

同济大学计算机系

计算机网络实验报告



实验名称	中型企业网络设计与实施
批 次	第 4 批
组 号	第 7 组
小组成员	
学院（系）	电子与信息工程学院
专 业	计算机科学与技术
任课教师	蒋海鹰
日 期	2023 年 5 月 30 日

1 实验目的

通过配置网络中的各项技术，实现一个复杂网络环境，满足模拟中型企业场景下的实际网络使用要求

2 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，路由器两台。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。

3 技术原理

VLAN 间的通信：虚拟局域网（VLAN）是通过交换机将逻辑上的网络分割成多个虚拟网段。VLAN 间的通信需要路由器来实现，因为每个 VLAN 都被视为一个独立的子网。路由器负责将数据包从源 VLAN 转发到目标 VLAN，实现不同 VLAN 之间的通信。这可以通过三层交换机的虚拟路由功能或路由器的单臂路由功能来实现。

子网规划：子网规划是将 IP 地址空间划分为多个较小的子网，以满足网络需求并有效管理 IP 地址。在规划子网时，我们需要确定每个子网的地址范围和子网掩码。子网掩码用于将 IP 地址分为网络地址和主机地址两部分，以便进行路由和子网内的通信。

OSPF（Open Shortest Path First）：OSPF 是一种内部网关协议（IGP），用于在自治系统内部的路由器之间交换路由信息。OSPF 使用链路状态算法来计算最短路径，并为数据包提供最佳路由。通过在网络中配置 OSPF，路由器可以共享彼此的路由信息，以便实现网络中的动态路由。

数据包过滤：数据包过滤是通过访问控制列表（ACL）来控制网络中数据包的流动。ACL 定义了特定条件下是否允许或禁止数据包通过特定接口或路由器。可以根据源 IP 地址、目标 IP 地址、协议类型、端口号等条件对数据包进行过滤和控制，以保护网络安全和实现网络策略。

NAT（Network Address Translation）：NAT 是一种网络地址转换技术，用于在私有网络和公共网络之间进行地址映射。当私有网络中的主机访问公共网络时，

NAT 会将私有 IP 地址转换为公共 IP 地址，以便数据包能够在公共网络上正确传输。PAT (Port Address Translation) 是一种 NAT 的形式，它通过在转换过程中使用不同的端口号来实现多个内部主机共享一个公共 IP 地址。

DHCP (Dynamic Host Configuration Protocol) : DHCP 是一种自动配置网络设备的协议。DHCP 服务器可以为网络中的设备分配 IP 地址、子网掩码、默认网关和其他网络配置信息。DHCP 服务器通过动态分配和管理 IP 地址池来简化网络管理，并允许设备在连接到网络时自动获取所需的网络配置。

端口聚合: 端口聚合是将多个物理端口组合成一个逻辑端口的技术。通过将多个物理链路捆绑在一起，端口聚合可以提高链路的可靠性和带宽利用率。当一个物理链路出现故障时，端口聚合可以自动将流量转移到其他正常工作的链路上，提供冗余和负载均衡的功能。

