东南大學
SOUTHEAST UNIVERSITY

计算机网络专题实践

总结报告

组　　别 1

学　　号 09020326

姓　　名 何永麟

专　　业 计算机科学与技术

东南大学计算机科学与工程学院

二 0 23 年 4 月

计算机网络专题实践总结报告

1 课程任务及组员信息

1.1 课程任务

实验需求

- 业务需求：
  - 校园网内终端能够互访，能够访问 internet
  - 多个校区网络可以互通
  - 校园网外终端能够访问校内网络
- 安全可靠需求
  - 核心节点故障不影响网络
  - 具有一定防外网攻击能力
- 可维护需求
  - 网络可扩展，可维护
  - 网络故障能快速定位解决

实验任务分解

运用已学的计算机网络理论知识和技术， 利用华为自主研发的交换机和路由器， 自行设计并组建一张满足一定功能需求、性能需求、运维需求的校园园区网。

1. IP 地址规划：规划私网IP 地址，实验室内唯一。
2. VLAN：隔离广播域， PC 机不用二层互通
3. 校区内路由
   - 内网路由：
     - PC 机 DHCP 动态获取 IP 地址
     - 围绕核心交换机 OSPF，校园网内路由互通
     - 核心冗余保护：汇聚接入双核心交换机，节点保护 + 链路保护
   - internet 出口路由：路由器部署 internet 缺省路由
4. Internet 出口：部署 NAT，防火墙。通过东大校园网接入 Internet
5. 校区间路由：不同校区间通过 BGP 发布路由，使用BGP 策略过滤路由
6. 校外终端接入：远程用户 VPN 拨号接入校园网
7. 可维护性：攻防演练

课程目标

- 加深对所学计算机网络理论知识的理解
- 能够综合运用所学知识解决实际网络工程问题
- 提升个人的分析设计能力、工程实践能力、团队协作能力

1.2 组员信息

09020334 黄锦峰 (组长)

09020312 陈鑫　09020326 何永麟　09020329 康镭　09020333 饶梓骞

2 方案设计及任务分工

2.1 方案设计

2.1.1 网络拓扑图

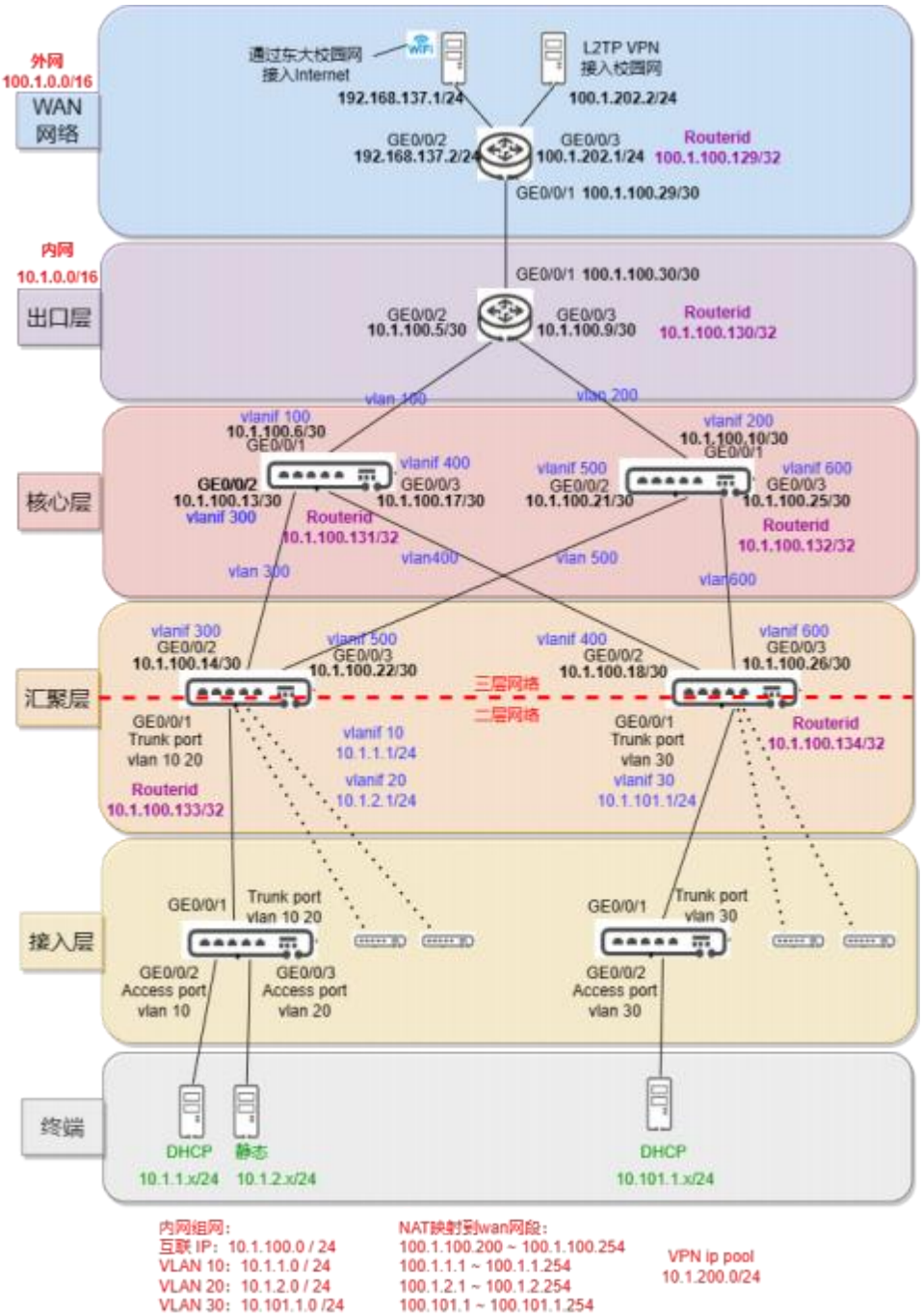

图 1: 网络拓扑图

2.1.2 IP 地址规划 & 各层功能规划

本小组校区内使用一个唯一 16 位网段， 10. 1.0.0/16

- 设备接口互联 IP 地址统一为 10. 1. 100.0/24 网段。
  - 每个接口网段使用其中 30 位前缀网段
  - 启用 OSPF Routerid 使用此网段内剩余 32 位 IP 地址
- 终端 IP 地址使用除 10.x. 100.0/24 网段外的网段
  - 普通终端 IP 地址 DHCP 动态分配；
  - 服务器、特殊终端静态分配，例如摄像头、打印机等终端

每小组校区接运营商网络 100. 1.0.0/16 网段

- 分配与校外网络对接的路由器接口地址，出口 NAT 地址池

设备接口互联 IP 地址，如上图所示，使用了 10. 1. 100.0/24 中前 30 位网段

- vlan 100 10. 1. 100.4/30
- vlan 200 10. 1. 100.8/30
- vlan 300 10. 1. 100. 12/30
- vlan 400 10. 1. 100. 16/30
- vlan 500 10. 1. 100.20/30
- vlan 600 10. 1. 100.24/30

vlan 10 为使用 DHCP 获取 ip 的网段，分配为 10. 1. 1.0/24，

vlan 20 为静态 ip 地址网段，分配为 10. 1.2.0/24，

vlan 30 为另一个区域 DHCP 获取 ip 的网段，分配为 10. 1. 101.0/24。

启用 OSPF ，Routerid 使用此网段内剩余 32 位 IP 地址，如上图所示，使用了

- 10. 1. 100. 130/32
- 10. 1. 100. 131/32
- 10. 1. 100. 132/32
- 10. 1. 100. 133/32
- 10. 1. 100. 134/32

NAT 地址池分配，将设计的内网的网段映射到 100. 1.0.0/16 网段，如下所示：

- 10. 1. 100.0 /24 → 100.1.100.200 ~ 100.1.100.254
- 10. 1. 1.0 /24 → 100.1.1.1 ~ 100.1.1.254
- 10. 1.2.0 /24 → 100.1.2.1 ~ 100.1.2.254
- 10. 1. 101.0 /24 → 100.1.101.1 ~ 100.1.101.254

WAN 层，接口地址分配，如图所示：

- Routerid：100. 1. 100. 129/32
- 路由器接口地址网段为 100. 1. 100.29/30
- 连接共享网络 PC 的接口地址为 192. 168. 137.2/24
- 连接 VPN 服务器的接口地址为 100. 1.202. 1/24

VPN 分配地址池为

- 10. 1.200.0/24

接入层到汇聚层：

- 减少广播域，每个广播域下建议最多接 256 个终端,IP 地址规划需考虑
- 交换机三层网络接口使用 VLANIF，需要预留互联 VLAN
- 接入交换机至汇聚交换机 Trunk 方式通过多个 VLAN
- 汇聚交换机作为终端接入网关, 配置 DHCP 服务和静态配置时需注意

