 is directly connected, FastEthernet1/0*  *O 10.0.130.8/30 [110/2] via 10.0.130.6, 00:43:12, FastEthernet1/0*  *[110/2] via 10.0.130.2, 00:43:12, FastEthernet0/1*  *C 10.0.130.128/30 is directly connected, Serial0/2/0*  *C 10.0.130.130/32 is directly connected, Serial0/2/0*  *100.0.0.0/24 is subnetted, 1 subnets*  *C 100.0.0.0 is directly connected, FastEthernet0/0*  *S\* 0.0.0.0/0 [1/0] via 100.0.0.1* |

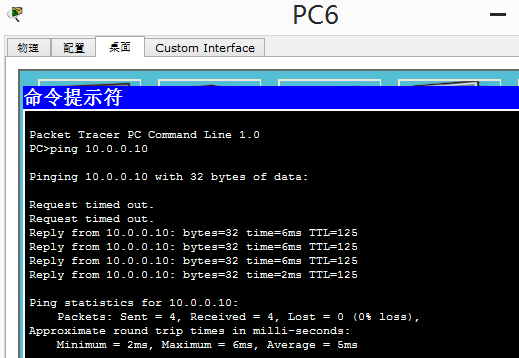
1. 在R3上查看IP路由表，R3可学习到总校区路由及缺省路由

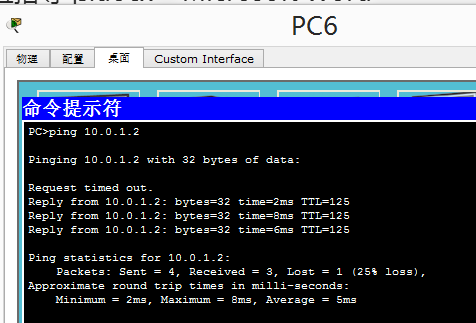
|  |
| --- |
| *R3#show ip route*  *Gateway of last resort is 10.0.130.129 to network 0.0.0.0*  *10.0.0.0/8 is variably subnetted, 13 subnets, 3 masks*  *O 10.0.0.0/24 [110/66] via 10.0.130.129, 00:06:07, Serial0/2/0*  *O 10.0.1.0/24 [110/66] via 10.0.130.129, 00:06:07, Serial0/2/0*  *O 10.0.2.0/24 [110/66] via 10.0.130.129, 00:06:07, Serial0/2/0*  *O 10.0.3.0/24 [110/66] via 10.0.130.129, 00:06:07, Serial0/2/0*  *C 10.0.5.0/24 is directly connected, FastEthernet0/0*  *O 10.0.128.1/32 [110/65] via 10.0.130.129, 00:06:07, Serial0/2/0*  *C 10.0.128.3/32 is directly connected, Loopback0*  *O 10.0.129.0/24 [110/66] via 10.0.130.129, 00:06:07, Serial0/2/0*  *O 10.0.130.0/30 [110/65] via 10.0.130.129, 00:06:07, Serial0/2/0*  *O 10.0.130.4/30 [110/65] via 10.0.130.129, 00:06:07, Serial0/2/0*  *O 10.0.130.8/30 [110/66] via 10.0.130.129, 00:06:07, Serial0/2/0*  *C 10.0.130.128/30 is directly connected, Serial0/2/0*  *C 10.0.130.129/32 is directly connected, Serial0/2/0*  *O\*E2 0.0.0.0/0 [110/1] via 10.0.130.129, 00:06:07, Serial0/2/0* |

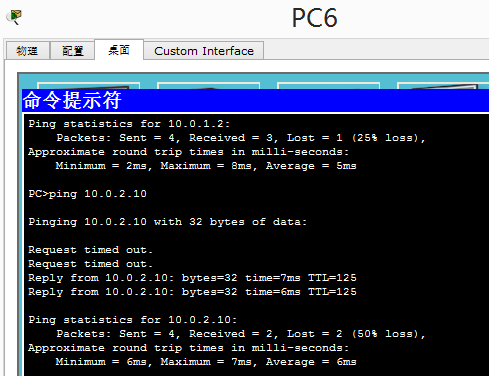
1. **路由业务测试**
2. 设置PC6 IP地址等参数。

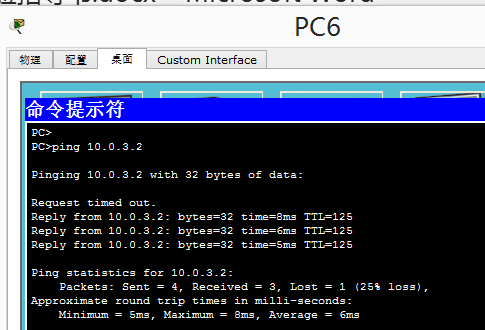


1. 在PC6上对其他主机进行ping测。









1. **保存配置并用U盘带走文件**

**GRE实验**

**实验8-2 GRE实验**

**学习目标**

* 了解GRE协议原理。
* 配置GRE实现私有网络跨越公网通信

**原理**

GRE(Generic Routing Encapsulation)即通用路由封装协议，是对某些网络层协议(如IP和IPX)的数据报进行封装，使这些被封装的数据报能够在另一个网络层协议(如IP)中传输。

GRE是VPN(Virtual Private Network)的第三层隧道协议，即在协议层之间采用了一种被称之为Tunnel(隧道)的技术。



**拓扑图**



图1拓扑

**操作步骤**

将《PPP实验》中保存的拓扑打开， 总校区中出口路由器R1和分校区A的路由器R2都已经接入了Internet ，可在两台出口路由器上部署GRE VPN实现总校区和分校区A之间的互联互通。

1. 配置GRE
2. R1上配置GRE协议

|  |
| --- |
| *R1>enable*  *R1#conf t*  *R1(config)#interface tunnel 0 //创建隧道接口*  *R1(config-if)#ip add 10.0.130.133 255.255.255.252 //配置隧道IP地址*  *R1(config-if)#tunnel mode gre ip //设置隧道为GRE*  *R1(config-if)#tunnel source fastEthernet 0/0 //设置隧道源IP*  *R1(config-if)#tunnel destination 200.0.0.2 //设置隧道目的IP* |

1. R2上配置GRE协议

|  |
| --- |
| *R2>enable*  *R2#conf t*  *R2(config)#interface tunnel 0 //创建隧道接口*  *R2(config-if)#ip add 10.0.130.134 255.255.255.252 //配置隧道IP地址*  *R2(config-if)#tunnel mode gre ip //设置隧道为GRE*  *R2(config-if)#tunnel source fastEthernet 0/0 //设置隧道源IP*  *R2(config-if)#tunnel destination 100.0.0.2 //设置隧道目的IP* |