4 实现功能

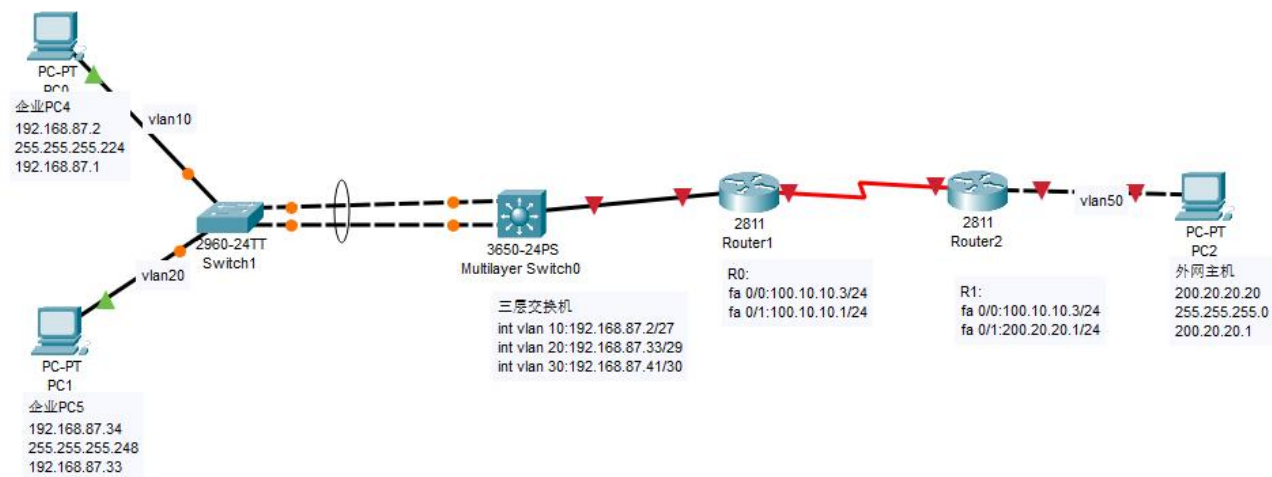
- 在企业内部所有计算机都能互相访问
- 除财务部门以外且都能访问互联网
- 假定中国电信的一台主机 ip 地址为 200.20.20.20/24
- 财务部不能访问外网必须使用访问控制列表方式
- 私有地址不允许出外网

5 实验设备

S3650 三层交换机一台，S2960 二层交换机一台，R2811 路由器两台，若干台 PC 终端

6 网络拓扑图和地址规划

网络拓扑关系图如下:



ip 地址规划如下:

部门	vlan	内部网段	子网掩码	网关	可用 ip 范围
企业服务部	10	192.168.87.0/27	255.255.255.224	192.168.87.1	192.168.87.2-30
财务部	20	192.168.87.32/29	255.255.255.248	192.168.87.33	192.168.87.34-40

7 实验过程

步骤一 配置二层交换机

我们首先对双层交换机进行配置, 将双层交换机的两个端口划分到 vlan10 和 vlan20 中, 实验代码如下:

```

1 switch # configure terminal
2 switch ( config ) # vlan 10
3 switch ( config -vlan ) # exit
4 switch ( config ) # vlan 20
5 switch ( config -vlan ) # exit
6 switch ( config ) # interface fastethernet 0/1
7 switch ( config -if ) # switchport access vlan 10
8 switch ( config -if ) # interface fastethernet 0/2
9 switch ( config -if ) # switchport access vlan 20
10 switch ( config -if ) # exit

```

接下来, 我们对二层交换机的 fa 0/3 端口和 fa 0/4 端口进行聚合, 并将这两个端口设置为 trunk 模式:

```

1 switch ( config ) # interface aggregate port 1
2 switch ( config -if ) # switchport mode trunk

```

```

3 switch ( config - if ) # exit
4 switch ( config ) # interface range fast ethernet 0/3 -4
5 switch ( config -if -range ) # port -group 1

```

步骤二：配置三层交换机 接下来，我们需要对三层交换机进行配置。我们首先在三层交换机上设置 vlan10, vlan20 和 vlan50，并将 fa 0/4 口划入 vlan50 中。

```

1 switch # configure terminal
2 switch ( config ) # vlan 10
3 switch ( config -vlan ) # exit
4 switch ( config ) # vlan 20
5 switch ( config -vlan ) # exit
6 switch ( config ) # vlan 50
7 switch ( config -vlan ) # exit
8 switch ( config ) # int fa 0/4
9 switch ( config -if ) # switchport access vlan 50
10 switch ( config -if ) # exit

```

在这之后，我们需要对三层交换机的 fa 0/1 和 fa 0/2 进行端口聚合。

```

1 switch ( config ) # interface aggregate port 1
2 switch ( config -if ) # switchport mode trunk
3 switch ( config -if ) # exit
4 switch ( config ) # interface fa 0/1 -2
5 switch ( config -if -range ) # port -group 1
6 switch ( config -if -range ) # exit

