东南大學
SOUTHEAST UNIVERSITY

计算机网络专题实践
总结报告

组　　别 第一组

学　　号 09020312

姓　　名 陈鑫

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 四 月

目录

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

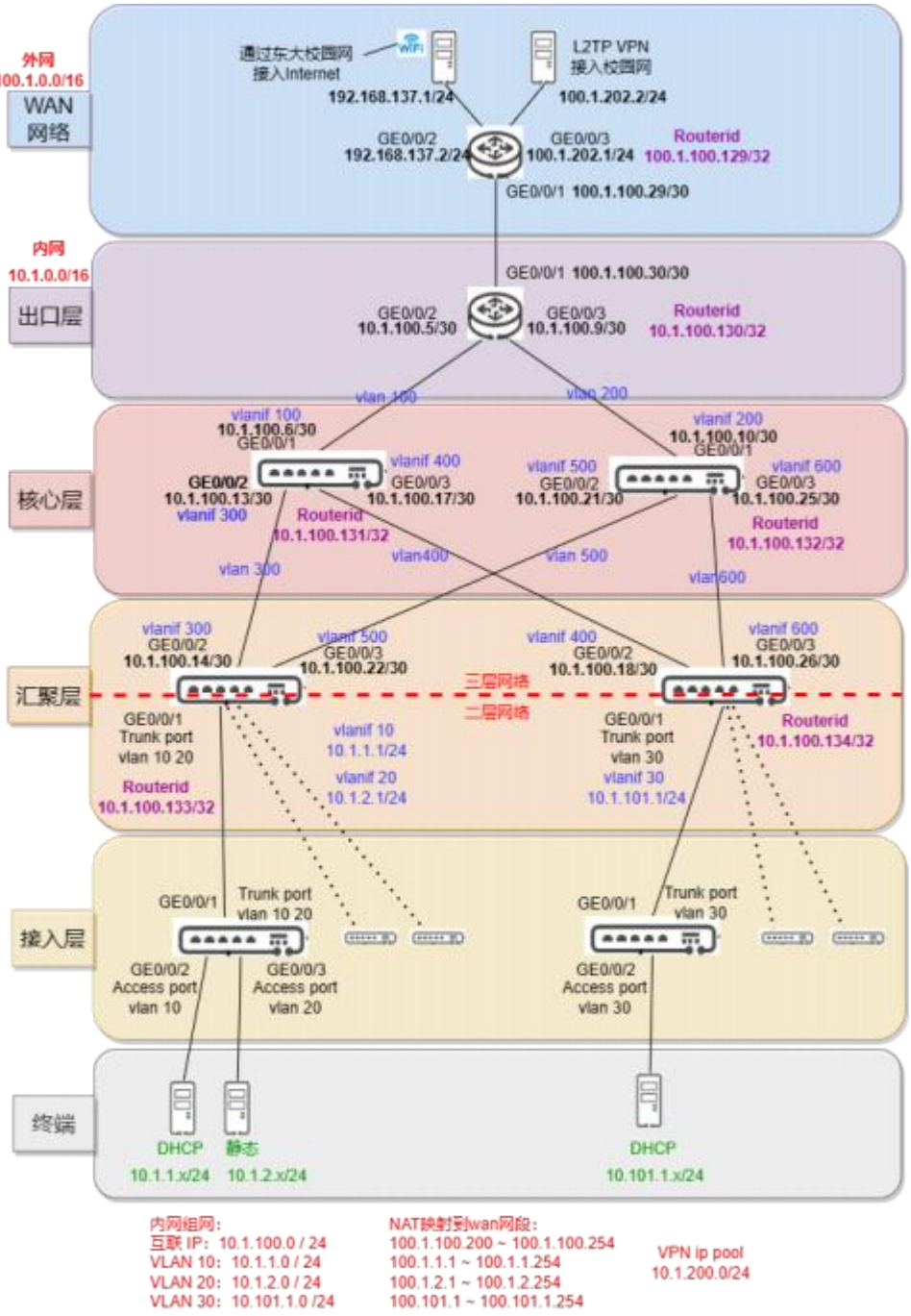


图 1: 网络拓扑图

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

本次实践，我主要参与了IP地址和vlan规划的讨论，并负责核心层1的OSPF和vlan配置，以及BGP配置和BGP过滤的实现。

3.1 核心层配置

3..1.1 vlan配置

端口 vlan 设置成 access

```
#交换机上全局开启 VLAN 资源，batch 可以创建多个
[Switch_1] vlan batch 10 20 30

#接 PC 机接口设置为 access 接口，并配置缺省 VLAN
[Switch_1] interface gigabitethernet 0/0/1 //进入接口视图
[Switch_1-GigabitEthernet0/0/1] port link-type access //配置 access 类型
[Switch_1-GigabitEthernet0/0/1] port default vlan 10 //配置缺省 VLAN，VLAN10 与这个端口关联了
```

端口设置成 trunk

```
#接 2 号交换机接口 设置为 Trunk 接口，并配允许通过的 VLAN
[Switch_1] interface gigabitethernet 0/0/2
[Switch_1-GigabitEthernet0/0/2] port link-type trunk //配置 trunk 类型
[Switch_1-GigabitEthernet0/0/2] port trunk allow-pass vlan 10//允许接口上VLAN 10 通过，VLAN 10 与这个端口关联了
[Switch_1-GigabitEthernet0/0/2] quit
```

vlanif 绑定

```
# 配置 Switch 1，交换机需要通过 VLANIF 配置 IP 地址

#与 PC 连接的端口，首先设置二层
[Switch_1] vlan batch 10 100
[Switch_1] interface gigabitethernet 0/0/1
[Switch_1-GigabitEthernet0/0/1] port link-type access
[Switch_1-GigabitEthernet0/0/1] port default vlan 10
[Switch_1-GigabitEthernet0/0/1] quit

#对应的 VLAN 上启用三层
[Switch_1] interface vlanif 10
