|  |
| --- |
| **实验编号：**  **2018-2019学年 第2学期** |

**杭州电子科技大学**

**实 验 报 告**

**课程名称： 路由与交换技术**

**实验题目： 实验一**

**班 级： 16272412**

**学 号： 16272203**

**姓 名： 黄萍萍**

**指导老师： 伍益明**

2019年 5月

|  |  |
| --- | --- |
| **实验总评分** |  |

**实验分组名单**

**组 长： 叶艳雪16272205**

**小组成员： 黄萍萍16272203**

**小组成员： 叶艳雪16272205**

**小组成员： 陈建**

**小组成员： 陈建东**

**小组成员： 付昭华**

**小组成员： 荆仁**

**报告日期： 2019/06/04**

评分依据及得分情况

|  |  |  |
| --- | --- | --- |
| 一级评价指标 | 二级评价指标 | 实际得分 |
| 实验设计方案（30分） | 实验目的明确（5分） |  |
| 本实验总体设计思路（10分） |  |
| 实验设计流程图（10分） |  |
| 对设计方案的创新性分析（5分） |  |
| 实验实现过程（40分） | 详细记录项目实现过程中遇到的问题、原因及解决方法（10分） |  |
| 过程数据、图表记录详实（20分） |  |
| 书写规范性、认真程度（10分） |  |
| 对实验的进一步思考（15分） | 考虑改进思路（5分） |  |
| 资料的组织的能力、分析解决问题的能力（5分） |  |
| 对本实验的设计、难易程度等建议（5分） |  |
| 参考文献（5分） | 标注参考资料出处、包括阅读书籍、论文、网络资源等（5分） |  |
| 附录（10分） | 源码（6分） |  |
| 图表（2分） |  |
| 注释及其他（2分） |  |
| 合计 | |  |

备注：对于被认定为抄袭或复制他人成果的实验，直接判定为0分。

**实验一 小型交换机网络实验**

**1.实验内容**

使用 4 台交换机组建一个小型交换机网络，按照接入层、汇聚层的层次概念进行网络拓扑设计、设备命名和 VLAN 划分，配置 VTP、MSTP、LACP等协议，实现 VLAN 互通和隔离，实现网络的安全、稳定、可靠，无回路无广播风暴，并且具有一定扩展能力和提高管理的方便性。

**2.实验目的及要求**

本实验是对局域网交换技术的理解和实现，需了解小型交换机网络的常用拓扑结构，理解接入层，汇聚层，核心层交换机的主要作用并实现VLAN的划分和广播域的隔离，以及不同VLAN间数据通过有路由功能的设备互通的方法。

组建完成的交换机网络应安全、稳定、可靠，无回路无广播风暴，并且具有一定扩展能力和提高管理的方便性。

**3.实验方案及流程图**

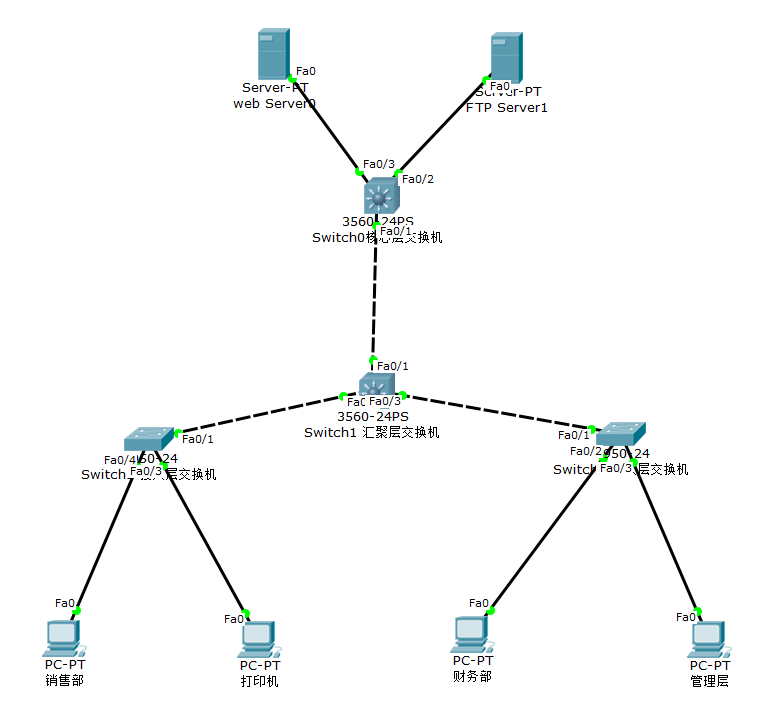


1. 网络拓扑结构设计
2. VLAN的互通与隔离
   * VLAN的划分和命名设计
   * 配置vtp
   * VLAN的创建和配置
   * 实现不同VLAN互通
   * 测试全网络连通性
3. 配置多生成树/链路聚合协议

* 新增冗余备份交换机
* 配置各交换机生成树协议
* 指定各VLAN的主根及辅助根
* 配置非根网桥的端口速链路及BPDU保护
* 根网桥之间配置以太网通道（链路聚合）
* 抓包分析VLAN间通信的转发路径

**4.实验步骤**

1. **网络拓扑结构设计**



1. **VLAN的互通与隔离**
   * **VLAN的划分和命名设计**

VLAN划分及命名设计，确定所属网段

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| VLAN | VLAN 10 | VLAN 20 | VLAN 30 | VLAN 40 |
| 网段 | 192.168.10.0/24 | 192.168.20.0/24 | 192.168.30.0/24 | 192.168.40.0/24 |
| 所属部门 | 销售部 | 打印机 | 财务部 | 管理层 |
| 接入层交换机 | Sw1 | Sw1 | Sw2 | Sw2 |
| 网关地址 | 192.168.10.254 | 192.168.20.254 | 192.168.30.254 | 192.168.40.254 |

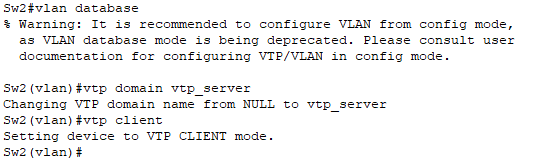
配置各部门接入设备IP地址如下，并开启各路由器端口

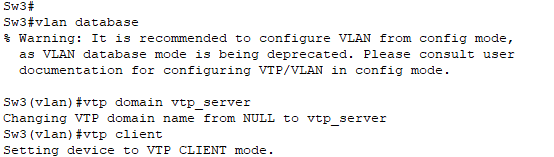
|  |  |
| --- | --- |
| 终端 | IP地址 |
| pc 1 销售部 | 192.168.10.1 |
| pc 2 打印机 | 192.168.20.1 |
| pc 3 财务部 | 192.168.30.1 |
| pc 4 管理层 | 192.168.40.1 |

* + **配置vtp**

配置vtp服务端和客户端

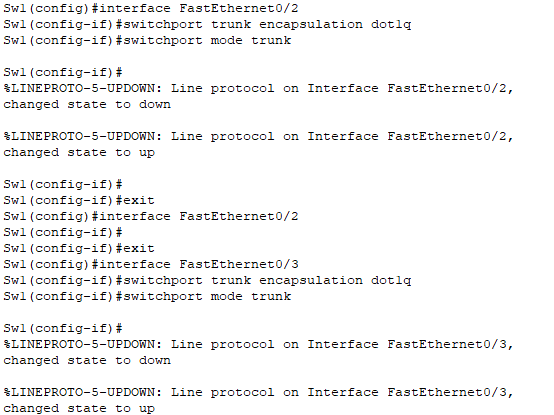
|  |  |  |  |
| --- | --- | --- | --- |
| 配置  V  T  P | Sw1 | Sw1#vlan database  Sw1(vlan)#vtp domain vtp\_server  Sw1(vlan)#vtp server | 进入VLAN配置模式  设置VTP管理域名称为 vtp\_server  设置交换机为服务器模式 |
| Sw2 | Sw2#vlan database  Sw2(vlan)#vtp domain vtp\_server  Sw2(vlan)#vtp client | 进入VLAN配置模式  设置vtp管理域名称vtp\_server  设置交换机为客户端模式 |
| Sw3 | Sw3#vlan database  Sw3(vlan)#vtp domain vtp\_server  Sw3(vlan)#vtp client | 进入VLAN配置模式  设置vtp管理域名称vtp\_server  设置交换机为客户端模式 |

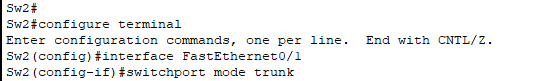




配置交换机上级端口为trunk模式

|  |  |  |  |
| --- | --- | --- | --- |
| 配置TRUNK | Sw1 | Sw1(config)#interface FastEthernet0/2  Sw1(config-if)#switchport trunk encapsulation dot1q  Sw1(config-if)#switchport mode trunk  Sw1(config-if)#exit  Sw1(config)#interface FastEthernet0/3  Sw1(config-if)#switchport trunk encapsulation dot1q  Sw1(config-if)#switchport mode trunk | sw1的FastEthernet0/2、FastEthernet0/3接口配置为trunk模式，允许不同vlan的数据包通过 |
| Sw2 | Sw2(config)#interface FastEthernet0/1  Sw2(config-if)#switchport mode trunk  Sw2(config-if)#exit | sw2的FastEthernet0/1接口配置为trunk模式 |
| Sw3 | Sw3(config-if)#interface FastEthernet0/1  Sw3(config-if)#switchport mode trunk  Sw3(config-if)#exit | sw2的FastEthernet0/1接口配置为trunk模式 |



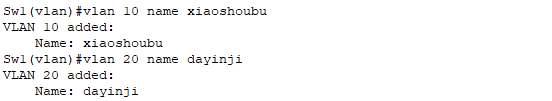


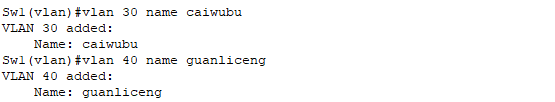
https://uploader.shimo.im/f/uKbl3RiZ3ls9cwi3.png!thumbnail