```

接下来我们在三个 vlan 中配置网关的 ip 地址

```

1 switch ( config ) # interface vlan10
2 switch ( config -if ) # ip address 192 . 168 .87 . 1 255.255.255 .224
3 switch ( config -if ) #no shutdown
4 switch ( config -if ) # exit
5 switch ( config ) # interface vlan20
6 switch ( config -if ) # ip address 192 . 168.87.33 255.255.255 .248
7 switch ( config -if ) #no shutdown
8 switch ( config -if ) # exit
9 switch ( config ) # interface vlan50
10 switch ( config -if ) # ip address 192 . 168.87.41 255.255.255 .252
11 switch ( config -if ) #no shutdown
12 switch ( config -if ) # exit

```

接下来我们在三层交换机上配置 OSPF 协议以及静态路由。

```

1 switch ( config ) # router ospf
2 switch ( config - router ) # network 192 . 168 . 87 . 0 255 . 255 . 255 . 224 area 0
3 switch ( config - router ) # network 192 . 168 . 87 . 32 255 . 255 . 255 . 248 area 0
4 switch ( config - router ) # network 192 . 168 . 87 . 40 255 . 255 . 255 . 252 area 0
5 switch ( config - router ) # end
6
7 switch ( config ) # ip route 0 . 0 . 0 . 0 0 . 0 . 0 . 0 192 . 168 . 87 . 42

```

步骤三：配置内网路由器 在这一步中，我们首先对内网路由器 Router1 进行配置，我们先后配置了 Router1 的 fa 1/0 口和 Serial 1/2 口。

```

1 Router1 # configure terminal
2 Router1 ( config ) # interface fast ethernet 1/0
3 Router1 ( config - if ) # ip address 192 . 168 . 87 . 42 255 . 255 . 255 . 252
4 Router1 ( config - if ) # no shutdown
5 Router1 ( config ) # interface serial 1/2
6 Router1 ( config - if ) # ip address 100 . 10 . 10 . 1 255 . 255 . 255 . 248
7 Router1 ( config - if ) # clock rate 64000
8 Router1 ( config - if ) # no shutdown

```

接下来我们在内网路由器上配置 OSPF 协议

```

1 Router1 ( config ) # router ospf
2 Router1 ( config - router ) # network 192 . 168 . 87 . 42 0 . 0 . 0 . 0 area 0
3 Router1 ( config - router ) # network 100 . 10 . 10 . 0 0 . 0 . 0 . 255 area 0
4 Router1 ( config - router ) # exit

```

步骤四：利用 NAT 作地址映射 在这一步中，我们使用 NAT 将内网地址映射到外网并配置静态路由。

```

1 Router1 ( config ) # interface serial 1/2
2 Router1 ( config - if ) # ip nat outside
3 Router1 ( config ) # interface fast ethernet 1/0
4 Router1 ( config - if ) # ip nat inside
5 Router1 ( config - if ) # exit
6 Router1 ( config ) # ip nat pool onlyone 100 . 10 . 10 . 2 100 . 10 . 10 . 2 netmask
7 255 . 255 . 255 . 0
8 Router1 ( config ) # access - list 1 permit 192 . 168 . 87 . 0 0 . 0 . 0 . 255
9 Router1 ( config ) # ip nat inside source list 1 pool onlyone overload
10
11 Router1 ( config ) # ip route 0 . 0 . 0 . 0 0 . 0 . 0 . 0 100 . 10 . 10 . 3

```

步骤五：配置外网路由 在这一步中，我们对外网路由进行配置。

```
1 Router2# configure terminal
2 Router2 ( config )# interface serial 1/2
3 Router2 ( config - if )# ip address 100.10.10.3 255.255.255.0
4 Router2 ( config - if )#no shutdown
5 Router2 ( config )# interface fastethernet 1/0
6 Router2 ( config - if )# ip address 200.20.20.1 255.255.255.0
7 Router2 ( config - if )#no shutdown
```

步骤六：配置控制访问列表 在这一步中，我们在内网路由器上配置控制访问列表以禁止财务部对外网的访问：

```
1 Router1 ( config )# access - list 2 deny 192.168.87.32 0.0.0.7
2 Router1 ( config )# access - list 2 permit any
3 Router1 ( config )# interface fastethernet 1/0
4 Router1 ( config - if )# ip access -group 2 in
5 Router1 ( config - if )#end
```