内网路由: 汇聚、核心、出口路由器

- 不同网段之间：汇聚、核心、出口路由器使用 OSPF 发布路由
- OSPF 需要配置 router-id，并部署 area 0 将接口链路状态发布出去，注意反掩码。
- 核心层交换机，还需要破除环路造成的路由循环，使用 undo stp enable ，防止路由循环。

Internet 出口路由: 出口路由器

- 出口路由器设置缺省静态路由，指向运营商出口, 缺省路由通过 OSPF 发布到内网中。
- 运营商路由器部署静态路由，静态进入互联 ip 网段应为 NAT 转化后的地址。
- 为测试防火墙功能，也需要配置到内网 ip 的路由， IP 地址为内网的地址。

Internet 出口规划：运营商路由器

- 出口路由器部署 NAT ，ip 地址池规划，对外网来说内网的 ip 地址是不可见的，但在验证防火墙时，还是 ping 内网的地址，模拟攻击。
- 出口路由器部署 ACL 包过滤防火墙功能，查看私网、公网的 mapping 关系, 防止内网主机被攻击。
- 运营商路由器部署静态路由，静态进入互联 ip 网段应为 NAT 转化后的地址。
- 通过 PC 机共享网络，实现内网主机访问外网，设置静态路由到共享网络。

校区间路由规划： BGP

- 校区间使用 BGP 发布路由, 设置 BGP AS 号，设置 BGP 邻居，发布 BGP 路由。
- 使用 BGP 策略过滤不符合规则路由

校外终端接入： VPN 规划，出口路由器

- 出口路由器部署 L2TP VPN ，PC 使用windows 自带客户端， VPN 接入网络。（或者）出口路由器部署 L2TP VPN 。PC 安装 UniVPN 客户端， VPN 接入网络
- 设置 VPN 对应接入内网的 ip 地址池， VPN 客户端接入后，使用VPN 地址池中的地址。
- 部署 ACL 包过滤防火墙功能， L2TP 用户只能访问PC 机，不能访问摄像头。

2.1.3 效果检验规划

- 各层设备配置检验

```
# 查 看vlan 配 置
display vlan
# 端 口 ip 配 置
display ip interface brief
# 查 看 DHCP 地 址 池 信 息
display ip pool interface vlanif10
# OSPF 配 置
display ospf peer
display ospf routing
display ip routing
```

检查各层设备配置是否正确。

- 内网路由测试

```
PC 机 间 都 能 互 通
各 层 的 设 备 都 能 ping 通 PC
```

内网访问外网路由，共享网络

```
PC ping 通 运 营 商 路 由 器
PC ping 通www .baidu .com 且 都 能 够 上 网
```

外网访问内网，防火墙测试

```
# PC1 ： DHCP 动 态 获 取 IP地 址 ， PC2 ： 静 态 配 置 IP地 址
# 启 用 防 火 墙 ， 查 看ACL 包 过 滤 规 则
运 营 商 路 由 器 ， 能 够 ping 通 PC1 ， 无 法 ping 通 PC2
```

VPN 连接测试

```
# PC1 ： DHCP 动 态 获 取 IP地 址 ， PC2 ： 静 态 配 置 IP地 址 ， PC_vpn ： 用 于VPN连 接 的 主 机
远 程 连 接 的PC_vpn 上 显 示VPN连 接 成 功。
PC_vpn 可 以 访 问 内 网 的 设 备。
部 署 ACL 包 过 滤 防 火 墙 功 能 ， L2TP用 户 只 能 访 问PC1 ， 不 能 访 问PC2
```

BGP 路由测试

```
# 本 小 组 为 BGP AS1
AS1 中 的PC 能 访 问AS2 中 的PC 而 无 法 访 问AS3 中 的PC
AS1 与 AS2 中 的 静 态 配 置 IP地 址 的PC均 不 能 被 访 问
```

2.2 任务分工

表 1: 任务分工

任务	陈鑫	何永麟	康镭	饶梓骞	黄锦峰
IP 地址规划	√	√	√	√	√
VLAN 规划	√	√	√	√	√
DHCP 配置		√		√	
OSPF	√	√		√	√
缺省静态路由			√		√
NAT				√	√
防火墙		√	√		√
PC 机共享网络		√	√	√	
BGP	√				√
L2TP VPN					√

表 2: 配置的设备分工

设备	陈鑫	何永麟	康镭	饶梓骞	黄锦峰	内容
模拟 PC 类普通终端			√	√		DHCP
模拟摄像头类终端			√			静态地址
ace_access_SW_ 1			√			VLAN(access 、 trunk)
ace_access_SW_2			√			VLAN(access 、 trunk)
ace_converge_SW_ 1		√				VLAN 、IP 、DHCP 、OSPF
ace_converge_SW_2				√		VLAN 、IP 、DHCP 、OSPF
ace_Kernel_SW_ 1	√					VLAN 、IP 、OSPF
ace_Kernel_SW_2					√	VLAN 、IP 、OSPF
ace_AR_out					√	IP 、缺省静态路由、 OSPF 、NAT 、防火墙、 BGP 、VPN
ace_AR_wan			√		√	IP、缺省静态路由
PC 机共享网络		√		√		利用东大校园网模拟接到 internet
L2TP 客户端接入					√	VPN

3　个人承担任务的实现

所选设备的配置操作

设备名	Ace_converge_SW_1	
序号	配置的内容	验证序号
1	vlan划分，接口配置，trunk端口配置	1
2	Vlanif配置	2
3	DHCP配置	3
4	OSPF配置	4
5	ACL防火墙配置	5
6	共享网络Internet	6

配置代码

第一次登录设备需要进行的操作，以及每次都需要的save 操作
#先进入无配置的用户文件中
<HUAWEI>startup saved-configuration admintemp.cfg
<HUAWEI>reboot fast
#改名，根据你选取设备的名字
<HUAWEI> system-view
[HUAWEI] sysname 123456

有关保存的操作
<HUAWEI> save 123456.cfg #将当先配置保存进 flash:/ 123456.cfg
<HUAWEI> copy 123456.cfg 123456bk.cfg #备份一下

设置备份文件，可以设置一下，以防不测

3.1 vlan划分以及接口的配置

[Switch_1] vlan batch 10 20 300 500 #交换机上全局开启 VLAN 资源
#进入接口视图
[Switch_1] interface gigabitethernet 0/0/2 #接PC机接口设置access接口，配置缺省VLAN
[Switch_1-GigabitEthernet0/0/2] port link-type access #配置 access 类型
[Switch_1-GigabitEthernet0/0/2] port default vlan 300 #配置缺省 VLAN，VLAN300 关联该端口
[Switch_1-GigabitEthernet0/0/2] quit
[Switch_1] interface gigabitethernet 0/0/3 #接PC机接口设置access接口，配置缺省VLAN
[Switch_1-GigabitEthernet0/0/3] port link-type access #配置 access 类型
[Switch_1-GigabitEthernet0/0/3] port default vlan 500 #配置缺省 VLAN，VLAN300 关联该端口
[Switch_1-GigabitEthernet0/0/3] quit

（trunk接口配置）
#接 ace_coverge_SW_1 接口 设置为 Trunk 接口，并配允许通过的 VLAN
[Switch_1] interface gigabitethernet 0/0/1
[Switch_1-GigabitEthernet0/0/1] port link-type trunk //配置 trunk 类型
[Switch_1-GigabitEthernet0/0/1] port trunk allow-pass vlan 10 20//允许接口上 VLAN 10 20 通过，VLAN 10 20 与这个端口关联了
[Switch_1-GigabitEthernet0/0/1] quit

3.2 vlanif配置

配置 ace_coverge_SW1，交换机需要通过 VLANIF 配置 IP 地址
#与接入层ace_access_SW_1连接的端口
#对应的 VLAN 上启用三层
[Switch_1] interface vlanif 10
[Switch_1-Vlanif10] ip address 10.1.1.1 24
[Switch_1-Vlanif10] quit

[Switch_1] interface vlanif 20
[Switch_1-Vlanif20] ip address 10.1.2.1 24
[Switch_1-Vlanif20] quit

#与核心层ace_Kernel_SW_1连接的端口
#对应的 VLAN 上启用三层
[Switch_1] interface vlanif 300
[Switch_1-Vlanif300] ip address 10.1.100.14 30
[Switch_1-Vlanif300] quit

#与核心层ace_Kernel_SW_2连接的端口，
#对应的 VLAN 上启用三层
[Switch_1] interface vlanif 500
[Switch_1-Vlanif500] ip address 10.1.100.22 30
[Switch_1-Vlanif500] quit

3.3 DHCP配置

1）使能 DHCP Server.
[Switch_1] dhcp enable
2）配置 DHCP 地址池相关信息
已经配置了接口 IP 地址，在此配置基础上增加地址池配置：
[Switch_1] interface vlanif 10
#选择本 VLANIF 接口网段作为 DHCP server 分配的 IP 地址池网段
[Switch_1-Vlanif10] dhcp select interface
#可选，设置 DHCP 分配的网关地址。
[Switch_1-Vlanif10] dhcp server gateway-list 10.1.1.1 //不配置时会自动选择该接口的 ip 地址作为网关地址。
#设置 DHCP 分配的 DNS 服务器地址。
[Switch_1-Vlanif10] dhcp server dns-list 114.114.114.114 //可尝试修改 dns server 地址，抓包/PC 机 ipconfig 可见