* + **VLAN的创建和配置**

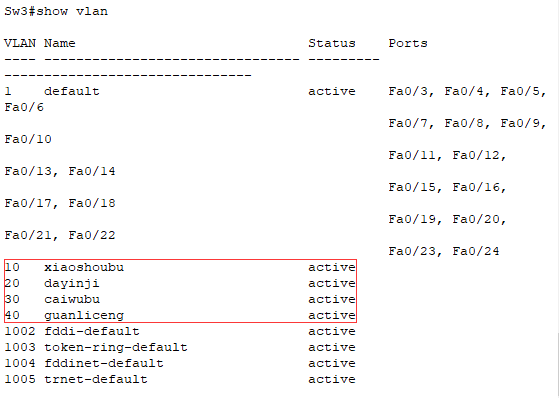
划分VLAN

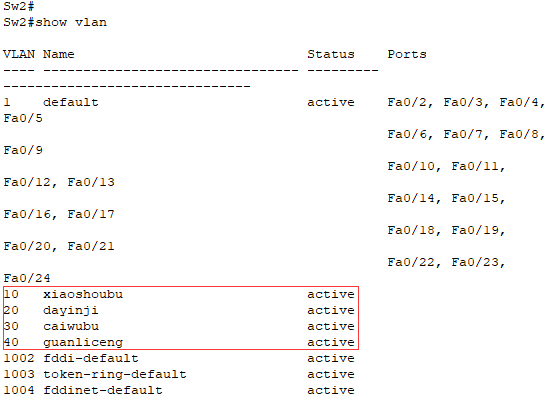
|  |  |  |  |
| --- | --- | --- | --- |
| 创建VLAN | Sw1 | Sw1#vlan database  Sw1(vlan)#vlan 10 name xiaoshoubu  Sw1(vlan)#vlan 20 name dayinji  Sw1(vlan)#vlan 30 name caiwubu  Sw1(vlan)#vlan 40 name guanliceng | 进入vtp配置模式  创建VLAN10 命名销售部  创建VLAN20 命名打印机  创建VLAN30 命名财务部  创建VLAN40 命名管理层 |
| Sw2 | Sw2#show vlan | 查看VLAN |
| Sw3 | Sw3#show vlan | 查看VLAN |





查看sw2 sw3 VLAN状态，可见VLAN与vtp server同步

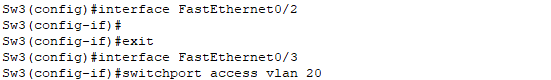


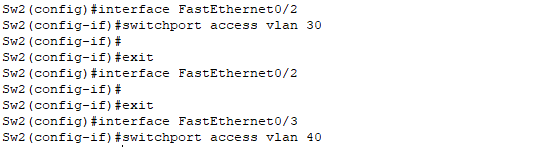
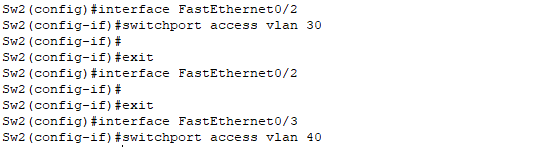


将sw2、sw3交换机与VLAN内设备互联的接口与指定VLAN绑定

|  |  |  |  |
| --- | --- | --- | --- |
| 绑定接口与v  l  a  n | Sw2 | Sw2(config)#interface FastEthernet0/2  Sw2(config-if)#switchport access vlan 30  Sw2(config-if)#exit  Sw2(config)#interface FastEthernet0/3  Sw2(config-if)#switchport access vlan 40 | 将Fa0/2划分到VLAN30  将Fa0/3划分到VLAN40 |
| Sw3 | Sw3(config)#interface FastEthernet0/4  Sw3(config-if)#switchport access vlan 10  Sw3(config-if)#end  Sw3(config)#interface FastEthernet0/3  Sw3(config-if)#switchport access vlan 20 | 将Fa0/4划分到VLAN10  将Fa0/3划分到VLAN20 |

https://uploader.shimo.im/f/mvrpdUYnrIkpapKT.png!thumbnail

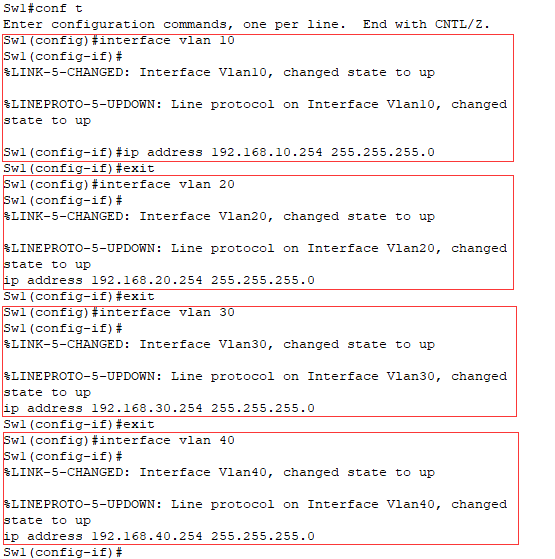


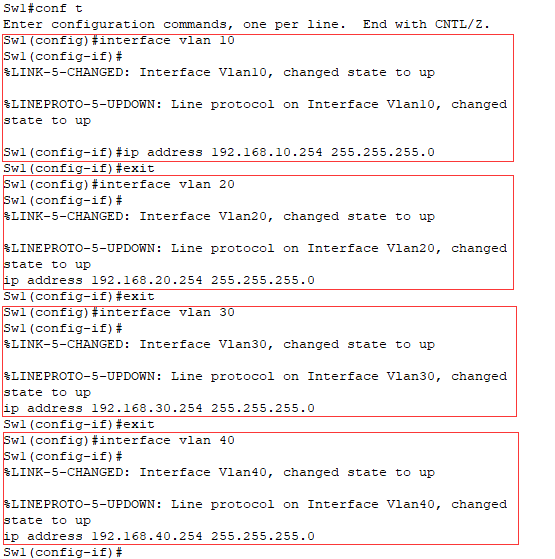


* + **实现不同VLAN互通**

Sw1配置VLAN 网段及网关ip

|  |  |  |  |
| --- | --- | --- | --- |
| 配置V  L  A  N 网段及网关ip | Sw1 | Sw1#conf t  Sw1(config)#interface vlan 10  Sw1(config-if)#ip address 192.168.10.254 255.255.255.0  Sw1(config-if)#exit  Sw1(config)#interface vlan 20  Sw1(config-if)#ip address 192.168.20.254 255.255.255.0  Sw1(config-if)#exit  Sw1(config)#interface vlan 30  Sw1(config-if)#ip address 192.168.30.254 255.255.255.0  Sw1(config-if)#exit  Sw1(config)#interface vlan 40  Sw1(config-if)#ip address 192.168.40.254 255.255.255.0 | 配置 VLAN10 的 ip 网关、掩码  配置 VLAN20 的 ip 网关、掩码  配置 VLAN30 的 ip 网关、掩码  配置 VLAN40 的 ip 网关、掩码 |





三层交换机开启路由功能，实现不同VLAN可互相访问

|  |  |  |  |
| --- | --- | --- | --- |
| 开启路由 | Sw1 | Sw1(config)#ip routing | 三层交换机开启路由功能 |

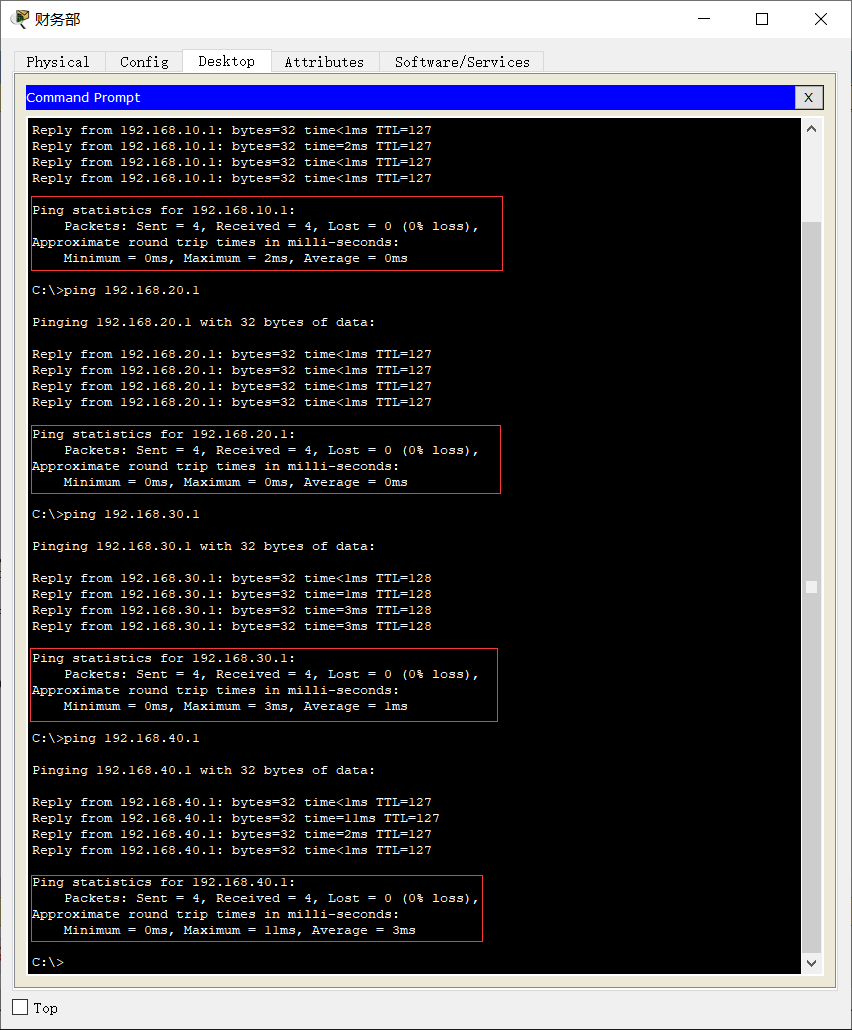
https://uploader.shimo.im/f/6hIItjjcVNI0c0I0.png!thumbnail