[Switch_1-Vlanif10] ip address 10.10.10.1 24
[Switch_1-Vlanif10] quit

#与路由器连接的端口，首先设置二层
[Switch_1] interface gigabitethernet 0/0/2
[Switch_1-GigabitEthernet0/0/2] port link-type access
[Switch_1-GigabitEthernet0/0/2] port default vlan 100
[Switch_1-GigabitEthernet0/0/2] quit
```

#对应的 VLAN 上启用三层
[Switch_1] interface vlanif 100
[Switch_1-Vlanif100] ip address 100.10.10.1 24
[Switch_1-Vlanif100] quit
查看配置
display vlan

3.1.2 OSPF 配置

配置 ospf router-id ，作为 OSPF 路由器标识。Router-id 网络里唯一，不能冲突
不同网段之间：汇聚、核心、出口路由器使用OSPF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 200.10.10.1 255.255.255.255

#启动 OSPF 服务
[Switch_1] ospf 1 router-id 200.10.10.1 //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 100.10.10.0 0.0.0.255

至 PC 机网段，可以有两种方式，可以选择一种使用：
A） 用 network 方式发布出去，1 类 LSA(Router LSA，stubnet)
[Switch_1-ospf-1-area-0.0.0.0] network 10.10.10.0 0.0.0.255
AR1 上启用 OSPF

#配置 ospf router-id ，作为 OSPF 路由器标识。注意反掩码

[AR_1]interface loopback 0
[AR_1_Loopbak0] ip address 200.10.70.1 255.255.255.255
[AR_1] ospf 1 router-id 200.10.70.1

#与交换机间接口上使能 OSPF，并把这个接口的链路状态发布出去。

[AR_1-ospf-1] area 0
[AR_1-ospf-1-area-0.0.0.0] network 100.10.10.0 0.0.0.255 //for switch1
[AR_1-ospf-1-area-0.0.0.0] network 100.10.20.0 0.0.0.255 //for switch2
[AR_1-ospf-1-area-0.0.0.0] network 100.10.30.0 0.0.0.255 //for switch3
[AR_1-ospf-1-area-0.0.0.0] quit
查看 OSPF,
display ospf peer #查看 OSPF 是否建立，状态是否为 Full 状态

