

计算机网络综合实验报告

——中型企业网络设计与实施



同济大学
TONGJI UNIVERSITY

院 系 _____ 电子与信息工程学院 _____

专 业 _____ 计算机科学与技术 _____

授课老师 _____ 蒋海鹰 _____

成 员 1 _____ 2153812 彭兆祥 _____

成 员 2 _____ 2152118 史君宝 _____

成 员 3 _____ 2159195 岑子威 _____

实验批次 _____ 第 1 批 第 12 组 _____

完成日期 _____ 2024. 5. 28 _____

一、实验名称

中型企业网络设计与实施

二、实验目的

综合路由器以及两层、三层交换机的网络技术进行实验，在完成中小型企业网络设计与实施的过程中，全面掌握计算机网络通信技术的原理及实现步骤。具体目标为进行网络地址规划，使得网段且以最节约地址的方式且子网地址连续做 ip 地址规划，企业内部的 pc 都自动获得 ip 地址，企业内部 pc 都通过合法地址接入到外网。

三、背景描述

假设现有某企业网，有三层交换机一台，二层交换机一台，路由器一台。企业网采用三层架构，二层和三层交换机连接采用聚合方式。

企业技术部(15 台)、财务部门(4 台)分属不同的 VLAN，企业申请了中国电信两个合法 ip 地址：100.10.10.1/24、100.10.10.2/24。




注：拓扑图中企业内部所有地址都来源于 192.168.x.0（其中 x=批号*20+组号如第一批第五小组 x 就等于 25）网段且以最节约地址的方式做连续 ip 地址规划。

需求：

在企业内部所有计算机都能自动获得 Ip 地址且能互相访问，除财务部门以外且都能访问互联网（假定中国电信的一台主机 ip 地址为 200.20.20.20/24，财务部不能访问外网必须使用访问控制列表方式，私有地址不允许出外网）。

四、技术原理

4.1 技术概要

-  两层交换机技术：vlan、端口聚合（或生成树）
-  三层交换机技术：vlan、端口聚合（或生成树）、静态路由、ospf、dhcp 中继
-  内网路由器技术：ospf、dhcp server、访问控制列表、静态路由、NAT 网络地址转换

4.2 技术详解

Vlan

Vlan（虚拟局域网）是对连接到的第二层交换机端口的网络用户的逻辑分段，不受网络用户的物理位置限制而根据用户需求进行网络分段。一个 Vlan 可以在一个交换机或者跨交换机实现。Vlan

可以根据网络用户的位置、作用、部门或者根据网络用户所使用的应用程序和协议来进行分组。基于交换机的虚拟局域网能够为局域网解决冲突域、广播域、带宽问题。

Vlan 最大的特性是不受物理位置的限制,可以进行灵活的划分。Vlan 具备了一个物理网段所具备的特性。相同 Vlan 内的主机可以互相直接访问,不同 Vlan 间的主机之间互相访问必须经由路由设备进行转发。广播数据包只可以在本 Vlan 内进行传播,不能传输到其他 Vlan 中。

端口聚合

端口/链路聚合,是指把交换机上多个物理端口捆绑合成一个逻辑端口(称为 Aggregate Port),这样在交换机之间形成一条拥有较大宽带的链路(ether channel),还可以实现负载均衡,并提供冗余链路。

提高链路带宽,当交换机之间存在多条冗余链路,由于生成树的原因,实际带宽仍只有一条物理链路的带宽,很容易形成网络瓶颈。采用端口聚合后,单条逻辑链路的带宽,等于所有物理链路的总和。

支持负载均衡,可根据报文的 MAC 地址、IP 地址等特征值把流量均匀地分配给各成员链路,避免单根链路流量饱和。

提供链路备份,当一条成员链路断开时,该成员链路的流量将自动地分配到其它有效成员链路上去。

防止网络环路,聚合链路组内成员链路收到的广播或者多播报文,将不会被转发到其它成员链路上。

在一个端口汇聚组(channel-group)中,端口号最小的作为主端口,其他的作为成员端口。聚合端口的特性必须一致,包括接口速率、双工模式、链路类型、VLAN 属性等,并且聚合功能需要在链路两端同时配置方能生效。