3.4 OSPF配置

1） 交换机上启用 OSPF 并发布路由
#配置 ospf router-id ，作为 OSPF 路由器标识。Router-id 网络里唯一，不能冲突
[Switch_1]interface loopback 0
[Switch_1-Loopback0] ip address 10.1.100.133 255.255.255.255
#启动 OSPF 服务
[Switch_1] ospf 1 router-id 10.1.100.133 //1 的作用是进程号，路由器内部使用，用于为
VPN 网络分别不同的独立进程
#配置 OSPF area，本实验仅部署 area 0
[Switch_1-ospf-1] area 0
#与路由器间接口上使能 OSPF，并把这个的接口链路状态发布出去.注意反掩码
[Switch_1-ospf-1-area-0.0.0.0] network 10.1.100.12 0.0.0.3
[Switch_1-ospf-1-area-0.0.0.0] network 10.1.100.20 0.0.0.3
[Switch_1-ospf-1-area-0.0.0.0] network 10.1.1.0 0.0.0.255
[Switch_1-ospf-1-area-0.0.0.0] network 10.1.2.0 0.0.0.255
[Switch_1-ospf-1-area-0.0.0.0] quit
[Switch_1-ospf-1]import-route direct
```

## 3.5 ACL过滤防火墙配置

1.在Router上配置安全区域和安全域间
<Huawei> system-view
[Huawei] firewall zone trust
[Huawei-zone-trust] priority 14
[Huawei-zone-trust] quit
[Huawei] firewall zone untrust
[Huawei-zone-untrust] priority 1
[Huawei-zone-untrust] quit
[Huawei] firewall interzone trust untrust
[Huawei-interzone-trust-untrust] firewall enable
[Huawei-interzone-trust-untrust] quit

2.在Router上配置安全区域和安全域间
[Huawei] interface gigabitethernet 0/0/2 // 1 号核心层交换机区域
[Huawei-GigabitEthernet0/0/0] zone trust
[Huawei-GigabitEthernet0/0/0] quit
[Huawei] interface gigabitethernet 0/0/3 // 2 号核心层交换机区域
[Huawei-GigabitEthernet0/0/1] zone trust
[Huawei-GigabitEthernet0/0/1] quit
[Huawei] interface gigabitethernet 0/0/1 // 外网非信任区域
[Huawei-GigabitEthernet0/0/1] zone untrust
[Huawei-GigabitEthernet0/0/1] quit

3.在Router上配置ACL
[Huawei] acl 3102
[Huawei-acl-adv-3102] rule permit ip destination 10.1.1.0 0.0.0.255
[Huawei-acl-adv-3102] rule permit ip destination 10.101.1.0 0.0.0.255
[Huawei-acl-adv-3102] rule deny ip
```

```
[Huawei-acl-adv-3102] quit
```

4在Router上配置包过滤

```
[Huawei] firewall interzone trust untrust
[Huawei-interzone-trust-untrust] packet-filter 3102 inbound
[Huawei-interzone-trust-untrust] quit
```

5.验证配置结果

```
[Huawei] display firewall interzone trust untrust
interzone trust untrust
 firewall enable
 packet-filter default deny inbound
 packet-filter default permit outbound
 packet-filter 3102 inbound
```

3.6 共享Internet互联网设置

通过校园网Wifi接入Internet

首先选中WLAN，在WLAN属性中点击的共享，打开共享，选择以太网

查看WLAN中的DNS服务器ip地址

设置有线网卡ip地址，DNS服务器地址选择WLAN中的DNS服务器ip地址

IP地址为设计组网时预期的100.1.201.2，子网掩码为24位，默认网关应与IP地址在同一网段。

查看ipv4路由表，此时下一跳为0.0.0.0，所以删除此条，添加10.1.0.0和100.1.0.0的下一跳路由

```
IPv4 路由表
===========================================================================
活动路由:
网络目标        网络掩码          网关       接口   跃点数
          0.0.0.0          0.0.0.0     10.203.128.1   10.203.179.237     50
          0.0.0.0          0.0.0.0    192.168.137.1    192.168.137.3    281
     10.203.128.0    255.255.128.0         在链路上     10.203.179.237    306
   10.203.179.237  255.255.255.255         在链路上     10.203.179.237    306
   10.203.255.255  255.255.255.255         在链路上     10.203.179.237    306
        127.0.0.0        255.0.0.0         在链路上          127.0.0.1    331
        127.0.0.1  255.255.255.255         在链路上          127.0.0.1    331
  127.255.255.255  255.255.255.255         在链路上          127.0.0.1    331
     192.168.59.0    255.255.255.0         在链路上       192.168.59.1    291
     192.168.59.1  255.255.255.255         在链路上       192.168.59.1    291
   192.168.59.255  255.255.255.255         在链路上       192.168.59.1    291
    192.168.127.0    255.255.255.0         在链路上      192.168.127.1    291
    192.168.127.1  255.255.255.255         在链路上      192.168.127.1    291
  192.168.127.255  255.255.255.255         在链路上      192.168.127.1    291
    192.168.137.0    255.255.255.0         在链路上      192.168.137.3    281
    192.168.137.3  255.255.255.255         在链路上      192.168.137.3    281
  192.168.137.255  255.255.255.255         在链路上      192.168.137.3    281
        224.0.0.0        240.0.0.0         在链路上          127.0.0.1    331
        224.0.0.0        240.0.0.0         在链路上      192.168.127.1    291
        224.0.0.0        240.0.0.0         在链路上       192.168.59.1    291
        224.0.0.0        240.0.0.0         在链路上     10.203.179.237    306
        224.0.0.0        240.0.0.0         在链路上      192.168.137.3    281
  255.255.255.255  255.255.255.255         在链路上          127.0.0.1    331
  255.255.255.255  255.255.255.255         在链路上      192.168.127.1    291
  255.255.255.255  255.255.255.255         在链路上       192.168.59.1    291
  255.255.255.255  255.255.255.255         在链路上     10.203.179.237    306
  255.255.255.255  255.255.255.255         在链路上      192.168.137.3    281
===========================================================================
永久路由:
  网络地址          网络掩码  网关地址   跃点数
          0.0.0.0          0.0.0.0      220.10.10.1      默认
          0.0.0.0          0.0.0.0    192.168.137.1      默认
===========================================================================
```

添加后的ipv4路由表如下图所示：

```
IPv4 路由表
===========================================================================
活动路由:
网络目标        网络掩码          网关       接口   跃点数
          0.0.0.0          0.0.0.0     10.203.128.1    10.203.179.237      45
         10.1.0.0      255.255.0.0    192.168.137.2     192.168.137.1      26
     10.203.128.0    255.255.128.0         在链路上     10.203.179.237     301
   10.203.179.237  255.255.255.255         在链路上     10.203.179.237     301
   10.203.255.255  255.255.255.255         在链路上     10.203.179.237     301
       100.1.0.0      255.255.0.0    192.168.137.2     192.168.137.1      26
        127.0.0.0        255.0.0.0         在链路上          127.0.0.1     331
        127.0.0.1  255.255.255.255         在链路上          127.0.0.1     331
  127.255.255.255  255.255.255.255         在链路上          127.0.0.1     331
     192.168.59.0    255.255.255.0         在链路上       192.168.59.1     291
     192.168.59.1  255.255.255.255         在链路上       192.168.59.1     291
   192.168.59.255  255.255.255.255         在链路上       192.168.59.1     291
    192.168.127.0    255.255.255.0         在链路上      192.168.127.1     291
    192.168.127.1  255.255.255.255         在链路上      192.168.127.1     291
  192.168.127.255  255.255.255.255         在链路上      192.168.127.1     291
    192.168.137.0    255.255.255.0         在链路上      192.168.137.1     281
    192.168.137.1  255.255.255.255         在链路上      192.168.137.1     281
  192.168.137.255  255.255.255.255         在链路上      192.168.137.1     281
        224.0.0.0        240.0.0.0         在链路上          127.0.0.1     331
        224.0.0.0        240.0.0.0         在链路上      192.168.127.1     291
        224.0.0.0        240.0.0.0         在链路上       192.168.59.1     291
        224.0.0.0        240.0.0.0         在链路上     10.203.179.237     301
        224.0.0.0        240.0.0.0         在链路上      192.168.137.1     281
  255.255.255.255  255.255.255.255         在链路上          127.0.0.1     331
  255.255.255.255  255.255.255.255         在链路上      192.168.127.1     291
  255.255.255.255  255.255.255.255         在链路上       192.168.59.1     291
  255.255.255.255  255.255.255.255         在链路上     10.203.179.237     301
  255.255.255.255  255.255.255.255         在链路上      192.168.137.1     281
===========================================================================
永久路由:
  无
```