3.2 BGP配置

3.2.1 实验一：对于校区间两个网络 使用BGP发布路由 实现互通

1) 配置 AR 间接口 IP 地址 （首先要配置路由器之间的ip地址）

```
[AR_1] interface gigabitethernet 0/0/3
[AR_1-GigabitEthernet0/0/0] ip address 150.10.70.1 24
[AR_2] interface gigabitethernet 0/0/3
[AR_2-GigabitEthernet0/0/0] ip address 150.10.70.2 24
```

2) AR1 BGP 配置

#标识自己

```
[AR_1] bgp 65107 // 自治系统号
[AR_1-bgp] router-id 200.10.70.1
```

#找到对方路由器

[AR_1-bgp] peer 150.10.70.2 as-number 65108 //对端 IP 地址，对端自治系统号

#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

3) AR1 OSPF 引入 BGP 路由

[AR_1] ospf

[AR_1-ospf-1] import-route bgp

实验验证

1） 查看各设备路由情况

```
display ip routing-table
```

2） PC 间 ping 情况

3.2.2 实验二：使用BGP 策略过滤不符合规则

要求：路由 BGP/OSPF间引入路由，两校区间 PC机间可以互访 控制摄像头网段路由发布，两校区间 PC不能访问摄像头

我的理解就是，在路由器加一个过滤器，过滤去访问摄像头ip请求的报文

实验手册相关内容：

执行命令**system-view**，进入系统视图。

执行命令**bgp** { *as-number-plain* | *as-number-dot* }，进入BGP视图。

执行命令**ipv4-family unicast**，进入IPv4单播地址族视图。

执行命令**peer** { *group-name* | *ipv4-address* } **ip-prefix** *ip-prefix-name* **import**，配置对等体/对等体组基于IP前缀列表的入口路由过滤策略。

执行命令**peer** { *group-name* | *ipv4-address* } **capability-advertise orf** [**non-standard-compatible**] **ip-prefix** { **both** | **receive** | **send** }，配置BGP对等体（组）使能基于地址前缀的ORF功能。

缺省情况下，未使能BGP对等体（组）基于地址前缀的ORF功能。

检查配置结果
执行命令**display bgp peer** [*ipv4-address*] **verbose**，查看BGP peer详细信息。
执行命令**display bgp peer** *ipv4-address* **orf ip-prefix**，查看从指定对等体收到的基于地址前缀的ORF信息。

相关注释：
执行命令 peer { group-name | ipv4-address } ip-prefix ip-prefix-name import 可以配置基于 IP 前缀列表的入口路由过滤策略。这样的配置将允许网络管理员对从对等体或对等体组接收到的路由进行过滤。
命令说明如下：
peer：表示要配置的对等体或对等体组。
{ group-name | ipv4-address }：指定对等体组名称或对等体的 IPv4 地址。用于识别需要应用过滤策略的对等体或对等体组。
ip-prefix：表示要应用 IP 前缀列表策略。
ip-prefix-name：指定已定义的 IP 前缀列表名称，用于过滤接收到的路由。
import：表示应用过滤策略的方向是入口，即针对从对等体接收到的路由。
在使用这个命令之前，需要先创建一个 IP 前缀列表，用于定义允许或拒绝的 IP 前缀。例如：
ip ip-prefix ip-prefix-name permit x.x.x.x y
ip ip-prefix ip-prefix-name deny x.x.x.x y

其中 *x.x.x.x* 是 IP 地址，*y* 是子网掩码长度，*permit* 表示允许，*deny* 表示拒绝。应用了这个命令后，路由器将根据指定的 IP 前缀列表过滤从对等体或对等体组接收到的路由。这有助于提高网络安全性和稳定性，防止不需要的路由传播。

执行命令 *peer { group-name | ipv4-address } capability-advertise orf [non-standard-compatible] ip-prefix { both | receive | send }* 用于配置 BGP 对等体（组）以启用基于地址前缀的 ORF（Outbound Route Filtering）功能。ORF 可以让 BGP 对等体在传送路由更新之前，请求接收方根据特定策略对路由进行筛选。这样可以减少不必要的路由传播，降低对网络资源的消耗。
命令说明如下：
peer：表示要配置的 BGP 对等体或对等体组。
{ group-name | ipv4-address }：指定对等体组名称或对等体的 IPv4 地址。用于识别需要启用 ORF 功能的对等体或对等体组。
capability-advertise：表示要通告对等体的能力。
orf：表示启用 Outbound Route Filtering 功能。