至此，Vtp及VLAN划分，不同VLAN间网络互通完成。

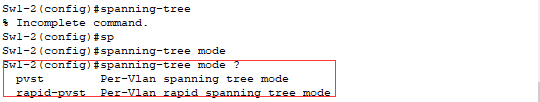
* + **测试全网络连通性**

测试连通性

使用pc3财务部ping其他各VLAN的主机，可见全部连通。



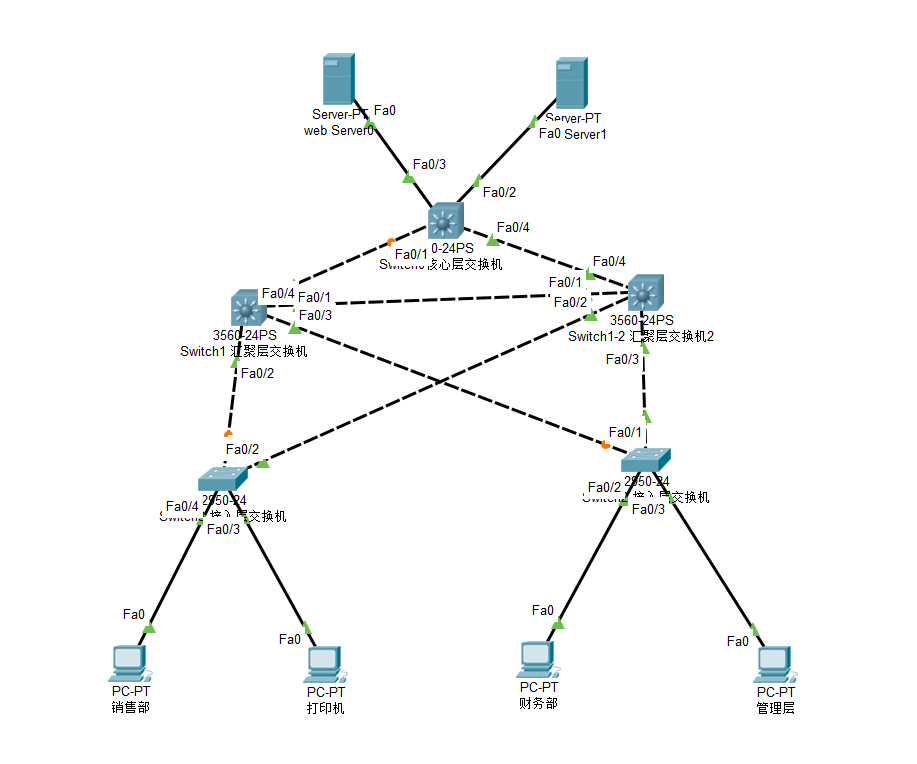
1. **配置多生成树协议**

由于Cisco packet tracer 7.2 不支持mstp，故采用pvst在VLAN间实现数据流量的均衡负载

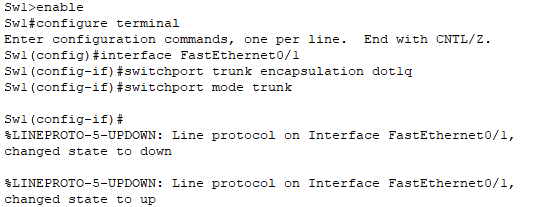
为实现主备冗余，需增加一台汇聚层交换机。

* **新增冗余备份交换机**

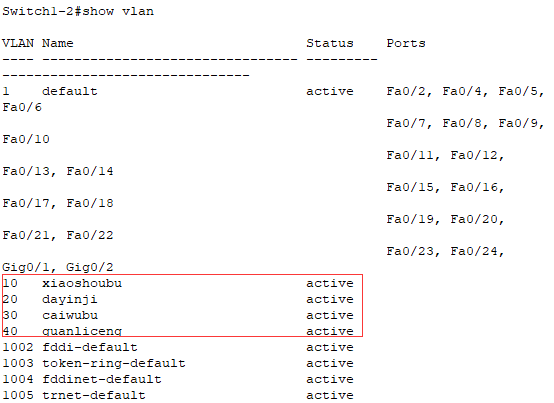
新建汇聚层交换机sw1-2，与上述配置相同，为sw1-2配置vtp client及与接入层、汇聚层交换机连接的各接口为trunk模式。拓扑图如下。



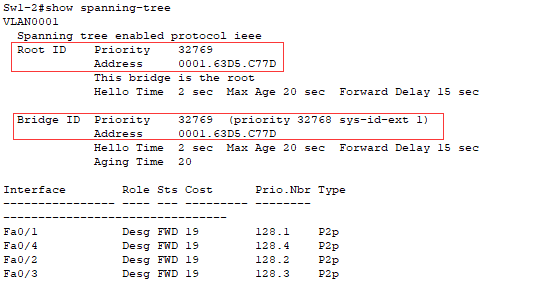
配置sw1与sw1-2连接的接口为trunk模式



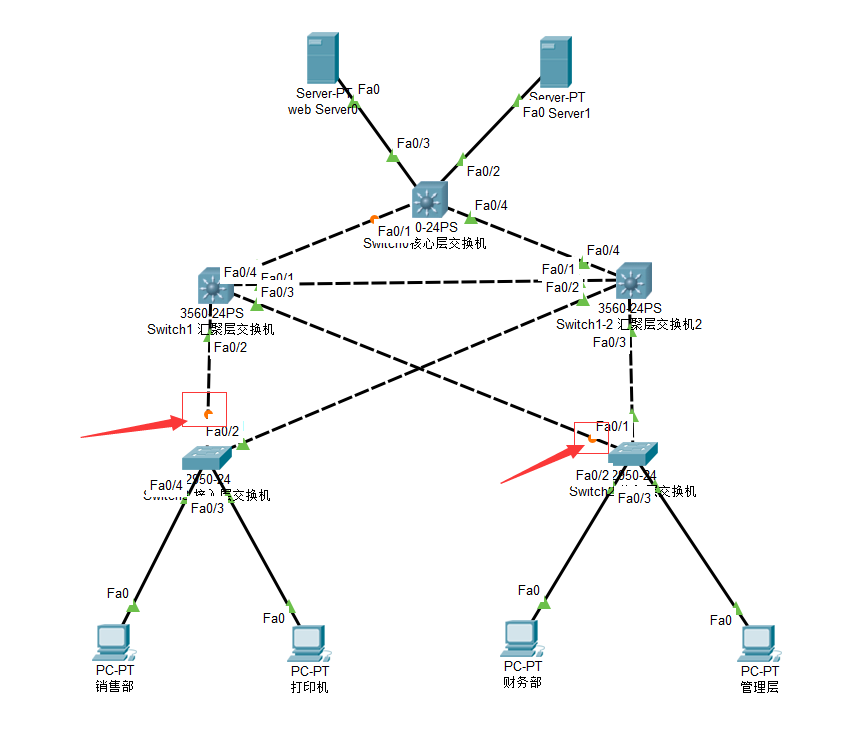
sw1-2基本配置完成，查看sw1-2 VLAN，可见与vtp server同步



查看当前生成树状态，可见当前各个交换机各个VLAN优先级相同 根交换机皆为sw1-2



查看网络拓扑结构可见 接入层交换机到sw1的端口为阻塞端口，与sw1-2为根桥结果相符。



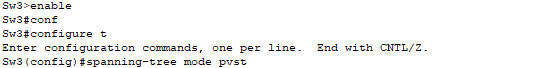
* **配置各交换机生成树协议**

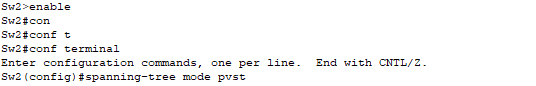
配置各交换机生成树协议为pvst模式

|  |  |  |  |
| --- | --- | --- | --- |
| 配置生成树协议 | Sw1 | Sw1#conf t  Sw3(config)#spanning-tree mode pvst | 配置spanning-tree为pvst模式 |
| Sw1-2 | Sw1-2#conf t  Sw3(config)#spanning-tree mode pvst | 配置spanning-tree为pvst模式 |
| Sw2 | Sw2#conf t  Sw3(config)#spanning-tree mode pvst | 配置spanning-tree为pvst模式 |
| Sw3 | Sw3#conf t  Sw3(config)#spanning-tree mode pvst | 配置spanning-tree为pvst模式 |

https://uploader.shimo.im/f/TDkinUepDVQC7FUe.png!thumbnail

https://uploader.shimo.im/f/uGB9Ec8PR8Ej9xEY.png!thumbnail





* **指定各VLAN的主根及辅助根**

选取多生成树的各VLAN的主根及辅助根，实现负载均衡

|  |  |  |  |
| --- | --- | --- | --- |
| 配置VLAN主根及辅助根 | Sw1 | Sw1>enable  Sw1#conf t  Sw1(config)#spanning-tree vlan 1,10,30 root primary  Sw1(config)#spanning-tree vlan 20,40 root secondary | 设置sw1为vlan1,10，30 的主根 20,40的辅助根 |
| Sw1-2 | Sw1-2>enable  Sw1-2#conf t  Sw1-2(config)#spanning-tree vlan 20,40 root primary  Sw1-2(config)#spanning-tree vlan 1,10,30 root secondary | 设置sw1-2为20 40 主根，vlan1,10，30的辅助根 |

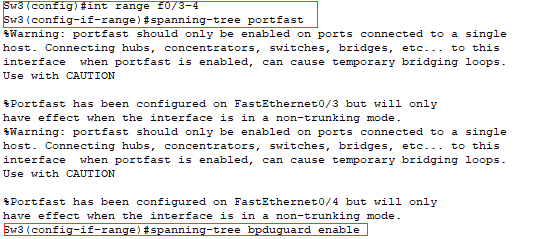
https://uploader.shimo.im/f/nXjoK1DzI0wZFbwq.png!thumbnail

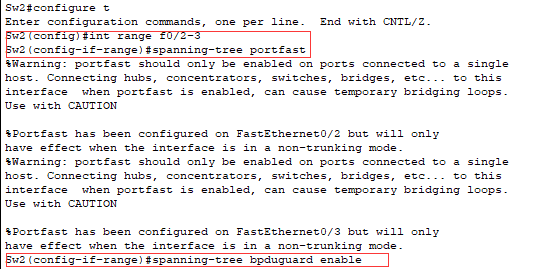
https://uploader.shimo.im/f/hfUoLbHPPdoHRo9i.png!thumbnail

* **配置非根网桥的端口速链路及BPDU保护**

配置非根网桥的与上网设备互联的端口为端口速链路及BPDU保护

|  |  |  |  |
| --- | --- | --- | --- |
| 配置端口速链路及B  P  D  U | Sw2 | Sw2#configure t  Sw2(config)#int range f0/2-3  Sw2(config-if-range)#spanning-tree portfast  Sw2(config-if-range)#spanning-tree bpduguard enable | 配置与终端互联的端口Fa0/2及Fa0/3为 port fast，使连接终端的端口快速进入转发状态，缩短工作站上线所需的时间  配置bpdu，执行STP域边界并保持活动拓扑可预测 |
| Sw3 | Sw3(config)#int range f0/3-4  Sw3(config-if-range)#spanning-tree portfast  Sw3(config-if-range)#spanning-tree bpduguard enable | 配置与终端互联的端口Fa0/4及Fa0/3 为port fast  配置bpdu |