快速生成树

生成树协议(spanning-tree),作用是在交换网络中提供冗余备份链路,并且解决交换网络中的环路问题。

生成树协议是利用 SPA 算法(生成树算法),在存在交换环路的网络中生成一个没有环路的树形网络。运用该算法将交换网络冗余的备份链路逻辑上断开,当主要链路出现故障时能够自动的切换到备份链路保证数据的正常转发。

生成树协议目前常见的版本有 STP(生成树协议 IEEE 802.1d)、RSTP(快速生成树协议 IEEE 802.1w)、MSTP(多生成树协议 IEEE 802.1s)。

生成树协议的特点是收敛时间长。当主要链路出现故障以后,到切换到备份链路需要 50 秒的时间。

快速生成树协议(RSIP)在生成树协议的基础上增加了两种端口角色：替换端口(alternate Port)和备份端口(backup Port)，分别做为根端口(root Port)和指定端口(designated Port)的冗余端口。当根端口或指定端口出现故障时，冗余端口不需要经过 50 秒的收敛时间，可以直接切换到替换端口或备份端口。从而实现 RSTP 协议小于 1 秒的快速收敛。

静态路由

路由器属于网络层设备，能够根据 IP 包头的信息，选择一条最佳路径，将数据包转发出去。实现不同网段的主机之间的互相访问。

路由器是根据路由表进行选路和转发的。而路由表里就是由一条条的路由信息组成。路由表的产生方式一般有 3 种：

直连路由：给路由器接口配置一个 IP 地址，路由器自动产生本接口 IP 所在网段的路由信息

静态路由：在拓扑结构简单的网络中，网管员通过手工的方式配置本路由器未知网段的路由信息，从而实现不同网段之间的连接。

动态路由：协议学习产生的路由在大规模的网络中，或网络拓扑相对复杂的情况下，通过在路由器上运行动态路由协议，路由器之间互相自动学习产生路由信息。

OSPF

OSPF(Open Shortest Path First, 开放式最短路径优先)协议，是目前网络中应用最广泛的路由协议之一。属于内部网关路由协议，能够适应各种规模的网络环境，是典型的链路状态(link-state)协议。

OSPF 路由协议通过向全网扩散本设备的链路状态信息，使网络中每台设备最终同步一个具有全网链路状态的数据库(LSDB)，然后路由器采用 OSPF 算法，以自己为根，计算到达其他网络的最短路径，最终形成全网路由信息。

OSPF 属于无类路由协议，支持 VLSM(变长子网掩码)。OSPF 是以组播的形式进行链路状态的通告的。

在大模型的网络环境中，OSPF 支持区域的划分，将网络进行合理规划。划分区域时必须存在 area0(骨干区域)。其他区域和骨干区域直接相连，或通过虚链路的方式连接。

DHCP 中继

DHCP 中继代理是在客户端和服务端之间转发 DHCP 数据包的主机或路由器。网络管理员可以使用 SD-WAN 设备的 DHCP 中继服务在本地 DHCP 客户端和远程 DHCP 服务器之间中继请求和答复。它允许本地主机从远程 DHCP 服务器获取动态 IP 地址。中继代理接收 DHCP 消息并生成要在另一个接口上发出的新 DHCP 消息。

DHCP Server

DHCP (Dynamic Host Configuration Protocol,动态主机配置协议) 通常被用在大型的局域网络中, 主要作用是集中的管理, 分配 IP 地址, 使网络环境中的主机动态的获得 IP 地址, Gateway 地址, DNS 服务器地址等信息, 并能够提升地址的使用率。DHCP 协议的服务分为两个部份: 一个是服务器端, 而另一个是客户端。所有的 IP 网络设定数据都由 DHCP 服务器集中管理, 并负责处理客户端的 DHCP 要求; 而客户端则会使用从服务器分配下来的 IP 环境数据。vlan 间的通信必须通过三层转发, 通常有两种方式, 一种是三层交换技术, 另一种就是单臂路由, 三层交换技术更加常用, 具有三层交换技术的交换机, 只要设置完 vlan, 并为每个 vlan 设置一个路由接口, 第三层交换机就会自动把子网内部的数据流限定在子网内, 并通过路由实现子网之间的数据包交换。