1. 在R2上对tunnel对端地址进行ping测

|  |
| --- |
| *R2(config-if)#do ping 10.0.130.133*  *Type escape sequence to abort.*  *Sending 5, 100-byte ICMP Echos to 10.0.130.133, timeout is 2 seconds:*  *!!!!!*  *Success rate is 100 percent (5/5), round-trip min/avg/max = 1/3/5 ms* |

1. 在R1和R2之间部署OSPF，实现总部和分校区A互联互通
2. 在R1上配置OSPF

|  |
| --- |
| *R1(config)#router ospf 1*  *R1(config)#* *no default-information originate*  *//模拟软件中GRE与OSPF下发缺省路由冲突，故此处删除缺省路由*  *R1(config-router)#network 10.0.130.133 0.0.0.0 area 0 //使能接口ospf*  *R1(config-router)#exit* |

1. 在R2上配置OSPF

|  |
| --- |
| *R2(config)#router ospf 1*  *R2(config-router)#router-id 10.0.128.2*  *R2(config-router)#network 10.0.128.2 0.0.0.0 area 0 //使能接口ospf*  *R2(config-router)#network 10.0.130.134 0.0.0.0 area 0 //使能接口ospf*  *R2(config-router)#network 10.0.4.1 0.0.0.0 area 0 //使能接口ospf* |

1. 在R2上查看OSPF 邻居关系

|  |
| --- |
| *R2#show ip ospf neighbor*  *Neighbor ID Pri State Dead Time Address Interface*  *10.0.128.1 0 FULL/ - 00:00:31 10.0.130.133 Tunnel0* |

1. 在各设备上查看IP路由表
2. 在R1上查看IP路由表，关注分校区A路由

|  |
| --- |
| *R1#show ip route*  *Gateway of last resort is 100.0.0.1 to network 0.0.0.0*  *Gateway of last resort is 100.0.0.1 to network 0.0.0.0*  *10.0.0.0/8 is variably subnetted, 16 subnets, 3 masks*  *O 10.0.0.0/24 [110/2] via 10.0.130.2, 00:13:02, FastEthernet0/1*  *[110/2] via 10.0.130.6, 00:13:02, FastEthernet1/0*  *O 10.0.1.0/24 [110/2] via 10.0.130.2, 00:13:02, FastEthernet0/1*  *O 10.0.2.0/24 [110/2] via 10.0.130.2, 00:13:02, FastEthernet0/1*  *[110/2] via 10.0.130.6, 00:13:02, FastEthernet1/0*  *O 10.0.3.0/24 [110/2] via 10.0.130.6, 00:13:02, FastEthernet1/0*  *O 10.0.4.0/24 [110/1001] via 10.0.130.134, 00:00:02, Tunnel0*  *O 10.0.5.0/24 [110/65] via 10.0.130.130, 00:13:02, Serial0/2/0*  *C 10.0.128.1/32 is directly connected, Loopback0*  *O 10.0.128.2/32 [110/1001] via 10.0.130.134, 00:00:02, Tunnel0*  *O 10.0.128.3/32 [110/65] via 10.0.130.130, 00:13:02, Serial0/2/0*  *O 10.0.129.0/24 [110/2] via 10.0.130.2, 00:13:02, FastEthernet0/1*  *[110/2] via 10.0.130.6, 00:13:02, FastEthernet1/0*  *C 10.0.130.0/30 is directly connected, FastEthernet0/1*  *C 10.0.130.4/30 is directly connected, FastEthernet1/0*  *O 10.0.130.8/30 [110/2] via 10.0.130.2, 00:13:02, FastEthernet0/1*  *[110/2] via 10.0.130.6, 00:13:02, FastEthernet1/0*  *C 10.0.130.128/30 is directly connected, Serial0/2/0*  *C 10.0.130.130/32 is directly connected, Serial0/2/0*  *C 10.0.130.132/30 is directly connected, Tunnel0*  *100.0.0.0/24 is subnetted, 1 subnets*  *C 100.0.0.0 is directly connected, FastEthernet0/0*  *S\* 0.0.0.0/0 [1/0] via 100.0.0.1* |

1. 在R2上查看IP路由表，R2可学习到总校区及分校区B路由

|  |
| --- |
| *R2#show ip route*  *Gateway of last resort is 10.0.130.129 to network 0.0.0.0*    *10.0.0.0/8 is variably subnetted, 16 subnets, 4 masks*  *S 10.0.0.0/8 [1/0] via 10.0.130.133*  *O 10.0.0.0/24 [110/1002] via 10.0.130.133, 00:00:24, Tunnel0*  *O 10.0.1.0/24 [110/1002] via 10.0.130.133, 00:00:24, Tunnel0*  *O 10.0.2.0/24 [110/1002] via 10.0.130.133, 00:00:24, Tunnel0*  *O 10.0.3.0/24 [110/1002] via 10.0.130.133, 00:00:24, Tunnel0*  *C 10.0.4.0/24 is directly connected, FastEthernet0/1*  *O 10.0.5.0/24 [110/1065] via 10.0.130.133, 00:00:24, Tunnel0*  *C 10.0.128.0/24 is directly connected, Loopback0*  *O 10.0.128.1/32 [110/1001] via 10.0.130.133, 00:00:24, Tunnel0*  *O 10.0.128.3/32 [110/1065] via 10.0.130.133, 00:00:24, Tunnel0*  *O 10.0.129.0/24 [110/1002] via 10.0.130.133, 00:00:24, Tunnel0*  *O 10.0.130.0/30 [110/1001] via 10.0.130.133, 00:00:24, Tunnel0*  *O 10.0.130.4/30 [110/1001] via 10.0.130.133, 00:00:24, Tunnel0*  *O 10.0.130.8/30 [110/1002] via 10.0.130.133, 00:00:24, Tunnel0*  *O 10.0.130.128/30 [110/1064] via 10.0.130.133, 00:00:24, Tunnel0*  *C 10.0.130.132/30 is directly connected, Tunnel0*  *C 200.0.0.0/24 is directly connected, FastEthernet0/0*  *S\* 0.0.0.0/0 [200/0] via 200.0.0.1* |