其余为路由操作。

}

4　实现结果测试与分析

4.1 vlan配置，trunk配置

```
[ace_converge_SW_1]disp vlan
The total number of VLANs is: 5
--------------------------------------------------------------------------------
U: Up;         D: Down;         TG: Tagged;         UT: Untagged;
MP: Vlan-mapping;               ST: Vlan-stacking;
#: ProtocolTransparent-vlan;    *: Management-vlan;
--------------------------------------------------------------------------------

VID  Type    Ports
--------------------------------------------------------------------------------
1    common  UT:GE0/0/1(U)      GE0/0/4(D)      GE0/0/5(D)      GE0/0/6(D)
                GE0/0/7(D)      GE0/0/8(D)      GE0/0/9(D)      GE0/0/10(D)
                GE0/0/11(D)     GE0/0/12(D)     GE0/0/13(D)     GE0/0/14(D)
                GE0/0/15(D)     GE0/0/16(D)     GE0/0/17(D)     GE0/0/18(D)
                GE0/0/19(D)     GE0/0/20(D)     GE0/0/21(D)     GE0/0/22(D)
                GE0/0/23(D)     GE0/0/24(D)     GE0/0/25(D)     GE0/0/26(D)
                GE0/0/27(D)     GE0/0/28(D)
10   common  TG:GE0/0/1(U)
20   common  TG:GE0/0/1(U)
300  common  UT:GE0/0/2(U)
500  common  UT:GE0/0/3(U)

VID  Status  Property      MAC-LRN Statistics Description
--------------------------------------------------------------------------------
1    enable  default       enable  disable    VLAN 0001
10   enable  default       enable  disable    VLAN 0010
20   enable  default       enable  disable    VLAN 0020
300  enable  default       enable  disable    VLAN 0300
500  enable  default       enable  disable    VLAN 0500
```

成功配置vlan10 20 300 500 至相应的交换机接口上

4.2 vlanif配置

```
[ace_converge_SW_1]disp ip inter brief
*down: administratively down
^down: standby
(l): loopback
(s): spoofing
(E): E-Trunk down
The number of interface that is UP in Physical is 7
The number of interface that is DOWN in Physical is 1
The number of interface that is UP in Protocol is 6
The number of interface that is DOWN in Protocol is 2

Interface                         IP Address/Mask      Physical   Protocol
LoopBack0                         10.1.100.133/32      up         up(s)
MEth0/0/1                         192.10.20.4/24       down       down
NULL0                             unassigned           up         up(s)
Vlanif1                           unassigned           up         down
Vlanif10                          10.1.1.1/24          up         up
Vlanif20                          10.1.2.1/24          up         up
Vlanif300                         10.1.100.14/30       up         up
Vlanif500                         10.1.100.22/30       up         up
```

```
[ace_converge_SW_1]display ip routing
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
Routing Tables: Public
         Destinations : 30        Routes : 30

Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface

        0.0.0.0/0   O_ASE   150  1           D   10.1.100.21     Vlanif500
       10.1.1.0/24  Direct  0    0           D   10.1.1.1        Vlanif10
       10.1.1.1/32  Direct  0    0           D   127.0.0.1       Vlanif10
       10.1.2.0/24  Direct  0    0           D   10.1.2.1        Vlanif20
       10.1.2.1/32  Direct  0    0           D   127.0.0.1       Vlanif20
     10.1.100.4/30  OSPF    10   2           D   10.1.100.13     Vlanif300
     10.1.100.8/30  OSPF    10   2           D   10.1.100.21     Vlanif500
    10.1.100.12/30  Direct  0    0           D   10.1.100.14     Vlanif300
    10.1.100.14/32  Direct  0    0           D   127.0.0.1       Vlanif300
    10.1.100.16/30  OSPF    10   2           D   10.1.100.13     Vlanif300
    10.1.100.20/30  Direct  0    0           D   10.1.100.22     Vlanif500
    10.1.100.22/32  Direct  0    0           D   127.0.0.1       Vlanif500
    10.1.100.24/30  OSPF    10   2           D   10.1.100.21     Vlanif500
   10.1.100.133/32  Direct  0    0           D   127.0.0.1       LoopBack0
     10.1.101.0/24  OSPF    10   3           D   10.1.100.21     Vlanif500
      10.4.10.0/24  O_ASE   150  1           D   10.1.100.21     Vlanif500
      10.4.20.0/24  O_ASE   150  1           D   10.1.100.21     Vlanif500
      10.4.30.0/24  O_ASE   150  1           D   10.1.100.21     Vlanif500
      10.4.40.0/24  O_ASE   150  1           D   10.1.100.21     Vlanif500
     10.4.100.4/30  O_ASE   150  1           D   10.1.100.21     Vlanif500
     10.4.100.8/30  O_ASE   150  1           D   10.1.100.21     Vlanif500
    10.4.100.12/30  O_ASE   150  1           D   10.1.100.21     Vlanif500
    10.4.100.16/30  O_ASE   150  1           D   10.1.100.21     Vlanif500
    10.4.100.20/30  O_ASE   150  1           D   10.1.100.21     Vlanif500
    10.4.100.24/30  O_ASE   150  1           D   10.1.100.21     Vlanif500
     10.4.220.0/24  O_ASE   150  1           D   10.1.100.21     Vlanif500
   10.4.220.166/32  O_ASE   150  1           D   10.1.100.21     Vlanif500
     100.4.10.0/24  O_ASE   150  1           D   10.1.100.21     Vlanif500
      127.0.0.0/8   Direct  0    0           D   127.0.0.1       InLoopBack0
      127.0.0.1/32  Direct  0    0           D   127.0.0.1       InLoopBack0
```

成功配置vlanif 10 20 300 500，并配置接口ip地址

4.3 DHCP配置

```
[ace_converge_SW_1]display ip pool interface vlanif10
  Pool-name         : Vlanif10
  Pool-No           : 0
  Lease             : 1 Days 0 Hours 0 Minutes
  Domain-name       : -
  DNS-server0       : 114.114.114.114
  NBNS-server0      : -
  Netbios-type      : -
  Position          : Interface
  Status            : Unlocked
  Gateway-0         : 10.1.1.1
  Network           : 10.1.1.0
  Mask              : 255.255.255.0
  VPN instance      : --
  Logging           : Disable
  Conflicted address recycle interval: -
  Address Statistic: Total       :253       Used        :0
                     Idle        :253       Expired     :1
                     Conflict    :0         Disabled    :0

 ------------------------------------------------------------------------------
  Network section
        Start           End       Total    Used Idle(Expired) Conflict Disabled
 ------------------------------------------------------------------------------
       10.1.1.1      10.1.1.254     253       0        253(1)       0     0
 ------------------------------------------------------------------------------
```