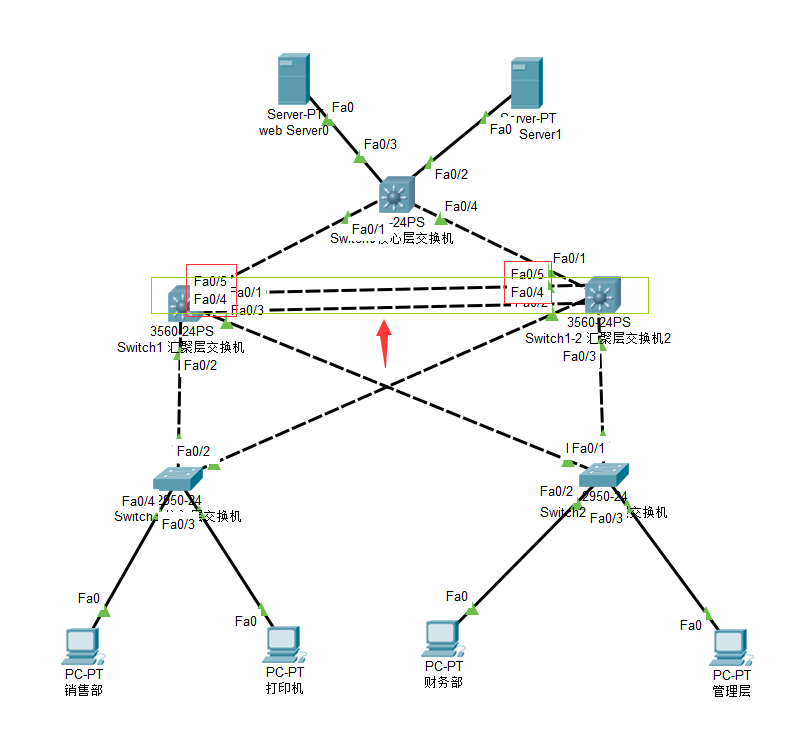




* **根网桥之间配置以太网通道（链路聚合）**

在根网桥之间配置以太网通道

增加根桥之间的冗余链路如下，实现链路聚合，使网络安全、稳定、可靠。

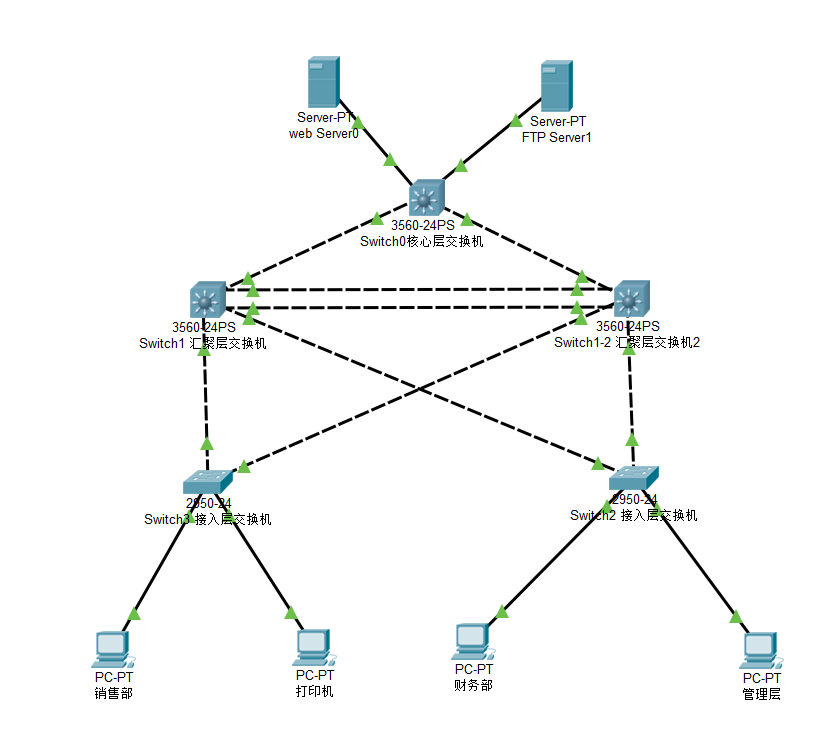


|  |  |  |  |
| --- | --- | --- | --- |
| 配置以太网通道 | Sw1 | Sw1(config)#interface FastEthernet0/5  Sw1(config-if)#switchport trunk encapsulation dot1q  Sw1(config-if)#switchport mode trunk  Sw1(config-if)#int range f0/4-5  Sw1(config-if-range)#channel-group 1 mode on | 新增链路端口配置为trunk  将f0/4-5组合为以太通道，提高带宽负载均衡且容错。 |
| Sw1-2 | Sw1-2(config)#interface FastEthernet0/5  Sw1-2(config-if)#switchport trunk encapsulation dot1q  Sw1-2(config-if)#switchport mode trunk  Sw1-2(config-if)#int range f0/4-5  Sw1-2(config-if-range)#channel-group 1 mode on | 新增链路端口配置为trunk  将f0/4-5组合为以太通道 |

https://uploader.shimo.im/f/fpZNXg2IdIAxd9iy.png!thumbnail

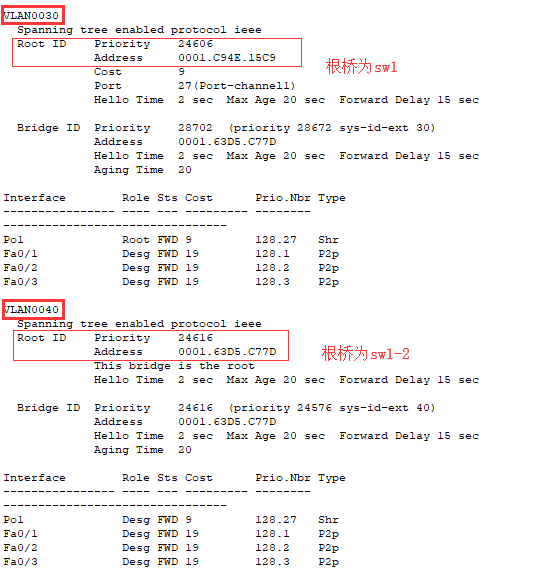
https://uploader.shimo.im/f/Jv31vbg4MP4gKzUj.png!thumbnail

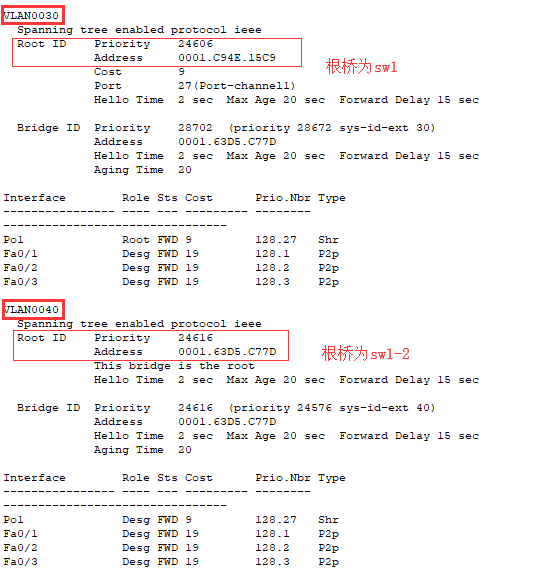
配置完成，此时可见各交换机各端口皆为畅通，供不同的VLAN的生成树使用。



 查看多生成树状态，可见不同VLAN根桥不同



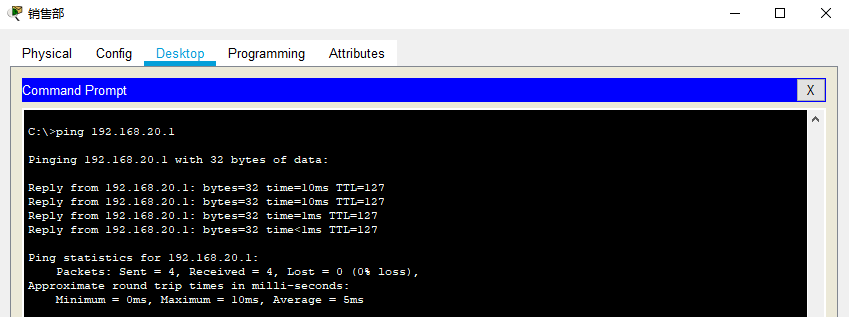




* **抓包分析VLAN间通信的转发路径**

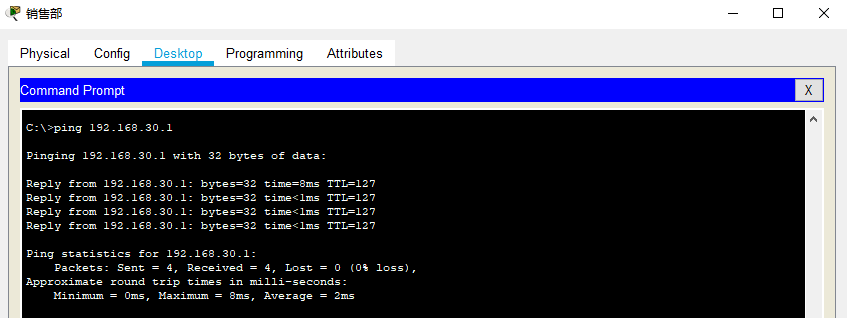
在不同VLAN间发送icmp数据包，抓包验证包转发路径

VLAN10销售部ping VLAN20打印机（不同根网桥的VLAN之间通信）





VLAN10销售部ping VLAN30财务部（相同根网桥的VLAN之间通信）





**5.对实验的进一步思考**

黄萍萍：本实验模仿现实生活中局域网的设计，根据功能、部门来对接入层交换机进行VLAN划分，以实现不同部门之间广播域的隔离，保障局域网内的通信更加安全可靠且不受物理设备的限制。同时，使用汇聚层三层交换机的路由功能实现VLAN间通信，即省去使用路由器，三层交换机也能提供更高效的转发。同时，为实现网络更高效可靠，增加冗余交换机及冗余链路，配置多生成树协议以实现各VLAN间流量负载均衡，且在流量转发的中心——各VLAN的根网桥之间配置链路聚合，扩展带宽，实现链路备份。

本实验所使用的是静态VLAN，即在接入层交换机上指定端口所属的VLAN，连接在该端口上的主机需与端口属于同一个VLAN。这种方式更适用于不会经常移动客户机的网络需求，且用户可以自由定义端口所属VLAN，更利于管理。但是对于需要经常移动客户机的情况，需要确保交换机端口与接入的设备所属VLAN相同，否则会导致接入设备无法访问他原先的VLAN，增加网络管理员的工作量，此时可使用动态VLAN来规划交换机端口。

**6.参考文献**

VLAN配置

<https://wenku.baidu.com/view/4137460002020740be1e9b13.html>

pvst配置

**7.团队分工**

**8.附录（程序代码、图表等）**

**实验二 小型企业网络实验**

**1.实验内容**

使用 6 台路由器和 4 台交换机，组建一个小型企业网络，按照内网、外网的概念进行网络拓扑设计、区域划分、设备命名、IP 地址和 VLAN规划，配置静态路由、RIP、OSPF、NAT、ACL等协议，实现不同区域间（要求使用不同路由协议）的互通，以及内外网间的安全策略控制。

**2.实验目的及要求**

综合运用网络拓扑结构的知识在Cisco Packet Tracer 7.2上进行小型企业网络结构设计。分析网络建设需求，确定企业所拥有的网段，网络规模及内部网络划分并确定拓扑结构。为企业网络进行内外网划分、设备命名、ip地址规划，通过VLAN规划实现内部网络各功能部门的广播域隔离，通过三层交换机路由实现VLAN间设备互通。