步骤七：配置交换机DHCP 在这一步中，配置交换机的DHCP

```
Switch ( config )#server dhcp
1 Switch ( config )# ip helper-address 192.168.87.42
2
```

步骤八：配置路由器的DHCP 在这一步中，我们配置路由器的DHCP

```
Router 1 ( config )# server dhcp
1 Router1 ( config )# ip dhcp pool vlan10
2 Router1 ( dhcp-config )# network 192.18.87.2
3 255.255.255.0
4 Router1 ( dhcp-config )# default-router 192.168.87.1
5 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 )# ip dhcp pool vlan20
Router1 ( dhcp-config )# network 192.18.87.34
255.255.255.0
Router1 ( dhcp-config )# default-router 192.168.87.33
Router1 ( dhcp-config )# dns-server 8.8.8.8 8.8.2.2
Router1 ( dhcp-config )# lease 0 1
```

```
Router1 ( dhcp-config ) # exit
```

步骤九：测试 在这一步中，我们使用三台 PC 机来模拟企业服务部，财务部和外网 PC 机，PC4 代表企业服务部，PC5 代表财务部，PC6 代表外网PC 机。我们分别在每台 PC 机上 ping 另外两台PC。理论上的结果应该是企业服务部既可以访问外网，也可以财务部，财务部只能访问企业服务部；外网无法访问内网。

企业服务部：

```
1 192.168.87.2
2 255.255.255.224
3 192.168.87.1
```

财务部：

```
1 192.168.87.34
2 255.255.255.248
3 192.168.87.33
```

外网：

```
1 200.20.20.20
2 255.255.255.0
3 200.20.20.1
```


8 实验结果

在实验配置结束后，我们对各交换机、路由器的运行情况，各部门的网络联通性进行了测试和展示：

8.1 参考配置

```
interface aggregatePort 1
  switchport mode trunk
!
interface fastEthernet 0/1
  switchport access vlan 10
!
interface fastEthernet 0/2
  switchport access vlan 20
!
interface fastEthernet 0/3
  port-group 1
!
interface fastEthernet 0/4
  port-group 1
!
end
```

图 1: 二层交换机配置结

```
interface FastEthernet 0/2
  port-group 1
!
interface FastEthernet 0/4
  switchport access vlan 50
!
interface Vlan 10
  ip address 192.168.87.1 255.255.255.224
!
interface Vlan 20
  ip address 192.168.87.33 255.255.255.248
!
interface Vlan 50
  ip address 192.168.87.41 255.255.255.252
!
!
router ospf
  area 0.0.0.0
  network 192.168.87.0 255.255.255.224 area 0.0.0.0
  network 192.168.87.0 255.255.255.248 area 0.0.0.0
  network 192.168.87.0 255.255.255.252 area 0.0.0.0
  network 192.168.87.32 255.255.255.248 area 0.0.0.0
  network 192.168.87.40 255.255.255.252 area 0.0.0.0
!
ip route 0.0.0.0 0.0.0.0 Vlan 50 192.168.87.42 1 enabled

end
```

图 2: 三层交换机配置结果

```

R1700-1>en 14
Password:
R1700-1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1700-1(config)#show ip config

% Invalid input detected at '^' marker.

R1700-1(config)#show run\

% Invalid input detected at '^' marker.

R1700-1(config)#exit
R1700-1#
Configured from console by console
R1700-1#show running

Building configuration...
Current configuration : 1448 bytes
!
version 8.52 (building 6)
hostname R1700-1
!
access-list 1 permit 192.168.44.0 0.0.0.255
access-list 1 permit 192.168.87.0 0.0.0.255
access-list 2 deny 192.168.87.32 0.0.0.7
access-list 2 permit any
!
no service password-encryption
!
ip dhcp pool vlan10
  lease 0 1 0
  network 192.168.87.0 255.255.255.224
  dns-server 8.8.8.8 8.8.2.2
  default-router 192.168.87.1
!
ip dhcp pool vlan20
  lease 0 1 0
  network 192.168.87.32 255.255.255.224
  dns-server 8.8.8.8 8.8.2.2
  default-router 192.168.87.33
!