进行了vlanif10的DHCP配置，并向下发布

4.4 OSPF配置

查看OSPF是否建立，状态是否为Full状态

```
<ace_converge_SW_1>display ospf peer

         OSPF Process 1 with Router ID 10.1.100.133
                   Neighbors

 Area 0.0.0.0 interface 10.1.100.14(Vlanif300)'s neighbors
 Router ID: 10.1.100.131     Address: 10.1.100.13
   State: Full  Mode:Nbr is  Slave  Priority: 1
   DR: 10.1.100.14  BDR: 10.1.100.13  MTU: 0
   Dead timer due in 35  sec
   Retrans timer interval: 5
   Neighbor is up for 00:04:15
   Authentication Sequence: [ 0 ]

                   Neighbors

 Area 0.0.0.0 interface 10.1.100.22(Vlanif500)'s neighbors
 Router ID: 10.1.100.132     Address: 10.1.100.21
   State: Full  Mode:Nbr is  Slave  Priority: 1
   DR: 10.1.100.22  BDR: 10.1.100.21  MTU: 0
   Dead timer due in 40  sec
   Retrans timer interval: 5
   Neighbor is up for 00:15:02
   Authentication Sequence: [ 0 ]
```

```
<ace_converge_SW_1>display ospf routing

         OSPF Process 1 with Router ID 10.1.100.133
                   Routing Tables

 Routing for Network
 Destination        Cost  Type       NextHop         AdvRouter       Area
 10.1.1.0/24        1     Stub       10.1.1.1        10.1.100.133    0.0.0.0
 10.1.2.0/24        1     Stub       10.1.2.1        10.1.100.133    0.0.0.0
 10.1.100.12/30     1     Transit    10.1.100.14     10.1.100.133    0.0.0.0
 10.1.100.20/30     1     Transit    10.1.100.22     10.1.100.133    0.0.0.0
 10.1.100.133/32    0     Stub       10.1.100.133    10.1.100.133    0.0.0.0
 10.1.100.4/30      2     Stub       10.1.100.13     10.1.100.131    0.0.0.0
 10.1.100.8/30      2     Stub       10.1.100.21     10.1.100.132    0.0.0.0
 10.1.100.16/30     2     Transit    10.1.100.13     10.1.100.134    0.0.0.0
 10.1.100.24/30     2     Transit    10.1.100.21     10.1.100.134    0.0.0.0
 10.1.101.0/24      3     Stub       10.1.100.21     10.1.100.134    0.0.0.0

 Total Nets: 10
 Intra Area: 10  Inter Area: 0  ASE: 0  NSSA: 0
```

```
<ace_converge_SW_1>disp ospf routing

        OSPF Process 1 with Router ID 10.1.100.133
                Routing Tables

 Routing for Network
 Destination        Cost  Type       NextHop         AdvRouter       Area
 10.1.1.0/24        1     Stub       10.1.1.1        10.1.100.133    0.0.0.0
 10.1.2.0/24        1     Stub       10.1.2.1        10.1.100.133    0.0.0.0
 10.1.100.12/30     1     Transit    10.1.100.14     10.1.100.133    0.0.0.0
 10.1.100.20/30     1     Transit    10.1.100.22     10.1.100.133    0.0.0.0
 10.1.100.133/32    0     Stub       10.1.100.133    10.1.100.133    0.0.0.0
 10.1.100.4/30      2     Transit    10.1.100.13     10.1.100.131    0.0.0.0
 10.1.100.8/30      2     Transit    10.1.100.21     10.1.100.132    0.0.0.0
 10.1.100.16/30     2     Transit    10.1.100.13     10.1.100.134    0.0.0.0
 10.1.100.24/30     2     Transit    10.1.100.21     10.1.100.134    0.0.0.0
 10.1.101.0/24      3     Stub       10.1.100.21     10.1.100.134    0.0.0.0

 Routing for ASEs
 Destination        Cost      Type       Tag         NextHop         AdvRouter
 0.0.0.0/0          1         Type2      1           10.1.100.21     10.1.100.130
 10.4.10.0/24       1         Type2      1           10.1.100.21     10.1.100.130
 10.4.20.0/24       1         Type2      1           10.1.100.21     10.1.100.130
 10.4.30.0/24       1         Type2      1           10.1.100.21     10.1.100.130
 10.4.40.0/24       1         Type2      1           10.1.100.21     10.1.100.130
 10.4.100.4/30      1         Type2      1           10.1.100.21     10.1.100.130
 10.4.100.8/30      1         Type2      1           10.1.100.21     10.1.100.130
 10.4.100.12/30     1         Type2      1           10.1.100.21     10.1.100.130
 10.4.100.16/30     1         Type2      1           10.1.100.21     10.1.100.130
 10.4.100.20/30     1         Type2      1           10.1.100.21     10.1.100.130
 10.4.100.24/30     1         Type2      1           10.1.100.21     10.1.100.130
 10.4.220.0/24      1         Type2      1           10.1.100.21     10.1.100.130
 100.4.10.0/24      1         Type2      1           10.1.100.21     10.1.100.130
 100.4.30.0/24      1         Type2      1           10.1.100.21     10.1.100.130

 Total Nets: 24
 Intra Area: 10  Inter Area: 0  ASE: 14  NSSA: 0
```

```
<ace_converge_SW_1> display ip routing
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
Routing Tables: Public
         Destinations : 16        Routes : 16

Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface

       10.1.1.0/24  Direct  0    0           D   10.1.1.1        Vlanif10
       10.1.1.1/32  Direct  0    0           D   127.0.0.1       Vlanif10
       10.1.2.0/24  Direct  0    0           D   10.1.2.1        Vlanif20
       10.1.2.1/32  Direct  0    0           D   127.0.0.1       Vlanif20
     10.1.100.4/30  OSPF    10   2           D   10.1.100.13     Vlanif300
     10.1.100.8/30  OSPF    10   2           D   10.1.100.21     Vlanif500
    10.1.100.12/30  Direct  0    0           D   10.1.100.14     Vlanif300
    10.1.100.14/32  Direct  0    0           D   127.0.0.1       Vlanif300
    10.1.100.16/30  OSPF    10   2           D   10.1.100.13     Vlanif300
    10.1.100.20/30  Direct  0    0           D   10.1.100.22     Vlanif500
    10.1.100.22/32  Direct  0    0           D   127.0.0.1       Vlanif500
    10.1.100.24/30  OSPF    10   2           D   10.1.100.21     Vlanif500
   10.1.100.133/32  Direct  0    0           D   127.0.0.1       LoopBack0
     10.1.101.0/24  OSPF    10   3           D   10.1.100.21     Vlanif500
      127.0.0.0/8   Direct  0    0           D   127.0.0.1       InLoopBack0
      127.0.0.1/32  Direct  0    0           D   127.0.0.1       InLoopBack0
```

```
<ace_converge_SW_1>display ip routing
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
Routing Tables: Public
         Destinations : 17        Routes : 17

Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface

        0.0.0.0/0   O_ASE   150  1           D   10.1.100.21     Vlanif500
       10.1.1.0/24  Direct  0    0           D   10.1.1.1        Vlanif10
       10.1.1.1/32  Direct  0    0           D   127.0.0.1       Vlanif10
       10.1.2.0/24  Direct  0    0           D   10.1.2.1        Vlanif20
       10.1.2.1/32  Direct  0    0           D   127.0.0.1       Vlanif20
     10.1.100.4/30  OSPF    10   2           D   10.1.100.13     Vlanif300
     10.1.100.8/30  OSPF    10   2           D   10.1.100.21     Vlanif500
    10.1.100.12/30  Direct  0    0           D   10.1.100.14     Vlanif300
    10.1.100.14/32  Direct  0    0           D   127.0.0.1       Vlanif300
    10.1.100.16/30  OSPF    10   2           D   10.1.100.13     Vlanif300
    10.1.100.20/30  Direct  0    0           D   10.1.100.22     Vlanif500
    10.1.100.22/32  Direct  0    0           D   127.0.0.1       Vlanif500
    10.1.100.24/30  OSPF    10   2           D   10.1.100.21     Vlanif500
   10.1.100.133/32  Direct  0    0           D   127.0.0.1       LoopBack0
     10.1.101.0/24  OSPF    10   3           D   10.1.100.21     Vlanif500
      127.0.0.0/8   Direct  0    0           D   127.0.0.1       InLoopBack0
      127.0.0.1/32  Direct  0    0           D   127.0.0.1       InLoopBack0
```

汇聚层交换机与核心层交换机之间启动OSPF协议，将接口处的链路状态发布出去，总共能接收到10条路由信息。（连接BGP以后，可以得到其他组网内的ospf路由情况，总共是24条路由信息）

并且能够ping通外网段100.1.100.29的端口

```
C:\Users\86130>ping 100.1.100.29

正在 Ping 100.1.100.29 具有 32 字节的数据:
来自 100.1.100.29 的回复: 字节=32 时间<1ms TTL=252
来自 100.1.100.29 的回复: 字节=32 时间<1ms TTL=252
来自 100.1.100.29 的回复: 字节=32 时间<1ms TTL=252
来自 100.1.100.29 的回复: 字节=32 时间<1ms TTL=252

100.1.100.29 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
```

4.5 防火墙ACL配置测试

不可以ping通静态配置PC端（摄像头）（10.1.2.1）

```
<Router2>ping 10.1.2.1
  PING 10.1.2.1: 56  data bytes, press CTRL_C to break
    Request time out
    Request time out

  --- 10.1.2.1 ping statistics ---
    2 packet(s) transmitted
    0 packet(s) received
    100.00% packet loss
```

可以ping通DHCP配置的PC端（10.1.1.1）

```
<Router2>ping 10.1.1.1
  PING 10.1.1.1: 56  data bytes, press CTRL_C to break
    Reply from 10.1.1.1: bytes=56 Sequence=1 ttl=252 time=1 ms
    Reply from 10.1.1.1: bytes=56 Sequence=2 ttl=252 time=1 ms
    Reply from 10.1.1.1: bytes=56 Sequence=3 ttl=252 time=1 ms
    Reply from 10.1.1.1: bytes=56 Sequence=4 ttl=252 time=1 ms
    Reply from 10.1.1.1: bytes=56 Sequence=5 ttl=252 time=1 ms

  --- 10.1.1.1 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 1/1/1 ms
```

分析：外网只能向指定的网段发送包，发向其他网段的包会被过滤，防火墙acl过滤功能实现

4.6 共享网络测试

从PC机上Ping组内其余PC机以太网的IP地址，可以ping通

```
正在 Ping 10.1.101.230 具有 32 字节的数据:
来自 10.1.101.230 的回复: 字节=32 时间=2ms TTL=60
来自 10.1.101.230 的回复: 字节=32 时间=2ms TTL=60
来自 10.1.101.230 的回复: 字节=32 时间=2ms TTL=60
来自 10.1.101.230 的回复: 字节=32 时间=2ms TTL=60

10.1.101.230 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 = 2ms, 最长 = 2ms, 平均 = 2ms
```

此时，在组内其它电脑中，如下图所示，说明可以上网了

以下为静态DHCP的同学在共享网络后的上网效果展示

此时，组内的动态主机，也可以Ping通www.baidu.com，如下图所示

```
C:\Users\raoziqian>ping www.baidu.com

正在 Ping www.a.shifen.com [180.101.50.188] 具有 32 字节的数据:
来自 180.101.50.188 的回复: 字节=32 时间=26ms TTL=46
来自 180.101.50.188 的回复: 字节=32 时间=32ms TTL=46
来自 180.101.50.188 的回复: 字节=32 时间=11ms TTL=46
来自 180.101.50.188 的回复: 字节=32 时间=18ms TTL=46

180.101.50.188 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 = 11ms, 最长 = 32ms, 平均 = 21ms
```