[non-standard-compatible]: 可选参数，表示兼容非标准 ORF 实现。如果对等体使用的是非标准的 ORF 实现，可以添加此参数以实现兼容。
ip-prefix: 表示基于 IP 前缀的筛选策略。
{ both | receive | send }: 指定 ORF 功能的应用方向。
both: 同时应用于发送和接收方向。
receive: 仅应用于接收方向。
send: 仅应用于发送方向。
在缺省情况下，BGP 对等体（组）基于地址前缀的 ORF 功能是未启用的。执行上述命令可以启用该功能，从而提高网络效率和路由更新的可控性。

示例
譬如，我要过滤去目标ip为10.1.2.1的路由

定义一个 IP 前缀列表，用于匹配目标 IP 地址。创建一个 IP 前缀列表名为 filter-10.1.2.1，用于拒绝 IP 地址 10.1.2.1 的路由（假设子网掩码长度为 32）：

```
ip ip-prefix filter-10.1.2.1 deny 10.1.2.1 32
ip ip-prefix filter-10.1.2.1 permit 0.0.0.0 0 less-equal 32
```

第一条命令拒绝 IP 地址 10.1.2.1 的路由，第二条命令允许所有其他路由。
应用 IP 前缀列表到 BGP 对等体（组）的入站/出站方向。这取决于您是否希望在接收路由更新时过滤（入站），还是在发送路由更新时过滤（出站）。以下是两种方向的配置示例：
入站过滤：

```
peer { group-name | ipv4-address } ip-prefix filter-10.1.2.1 import
```

出站过滤：

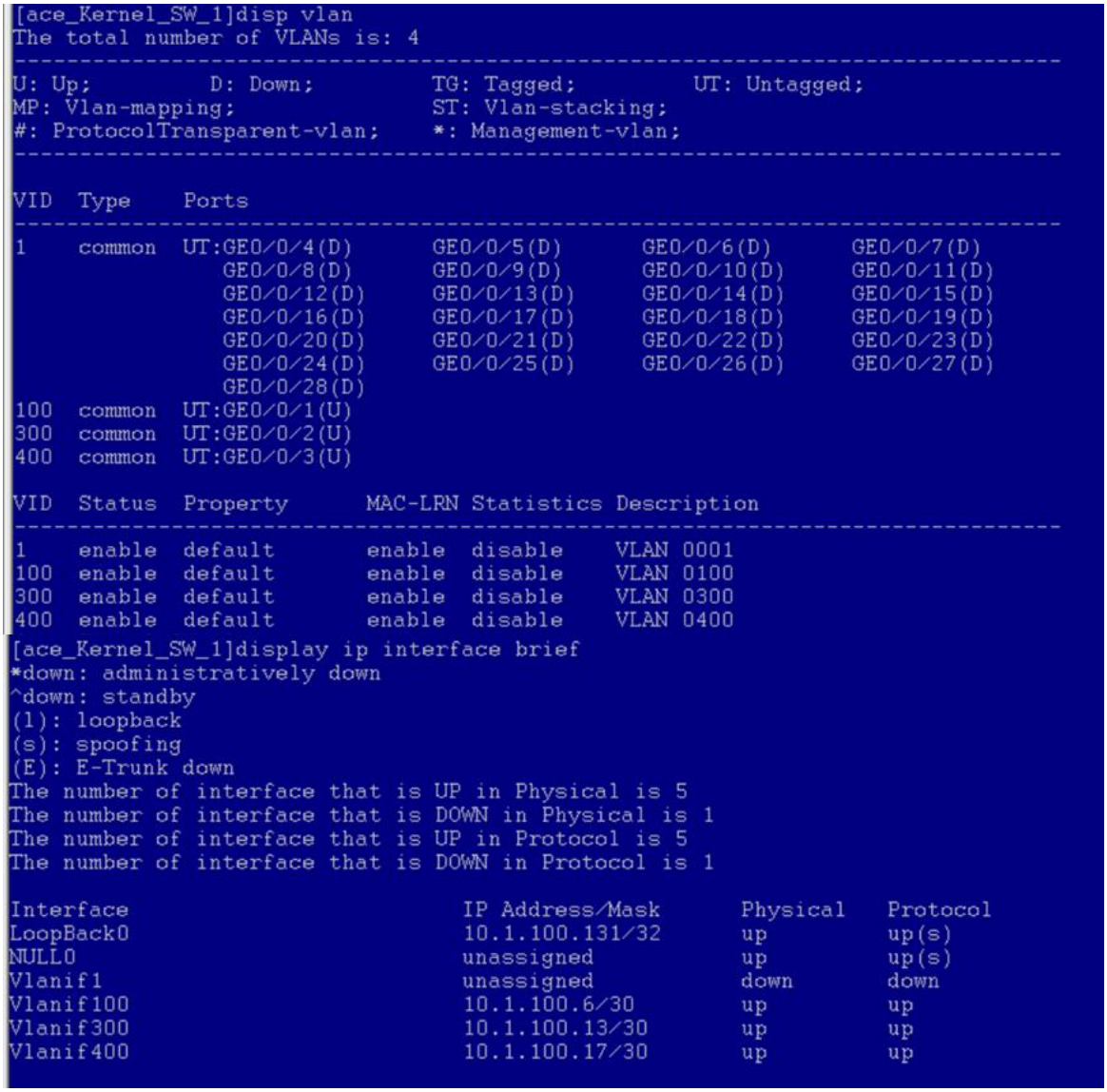
```
peer { group-name | ipv4-address } ip-prefix filter-10.1.2.1 export
```