```

```

!
default-router 192.168.87.1

ip dhcp pool vlan20
 lease 0 1 0
 network 192.168.87.32 255.255.255.224
 dns-server 8.8.8.8 8.8.2.2
 default-router 192.168.87.33

!
interface serial 1/2
 ip nat outside
 ip address 100.10.10.1 255.255.255.248
 clock rate 64000

interface serial 1/3
 clock rate 64000

interface FastEthernet 1/0
 ip nat inside
 ip access-group 2 in
 ip address 192.168.87.42 255.255.255.252
 duplex auto
 speed auto

interface FastEthernet 1/1
 ip nat outside
 duplex auto
 speed auto

interface Null 0

ip nat pool onlyone 100.10.10.2 100.10.10.2 netmask 255.255.255.0
ip nat inside source list 1 pool onlyone overload

router ospf
 network 100.10.0.0 0.0.0.255 area 0.0.0.0
 network 100.10.10.0 0.0.0.255 area 0.0.0.0
 network 192.168.44.42 0.0.0.0 area 0.0.0.0
 network 192.168.87.42 0.0.0.0 area 0.0.0.0

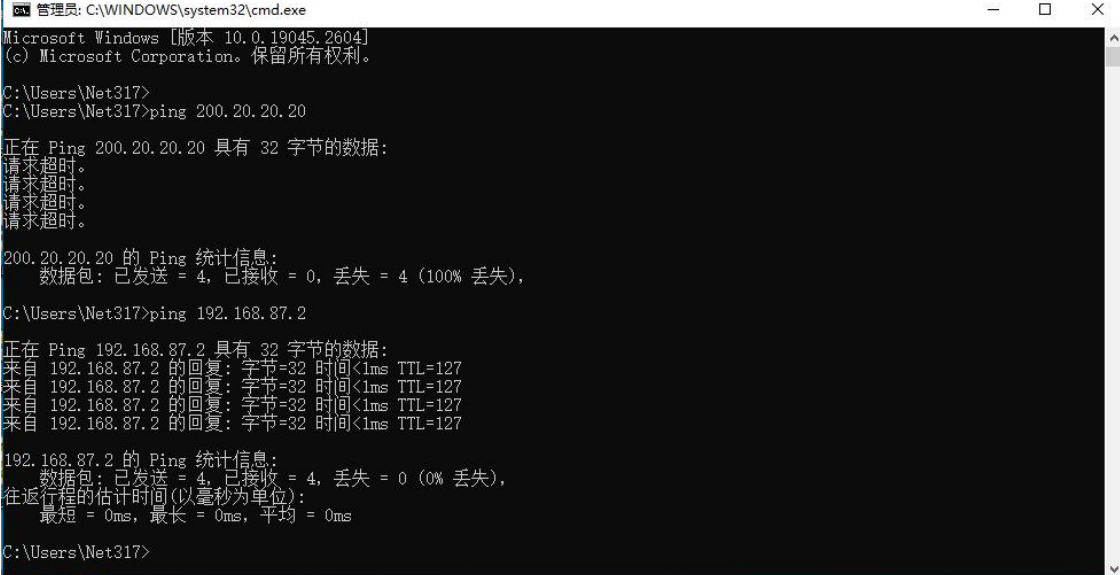
ip route 0.0.0.0 0.0.0.0 100.10.10.3

!
voice-port 2/0
!
voice-port 2/1
!
voice-port 2/2
!
voice-port 2/3
line con 0
line aux 0
line vty 0 4
 login
!
end

```

图 3: Router1 配置结果

8.2 测试结果网络联通性



```
管理员: C:\WINDOWS\system32\cmd.exe
Microsoft Windows [版本 10.0.19045.2604]
(c) Microsoft Corporation。保留所有权利。

C:\Users\Net317>
C:\Users\Net317>ping 200.20.20.20

正在 Ping 200.20.20.20 具有 32 字节的数据:
请求超时。
请求超时。
请求超时。
请求超时。

200.20.20.20 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 0, 丢失 = 4 (100% 丢失),

C:\Users\Net317>ping 192.168.87.2

正在 Ping 192.168.87.2 具有 32 字节的数据:
来自 192.168.87.2 的回复: 字节=32 时间<1ms TTL=127
来自 192.168.87.2 的回复: 字节=32 时间<1ms TTL=127
来自 192.168.87.2 的回复: 字节=32 时间<1ms TTL=127
来自 192.168.87.2 的回复: 字节=32 时间<1ms TTL=127

192.168.87.2 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
    往返行程的估计时间(以毫秒为单位):
        最短 = 0ms, 最长 = 0ms, 平均 = 0ms

C:\Users\Net317>
```