1. **修改SW1、SW2、R3上缺省路由**
2. 修改SW1缺省路由，并查看。

|  |
| --- |
| *SW1(config)#ip route 0.0.0.0 0.0.0.0 10.0.130.1 //设置缺省路由指向R1*  *SW1(config)#ip route 0.0.0.0 0.0.0.0 10.0.130.10 200 //设置备用缺省路由指向SW2*  *SW1#show ip route*  *Gateway of last resort is 10.0.130.1 to network 0.0.0.0*  *10.0.0.0/8 is variably subnetted, 15 subnets, 3 masks*  *C 10.0.0.0/24 is directly connected, Vlan101*  *C 10.0.1.0/24 is directly connected, Vlan102*  *C 10.0.2.0/24 is directly connected, Vlan103*  *O 10.0.3.0/24 [110/2] via 10.0.130.10, 03:09:44, Vlan13*  *O 10.0.4.0/24 [110/1002] via 10.0.130.1, 00:04:44, Vlan11*  *O 10.0.5.0/24 [110/66] via 10.0.130.1, 01:46:27, Vlan11*  *O 10.0.128.1/32 [110/2] via 10.0.130.1, 01:46:37, Vlan11*  *O 10.0.128.2/32 [110/1002] via 10.0.130.1, 00:04:44, Vlan11*  *O 10.0.128.3/32 [110/66] via 10.0.130.1, 01:46:27, Vlan11*  *C 10.0.129.0/24 is directly connected, Vlan2*  *C 10.0.130.0/30 is directly connected, Vlan11*  *O 10.0.130.4/30 [110/2] via 10.0.130.1, 01:46:37, Vlan11*  *[110/2] via 10.0.130.10, 01:46:37, Vlan13*  *C 10.0.130.8/30 is directly connected, Vlan13*  *O 10.0.130.128/30 [110/65] via 10.0.130.1, 01:46:37, Vlan11*  *O 10.0.130.132/30 [110/1001] via 10.0.130.1, 00:49:41, Vlan11*  *S\* 0.0.0.0/0 [1/0] via 10.0.130.1* |

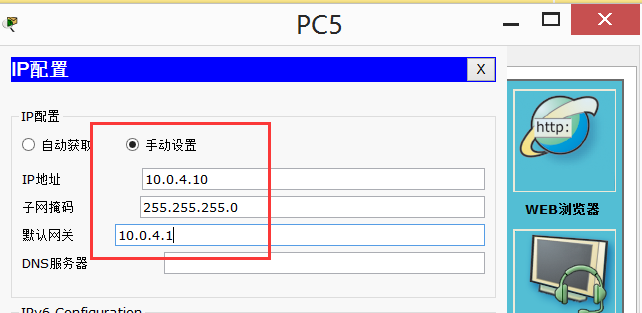
1. 修改SW2缺省路由，并查看。

|  |
| --- |
| SW2(config)#ip route 0.0.0.0 0.0.0.0 10.0.130.5 //设置缺省路由指向R1  SW2(config)#ip route 0.0.0.0 0.0.0.0 10.0.130.9 200 //设置备用缺省路由指向SW1  SW2#show ip route  Gateway of last resort is 10.0.130.1 to network 0.0.0.0  10.0.0.0/8 is variably subnetted, 15 subnets, 3 masks  C 10.0.0.0/24 is directly connected, Vlan101  O 10.0.1.0/24 [110/2] via 10.0.130.9, 03:12:49, Vlan13  C 10.0.2.0/24 is directly connected, Vlan103  C 10.0.3.0/24 is directly connected, Vlan104  O 10.0.4.0/24 [110/1002] via 10.0.130.5, 00:07:49, Vlan12  O 10.0.5.0/24 [110/66] via 10.0.130.5, 00:52:46, Vlan12  O 10.0.128.1/32 [110/2] via 10.0.130.5, 00:52:46, Vlan12  O 10.0.128.2/32 [110/1002] via 10.0.130.5, 00:07:49, Vlan12  O 10.0.128.3/32 [110/66] via 10.0.130.5, 00:52:46, Vlan12  C 10.0.129.0/24 is directly connected, Vlan2  O 10.0.130.0/30 [110/2] via 10.0.130.5, 00:52:46, Vlan12  [110/2] via 10.0.130.9, 00:52:46, Vlan13  C 10.0.130.4/30 is directly connected, Vlan12  C 10.0.130.8/30 is directly connected, Vlan13  O 10.0.130.128/30 [110/65] via 10.0.130.5, 00:52:46, Vlan12  O 10.0.130.132/30 [110/1001] via 10.0.130.5, 00:52:46, Vlan12  S\* 0.0.0.0/0 [1/0] via 10.0.130.5 |

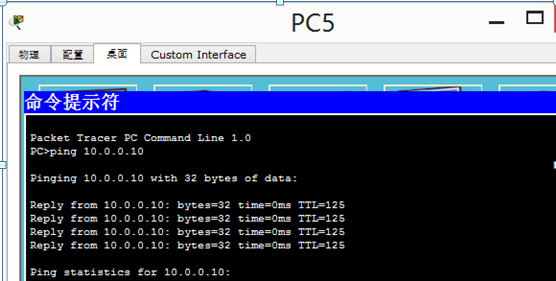
1. 修改R3缺省路由，并查看。

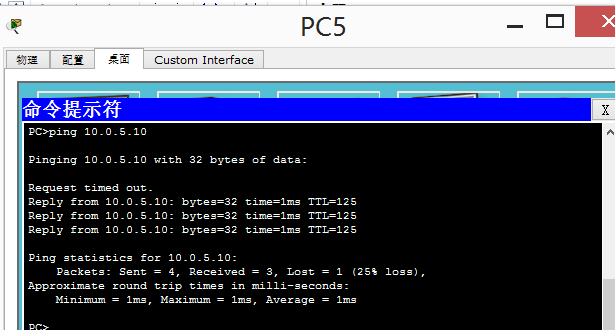
|  |
| --- |
| R3(config)#ip route 0.0.0.0 0.0.0.0 10.0.130.129 //设置缺省路由指向R1  R3#show ip route  Gateway of last resort is 10.0.130.1 to network 0.0.0.0  10.0.0.0/8 is variably subnetted, 16 subnets, 3 masks  O 10.0.0.0/24 [110/66] via 10.0.130.129, 00:54:49, Serial0/2/0  O 10.0.1.0/24 [110/66] via 10.0.130.129, 00:54:49, Serial0/2/0  O 10.0.2.0/24 [110/66] via 10.0.130.129, 00:54:49, Serial0/2/0  O 10.0.3.0/24 [110/66] via 10.0.130.129, 00:54:49, Serial0/2/0  O 10.0.4.0/24 [110/1065] via 10.0.130.129, 00:09:51, Serial0/2/0  C 10.0.5.0/24 is directly connected, FastEthernet0/0  O 10.0.128.1/32 [110/65] via 10.0.130.129, 00:54:49, Serial0/2/0  O 10.0.128.2/32 [110/1065] via 10.0.130.129, 00:09:51, Serial0/2/0  C 10.0.128.3/32 is directly connected, Loopback0  O 10.0.129.0/24 [110/66] via 10.0.130.129, 00:54:49, Serial0/2/0  O 10.0.130.0/30 [110/65] via 10.0.130.129, 00:54:49, Serial0/2/0  O 10.0.130.4/30 [110/65] via 10.0.130.129, 00:54:49, Serial0/2/0  O 10.0.130.8/30 [110/66] via 10.0.130.129, 00:54:49, Serial0/2/0  C 10.0.130.128/30 is directly connected, Serial0/2/0  C 10.0.130.129/32 is directly connected, Serial0/2/0  O 10.0.130.132/30 [110/1064] via 10.0.130.129, 00:54:49, Serial0/2/0  S\* 0.0.0.0/0 [1/0] via 10.0.130.129 |