访问控制列表

IP ACL(IP 访问控制列表或 IP 访问列表)是实现对流经路由器或交换机的数据包根据一定的规则进行过滤, 从而提高网络可管理性和安全性。

IP ACL 分为两种: 标准 IP 访问列表和扩展 IP 访问列表。

标准 IP 访问列表可以根据数据包的源 IP 地址定义规则,进行数据包的过滤

扩展 IP 访问列表可以根据数据包的源 IP、目的 IP、源端口、目的端口、协议来定义规则, 进行数据包的过滤。

IP ACL 基于接口进行规则的应用, 分为: 入栈应用和出栈应用。

入栈应用是指由外部经该接口进行路由器的数据包进行过滤。

出栈应用是指路由器从该接口向外转发数据时进行数据包的过滤。

NAT 网络地址转换

NAT 地址转换技术, 就是在局域网内部网络中使用内部私有地址, 而当内部中使用私有 IP 地址网络中计算机, 需要与外部 Internet 网络进行通讯时, 就在网关(可以理解为出口)处, 将内部地址替换成公用地址, 从而保证了内部网络和在外部公网(Internet)之间正常通讯。NAT 技术可以使更多的局域网内的多台计算机共享 Internet 连接, 这一功能很好地解决了公共 IP 地址紧缺的问题。

五、实现功能

网段以最节约地址的方式且子网地址连续做 ip 地址规划

企业内部的 pc 都自动获得 ip 地址, 企业内部 pc 都通过合法地址接入到外网

在企业内部所有计算机都能互相访问

除财务部门以外且都能访问外部主机 PC3

六、实验设备

S2126 双层交换机（1 台）、S3760 三层交换机（1 台）、R1700 路由器（2 台）、主机（3 台）、交叉线或直连线（若干）。

七、实验拓扑

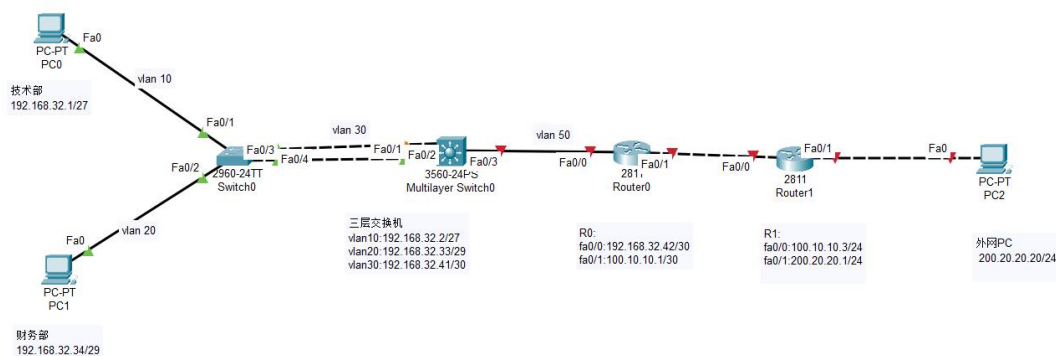


表 7.1 地址规划表

设备名称	设备地址	端口连接
S3760-1	VLAN10: 192.168.32.2/27	F0/1 连接到双层交换机的 F0/3 F0/2 连接到双层交换机的 F0/4
	VLAN20: 192.168.32.33/29	F0/1 连接到双层交换机的 F0/3 F0/2 连接到双层交换机的 F0/4
	VLAN50: 192.168.32.41/30	F0/3 连接到内网路由器的 F1/0
S2126G-1		F0/3 连接到三层交换机的 F0/1 F0/4 连接到三层交换机的 F0/2 F0/1 连接到 PC1 F0/2 连接到 PC2
R1700-1	F1/0: 192.168.32.42/30	F1/0 连接到三层交换机的 F0/3
	F1/1: 100.10.10.1/29	F1/1 连接到外网路由器的 F1/0
R1700-2	F1/1: 200.20.20.1/24	F1/0 连接到内网路由器的 F1/0

	F1/0:100.10.10.3/24	F1/1 连接到 PC3
PC1	192.168.32.1/27	
PC2	192.168.32.34/29	
PC3	200.20.20.20/24	

八、实验过程

1、配置三台 PC 机和接线

PC1 作为技术部,接二层交换机 fa0/1 口,设置 IP 地址 192.168.32.1/27,网关 192.168.32.2,掩码 255.255.255.224