其中，{ group-name | ipv4-address } 是对等体组名称或对等体的 IPv4 地址。
完成以上配置后，路由器将根据指定的 IP 前缀列表过滤去目标 IP 为 10.1.2.1 的路由

4 实现结果测试与分析

4.1 核心层配置效果检验

Vlan、vlanif配置
[]disp vlan
[]display ip interface brief



从图中可以看到，vlanif已配置成功并建立链接。

OSPF配置

检验

[] display ospf peer

[] display ospf routing

[] display ip routing

```
[ace_Kernel_SW_1]display ospf peer

        OSPF Process 1 with Router ID 10.1.100.131
                Neighbors

 Area 0.0.0.0 interface 10.1.100.6(Vlanif100)'s neighbors
 Router ID: 10.1.100.130     Address: 10.1.100.5
   State: Full  Mode:Nbr is  Slave  Priority: 1
   DR: 10.1.100.6  BDR: 10.1.100.5  MTU: 0
   Dead timer due in 28  sec
   Retrans timer interval: 5
   Neighbor is up for 00:08:26
   Authentication Sequence: [ 0 ]

                Neighbors

 Area 0.0.0.0 interface 10.1.100.13(Vlanif300)'s neighbors
 Router ID: 10.1.100.133     Address: 10.1.100.14
   State: Full  Mode:Nbr is  Master  Priority: 1
   DR: 10.1.100.14  BDR: 10.1.100.13  MTU: 0
   Dead timer due in 38  sec
   Retrans timer interval: 5
   Neighbor is up for 00:08:25
   Authentication Sequence: [ 0 ]

                Neighbors

 Area 0.0.0.0 interface 10.1.100.17(Vlanif400)'s neighbors
 Router ID: 10.1.100.134     Address: 10.1.100.18
   State: Full  Mode:Nbr is  Master  Priority: 1
   DR: 10.1.100.18  BDR: 10.1.100.17  MTU: 0
   Dead timer due in 40  sec
   Retrans timer interval: 2
   Neighbor is up for 00:08:27
   Authentication Sequence: [ 0 ]
```

```
[ace_Kernel_SW_1]display ospf routing

        OSPF Process 1 with Router ID 10.1.100.131
                Routing Tables

 Routing for Network
 Destination        Cost  Type       NextHop         AdvRouter       Area
 10.1.100.4/30      1     Transit    10.1.100.6      10.1.100.131    0.0.0.0
 10.1.100.12/30     1     Transit    10.1.100.13     10.1.100.131    0.0.0.0
 10.1.100.16/30     1     Transit    10.1.100.17     10.1.100.131    0.0.0.0
 10.1.1.0/24        2     Stub       10.1.100.14     10.1.100.133    0.0.0.0
 10.1.2.0/24        2     Stub       10.1.100.14     10.1.100.133    0.0.0.0
 10.1.100.8/30      2     Transit    10.1.100.5      10.1.100.132    0.0.0.0
 10.1.100.20/30     2     Transit    10.1.100.14     10.1.100.133    0.0.0.0
 10.1.100.24/30     2     Transit    10.1.100.18     10.1.100.134    0.0.0.0
 10.1.100.133/32    1     Stub       10.1.100.14     10.1.100.133    0.0.0.0