1. **路由业务测试**
2. 设置PC 5 IP地址等参数。

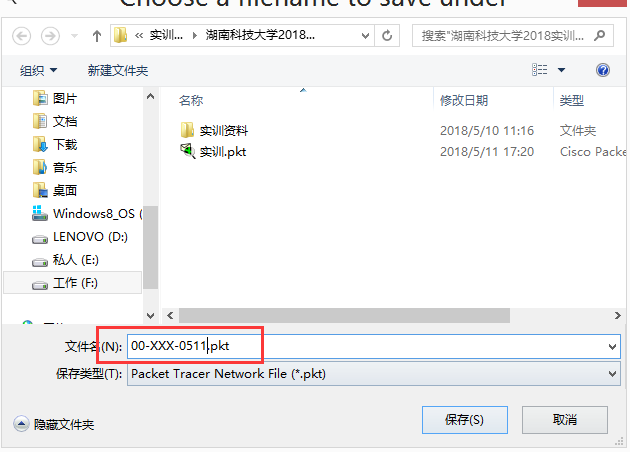


1. 在PC5上对其他主机进行ping测。





1. **保存配置并用U盘带走文件**



**ACL实验**

**实验9-1 ACL实验**

**学习目标**

* 了解ACL协议原理。
* 配置GRE实现私有网络跨越公网通信

**原理**

随着大规模开放式网络的开发，网络面临的威胁也就越来越多。网络安全问题成为网络管理员最为头疼的问题。一方面，为了业务的发展，必须允许对网络资源的开发访问，另一方面，又必须确保数据和资源的尽可能安全。网络安全采用的技术很多，而通过访问控制列表（ACL）可以对数据流进行过滤，是实现基本的网络安全手段之一。本章只研究基于IP的ACL。

ACL 概述

访问控制列表简称为ACL，它使用包过滤技术，在路由器上读取第三层及第四层包头中的信息如源地址、目的地址、源端口、目的端口等，根据预先定义好的规则对包进行过滤，从而达到访问控制的目的。ACL 分很多种，不同场合应用不同种类的ACL。

1. 标准ACL

标准ACL 最简单，是通过使用IP 包中的源IP 地址进行过滤，表号范围1-99；

2. 扩展ACL

扩展ACL 比标准ACL 具有更多的匹配项，功能更加强大和细化，可以针对包括协议类型、源地址、目的地址、源端口、目的端口、TCP 连接建立等进行过滤，表号范围100-199；

3. 命名ACL

以列表名称代替列表编号来定义ACL，同样包括标准和扩展两种列表。

在访问控制列表的学习中，要特别注意以下两个术语。

1. 通配符掩码：一个32 比特位的数字字符串,它规定了当一个IP 地址与其他的IP 地址进行比较时，该IP 地址中哪些位应该被忽略。通配符掩码中的“1”表示忽略IP 地址中对应的位，而“0”则表示该位必须匹配。两种特殊的通配符掩码是“255.255.255.255”和“0.0.0.0”，前者等价于关键字“any”，而后者等价于关键字“host”；

2. Inbound 和outbound：当在接口上应用访问控制列表时，用户要指明访问控制列表是应用于流入数据还是流出数据。总之，ACL 的应用非常广泛，它可以实现如下的功能：

1. 拒绝或允许流入（或流出）的数据流通过特定的接口；

2. 为DDR 应用定义感兴趣的数据流；

3. 过滤路由更新的内容；

4. 控制对虚拟终端的访问；

5. 提供流量控制。

**拓扑图**



图1拓扑

**操作步骤**

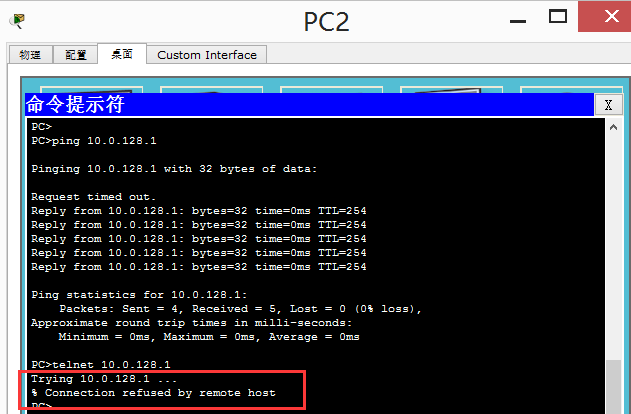
将《GRE实验》中保存的拓扑打开，要求校园网所有设备只允许图书馆所在网段进行telnet；服务器不允许宿舍终端访问。

1. 配置telnet安全防护
2. 在设备上设定ACL，并在line 0 4 中应用，以R1为例，其他设备配置相同。

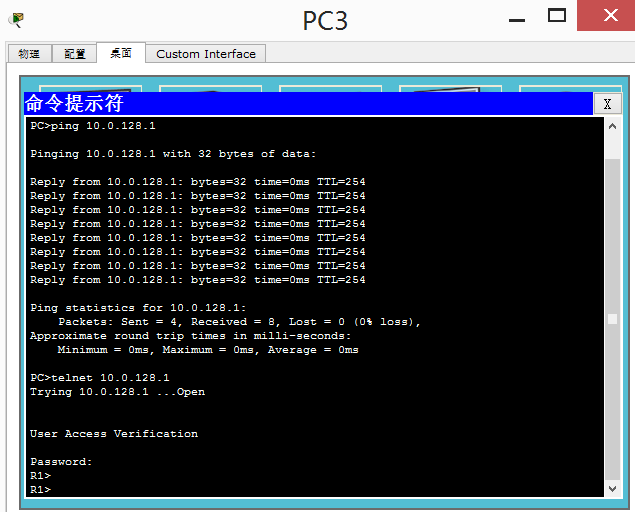
|  |
| --- |
| *R1>enable*  *R1#conf t*  *R1(config)#access-list 1 permit 10.0.2.0 0.0.0.255 //设置只允许图书馆网段*  *R1(config)#line vty 0 4*  *R1(config-line)#access-class 1 in //只允许acl1 允许地址telent本设备* |