}

4.7 交换机对内网的ping测试

ping 10.1.1.61

```
<ace_converge_SW_1>ping 10.1.1.61
  PING 10.1.1.61: 56  data bytes, press CTRL_C to break
    Reply from 10.1.1.61: bytes=56 Sequence=1 ttl=128 time=1 ms
    Reply from 10.1.1.61: bytes=56 Sequence=2 ttl=128 time=1 ms
    Reply from 10.1.1.61: bytes=56 Sequence=3 ttl=128 time=1 ms
    Reply from 10.1.1.61: bytes=56 Sequence=4 ttl=128 time=1 ms
    Reply from 10.1.1.61: bytes=56 Sequence=5 ttl=128 time=1 ms

  --- 10.1.1.61 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 1/1/1 ms
```

ping 10.1.2.2

```
<ace_converge_SW_1>ping 10.1.2.2
  PING 10.1.2.2: 56  data bytes, press CTRL_C to break
    Reply from 10.1.2.2: bytes=56 Sequence=1 ttl=128 time=1 ms
    Reply from 10.1.2.2: bytes=56 Sequence=2 ttl=128 time=1 ms
    Reply from 10.1.2.2: bytes=56 Sequence=3 ttl=128 time=1 ms
    Reply from 10.1.2.2: bytes=56 Sequence=4 ttl=128 time=1 ms
    Reply from 10.1.2.2: bytes=56 Sequence=5 ttl=128 time=1 ms

  --- 10.1.2.2 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 1/1/1 ms
```

ping 10.1.101.230

```
<ace_converge_SW_1>ping 10.1.101.230
  PING 10.1.101.230: 56  data bytes, press CTRL_C to break
    Reply from 10.1.101.230: bytes=56 Sequence=1 ttl=62 time=1 ms
    Reply from 10.1.101.230: bytes=56 Sequence=2 ttl=62 time=1 ms
    Reply from 10.1.101.230: bytes=56 Sequence=3 ttl=62 time=1 ms
    Reply from 10.1.101.230: bytes=56 Sequence=4 ttl=62 time=1 ms
    Reply from 10.1.101.230: bytes=56 Sequence=5 ttl=62 time=1 ms

  --- 10.1.101.230 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 1/1/1 ms
```

}

5 心得体会

5.1 vlan划分以及接口的配置

运用上个学期计算机网络课程实验中的相关方法进行汇聚层交换机vlan配置，并配置trunk端口用于接受，进一步了解了vlan和trunk接口和access接口的联系与区别，能够熟练的进行网络的vlan配置，使得物理连接的两台设备甚至多台设备能够有条件的访问。

5.2 vlanif配置

通过vlanif的配置，加深了我对vlanif和vlan 的理解，了解了二层和三层业务的区别以及使用方法，并可以借此配置接口的ip地址。

5.3 DHCP配置

第三部分进行了DHCP的配置。在配置DHCP中，我错误的将对外上传的vlanif 300 500 接口和vlanif 20 接口也进行了DHCP的配置。由于DHCP是向下传递的，目的是可以让PC机通过DHCP获取IP地址，再加上vlan20对应的设备是需要静态地址的摄像头，因此只需要配置vlanif 10 接口的DHCP。

5.4 OSPF配置

第四部分进行了OSPF的路由协议配置，OSPF协议将该交换机上的向外的接口链路状态发布出去，使得该链路状态能被内网中交换机和路由器识别和接收。在配置中错误的将下层的网段也发送出去，可能会造成一定的判别错误。经过理解修改后，将下层链路状态删除。发布结束后可以接收到内网中全部链路状态信息，并且可以由PC机ping通内网所有地址。

5.5 防火墙ACL配置

第五部分进行了acl防火墙过滤的配置。我们先进行了acl过滤规则的学习，了解如何运用acl规则进行包的过滤，并学会了如何开启防火墙进行网络安全防护。我们根据acl规则，设定了外网只能访问10.1.1.0以及10.1.100.0的网段，即是外网只能访问两台可供访问的由DHCP动态分配地址的PC端，内网中摄像头以及交换机路由器则不能被访问。在配置过程中，我们一开始采用了tcp方式进行acl的部署，但是数据包的传送是使用icmp协议的，所以我们应该是采用ip协议进行acl的部署。此外，我们小组在先前的讨论中，因为并没有了解清楚NAT和防火墙的工作顺序，认为外网段不知道内网的网段，所以我们以为acl过滤规则设置的可访问的网段应该是由NAT映射的外网段。但实际上防火墙过滤的实际上是由内网访问外网以后返回的数据包，而在内网向外网发送的时候就已经在NAT上留下了对应的路由信息，返回的数据包可以找到内网的地址。因此防火墙acl过滤规则的可访问地址应该就是内网对应的网段。

5.6 共享网络

在共享互联网的配置中，我们遇到了一些麻烦。一开始按照教程的配置方法我们无法成功进行互联网的共享。经过相应的学习之后，我们发现Internet共享的PC端的ip路由中并没有发向内网网段和外网段的下一跳，因此我们在PC机上进行了10.1.0.0和100.1.0.0的下一跳路由设置，即可共享Internet网络，使得内网中的主机都可以连接上Internet。

附录

A 联系作者

整个项目的文件都在 Github 上，欢迎大家提出意见和建议，或者直接联系我。

Email:756778953@qq.com

项目 Github 地址

B 技术参考文档

交换机产品文档

路由器产品文档

C 各层配置

切换与保存保存

```
# 切换起始文件，为默认的文件
<HUAWEI>startup saved-configuration admintemp .cfg
<HUAWEI>reboot fast

# 保存与备份
<HUAWEI> save xxx .cfg //将当先配置保存进flash :/ xxx
<HUAWEI> copy .cfg xxx .cfg xxxbk .cfg  //备份一下
```

检验

```
# 查看vlan 配置
display vlan
# 端口ip 配置
display ip interface brief
# 查看DHCP 地址池信息
display ip pool interface vlanif30
# OSPF 配置
display ospf peer
display ospf routing
# 查看路由表
display ip routing
display ospf routing
```

C.1 接入层

ace_access_SW_1

```
[] vlan batch 10 20

# 配 置 1 号 端 口 vlan trunk 10 20
[] interface gigabitethernet 0/0/1 //进 入 接 口 视 图
[0/0/1] port link-type trunk // 配 置 trunk 类 型
[0/0/1] port trunk allow-pass vlan 10 20// 允 许 接 口 上VLAN 10 20 通 过
[0/0/1] quit

# 配 置 2 号 端 口 vlan access 10
[] interface gigabitethernet 0/0/2 //进 入 接 口 视 图
[0/0/2] port link-type access // 配 置 access 类 型
[0/0/2] port default vlan 10 // 配 置
[0/0/2] quit

# 配 置 3 号 端 口 vlan access 20
[]interface gigabitethernet 0/0/3
[0/0/3]port link-type access
[0/0/3]port default vlan 20
[0/0/3]quit
```

ace_access_SW_2

```
[]vlan batch 30

# 配 置 1 号 端 口 vlan trunk 30
[]interface gigabitethernet 0/0/1
[0/0/1]port link-type trunk
[0/0/1]port trunk allow-pass vlan 30
[0/0/1]quit

# 配 置 2 号 端 口 vlan access 30
[]interface gigabitethernet 0/0/2
[0/0/2]port link-type access
[0/0/2]port default vlan 30
[0/0/2]quit
```

C.2 汇聚层

ace_converge_SW_1

vlan & vlanif

```
[] vlan batch 10 20 300 500 # 交 换 机 上 全 局 开 启 VLAN 资 源

# access 配 置
[] interface gigabitethernet 0/0/2 #接PC机 接 口 设 置 access 接 口 ， 配 置 缺 省 VLAN
[0/0/2] port link-type access #配 置 access 类 型
[0/0/2] port default vlan 300 #配 置 缺 省 VLAN ， VLAN300 关 联 该 端 口
[0/0/2] quit
```

```
[] interface gigabitethernet 0/0/3 #接PC机 接 口 设 置 access 接 口 ， 配 置 缺 省 VLAN
[0/0/3] port link-type access #配 置 access 类 型
[0/0/3] port default vlan 500 #配 置 缺 省 VLAN ， VLAN300 关 联 该 端 口
[0/0/3] quit

# trunk 配 置
[] interface gigabitethernet 0/0/1
[0/0/1] port link-type trunk // 配 置 trunk 类 型
[0/0/1] port trunk allow-pass vlan 10 20// 允 许 接 口 上VLAN 10 20 通 过
[0/0/1] quit

# vlanif 配 置
# 与 接 入 层 ace_access_SW_1连 接 的 端 口
#对 应 的 VLAN 上 启 用 三 层
[] interface vlanif 10
[Vlanif10] ip address 10.1.1.1 24
[Vlanif10] quit

[] interface vlanif 20
[Vlanif20] ip address 10.1.2.1 24
[Vlanif20] quit

# 与 核 心 层 ace_Kernel_SW_1连 接 的 端 口
#对 应 的 VLAN 上 启 用 三 层
[] interface vlanif 300
[Vlanif300] ip address 10 .1 .100 .14 30
[Vlanif300] quit

# 与 核 心 层 ace_Kernel_SW_2连 接 的 端 口,
#对 应 的 VLAN 上 启 用 三 层
[] interface vlanif 500
[Vlanif500] ip address 10 .1 .100 .22 30
[Vlanif500] quit
```