全网络互通的实现上，并通过网络地址转换实现内外网可互相访问；通过使用RIP协议实现内网有路由功能的设备路由信息互通，使得内网全网可达；通过使用ospf协议实现外网路由之间信息互通，使得外网全网可达；在企业出口路由器上实现不同路由协议的互通，使得内外网不同区域间全网可达。

在访问控制上，通过过在出口路由器上配置ACL，以实现对内外网访问策略的控制；NAT的配置，限制某些VLAN的用户不得访问外网。

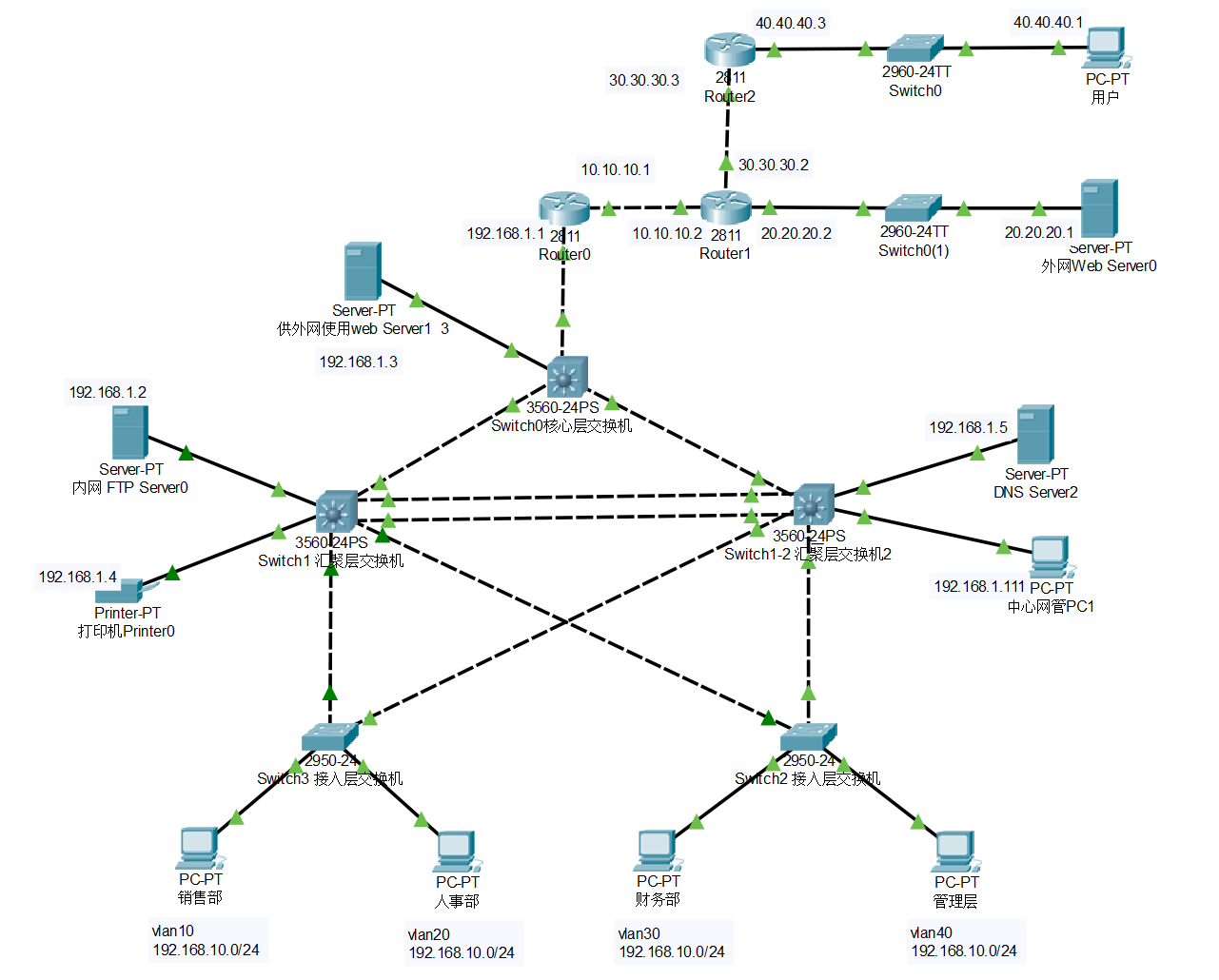
**3.实验方案及流程图**

1. 网络拓扑结构设计
2. 企业网络需求分析
   * VLAN的划分
   * 设备接入规划
   * 内外网地址转换规划
   * 访问控制策略规划
3. 企业网络的实现
   * VLAN，多生成树，以太网通道，DHCP
   * 静态路由，RIP，OSPF，连通测试
   * NAT网络地址转换配置
   * 配置ACL访问控制表
   * 内外网访问测试



**4.实验步骤**

1. **网络拓扑结构设计**



公司拥有一个核心出口路由器，用于与外网通信。交换机分为核心层、汇聚层、接入层三个层次。接入设备包含各部门PC，打印机、ftp服务器、web服务器、dns服务器、中心网管PC。

1. **企业网络需求分析**

为简单起见，对企业网络进行如下规划：

* 公司所拥有的外网网络地址范围为10.10.10.0/24，出口路由器的外网ip为10.10.10.1
* 公司内网使用的网络地址范围为192.168.0.0/16，网关路由器的内网ip为192.168.1.1
  + **VLAN的划分**

为实现各部门广播域的隔离，进行如下VLAN划分及命名设计：

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| VLAN | VLAN 10 | VLAN 20 | VLAN 30 | VLAN 40 | VLAN99 |
| 网段 | 192.168.10.0/24 | 192.168.20.0/24 | 192.168.30.0/24 | 192.168.40.0/24 | 192.168.1.0/24 |
| 所属部门 | 销售部 | 人事部 | 财务部 | 管理层 | 外网出口 |
| 接入交换机 | Sw1 | Sw1 | Sw2 | Sw2 | Sw0/Router0 |
| 网关地址 | 192.168.10.254 | 192.168.20.254 | 192.168.30.254 | 192.168.40.254 | 192.168.1.254 |
| 根交换机 | Sw1 | Sw2 | Sw1 | Sw2 | —— |

* + **设备接入规划**

对内网公用设备的接入规划及使用限制如下：

|  |  |  |  |
| --- | --- | --- | --- |
| 交换机 | 接入设备 | ip地址 | 允许访问 |
| Sw0 | Web server 1 | 192.168.1.3 | 所有内外网用户皆可 |
| Sw1 | ftp服务器 | 192.168.1.2 | 所有内网用户 |
| 打印机 | 192.168.1.4 | 所有内网用户 |
| Sw1-2 | Dns server | 192.168.1.5 | 所有内网用户 |
| 中心网管 | 192.168.1.111 | 所有内网用户 |

注：由于销售部与财务部会更多的使用打印机与ftp服务器，因此将这两个设备接在VLAN10和VLAN30的根交换机Sw1上，使内网通信更加高效；Web server 1需要给外网用户提供服务，因此接在核心层交换机Sw0上，提供更快的访问；而全内网公用的Dns server和中心网管则接在负载较小的汇聚层交换机Sw1-2上

* + **内外网地址转换规划**

内外网互通

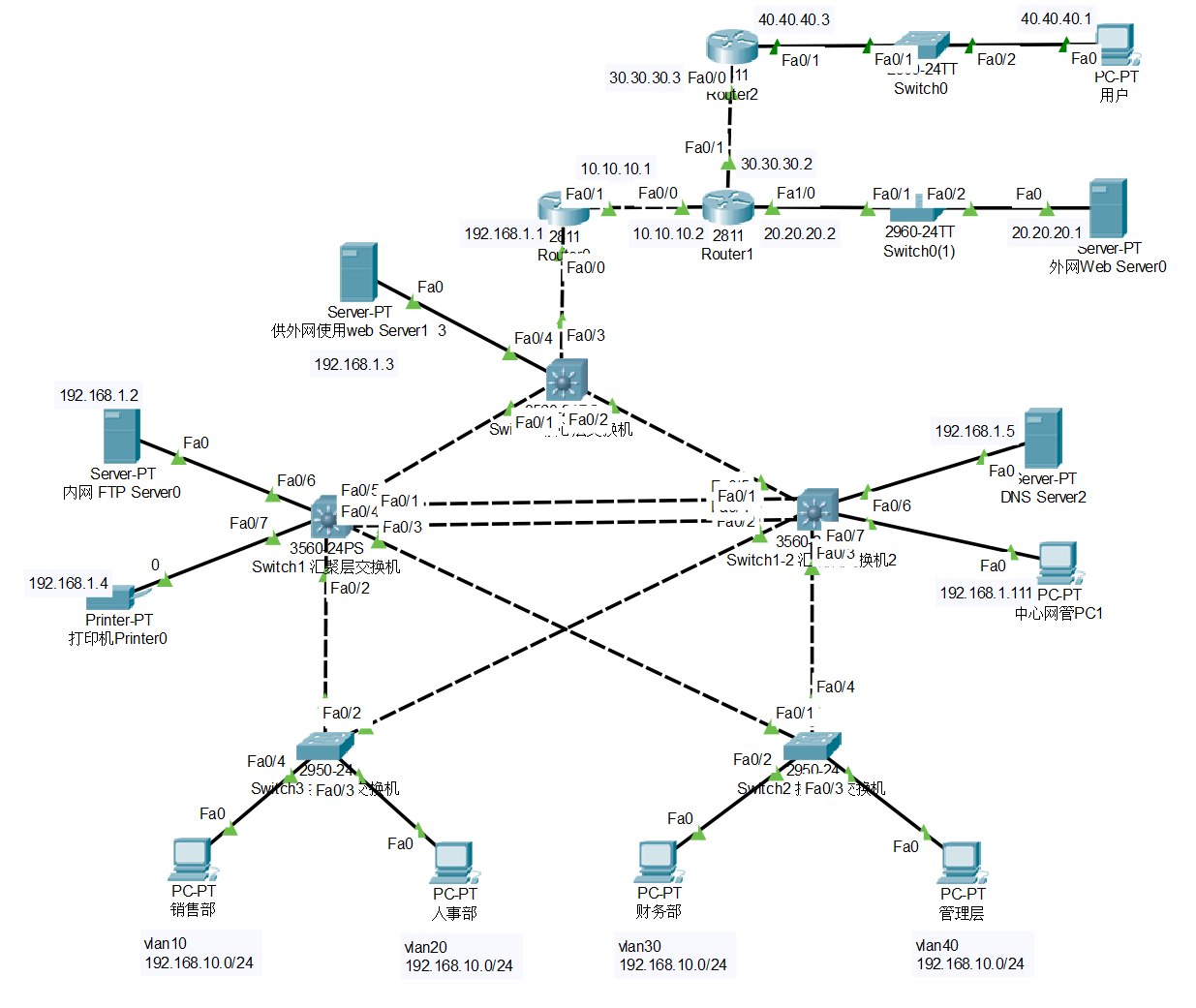
为实现外网可访问内网Web server 1及内网销售部与人事部可访问外网，在出口路由器上实现网络地址转换，转换规则如下

|  |  |  |
| --- | --- | --- |
|  | 内网地址 | 外网地址 |
| Web server 1 | 192.168.1.3 | 10.10.10.10 |
| 可访问外网的用户 |  | 10.10.10.100-10.10.10.200 |