1. 使用PC2 和PC3进行测试。

PC2所在网段不能telnet R1



PC3所在网段不能telnet R1，符合项目要求。



1. 在SW1和SW2上部署ACL，实现不允许宿舍访问服务器。
2. 在SW1上部署ACL

|  |
| --- |
| *SW1(config)#access-list 10 deny 10.0.1.0 0.0.0.255 //设置ACL*  *SW1(config)#access-list 10 deny 10.0.3.0 0.0.0.255*  *SW1(config)#access-list 10 permit any*  *SW1(config)#interface vlan 101*  *SW1(config-if)#ip access-group 10 out R1(config-router)#exit //调用ACL* |

1. 在SW1上查看ACL

|  |
| --- |
| *SW1#show ip access-lists*  *Standard IP access list 10*  *deny 10.0.1.0 0.0.0.255*  *deny 10.0.3.0 0.0.0.255*  *permit any* |

1. 在SW2上部署ACL

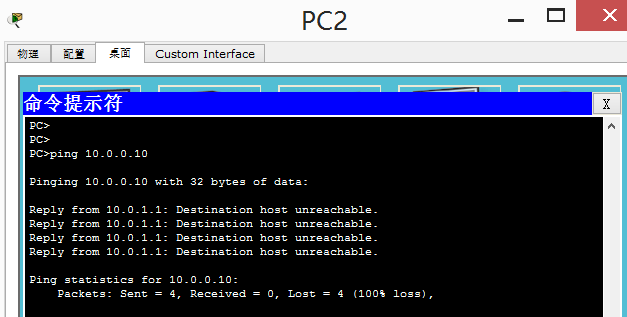
|  |
| --- |
| *SW2(config)#access-list 10 deny 10.0.1.0 0.0.0.255 //设置ACL*  *SW2(config)#access-list 10 deny 10.0.3.0 0.0.0.255*  *SW2(config)#access-list 10 permit any*  *SW2(config)#interface vlan 101*  *SW2(config-if)#ip access-group 10 out R1(config-router)#exit //调用ACL* |

1. 在SW2上查看ACL

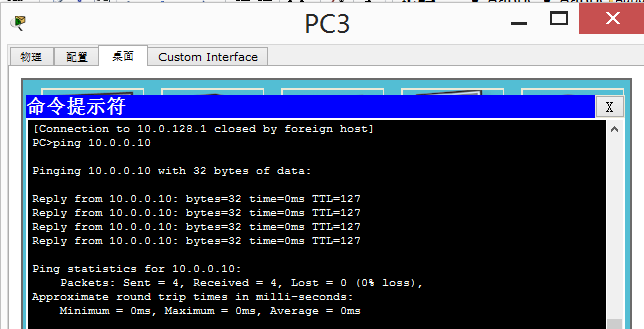
|  |
| --- |
| *SW2#show ip access-lists*  *Standard IP access list 10*  *deny 10.0.1.0 0.0.0.255*  *deny 10.0.3.0 0.0.0.255*  *permit any* |

1. 使用PC2和PC3进行测试

PC2不能访问服务器地址10.0.0.10，符合项目需求



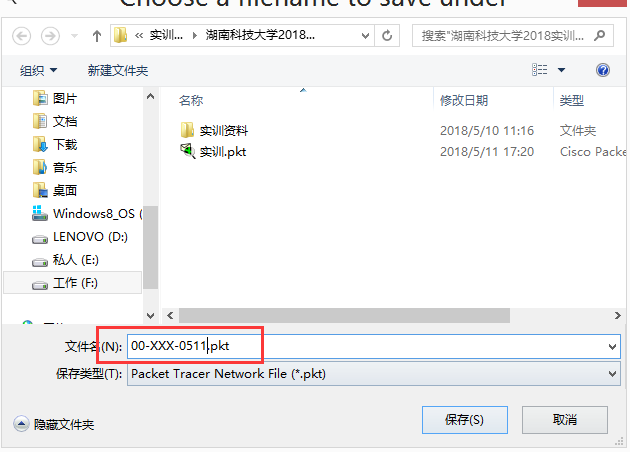
PC3可以能访问服务器地址10.0.0.10，符合项目需求



1. 在SW1上查看ACL

|  |
| --- |
|  |

1. **保存配置并用U盘带走文件**



**NAT实验**

**实验9-2 NAT实验**

**学习目标**

* 了解NAT协议原理。
* 配置NAT，实现校园网络对Inetnet的访问。

**原理**

Internet 技术的飞速发展，使越来越多的用户加入到互联网，因此IP 地址短缺已成为一个十分突出的问题。NAT(Network Address Translation，网络地址翻译)是解决IP 地址短缺的重要手段。

NAT 是一个IETF 标准，允许一个机构以一个地址出现在Internet 上。NAT 技术使得一个私有网络可以通过Internet 注册IP 连接到外部世界，位于Inside 网络和Outside 网络中的NAT 路由器在发送数据包之前，负责把内部IP 地址翻译成外部合法IP 地址。NAT 每个局域网节点的IP 地址转换成一个合法IP 地址，反之亦然。它也可以应用到防火墙技术里，把个别IP 地址隐藏起来不被外界发现，对内部网络设备起到保护的作用，同时，它还帮助网络可以超越地址的限制，合理地安排网络中的公有Internet 地址和私有IP 地址的使用。

NAT 有三种类型：静态NAT、动态NAT 和端口地址转换（PAT）。

1．静态NAT

静态NAT 中，内部网络中的每个主机都被永久映射成外部网络中的某个合法的地址。静态地址转换将内部本地地址与内部合法地址进行一对一的转换，且需要指定和哪个合法地址进行转换。如果内部网络有E-mail 服务器或FTP 服务器等可以为外部用户提供的服务，这些服务器的IP 地址必须采用静态地址转换，以便外部用户可以使用这些服务。