DHCP 配置

```
# 使 能 DHCP Server .
[] dhcp enable
# 配 置 DHCP 地 址 池 相 关 信 息 ， 已 经 配 置 了 接 口 IP 地 址 ， 在 此 配 置 基 础 上 增 加 地 址 池 配 置:
[] interface vlanif 10
# 选 择 本 VLANIF 接 口 网 段 作 为 DHCP server 分 配 的 IP 地 址 池 网 段
[Vlanif10] dhcp select interface
# 可 选 ， 设 置 DHCP 分 配 的 网 关 地 址。
[Vlanif10] dhcp server gateway-list 10.1.1.1 // 不 配 置 时 自 动 选 择 该 接 口 的 ip 地 址 作 为
    网 关 地 址 。
# 设 置 DHCP 分 配 的 DNS 服 务 器 地 址。
[Vlanif10] dhcp server dns-list 114.114.114.114
```

OSPF 配置

```
# 交 换 机 上 启 用 OSPF 并 发 布 路 由
```

```
# 配置ospf router-id，作为OSPF路由器标识。Router-id网络里唯一，不能冲突
[]interface loopback 0
[Loopback0] ip address 10 .1 .100 .133 255 .255 .255 .255

# 启动OSPF服务
[] ospf 1 router-id 10.1.100.133 //1的作用是进程号

# 配置OSPF area，本实验仅部署area 0
[ospf-1] area 0
#与路由器间接口上使能OSPF，并把这个的接口链路状态发布出去.注意反掩码
[ospf-1-area-0.0.0.0] network 10.1.100.12 0.0.0.3
[ospf-1-area-0.0.0.0] network 10.1.100.20 0.0.0.3
[ospf-1-area-0.0.0.0] network 10.1.1.0 0.0.0.255
[ospf-1-area-0.0.0.0] network 10.1.2.0 0.0.0.255
[ospf-1-area-0.0.0.0] quit
[ospf-1]import-route direct
```

ace_converge_SW_2

vlan & vlanif

```
[] vlan batch 30 400 600

# 1号接口配置Trunk
[]interface gigabitethernet 0/0/1
[] interface gigabitethernet 0/0/1
[0/0/1] port link-type trunk // 配置trunk类型
[0/0/1] port trunk allow-pass vlan 30// 允许接口上VLAN 30通过
[0/0/1] quit

# 2 3号接口配置access
[] interface gigabitethernet 0/0/2 #接口设置access接口，配置缺省VLAN
[0/0/2] port link-type access // 配置access类型
[0/0/2] port default vlan 400 // 配置缺省VLAN，VLAN400与这个端口关联
[0/0/2] quit

[] interface gigabitethernet 0/0/3
[0/0/3] port link-type access // 配置access类型
[0/0/3] port default vlan 600 // 配置缺省VLAN，VLAN400与这个端口关联了
[0/0/3] quit

# vlanif 配置
[] interface vlanif 30 #设置vlanif
[Vlanif30] ip address 10.1.101.1 24 #设置ip地址
[Vlanif30] quit
[] interface vlanif 400
[Vlanif400] ip address 10 .1 .100 .18 30
[Vlanif400] quit
[] interface vlanif 600
[Vlanif600] ip address 10 .1 .100 .26 30
[Vlanif600] quit
```

DHCP

```
[] dhcp enable
[] interface vlanif 30
[Vlanif30] dhcp select interface
[Vlanif30] dhcp server gateway-list 10.1.101.1
[Vlanif30] dhcp server dns-list 114.114.114.114
[Vlanif30] quit
```

OSPF

```
[] interface loopback 0
[LoopBack0] ip address 10 .1 .100 .134 255 .255 .255 .255
[LoopBack0] ospf 1 router-id 10.1.100.134
[ospf-1] area 0
# 与路由器间接口上使能OSPF， 并把这个的接口链路状态发布出去.注意反掩码
[ospf-1-area-0.0.0.0] network 10.1.100.16 0.0.0.3
[ospf-1-area-0.0.0.0] network 10.1.100.24 0.0.0.3
[ospf-1-area-0.0.0.0] network 10.1.101.0 0.0.0.255
```

C.3 核心层

ace_Kernel_SW_1

vlan & vlanif

```
[] vlan batch 100 300 400     // 启用 vlan 100 300 400

[] interface gigabitethernet 0/0/1
[0/0/1] port link-type access
[0/0/1] port default vlan 100

[]interface gigabitethernet 0/0/2
[0/0/2] port link-type access
[0/0/2] port default vlan 300

[]interface gigabitethernet 0/0/3
[0/0/3] port link-type access
[0/0/3] port default vlan 400
# 绑定ip地址
[] interface vlanif 100
[Vlanif200] ip address 10 .1 .100 .6 30
[Vlanif200] quit

[] interface vlanif 300
[Vlanif500] ip address 10 .1 .100 .13 30
[Vlanif500] quit

[] interface vlanif 400
[Vlanif600] ip address 10 .1 .100 .17 30
```

```
[Vlanif600] quit
```

OSPF

```
[] interface loopback 0
[] ip address 10 .1 .100 .131 255 .255 .255 .255
[] ospf 1 router-id 10.1.100.131
[ospf-1] area 0
[ospf-1-area-0.0.0.0] network 10.1.100.6 0.0.0.3
[ospf-1-area-0.0.0.0] network 10.1.100.13 0.0.0.3
[ospf-1-area-0.0.0.0] network 10.1.100.17 0.0.0.3
```

环路

```
[] undo stp enable
```

ace_Kernel_SW_2

vlan & vlanif

```
[] vlan batch 200 500 600     // 启 用 vlan 200 500 600
[] interface gigabitethernet 0/0/1
[0/0/1] port link-type access
[0/0/1] port default vlan 200

[]interface gigabitethernet 0/0/2
[0/0/2] port link-type access
[0/0/2] port default vlan 500

[]interface gigabitethernet 0/0/3
[0/0/3] port link-type access
[0/0/3] port default vlan 600

# 绑 定 ip 地 址
[] interface vlanif 200
[Vlanif200] ip address 10 .1 .100 .10 30
[Vlanif200] quit

[] interface vlanif 500
[Vlanif500] ip address 10 .1 .100 .21 30
[Vlanif500] quit

[] interface vlanif 600
[Vlanif600] ip address 10 .1 .100 .25 30
[Vlanif600] quit
```

ospf

```
[] interface loopback 0
[] ip address 10 .1 .100 .132 255 .255 .255 .255
[] ospf 1 router-id 10.1.100.132
```

```
#配置OSPF area，本实验仅部署area 0
#与路由器间接口上使能OSPF，并把这个的接口链路状态发布出去.
[ospf-1] area 0
注意反掩码
[ospf-1-area-0.0.0.0] network 10.1.100.8 0.0.0.3
[ospf-1-area-0.0.0.0] network 10.1.100.20 0.0.0.3
[ospf-1-area-0.0.0.0] network 10.1.100.24 0.0.0.3
```

环路

```
undo stp enable
```

C.4 出口层

ace_AR_out

ip 配置

```
[] interface gigabitethernet 0/0/1
[0/0/1] undo portswitch // 与AR型号相关，接口缺省是二层口，需要转换为3层口。
[0/0/1] ip address 100.1.100.30 30
[0/0/1] quit
[] interface gigabitethernet 0/0/2
[0/0/2] undo portswitch
[0/0/2] ip address 10.1.100.5 30
[0/0/2] quit
[] interface gigabitethernet 0/0/3
[0/0/3] undo portswitch
[0/0/3] ip address 10.1.100.9 30
[0/0/3] quit
```

OSPF

```
[] interface loopback 0
[] ip address 10.1.100.130 255.255.255.255
[] ospf 1 router-id 10.1.100.130
[ospf-1] area 0
#将下面两个接口的路由发布出去，注意反掩码
[ospf-1-area-0.0.0.0] network 10.1.100.4 0.0.0.3
[ospf-1-area-0.0.0.0] network 10.1.100.8 0.0.0.3
```