* + **访问控制策略规划**

访问控制策略

1. 允许外网访问内网Web server 1
2. 允许内网销售部与人事部对外网发起tcp访问
3. 允许内网对外网进行icmp访问测试
4. 允许内外网之间的RIP、ospf通信
5. 中心网管不能访问外网
6. 禁止除以上允许的访问以外的其他所有访问
   * **端口配置拓扑图**



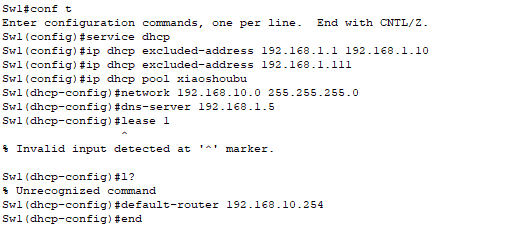
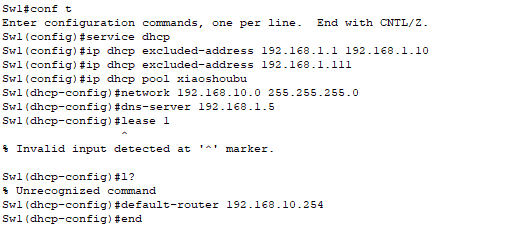
1. **企业网络的实现**
   * **VLAN，多生成树，以太网通道，DHCP**

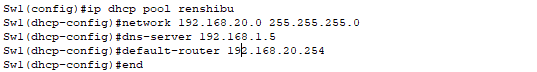
VLAN，多生成树，以太网通道

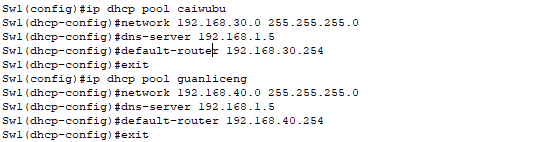
VLAN规划和接入层/汇聚层布置，及多生成树、链路聚合实现与实验1相同。

另外，为方便管理，在三层交换机为每一个VLAN配置DHCP server 让各部门的员工能自动学习到IP地址

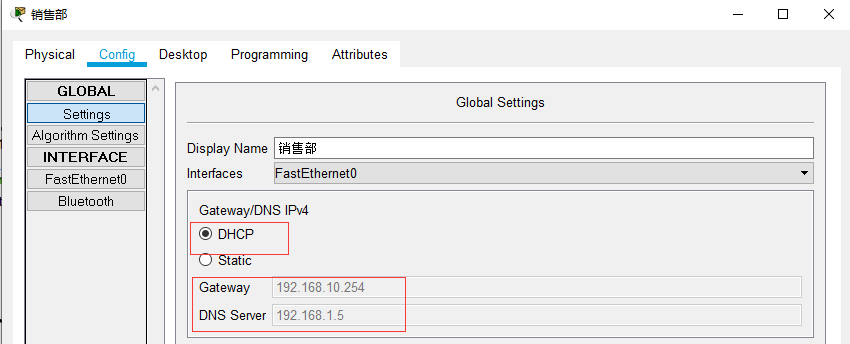
|  |  |  |  |
| --- | --- | --- | --- |
| 三层交换机  D  H  C  P配置 | Sw1 | Sw1#conf t  Sw1(config)#service dhcp  Sw1(config)#ip dhcp excluded-address 192.168.1.1 192.168.1.10  Sw1(config)#ip dhcp excluded-address 192.168.1.111  Sw1(config)#ip dhcp pool xiaoshoubu  Sw1(dhcp-config)#network 192.168.10.0 255.255.255.0  Sw1(dhcp-config)#dns-server 192.168.1.5  Sw1(dhcp-config)#default-router 192.168.10.254  Sw1(dhcp-config)#end  Sw1#conf t  Sw1(config)#ip dhcp pool renshibu  Sw1(dhcp-config)#network 192.168.20.0 255.255.255.0  Sw1(dhcp-config)#dns-server 192.168.1.5  Sw1(dhcp-config)#default-router 192.168.20.254  Sw1(dhcp-config)#end  Sw1#conf t  Sw1(config)#ip dhcp pool caiwubu  Sw1(dhcp-config)#network 192.168.30.0 255.255.255.0  Sw1(dhcp-config)#dns-server 192.168.1.5  Sw1(dhcp-config)#default-router 192.168.30.254  Sw1(dhcp-config)#exit  Sw1(config)#ip dhcp pool guanliceng  Sw1(dhcp-config)#network 192.168.40.0 255.255.255.0  Sw1(dhcp-config)#dns-server 192.168.1.5  Sw1(dhcp-config)#default-router 192.168.40.254  Sw1(dhcp-config)#exit | 开启DHCP服务  指定保留地址（公用设备及中心网管的）段  创建销售部地址池  指定要通过DHCP分配的网段  指定dns server  指定默认路由  创建人事部地址池  创建财务部地址池  创建管理层地址池 |

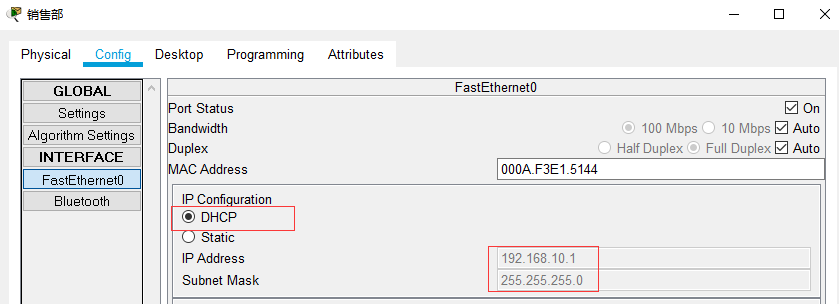






配置完成，接入设备开启DHCP，成功获取默认网关，dns及ip地址





* + **静态路由，RIP，OSPF，连通测试**

路由配置

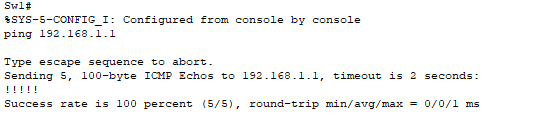
为switch1配置静态路由，使其默认网关为路由器R0

|  |  |  |  |
| --- | --- | --- | --- |
| 静态路由 | Sw1 | Sw1(config)#ip route 0.0.0.0 0.0.0.0 192.168.1.1 | 指定默认网关 |

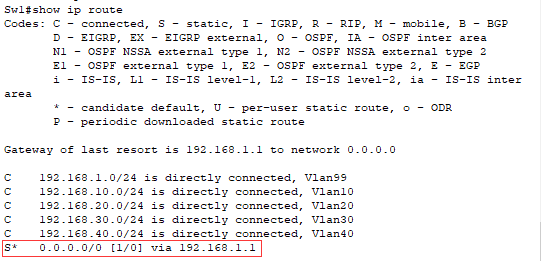


注意：由于三层交换机处理VLAN间路由，路由器不具备处理trunk数据包的能力。因此，需注意与路由器相连的交换机接口应划入与路由器接口所在网段对应的VLAN，而不是使用trunk模式。而互连的交换机之间所属的VLAN应相同或都设置为trunk模式

从交换机sw1到出口路由器的连通测试，可见静态路由生效：

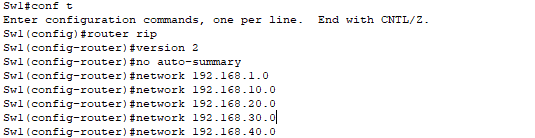


查看sw1路由表如下

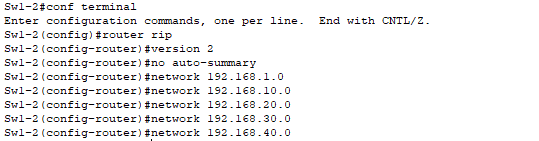


路由器R1与交换机之间使用RIP协议

|  |  |  |  |
| --- | --- | --- | --- |
| R1与交换机之间配置RIP协议 | Sw1 | Sw1#conf t  Sw1(config)#router rip  Sw1(config-router)#version 2  Sw1(config-router)#no auto-summary  Sw1(config-router)#network 192.168.1.0  Sw1(config-router)#network 192.168.10.0  Sw1(config-router)#network 192.168.20.0  Sw1(config-router)#network 192.168.30.0  Sw1(config-router)#network 192.168.40.0 | 开启RIP  指定RIP版本  不自动修改  声明直连的网段 |
| R1 | Router0>enable  Router0#conf t  Router0(config)#router rip  Router0(config-router)#version 2  Router0(config-router)#no auto-summary  Router0(config-router)#network 192.168.1.0  Router0(config-router)#end | 开启RIP  指定RIP版本  不自动修改  声明直连的网段 |

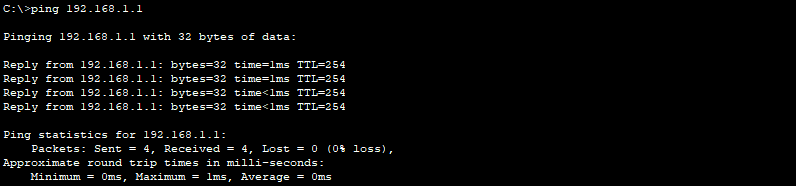






连通测试

销售部ping网关192.168.1.1 连通



路由器之间配置OSPF

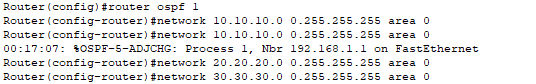
为各路由配置ip地址

|  |  |  |
| --- | --- | --- |
| 路由器配置接口ip地址 | Router0 | Router0(config)#interface FastEthernet0/1  Router0(config-if)#ip address 10.10.10.1 255.0.0.0 |
| Router1 | Router(config)#interface FastEthernet0/0  Router(config-if)#ip address 10.10.10.2 255.0.0.0  Router(config)#interface FastEthernet0/1  Router(config-if)#ip address 20.20.20.2 255.255.255.0  Router(config)#interface FastEthernet1/0  Router(config-if)#ip address 30.30.30.2 255.0.0.0 |
| Router2 | Router(config)#interface FastEthernet0/0  Router(config-if)#ip address 30.30.30.3 255.0.0.0  Router(config)#interface FastEthernet0/1  Router(config-if)#ip address 40.40.40.3 255.0.0.0 |