2．动态NAT

动态NAT 首先要定义合法地址池，然后采用动态分配的方法映射到内部网络。动态NAT是动态一对一的映射。

3．PAT

PAT 则是把内部地址映射到外部网络的IP 地址的不同端口上,从而可以实现多对一的映射。PAT 对于节省IP 地址是最为有效的。

**拓扑图**



图1拓扑

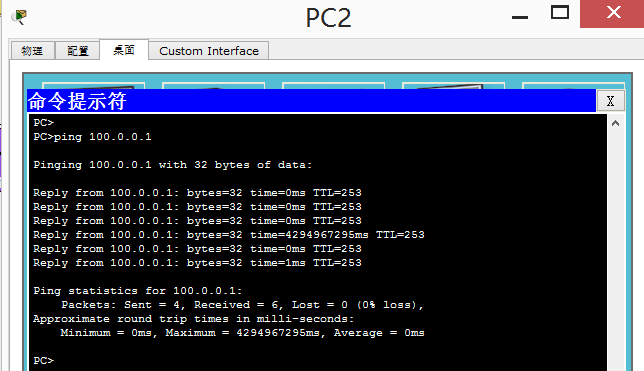
**操作步骤**

将《ACL实验》中保存的拓扑打开，要求校园网所有业务均可通过出口路由器访问外网，需在总校区R1，和分校区A R2上部署NAT，分校区B通过总校区访问外网。

1. 配置R1 NAT
2. 配置R1 NAT。

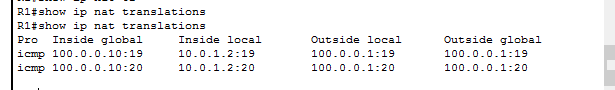
|  |
| --- |
| *R1>enable*  *R1#conf t*  *R1(config)#ip nat pool NAT 100.0.0.10 100.0.0.10 netmask 255.255.255.0*  *//设置NAT公网地址池*  *R1(config)#access-list 20 permit any //允许所有业务进行NAT*  *R1(config)#ip nat inside source list 20 pool NAT overload //设置NAT*  *R1(config)#interface f0/0*  *R1(config-if)#ip nat outside //设置NAT 出接口*  *R1(config-if)#int fa0/1*  *R1(config-if)#ip nat inside //设置NAT 入接口*  *R1(config-if)#int fa1/0*  *R1(config-if)#ip nat inside //设置NAT 入接口*  *R1(config-if)#int s0/2/0*  *R1(config-if)#ip nat inside //设置NAT 入接口* |

1. 使用PC对公网进行访问测试。



PC2能访问外网，NAT成功。

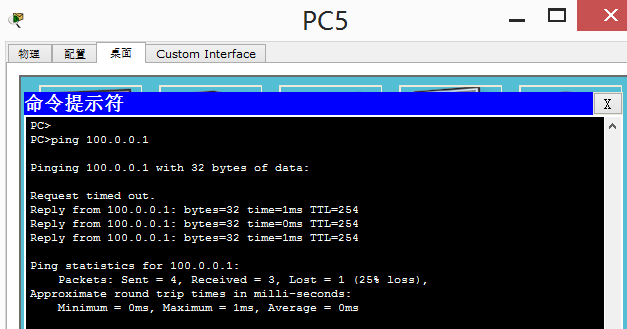
1. PAT 的过期时间是60 秒，Ping测后立即在R1上查看NAT 会话



1. 配置R2 NAT
2. 配置R2 NAT。

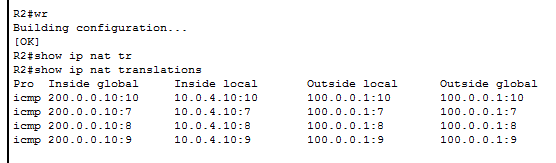
|  |
| --- |
| *R2>enable*  *R2#conf t*  *R2(config)#ip nat pool NAT 200.0.0.10 200.0.0.10 netmask 255.255.255.0*  *//设置NAT公网地址池*  *R2(config)#access-list 20 permit any //允许所有业务进行NAT*  *R2(config)#ip nat inside source list 20 pool NAT overload //设置NAT*  *R2(config)#interface f0/0*  *R2(config-if)#ip nat outside //设置NAT 出接口*  *R2(config-if)#int fa0/1*  *R2(config-if)#ip nat inside //设置NAT 入接口* |

1. 使用PC对公网进行访问测试。



PC5能访问外网，NAT成功。

1. PAT 的过期时间是60 秒，Ping测后立即在R2上查看NAT 会话



1. **保存配置并用U盘带走文件**

# 文 档 概 述

本规范适用范围为XX校园网网络设备及业务测试，测试内容包括网络设备安装、加电、设备所涉及业务的测试。

本规范所引用标准及具体技术要求见各测试项。

## 设备测试原则

完成基本单点验收测试，作为XX校园网测试依据，指导大家完成单站测试及业务测试。

要求完成设备硬件的全面测试；系统维护功能测试；完成基础配置协议的功能测试。

## 测试条件

设备单点验收测试前需要完成以下工作：

* 设备硬件安装工作；
* 设备加电工作，完成初始化配置；
* 设备到ODF端链路布放；
* 设备和链路标签制作；
* 设备物理连接及协议部署完成。

# 测 试 内 容

T02-01 软件版本检查

|  |  |
| --- | --- |
| 验收目的 | 检查软件版本。 |
| 预置条件 | 设备加电并运行正常，涉及R1—R3, SW1—SW6。 |
| 测试过程 | 使用show version检查软件版本。 |
| 预期结果 | [R1]show version //查看版本  Cisco IOS Software, 2800 Software (C2800NM-ADVIPSERVICESK9-M), Version 12.4(15)T1, RELEASE SOFTWARE (fc2)  Technical Support: http://www.cisco.com/techsupport  Copyright (c) 1986-2007 by Cisco Systems, Inc.  Compiled Wed 18-Jul-07 06:21 by pt\_rel\_team  ROM: System Bootstrap, Version 12.1(3r)T2, RELEASE SOFTWARE (fc1)  Copyright (c) 2000 by cisco Systems, Inc.  System returned to ROM by power-on  System image file is "c2800nm-advipservicesk9-mz.124-15.T1.bin"  This product contains cryptographic features and is subject to United  States and local country laws governing import, export, transfer and  use. Delivery of Cisco cryptographic products does not imply  third-party authority to import, export, distribute or use encryption.  Importers, exporters, distributors and users are responsible for  compliance with U.S. and local country laws. By using this product you  agree to comply with applicable laws and regulations. If you are unable  to comply with U.S. and local laws, return this product immediately.  A summary of U.S. laws governing Cisco cryptographic products may be found at:  http://www.cisco.com/wwl/export/crypto/tool/stqrg.html  If you require further assistance please contact us by sending email to  export@cisco.com.  cisco 2811 (MPC860) processor (revision 0x200) with 60416K/5120K bytes of memory  Configuration register is 0x2102 |
| 测试结果 | 通过 □ 未通过 □ 不涉及 □ |
| 测试说明 |  |

**T03 连通性测试**

## T03-01 链路质量测试

|  |  |
| --- | --- |
| 验收目的 | 测试互联链路质量。 |
| 预置条件 | 设备加电运行正常，完成设备之间物理连接，配置IP地址，涉及R1—R3, SW1—SW6。 |
| 测试过程 | 在设备上ping和上联设备互联接口地址，ping包个数为100个，ping大包2000默认。 |
| 预期结果 | R1—Internet  R1#ping  Protocol [ip]:  Target IP address: 100.0.0.1  Repeat count [5]: 100  Datagram size [100]: 2000  Timeout in seconds [2]:  Extended commands [n]:  Sweep range of sizes [n]:  Type escape sequence to abort.  Sending 100, 2000-byte ICMP Echos to 100.0.0.1, timeout is 2 seconds:  !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!  Success rate is 100 percent (100/100), round-trip min/avg/max = 0/2/4294967295 ms |
| 测试结果 | 通过 □ 未通过 □ 不涉及 □ |
| 测试说明 |  |