 10.1.101.0/24      2     Stub       10.1.100.18     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           10.1.100.5      10.1.100.13
0
 10.4.10.0/24       1         Type2      1           10.1.100.5      10.1.100.13
0
 10.4.20.0/24       1         Type2      1           10.1.100.5      10.1.100.13
0
 10.4.30.0/24       1         Type2      1           10.1.100.5      10.1.100.13
0
 10.4.40.0/24       1         Type2      1           10.1.100.5      10.1.100.13
0
 10.4.100.4/30      1         Type2      1           10.1.100.5      10.1.100.13
0
 10.4.100.8/30      1         Type2      1           10.1.100.5      10.1.100.13
0
 10.4.100.12/30     1         Type2      1           10.1.100.5      10.1.100.13
0
 10.4.100.16/30     1         Type2      1           10.1.100.5      10.1.100.13
0
 10.4.100.20/30     1         Type2      1           10.1.100.5      10.1.100.13
0
 10.4.100.24/30     1         Type2      1           10.1.100.5      10.1.100.13
0
 10.4.220.0/24      1         Type2      1           10.1.100.5      10.1.100.13
0
 10.4.220.166/32    1         Type2      1           10.1.100.5      10.1.100.13
0
 100.4.10.0/24      1         Type2      1           10.1.100.5      10.1.100.13
0

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

从图中可以看到ospf路由表记录了各路由信息，说明ospf配置成功。

4.2 BGP配置效果检验

BGP路由表:

可以看到，路由表中已有其他园区网的路由

```
[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
```

BGP测试

我们是 group1 ping group2

可以访问动态主机 不能访问静态主机:

```
C:\Users\raoziqian>ping 10.4.30.77

正在 Ping 10.4.30.77 具有 32 字节的数据:
来自 10.4.30.77 的回复: 字节=32 时间=1ms TTL=122
来自 10.4.30.77 的回复: 字节=32 时间=1ms TTL=122
来自 10.4.30.77 的回复: 字节=32 时间=1ms TTL=122
来自 10.4.30.77 的回复: 字节=32 时间=1ms TTL=122

10.4.30.77 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 = 1ms，最长 = 1ms，平均 = 1ms
```

```
C:\Users\raoziqian>ping 10.4.20.1

正在 Ping 10.4.20.1 具有 32 字节的数据:
请求超时。
请求超时。

10.4.20.1 的 Ping 统计信息:
    数据包: 已发送 = 2，已接收 = 0，丢失 = 2 (100% 丢失)，
```

查看 group1 ping 我们小组的情况，查看是否进行了BGP过滤 ping DHCP 获取的IP地址

```
正在 Ping 10.1.1.61 具有 32 字节的数据:
来自 10.1.1.61 的回复: 字节=32 时间=1ms TTL=122
来自 10.1.1.61 的回复: 字节=32 时间=1ms TTL=122
来自 10.1.1.61 的回复: 字节=32 时间=1ms TTL=122
来自 10.1.1.61 的回复: 字节=32 时间=2ms TTL=122

10.1.1.61 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 = 1ms, 最长 = 2ms, 平均 = 1ms

正在 Ping 10.1.2.2 具有 32 字节的数据:
请求超时。

10.1.2.2 的 Ping 统计信息:
    数据包: 已发送 = 1, 已接收 = 0, 丢失 = 1 (100% 丢失),
Control-C
^C
```

PING 内网任一组网网段 IP