图 5: 财务部门网络联通测试

财务部 财务部能访问企业内的其他计算机，但不能访问外网

```
选择 管理员: C:\WINDOWS\system32\cmd.exe
往返行程的估计时间(以毫秒为单位):
    最短 = 20ms, 最长 = 21ms, 平均 = 20ms

C:\Users\Net317>ping 192.168.87.34

正在 Ping 192.168.87.34 具有 32 字节的数据:
来自 192.168.87.34 的回复: 字节=32 时间<1ms TTL=127
来自 192.168.87.34 的回复: 字节=32 时间<1ms TTL=127
来自 192.168.87.34 的回复: 字节=32 时间<1ms TTL=127
来自 192.168.87.34 的回复: 字节=32 时间<1ms TTL=127

192.168.87.34 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
往返行程的估计时间(以毫秒为单位):
    最短 = 0ms, 最长 = 0ms, 平均 = 0ms

C:\Users\Net317>ping 200.20.20.20

正在 Ping 200.20.20.20 具有 32 字节的数据:
来自 200.20.20.20 的回复: 字节=32 时间=20ms TTL=125
来自 200.20.20.20 的回复: 字节=32 时间=20ms TTL=125
来自 200.20.20.20 的回复: 字节=32 时间=20ms TTL=125
来自 200.20.20.20 的回复: 字节=32 时间=21ms TTL=125

200.20.20.20 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
往返行程的估计时间(以毫秒为单位):
    最短 = 20ms, 最长 = 21ms, 平均 = 20ms

C:\Users\Net317>S-
```

图 6: 企业技术部门网络联通测试

企业技术部 企业技术部分既能访问企业内的其他计算机，也能访问外网

```
管理员: C:\WINDOWS\system32\cmd.exe
Microsoft Windows [版本 10.0.19045.2604]
(c) Microsoft Corporation。保留所有权利。

C:\Users\Net317>ping 192.168.87.2

正在 Ping 192.168.87.2 具有 32 字节的数据:
来自 200.20.20.1 的回复: 无法访问目标主机。
来自 200.20.20.1 的回复: 无法访问目标主机。
来自 200.20.20.1 的回复: 无法访问目标主机。
来自 200.20.20.1 的回复: 无法访问目标主机。

192.168.87.2 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),

C:\Users\Net317>
C:\Users\Net317>
C:\Users\Net317>ping 192.168.87.34

正在 Ping 192.168.87.34 具有 32 字节的数据:
来自 200.20.20.1 的回复: 无法访问目标主机。
来自 200.20.20.1 的回复: 无法访问目标主机。
来自 200.20.20.1 的回复: 无法访问目标主机。
来自 200.20.20.1 的回复: 无法访问目标主机。

192.168.87.34 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),

C:\Users\Net317>
```

图 7: 互联网访问私有地址测试

互联网 外网中的计算机不能访问企业内的计算机

9 实验总结

在完成计算机网络综合实验的过程中，我们对较实用网络的架构和配置有了更深入的理解。通过实验，我们了解了实际使用的网络架构中常见的设备和协议，并学会了配置和管理这些设备。

首先，我们了解到实际使用的网络架构采用了三层架构，其中包括三层交换机、二层交换机和路由器。三层交换机和二层交换机通过聚合方式连接，这样可以提高带宽和冗余度，增强网络的可靠性和性能。

在实验中，我们将不同部门划分为不同的 VLAN，例如企业技术部和财务部门，通过 VLAN 的划分可以实现逻辑上的隔离和安全性控制。我们配置了企业申请的两个合法 IP 地址：100.10.10.1/24 和 100.10.10.2/24。这些 IP 地址用于企业网内部的通信，而企业内部所有地址都来源于 192.168.x.0 网段，其中 x 的计算方式是批号乘以 20 再加上组号。