## **T04 协议状态查询**

检查各节点设备协议状态。

### T04-01 OSPF协议邻居状态查询

|  |  |
| --- | --- |
| 验收目的 | 检查本节点OSPF协议邻居状态。 |
| 预置条件 | 设备加电运行正常，完成各节点连接，OSPF协议收敛完成，涉及R1—R3, SW1—SW2。 |
| 测试过程 | 1、使用show ip ospf neighbor命令，查看本节点设备OSPF邻居信息； |
| 预期结果 | 本节点OSPF邻居关系与规划设计相一致，并邻居关系建立正常。实例如下：  R1#show ip ospf neighbor  Neighbor ID Pri State Dead Time Address Interface  10.0.128.3 0 FULL/ - 00:00:37 10.0.130.130 Serial0/2/0  10.0.129.1 1 FULL/DR 00:00:31 10.0.130.2 FastEthernet0/1  10.0.129.2 1 FULL/DR 00:00:31 10.0.130.6 FastEthernet1/0  10.0.128.2 0 FULL/ - 00:00:31 10.0.130.134 Tunnel0  R1# |
| 测试结果 | 通过 □ 未通过 □ 不涉及 □ |
| 测试说明 |  |

### T04-02 HSRP协议状态查询

|  |  |
| --- | --- |
| 验收目的 | 检查本节点HSRP协议是否正常。 |
| 预置条件 | 设备加电运行正常， HSRP协议收敛完成，涉及SW1—SW2。 |
| 测试过程 | 1、使用show standby brief命令，查看HSRP状态是否正常。 |
| 预期结果 | 本节点HSRP状态正常，符合拓扑要求：  SW1#show standby brief  P indicates configured to preempt.  |  Interface Grp Pri P State Active Standby Virtual IP  Vl2 2 105 P Active local 10.0.129.2 10.0.129.254  Vl1 101 105 P Active local 10.0.0.252 10.0.0.1  Vl1 103 100 P Standby 10.0.2.252 local 10.0.2.1  SW1# |
| 测试结果 | 通过 □ 未通过 □ 不涉及 □ |
| 测试说明 |  |

### T04-03 Ether-channel协议状态查询

|  |  |
| --- | --- |
| 验收目的 | 检查本节点Ether-channel协议是否正常。 |
| 预置条件 | 设备加电运行正常， Ether-channel协议收敛完成，涉及SW1—SW2。 |
| 测试过程 | 1、使用show etherchannel port-channel命令，查看Ether-channel状态是否正常。 |
| 预期结果 | 本节点HSRP状态正常，符合拓扑要求：  SW1#show etherchannel port-channel  Channel-group listing:  ----------------------  Group: 12  ----------  Port-channels in the group:  ---------------------------  Port-channel: Po12 (Primary Aggregator)  ------------  Age of the Port-channel = 00d:00h:43m:19s  Logical slot/port = 2/12 Number of ports = 2  GC = 0x00000000 HotStandBy port = null  Port state = Port-channel  Protocol = LACP  Port Security = Disabled  Ports in the Port-channel:  Index Load Port EC state No of bits  ------+------+------+------------------+-----------  0 00 Gig0/1 Active 0  0 00 Gig0/2 Active 0  Time since last port bundled: 00d:00h:43m:19s Gig0/2 |
| 测试结果 | 通过 □ 未通过 □ 不涉及 □ |
| 测试说明 |  |

T04-04 RSTP协议状态查询

|  |  |
| --- | --- |
| 验收目的 | 检查本节点RSTP协议是否正常。 |
| 预置条件 | 设备加电运行正常， RSTP协议收敛完成，涉及SW1—SW6。 |
| 测试过程 | 1、使用show spanning-tree命令，查看RSTP状态是否正常。 |
| 预期结果 | 本节点RSTP状态正常，符合拓扑要求：  SW1#show spanning-tree  VLAN0001  Spanning tree enabled protocol rstp  Root ID Priority 32769  Address 0003.E436.CA98  This bridge is the root  Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec  Bridge ID Priority 32769 (priority 32768 sys-id-ext 1)  Address 0003.E436.CA98  Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec  Aging Time 20  Interface Role Sts Cost Prio.Nbr Type  ---------------- ---- --- --------- -------- --------------------------------  Po12 Desg FWD 3 128.28 Shr  VLAN0002  Spanning tree enabled protocol rstp  Root ID Priority 24578  Address 0003.E436.CA98  This bridge is the root  Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec  Bridge ID Priority 24578 (priority 24576 sys-id-ext 2)  Address 0003.E436.CA98  Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec  Aging Time 20  Interface Role Sts Cost Prio.Nbr Type  ---------------- ---- --- --------- -------- --------------------------------  Fa0/5 Desg FWD 19 128.5 P2p  Fa0/4 Desg FWD 19 128.4 P2p  Fa0/3 Desg FWD 19 128.3 P2p  Po12 Desg FWD 3 128.28 Shr  VLAN0011  Spanning tree enabled protocol rstp  Root ID Priority 24587  Address 0003.E436.CA98  This bridge is the root  Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec  Bridge ID Priority 24587 (priority 24576 sys-id-ext 11)  Address 0003.E436.CA98  Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec  Aging Time 20  Interface Role Sts Cost Prio.Nbr Type  ---------------- ---- --- --------- -------- --------------------------------  Fa0/1 Desg FWD 19 128.1 P2p  Po12 Desg FWD 3 128.28 Shr  VLAN0013  Spanning tree enabled protocol rstp  Root ID Priority 24589  Address 0003.E436.CA98  This bridge is the root  Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec  Bridge ID Priority 24589 (priority 24576 sys-id-ext 13)  Address 0003.E436.CA98  Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec  Aging Time 20  Interface Role Sts Cost Prio.Nbr Type  ---------------- ---- --- --------- -------- --------------------------------  Po12 Desg FWD 3 128.28 Shr  VLAN0101  Spanning tree enabled protocol rstp  Root ID Priority 24677  Address 0003.E436.CA98  This bridge is the root  Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec  Bridge ID Priority 24677 (priority 24576 sys-id-ext 101)  Address 0003.E436.CA98  Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec  Aging Time 20  Interface Role Sts Cost Prio.Nbr Type  ---------------- ---- --- --------- -------- --------------------------------  Fa0/3 Desg FWD 19 128.3 P2p  Po12 Desg FWD 3 128.28 Shr  VLAN0102  Spanning tree enabled protocol rstp  Root ID Priority 24678  Address 0003.E436.CA98  This bridge is the root  Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec  Bridge ID Priority 24678 (priority 24576 sys-id-ext 102)  Address 0003.E436.CA98  Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec  Aging Time 20  Interface Role Sts Cost Prio.Nbr Type  ---------------- ---- --- --------- -------- --------------------------------  Fa0/4 Desg FWD 19 128.4 P2p  Po12 Desg FWD 3 128.28 Shr  VLAN0103  Spanning tree enabled protocol rstp  Root ID Priority 24679  Address 0005.5EA7.B684  Cost 3  Port 28(Port-channel 12)  Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec  Bridge ID Priority 28775 (priority 28672 sys-id-ext 103)  Address 0003.E436.CA98  Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec  Aging Time 20  Interface Role Sts Cost Prio.Nbr Type  ---------------- ---- --- --------- -------- --------------------------------  Fa0/5 Desg FWD 19 128.5 P2p  Po12 Root FWD 3 128.28 Shr  VLAN0104  Spanning tree enabled protocol rstp  Root ID Priority 24680  Address 0005.5EA7.B684  Cost 3  Port 28(Port-channel 12)  Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec  Bridge ID Priority 28776 (priority 28672 sys-id-ext 104)  Address 0003.E436.CA98  Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec  Aging Time 20  Interface Role Sts Cost Prio.Nbr Type  ---------------- ---- --- --------- -------- --------------------------------  Po12 Desg FWD 3 128.28 Shr |
| 测试结果 | 通过 □ 未通过 □ 不涉及 □ |
| 测试说明 |  |