PC2 作为财务部,接二层交换机 fa0/2 口,设置 IP 地址 192.168.32.34/29,网关 192.168.32.33,掩码 255.255.255.248

PC3 作为互联网,接外网路由器 fa1/0 口,设置 IP 地址 200.20.20.20/24,网关 200.20.20.1,掩码 255.255.255.0

2、配置双层交换机 vlan,配置聚合端口

3、配置三层交换机 vlan,配置聚合端口

4、三层交换机配置 ospf 路由、dhcp

5、配置内网路由器 (ospf、dhcp server、访问控制列表、NAT)

配置静态路由到 100.10.10.3

6、配置外网路由器 (ip 和 ospf)

7、在内网路由器上,配置访问控制列表

8、测试互联网连通性

九、测试结果

技术部 PC 测试 从 PC0 (技术部) ping 192.168.32.34 (连通) ping 200.20.20.20 (连通)

财务部 PC 测试 从 PC1 (财务部) ping 192.168.32.1 (连通) ping 200.20.20.20 (阻塞)

外部主机 从外部主机 ping 192.168.32.1 (阻塞) ping 192.168.32.34 (阻塞)

十、参考配置

10.1 双层交换机

```
switch#conf t
switch(config)#vlan 10
switch(config-vlan)#exit
switch(config)#vlan 20
switch(config-vlan)#exit
switch(config)#int fa 0/1
switch(config-if)#sw acc vlan 10
switch(config-if)#int fa 0/2
switch(config-if)#sw acc vlan 20
switch(config-if)#exit
switch(config)#int aggr 1
switch(config-if)#sw mode tr
switch(config-if)#exit
switch(config)#int rang fa 0/3-4
switch(config-if-range)#port-group 1
```

10.2 三层交换机

```
switch#conf t
switch(config)#vlan 10
switch(config-vlan)#exit
switch(config)#vlan 20
switch(config-vlan)#exit
switch(config)#vlan 30
switch(config-vlan)#exit
switch(config)#int fa 0/3
switch(config-if)#sw acc vlan 50
switch(config-if)#exit
//配置聚合端口
switch(config)#int aggr 1
switch(config-if)#sw mode tr
switch(config-if)#exit
switch(config)#int rang fa 0/1-2
switch(config-if-range)#port-group 1
switch(config-if-range)#exit
//配置网段接口 ip
switch(config)#int vlan 10
switch(config-if)#ip add 192.168.32.2 255.255.255.224
switch(config-if)#no sh
switch(config-if)#exit
switch(config)#int vlan20
switch(config-if)#ip add 192.168.32.33 255.255.255.248
```



```

switch(config-if)#no sh
switch(config-if)#exit
switch(config)#int vlan 50
switch(config-if)#ip add 192.168.32.41 255.255.255.252
switch(config-if)#no sh
switch(config-if)#exit
//配置 ospf 路由、配置 dhcp、配置静态路由
switch(config)#router ospf
switch(config-router)#network 192.168.32.0 255.255.255.224 area 0
switch(config-router)#network 192.168.32.32 255.255.255.248 area 0
switch(config-router)#network 192.168.32.40 255.255.255.252 area 0
switch(config-router)#end
switch(config)#service dhcp
switch(config)#ip helper-add 192.168.32.42
switch(config)#ip route 0.0.0.0 0.0.0.0 192.168.32.42
//配置静态路由
switch(config)#ip route 0.0.0.0 0.0.0.0 100.10.10.3
    
```