为各路由配置OSPF

|  |  |  |  |
| --- | --- | --- | --- |
| 路由器配置O  S  P  F | Router0 | Router0(config)#router ospf 1  Router0(config-router)#network 10.10.10.0 0.255.255.255 area 0 | 开启OSPF协议  宣告10.10.10.0网段 |
| Router1 | Router(config)#router ospf 1  Router(config-router)#network 10.10.10.0 0.255.255.255 area 0  Router(config-router)#network 20.20.20.0 0.255.255.255 area 0  Router(config-router)#network 30.30.30.0 0.255.255.255 area 0 | 开启OSPF协议  在area0宣告10.10.10.0，20.20.20.0，30.30.30.0网段 |
| Router2 | Router(config)#router ospf 1  Router(config-router)#network 30.30.30.0 0.255.255.255 area 0  Router(config-router)#network 40.40.40.0 0.255.255.255 area 0 | 开启OSPF协议  宣告30.30.30.0，40.40.40.0网段 |

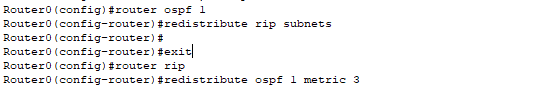






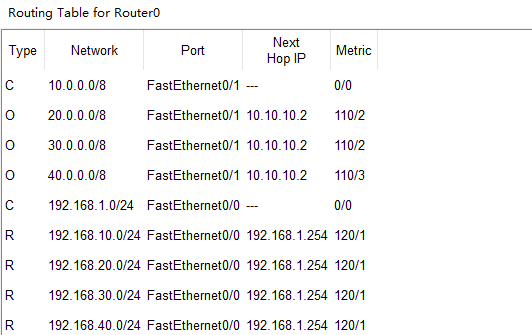
配置Router0的OSPF与rip互通

|  |  |  |  |
| --- | --- | --- | --- |
| 路由协议互通 | Router0 | Router0#conf t  Router0(config)#router ospf 1  Router0(config-router)#redistribute rip subnets  Router0(config-router)#exit  Router0(config)#router rip  Router0(config-router)#redistribute ospf 1 metric 3 | 在OSPF协议中重分发RIP  在RIP协议中重分发OSPF，跳数为3 |

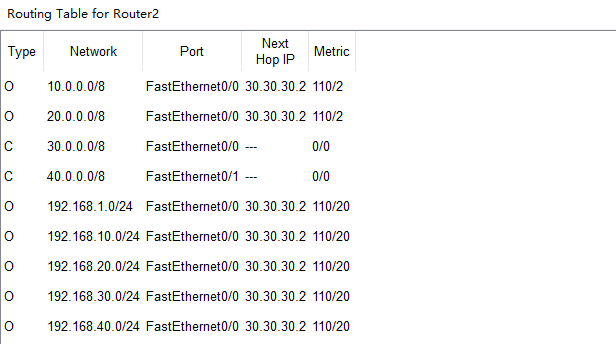


配置完成 查看路由表，可见各网段互通

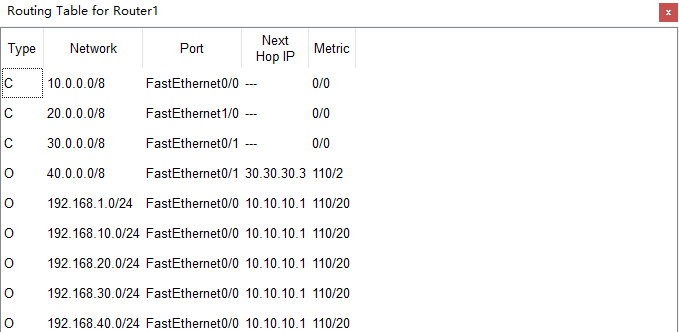
R0通过rip和OSPF学习到的路由表



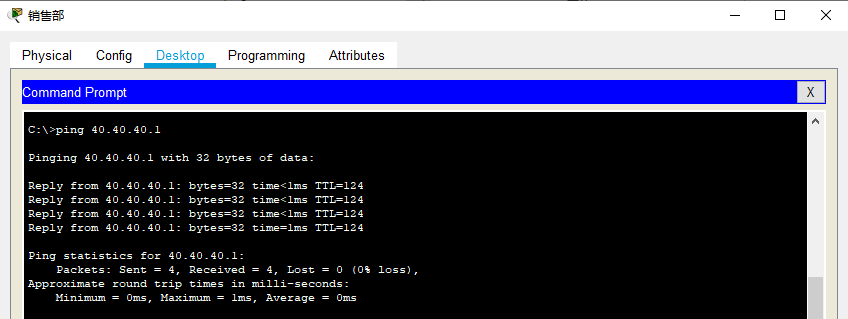
R1通过OSPF学习到的路由表



R2通过OSPF学习到的路由表



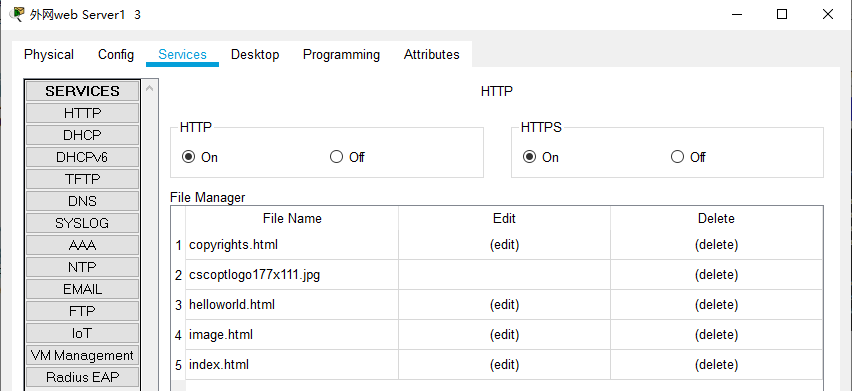
连通测试：局域网内销售部ping最远端路由 连通



* + **NAT网络地址转换配置**

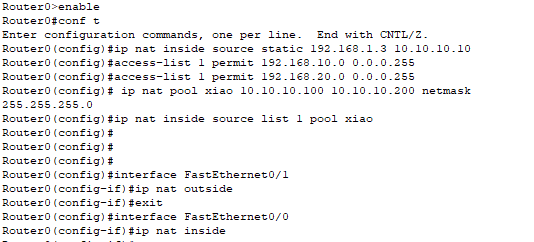
为r0配置NAT 使得外网可访问内网服务器，内网可改变ip访问外网

Web服务器开启http服务

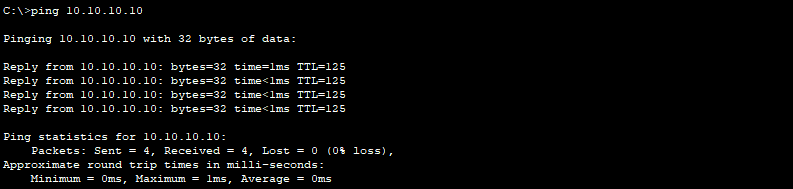


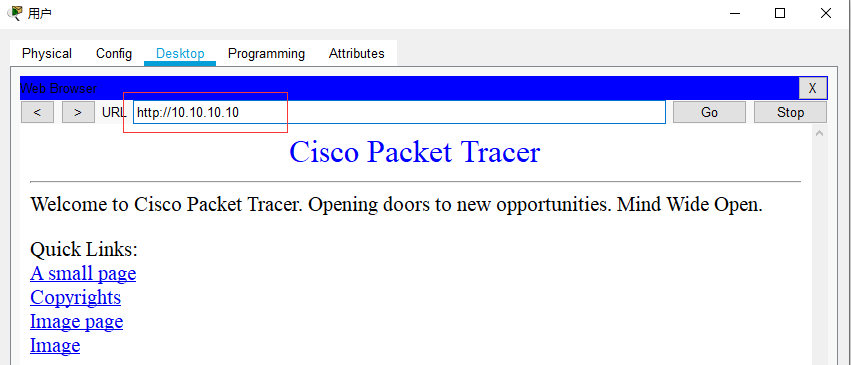
根据地址转换表，配置静态NAT 为web服务器指定外网地址，以供外网用户访问；配置动态NAT 允许销售部和人事部进行动态地址转换访问外网。

|  |  |  |  |
| --- | --- | --- | --- |
| N  A  T配置 | Route0 | Router0>enable  Router0#conf t  Router0(config)#ip nat inside source static 192.168.1.3 10.10.10.10  Router0(config)#access-list 1 permit 192.168.10.0 0.0.0.255  Router0(config)#access-list 1 permit 192.168.20.0 0.0.0.255  Router0(config)# ip nat pool xiao 10.10.10.100 10.10.10.200  netmask 255.255.255.0  Router0(config)#ip nat inside source list 1 pool xiao  Router0(config)#  Router0(config)#interface FastEthernet0/1  Router0(config-if)#ip nat outside  Router0(config-if)#exit  Router0(config)#interface FastEthernet0/0  Router0(config-if)#ip nat inside  Router0(config-if)# | 指定Web Server 静态NAT地址；  允许192.168.10.0、192.168.20.0访问公网；  创建NAT地址池，指定地址范围及子网掩码；  配置动态NAT映射，list1使用地址池xiao；  指定NAT外网接口；  指定NAT内网接口； |



测试1：外网用户访问内网web服务器，成功

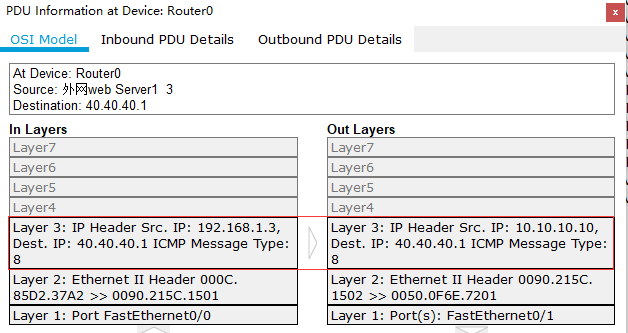




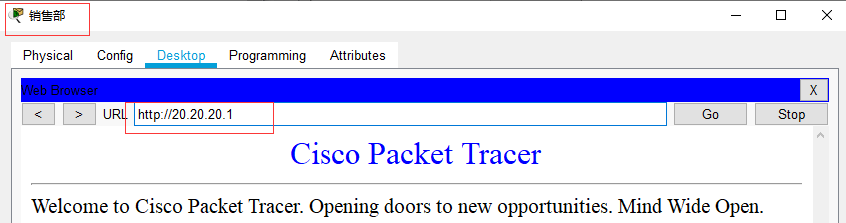
查看Route0 NAT转换表，可见web服务器内外网地址转换



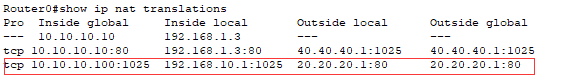
抓包可见web服务器地址转换



测试2：内网销售部用户访问外网web服务器2 成功



查看R0 NAT转换表，可见相应NAT转换记录



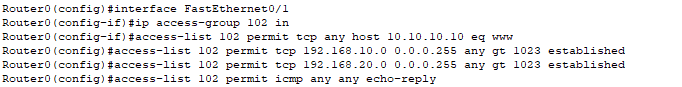
* + **配置ACL访问控制表**

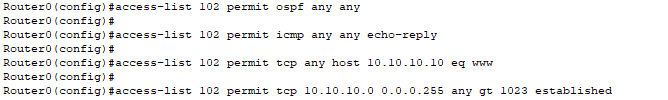
分析访问控制规则

1. 允许外网访问内网Web server 1
2. 允许内网销售部与人事部对外网发起tcp访问
3. 允许内网对外网进行icmp访问测试
4. 允许内外网之间的rip、OSPF通信
5. 中心网管不能访问外网（没有在动态NAT的ip地址转换池中的ip皆无法访问外网，因此已实现）
6. 禁止除以上允许的访问以外的其他所有访问