在实验过程中，我们学会了使用命令行界面或者网络管理软件来配置和管理网络设备，并完成了以下工作：

- **VLAN 间的通信：**实现 VLAN 间的通信需要通过路由器来实现。我们可以利用三层交换机的虚拟路由或者使用路由器的单臂路由来实现子网通信。常用的方式是利用三层交换机的虚拟路由，并将三层交换机和路由器相连的接口加入到相应的 VLAN 中。
- **子网规划：**在进行子网规划时，我们需要考虑网络中包含的不同网段。为了节约地址空间，我们可以从最大的子网开始规划。根据给定的要求，我们可以确定每个网段的地址范围和子网掩码。
- **OSPF：**在配置网络中的三层交换机和内网路由器时，需要确保它们包含对方的路由信息。我们可以使用 OSPF（Open Shortest Path First）或静态路由来实现这一点。建议使用 OSPF，如果三层交换机无法学习到内网路由器的路由信息，可能是链路断开或配置错误的原因，可以通过 ping 测试和检查配置进行排查和修复。
- **数据包过滤：**为了实现特定的网络访问控制，例如禁止财务网段访问外网，我们需要配置访问控制列表（ACL）。在内网路由器上配置 ACL，并将其应用于相应的以太网接口，可以实现对数据包的过滤和控制。
- **NAT：**由于私有地址不能直接访问外网，需要在内网路由器上配置网络地址转换（NAT）。根据给定的情况，选择 PAT（端口地址转换）技术来实现多个

内部地址共享一个公用地址。

- **DHCP**: 本次实验中没有具体涉及到 DHCP 配置,但需要注意 DHCP 服务器的设置和配置。可以将三层交换机作为 DHCP 服务器或 DHCP 中继,也可以使用内部路由器作为 DHCP 服务器。
- **端口聚合**: 在实验中我们学习了端口聚合的配置。可以在两层交换机和三层交换机上进行端口聚合操作,以提高链路的可靠性和带宽利用率。

10 心得体会

通过综合实验的网络配置,我们小组获得了以下几点心得体会:首先,网络配置需要准确的规划和设置。在开始配置之前,仔细研究文档和要求是至关重要的。对于 VLAN 间的通信,我了解到必须通过路由器来实现,并且每个 VLAN 都需要划分为一个网段。子网规划需要考虑地址的节约和可用性,从最大子网开始规划是一个不错的策略。

其次,排查和解决问题需要仔细观察和标注网络拓扑图。在拓扑图中清晰地标注接口、VLAN、IP、网关等信息,有助于迅速定位问题。同时,按照正确的配置顺序进行操作,并仔细检查配置的准确性,以确保网络的正常运行。特别是在涉及到路由器和三层交换机的配置时,检查 OSPF 和路由表的设置是必要的,确保路由信息的正确传递。

此外,灵活运用网络技术和工具对于网络配置和管理非常有帮助。在实验中,我了解到使用 OSPF 可以方便地实现路由信息的交换,使用访问控制列表可以实现数据包的过滤,使用 NAT 可以解决私有地址无法直接访问外网的问题。此外,端口聚合可以提高链路的可靠性和带宽利用率。

在配置过程中,我们遇到了一些挑战和问题。例如,当配置 VLAN 时,需要确保所有相关设备都正确地加入到相应的 VLAN 中,以确保通信的正常进行。此外,配置路由和 ACL 时,需要仔细规划和定义访问控制策略,以满足安全性和性能的需求。

最后,这次实验让我深刻认识到网络配置和管理的重要性。网络是现代通信的核心,良好的网络配置不仅可以提高效率,还可以确保数据的安全和稳定传输。因此,深入了解网络配置和管理的知识是非常有益的,这将对我今后在网络领域的学习和职业发展有着长远的影响。

总之,这次计算机网络综合实验让我们受益匪浅,不仅加深了我们对实际使用的网络架构架构和配置的理解,还提升了我们的网络设备管理技能。我们相信这些知识和经验将对我们今后的学习和职业发展产生积极的影响。