### T04-05 DHCP协议

|  |  |
| --- | --- |
| 验收目的 | 检查本节点DHCP协议是否正常。 |
| 预置条件 | 设备加电运行正常，DHCP协议收敛完成，涉及SW1—SW2。 |
| 测试过程 | 1、在PC端进行IP地址获取操作。  2、使用show ip dhcp binding命令，查看DHCP地址分配信息是否正常。  3、在PC端进行IP释放操作  4、在PC端重新获取IP。 |
| 预期结果 | 本节点DHCP 运行正常，符合拓扑要求：  1、    2、SW1#show ip dhcp binding  IP address Client-ID/ Lease expiration Type  Hardware address  10.0.1.2 0009.7C91.AC67 -- Automatic  3、 |
| 测试结果 | 通过 □ 未通过 □ 不涉及 □ |
| 测试说明 |  |

### T04-06 PPP协议

|  |  |
| --- | --- |
| 验收目的 | 检查本节点PPP协议是否正常。 |
| 预置条件 | 设备加电运行正常，PPP协议收敛完成，涉及R1、R3。 |
| 测试过程 | 1. 关闭串行端口； 2. 开启串行端口，重新进行PPP链路建立； 3. 使用 ping x.x.x.x 对端地址进行PING测， |
| 预期结果 | 重启端口后，PPP链路建立成功。  R1(config)#int s0/2/0  R1(config-if)#shut  R1(config-if)#no shut  R1(config-if)#do ping 10.0.130.130  Type escape sequence to abort.  Sending 5, 100-byte ICMP Echos to 10.0.130.130, timeout is 2 seconds:  !!!!!  Success rate is 100 percent (5/5), round-trip min/avg/max = 1/4/6 ms |
| 测试结果 | 通过 □ 未通过 □ 不涉及 □ |
| 测试说明 |  |

**T05 业务测试**

### T05-01 全网终端互通性测试

|  |  |
| --- | --- |
| 验收目的 | 检查全网终端是否按设计实现互联互通。 |
| 预置条件 | 设备加电运行正常，测试数据配置完成。  1. 测试环境搭建完成。 2. 涉及PC1—PC6 |
| 测试过程 | 1. 各PC之间两两ping测，测试互通性。 |
| 预期结果 | 1、除宿舍（PC2、PC4）不能访问服务器（PC1）外，其余都可访问。 |
| 测试结果 | 通过 □ 未通过 □ 不涉及 □ |
| 测试说明 |  |

### T05-02 外网访问测试

|  |  |
| --- | --- |
| 验收目的 | 检查各PC是否能正常访问外网。 |
| 预置条件 | 设备加电运行正常，测试数据配置完成。  1. 测试环境搭建完成。 2. 涉及PC1—PC6。 |
| 测试过程 | 1. 各PC对外网地址进行ping测，ping 100.0.0.1。 |
| 预期结果 | 所有PC都可对外网进行访问。 |
| 测试结果 | 通过 □ 未通过 □ 不涉及 □ |
| 测试说明 |  |

### T05-03 telnet业务测试

|  |  |
| --- | --- |
| 验收目的 | 检查telent是否正常。 |
| 预置条件 | 设备加电运行正常，测试数据配置完成。  1. 测试环境搭建完成。 2. 涉及R1—R3, SW1—SW6。 |
| 测试过程 | 1. 使用图书馆PC对设备进行telent。 2. 使用非图书馆PC对设备进行telent。。 |
| 预期结果 | 只有图书馆PC可对设备进行telnet。  对R1进行测试: |
| 测试结果 | 通过 □ 未通过 □ 不涉及 □ |
| 测试说明 |  |

### T05-04冗余测试

|  |  |
| --- | --- |
| 验收目的 | 进行冗余测试，当网络出现单点故障时是否会影响业务。 |
| 预置条件 | 设备加电运行正常，测试数据配置完成。  1. 测试环境搭建完成。 2. 涉及全网所有设备 |
| 测试过程 | 1. 在SW3（应该在PC1上，但模拟器中PC不支持扩展ping）上对外网业务进行traceroute。 2. 在SW3（应该在PC1上，但模拟器中PC不支持扩展ping）上对外网业务进行PING长包。 3. 关闭SW1 int vlan 11接口（模拟器存在bug，应该关闭F0/1接口，但F0/1关闭后vlan11不能down），查看SW3 ping测是否中断； 4. 在SW3上再次对外网业务进行traceroute，看路径是否切换。 5. 在SW3（应该在PC1上，但模拟器中PC不支持扩展ping）上对外网业务进行PING长包。 6. 打开SW1 int vlan 11接口，查看SW3 ping测是否中断； 7. 在SW3上再次对外网业务进行traceroute，看路径是否切换。 |
| 预期结果 | 当网络出现单点故障时，会有少许丢包，然后业务恢复。   1. SW3 traceroute 100.0.0.1；     2、SW3 ping 100.0.0.1；    3、关闭SW1上行接口      4、在SW3再次 traceroute 100.0.0.1；对比步骤1路径，发现流量转发路径进行了切换。    5、SW3 ping 100.0.0.1；    6、打开SW1上行接口      7、在SW3再次 traceroute 100.0.0.1；对比步骤1和4路径，发现流量转发路径进行了切换。 |
| 测试结果 | 通过 □ 未通过 □ 不涉及 □ |
| 测试说明 |  |