10.3 内部路由器

```

Router1#conf t
Router1(config)#int fa 1/0
Router1(config-if)#ip add 192.168.32.42 255.255.255.252
Router1(config)#no sh
Router1(config)#int fa 1/1
Router1(config-if)#ip add 100.10.10.1 255.255.255.0
Router1(config)#no sh
Router1(config)#router ospf //配置 ospf
Router1(config-router)#network 192.168.32.42 0.0.0.0 area 0
Router1(config-router)#network 100.10.10.0 0.0.0.0 area 0
Router1(config-router)#end
Router1(config)#service dhcp //配置 dhcp vlan10
Router1(config)#ip dhcp pool vlan10
Router1(dhcp-config)#network 192.168.32.0 255.255.255.224
Router1(dhcp-config)#default-router 192.168.32.2
Router1(dhcp-config)#dns-server 8.8.8.8 8.8.2.2
Router1(dhcp-config)#lease 0 1
Router1(dhcp-config)#exit
Router1(config)#service dhcp //配置 dhcp vlan 20
Router1(config)#ip dhcp pool vlan20
Router1(dhcp-config)#network 192.168.32.32 255.255.255.248
Router1(dhcp-config)#default-router 192.168.32.33
Router1(dhcp-config)#dns-server 8.8.8.8 8.8.2.2
    
```

```
Router1(dhcp-config)#lease 0 1
Router1(dhcp-config)#exit

Router1(config)#int fa 1/1 //配置 NAT
Router1(config-if)#ip nat outside
Router1(config)#int fa 1/0 //配置 NAT
Router1(config-if)#ip nat inside
Router1(config-if)#exit
Router1(config)#ip nat pool one 100.10.10.2 100.10.10.2 netmask
255.255.255.0 //配置 NAT
Router1(config)#access-list 1 permit 192.168.32.0 0.0.0.255
Router1(config)#ip nat inside source list 1 pool one overload
//内网路由器上，配置访问控制列表
Router1(config)#access-list 2 deny 192.168.32.32 0.0.0.7
Router1(config)#access-list 2 permit any
Router1(config)#int fa 1/0
Router1(config-if)#ip access-group 2 in
Router1(config-if)#end
```

10.4 外部路由器

```
Router2#conf t
Router2(config)#int fa 1/1
Router2(config-if)#ip add 200.20.20.1 255.255.255.0
Router2(config)#no sh
Router2(config)#int fa 1/0
Router2(config-if)#ip add 100.10.10.3 255.255.255.0
Router2(config)#no sh
```

十一、实验心得

本学期的计算机网络实验具有连贯性和继承性，从最初的交换机配置、路由配置、静态路由配置、OSPF 单区域配置实验，一直到最后的综合实验。前几次实验有源码参考，基本上只需按照书上的代码进行连接即可完成实验。然而，最后一次实验没有提供拓扑图和实验代码参考，需要我们结合前几次的经验和结果自主进行实验。

在综合实验中，我们需要尽可能地节省 IP 地址，因此进行了连续的 IP 地址规划，并结合各个子网下的主机数量需求进行 IP 地址的计算和划分：

技术部（15 台 PC）需要 15 个主机地址、1 个网关地址、1 个广播地址、1 个网段地址，总共 18 个地址。 $2^4 = 16$ ， $2^5 = 32$ ，所以需要 5 个位的主机位，则网络前缀为 $32-5=27$ 位。

在 192.168.32.0/27 网段中，可用地址范围为 192.168.32.1/27 至 192.168.32.30/27，其中 192.168.32.1/27 作为网关，192.168.32.31/27 是广播地址。

财务部（4 台 PC）需要 4 个主机地址、1 个网关地址、1 个广播地址、1 个网段地址，总共 7 个地址。 $2^2 = 4$ ， $2^3 = 8$ ，所以需要 3 个位的主机位，则网络前缀为 $32-3=29$ 位。

在 192.168.32.32/29 网段中，可用地址范围为 192.168.32.33/29 至 192.168.32.38/29，其中 192.168.32.33/29 作为网关，192.168.32.39/29 是广播地址。

三层交换机与路由器之间只需要 2 个可用 IP 地址。

网段为 192.168.32.40/30，可用地址为 192.168.32.41/30 和 192.168.32.42/30，广播地址为 192.168.32.43/30。

对于中小型企业网络的规划和配置，需要特别注意以下几点：接口 IP 的配置：确保接口配置正确，避免接口错误或 IP 地址输入错误；配置步骤的先后顺序：在配置过程中，遵循正确的步骤顺序，避免因步骤错误导致配置失败；阶段性测试：在完成几个主要配置步骤后，及时进行测试。例如，在配置完基本网络设置但未配置访问控制列表前，可以测试所有主机的通信情况。此时，所有内部主机（包括财务部）应该都能相互通信，并能访问互联网；访问控制列表配置：在配置访问控制列表后，再次测试，确保财务部无法访问互联网，而其他主机的通信情况保持正常。通过这些措施，可以及时发现并纠正配置中的错误，确保网络规划和配置的准确性和有效性。