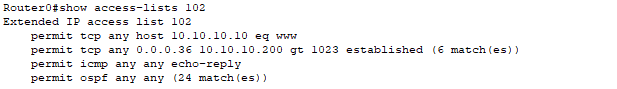
得出访问控制表如下：

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Router0 Fa0/1 in | | | | | |
| 协议类型 | 源地址 | 目的端口 | 目的地址 | 目的端口 | 转发状态 |
| http | Any | Any | 10.10.10.10 | 80 | 允许 |
| Tcp established | 10.10.10.100- 10.10.10.200 | Any | Any | >1023 | 允许 |
| Icmp echo-reply | Any | Any | Any | Any | 允许 |
| OSPF | Any | Any | Any | Any | 允许 |
| Any | Any | Any | Any | Any | 拒绝 |



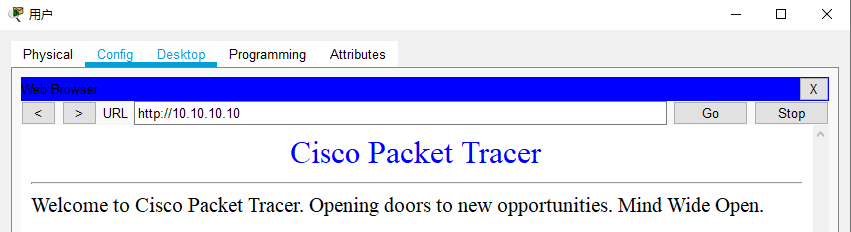


|  |  |  |  |
| --- | --- | --- | --- |
| A  C  L配置 | Router0 | Router0(config)#interface FastEthernet0/1  Router0(config-if)#ip access-group 102 in  Router0(config)#access-list 102 permit ospf any any  Router0(config)#access-list 102 permit icmp any any echo-reply  Router0(config)#access-list 102 permit tcp any host 10.10.10.10 eq www  Router0(config)#access-list 102 permit tcp any 10.10.10.100 10.10.10.200 gt 1023 established |  |

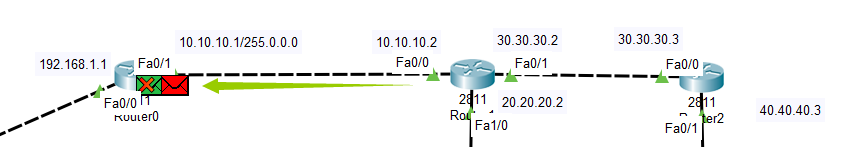


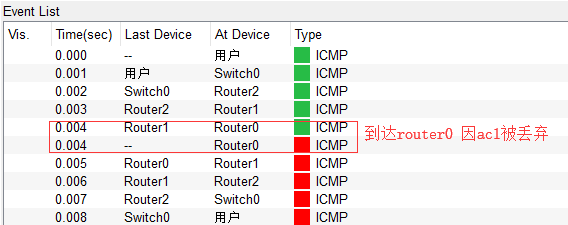
* + **内外网访问测试**

外网用户访问web服务器 成功

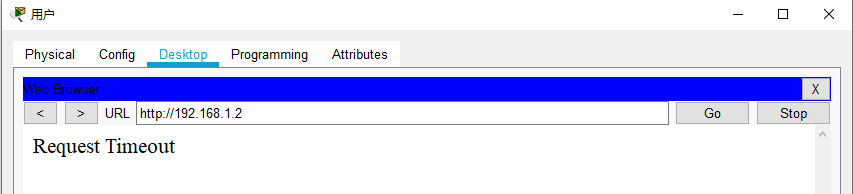


使用外网用户ping web服务器 由于非http，包被丢弃

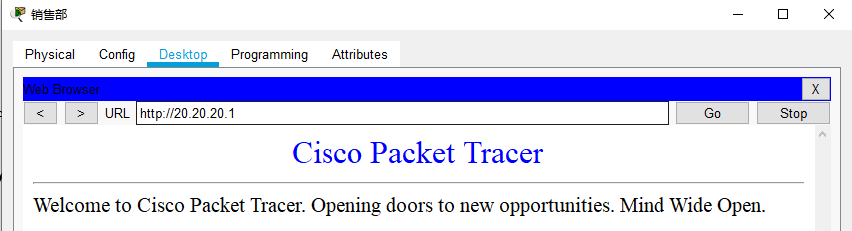




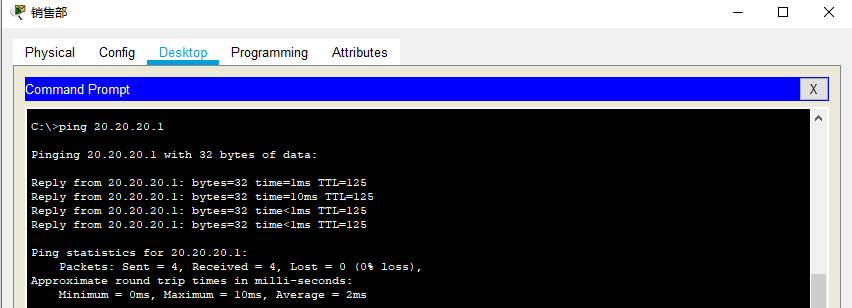
外网用户访问不在ACL允许范围内的内网ftp服务器 失败



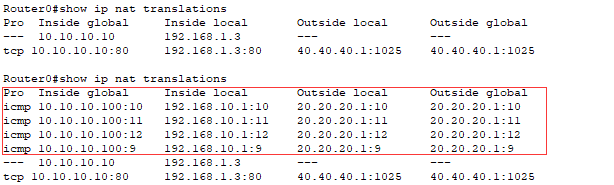
销售部使用http访问外网web服务器2 成功



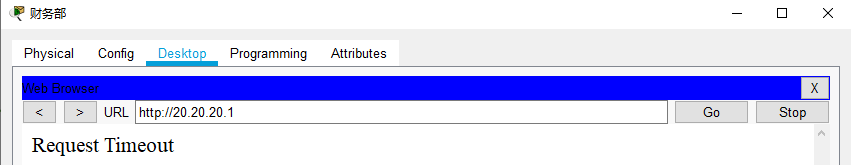
销售部ping 外网web服务器2 成功



查看路由器NAT 可见NAT转换



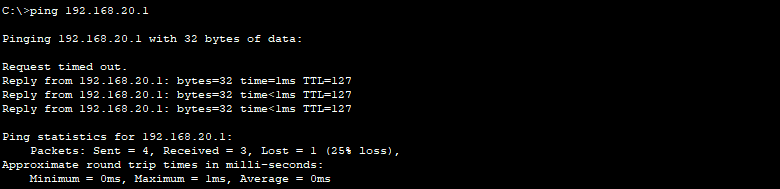
财务部访问外网服务器 由于没有NAT地址转换且不在访问控制表允许范围内，失败



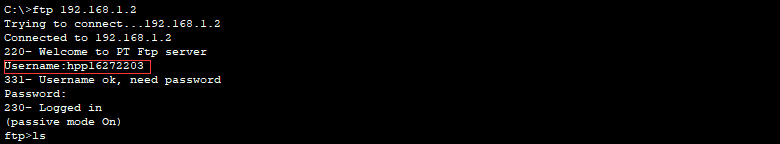
内网设备连接测试



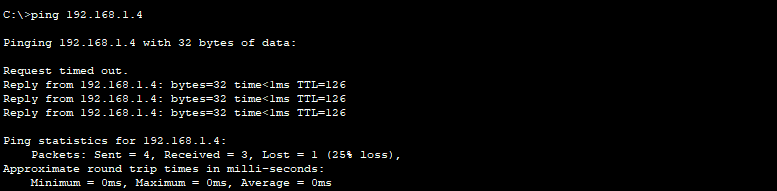
Ping其他VLAN设备 成功



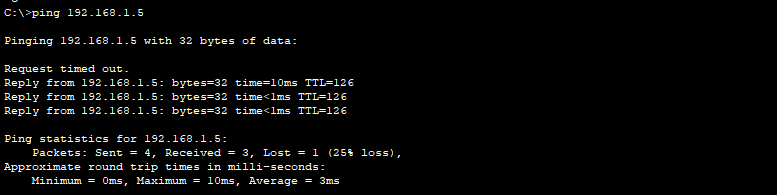
连接ftp 成功



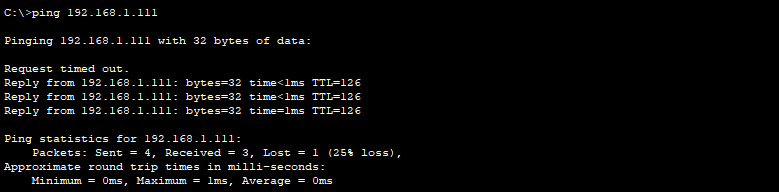
Ping打印机 成功



Ping dns服务器 成功



Ping中心网管 成功



**5.对实验的进一步思考**

黄萍萍：本实验规划了中小型企业的网路拓扑结构，并为其实现各类路由协议，使全网互通。且为网络安全考虑，进行了VLAN划分，NAT网络地址转换，出口路由器ACL访问控制表配置。可防止外网对内网除web服务器以外的访问，及防止外网对内网进行ping扫描，但同时允许部分内网网段对外网进行tcp访问，ping访问。相比在出口路由器上配置ACL，也可在可供外网访问web server接入的核心交换机上配置ACL，做DMZ的划分。另外，还可以在内部交换机配置ACL，限制内网不同VLAN对内网不同设备的访问。配置路由器ACL需注意运行路由协议包，如rip，OSPF等通过，否则会造成路由器无法正确学习到完整路由表。路由协议配置中，不同的AS可使用不同的路由协议，只需两者边界的路由器能使不同协议数据互相告知即可。

**6.参考文献**

**7.团队分工**

**8.附录（程序代码、图表等）**