```
正在 Ping 10.1.100.10 具有 32 字节的数据:
来自 10.1.100.10 的回复: 字节=32 时间=1ms TTL=250
来自 10.1.100.10 的回复: 字节=32 时间=1ms TTL=250
来自 10.1.100.10 的回复: 字节=32 时间=1ms TTL=250
来自 10.1.100.10 的回复: 字节=32 时间=1ms TTL=250

10.1.100.10 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 = 1ms, 最长 = 1ms, 平均 = 1ms
```

5 心得体会

5.1 遇到的问题及解决方法：

1）最后访问外网时能 ping 通路由器，但是不能连到外网。

解决方法：需要发布静态路由，发布静态路由之后可以 ping 通。

2）测试 ospf 时，对于左侧的部分，显示 100 对于的物理口一直 为 down，发现未创建 vlan。

解决方法：补充执行 vlan 100，需要先创建物理接口，再创建虚拟 接口。 （

3）PC 机和三层交换机 ping 不通。

解决方法：对于三层交换机的不同接口需要设置不同的 vlan,但是 在同一个接口的向下传输通道上需要设置相同的 VLAN,在本实验 中，二层交换机可以将它看作透明的，那么只有 PC 机和三层交换机 之间设置相同的 VLAN，数据才可以成功传输。

4）在 undo vlan 之后，需要按部重新设置接口 vlan,其中需要注意，相应的 IP 地址需要在对应的 VLAN 中配置。

5.2 实验心得与体会

通过本次实验，使用已经学习到的网络技术，组合构建一张校园园区网络。综合运用网络技术，实践网络工程能力。本次实验我们主要实现了：IP地址规划，VLAN配置，内网路由配置，NAT地址转换，防火墙部署，BGP配置，VPN配置等功能，充分通过实践复习了所学计网知识。

本次实践，我主要负责IP、VLAN规划，OSPF配置，BGP配置和过滤部分。在IP和VLAN规划中，小组成员充分讨论，积极查询资料，并最终得到一份IPvlan划分方案，在之后的实践课中，我根据实验手册完成OSPF配置，之后查询资料了解BGP配置与过滤的原理，并查询相关交换机器使用手册，设计BGP配置与过滤方案。

在实验过程中，我们遇到了不少困难和挑战。例如，在IP地址规划时，我们需要考虑子网划分和地址空间的合理利用，以避免地址浪费和网络拓扑结构的混乱；在配置OSPF时，我们要熟练掌握各种OSPF命令，了解各种参数的含义，以保证网络稳定运行。在解决这些问题的过程中，我们不仅提高了自己的动手能力，还锻炼了解决问题的能力。

在BGP配置和过滤部分，我们遇到了一些问题和挑战，但通过不断地摸索、实践和学习，我们总结了一些经验教训，

AS（自治系统）号选择与规划：在配置BGP时，需要为每个自治系统分配一个唯一的AS号。我们应该仔细规划AS号，以便在网络中实现有效的路由控制。在实际操作中，可以为内部自治系统分配私有AS号（64512-65535），而对于与外部互联的自治系统，需要向IANA申请一个公有AS号。

路由器ID的选取：在配置BGP时，需要为每个路由器分配一个唯一的路由器ID。为了简化配置和管理，我们可以使用路由器的某个接口IP地址作为路由器ID。同时，要确保网络中没有重复的路由器ID，以免导致路由混乱。

路由策略设计：在BGP中，我们可以使用路由策略来控制路由的选择、传播和过滤。在设计路由策略时，应充分考虑网络拓扑结构、流量需求和安全性要求。例如，可以通过优先级、权重和本地优先级等参数来控制路由的优选，通过AS-Path过滤、前缀列表和路由映射等方法来实现路由的过滤。

避免路由环路：在BGP配置中，需要注意避免路由环路的产生。可以通过合理设计AS-Path属性、设置BGP最大跳数限制等方法来实现。在实际操作中，我们可以使用“neighbor x.x.x.x allowas-in”命令来允许某个邻居接收包含自己AS号的路由，从而避免路由环路。

本次实践，小组成员充分合作，互帮互助，共同完成了本次校园网络的构建，培养了工程实践能力和团队合作能力。