路由器设置缺省静态路由指向运营商出口

```
[ace_AR_out] ip route-static 0.0.0.0 0.0.0.0 100.1.100.29 //下一跳地址

#对应的WAN需要回来
[ace_AR_wan] ip route-static 100.1.100.0 255.255.255.0 100.1.100.30
[ace_AR_wan] ip route-static 100.1.1.0 255.255.255.0 100.1.100.30
[ace_AR_wan] ip route-static 100.1.2.0 255.255.255.0 100.1.100.30
[ace_AR_wan] ip route-static 100.1.101.0 255.255.255.0 100.1.100.30
#实现防火墙功能时，进入内网的网段
[ace_AR_wan] ip route-static 10.1.100.0 255.255.255.0 100.1.100.30
```

```
[ace_AR_wan] ip route-static 10 .1 .1 .0 255 .255 .255 .0 100 .1 .100 .30
[ace_AR_wan] ip route-static 10 .1 .2 .0 255 .255 .255 .0 100 .1 .100 .30
[ace_AR_wan] ip route-static 10 .1 .101 .0 255 .255 .255 .0 100 .1 .100 .30

# 配 置 OSPF 将 缺 省 路 由 通 告 到 OSPF路 由 区 域
[] ospf 1 router-id 10.1.100.130
[ospf-1] default-route-advertise always

# 验 证 ： 显 示RouterA 的 IP路 由 表
[] display ip routing-table
# ping 命 令 验 证 连 通 性
# 使 用 **Tracert**命 令 验 证 连 通 性 ， 可 以 查 看 通 过 的 路 由
```

NAT

```
[] nat address-group 1 100 .1 .100 .200 100 .1 .100 .254 // 映 射 出 去 的 网 段
[] acl 2001
[acl-basic-2001] rule 5 permit source 10.1.100.0 0.0.0.255 // 10.1.100.0/24
[acl-basic-2001] quit

[] nat address-group 2 100 .1 .1 .1 100 .1 .1 .254 // 映 射 出 去 的 网 段
[] acl 2002
[acl-basic-2002] rule 5 permit source 10.1.1.0 0.0.0.255 // 10.1.1.0/24
[acl-basic-2002] quit

[] nat address-group 3 100 .1 .2 .1 100 .1 .2 .254 // 映 射 出 去 的 网 段
[] acl 2003
[acl-basic-2003] rule 5 permit source 10.1.2.0 0.0.0.255 // 10.1.2.0/24
[acl-basic-2003] quit

[] nat address-group 4 100 .1 .101 .1 100 .1 .101 .254 // 映 射 出 去 的 网 段
[] acl 2004
[acl-basic-2004] rule 5 permit source 10.1.101.0 0.0.0.255 // 10.1.101.0/24
[acl-basic-2004] quit

[] interface gigabitethernet 0/0/1
[0/0/1] nat outbound 2001 address-group 1
[0/0/1] nat outbound 2002 address-group 2
[0/0/1] nat outbound 2003 address-group 3
[0/0/1] nat outbound 2004 address-group 4
[0/0/1] quit
```

共享网络

. 将 WLAN 设置成共享

ACL 包过滤防火墙功能

```
# 配 置 安 全 区 域 和 安 全 域 间
[] firewall zone trust
[zone-trust] priority 14
[zone-trust] quit

[] firewall zone untrust
```

```
[zone-untrust] priority 1
[zone-untrust] quit

[] firewall interzone trust untrust
[interzone-trust-untrust] firewall enable
[interzone-trust-untrust] quit

[] interface gigabitethernet 0/0/2 // 2 号接口
[0/0/2] zone trust
[0/0/2] quit

[] interface gigabitethernet 0/0/3 // 3 号接口
[0/0/3] zone trust
[0/0/3] quit

[Huawei] interface gigabitethernet 0/0/1 // 外网非信任区域
[0/0/1] zone untrust
[0/0/1] quit

#在AR_out 上配置ACL规则,
[]acl 3102
[acl-adv-3102] rule permit ip destination 100 .1 .1 .0 0 .0 .0 .255 //vlan10
[acl-adv-3102] rule permit ip destination 100 .1 .101 .0 0 .0 .0 .255 //vlan30
[acl-adv-3102] rule deny ip
[acl-adv-3102] quit

# 在Router 上配置包过滤。
[] firewall interzone trust untrust
[interzone-trust-untrust] packet-filter 3102 inbound
[interzone-trust-untrust] quit
[]display firewall interzone trust untrust
```

BGP 策略

```
# 标识自己
[AR_1] bgp 65001 // 自治系统号， 我们是第1组
[AR_1-bgp] router-id 10.1.100.130

# 找到对方路由器， 配置EBGP 连接
[AR_1-bgp] peer [ipB] as-number 65002 //对端 IP 地址， 对端自治系统号

例如： [AR_1-bgp] **peer 172 .16 .1 .2 as-number 65009**

# 查看对等体的连接状态
[AR_1-bgp] display bgp peer


#引入路由， 对外发布。路由协议可以引入多种其他的路由协议， 比如static 静态路由,
    direct 直连路
由,ospf 路由等。 可以根据现网应用情况选择。
[AR_1-bgp] ipv4-family unicast
```

```
[AR_1-bgp-af-ipv4] import-route direct // 引入直连路由
[AR_1-bgp-af-ipv4] import-route ospf 1 // 引入OSPF路由
[AR_1-bgp] quit

# AR1 OSPF 引入 BGP 路由
[AR_1] ospf
[AR_1-ospf-1] import-route bgp

# 测试
[] display bgp routing-table
```

VPN

```
# 配置L2TP用户的用户名为 **huawei** ， 密码为 **123** ， 用户类型固定为 **ppp**
[LNS] aaa
[LNS-aaa] local-user huawei password
123
123
[LNS-aaa] local-user huawei service-type ppp
[LNS-aaa] q

# 定义一个地址池， 为拨入用户分配地址。
[LNS] ip pool lns
[LNS-ip-pool-lns] network 10.1.200.0 mask 24
[LNS-ip-pool-lns] gateway-list 10.1.200.1
[LNS-ip-pool-lns] quit

# 配置虚拟接口模板
[LNS] interface virtual-template 1
[LNS-Virtual-Template1] ip address 10 .1 .200 .1 255 .255 .255 .0
[LNS-Virtual-Template1] ppp authentication-mode chap
[LNS-Virtual-Template1] remote address pool lns
[LNS-Virtual-Template1] quit
# 使能L2TP功能， 并创建L2TP组编号为 **1**。
[LNS] l2tp enable
[LNS] l2tp-group 1

# 禁止隧道认证功能， Windows 10 不支持隧道认证。
[LNS-l2tp1] undo tunnel authentication
# 配置LNS绑定虚拟接口模板。
[LNS-l2tp1] allow l2tp virtual-template 1
```

在 Windows 电脑上配置 L2TP VPN 连接

windows 10 启动 L2TP

C.5 WAN 层

ace_AR_wan

ip 配置

```
[] interface gigabitethernet 0/0/1
```

```
[0/0/1] undo portswitch
[0/0/1] ip address 100 .1 .100 .29 30
[0/0/1] quit
[] interface gigabitethernet 0/0/2
[0/0/2] undo portswitch
[0/0/2] ip address 100.1.201.1 24
[0/0/2] quit
[] interface gigabitethernet 0/0/3
[0/0/3] undo portswitch
[0/0/3] ip address 10.1.202.1 24
[0/0/3] quit

[] interface loopback 0
[Loopback0] ip address 100 .1 .100 .129 255 .255 .255 .255
[Loopback0]quit
# 查 看 ip 配 置
[] display ip interface brief
```

进入内网的静态路由

```
# 对 应 的 WAN 需 要 回 来 的 静 态 路 由
[ace_AR_wan] ip route-static 100 .1 .100 .0 255 .255 .255 .0 100 .1 .100 .30
[ace_AR_wan] ip route-static 100 .1 .1 .0 255 .255 .255 .0 100 .1 .100 .30
[ace_AR_wan] ip route-static 100 .1 .2 .0 255 .255 .255 .0 100 .1 .100 .30
[ace_AR_wan] ip route-static 100 .1 .101 .0 255 .255 .255 .0 100 .1 .100 .30
# 为 测 试 防 火 墙 的 静 态 路 由
[ace_AR_wan] ip route-static 10 .1 .100 .0 255 .255 .255 .0 100 .1 .100 .30
[ace_AR_wan] ip route-static 10 .1 .1 .0 255 .255 .255 .0 100 .1 .100 .30
[ace_AR_wan] ip route-static 10 .1 .2 .0 255 .255 .255 .0 100 .1 .100 .30
[ace_AR_wan] ip route-static 10 .1 .101 .0 255 .255 .255 .0 100 .1 .100 .30
```

走向校园网的缺省静态路由

```
[ace_AR_wan] ip route-static 0 .0 .0 .0 0 .0 .0 .0 100 .1 .201 .2 // 下 一 跳 地 址
[ace_AR_wan] ospf 1 router-id 100.1.100.129
[ospf-1] default-route-advertise always
```

共享网络，运营商路由器路由配置

```
[ace_AR_wan] ip route-static 0 .0 .0 .0 0 .0 .0 .0 100 .1 .201 .2 // 下 一 跳 地 址
[] ospf 1 router-id 100.1.100.129
[ospf-1] default-route-advertise always
```