东南大學
SOUTHEAST UNIVERSITY

计算机网络专题实践

总结报告

组　　别 1

学　　号 09020334

姓　　名 黄锦峰

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

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

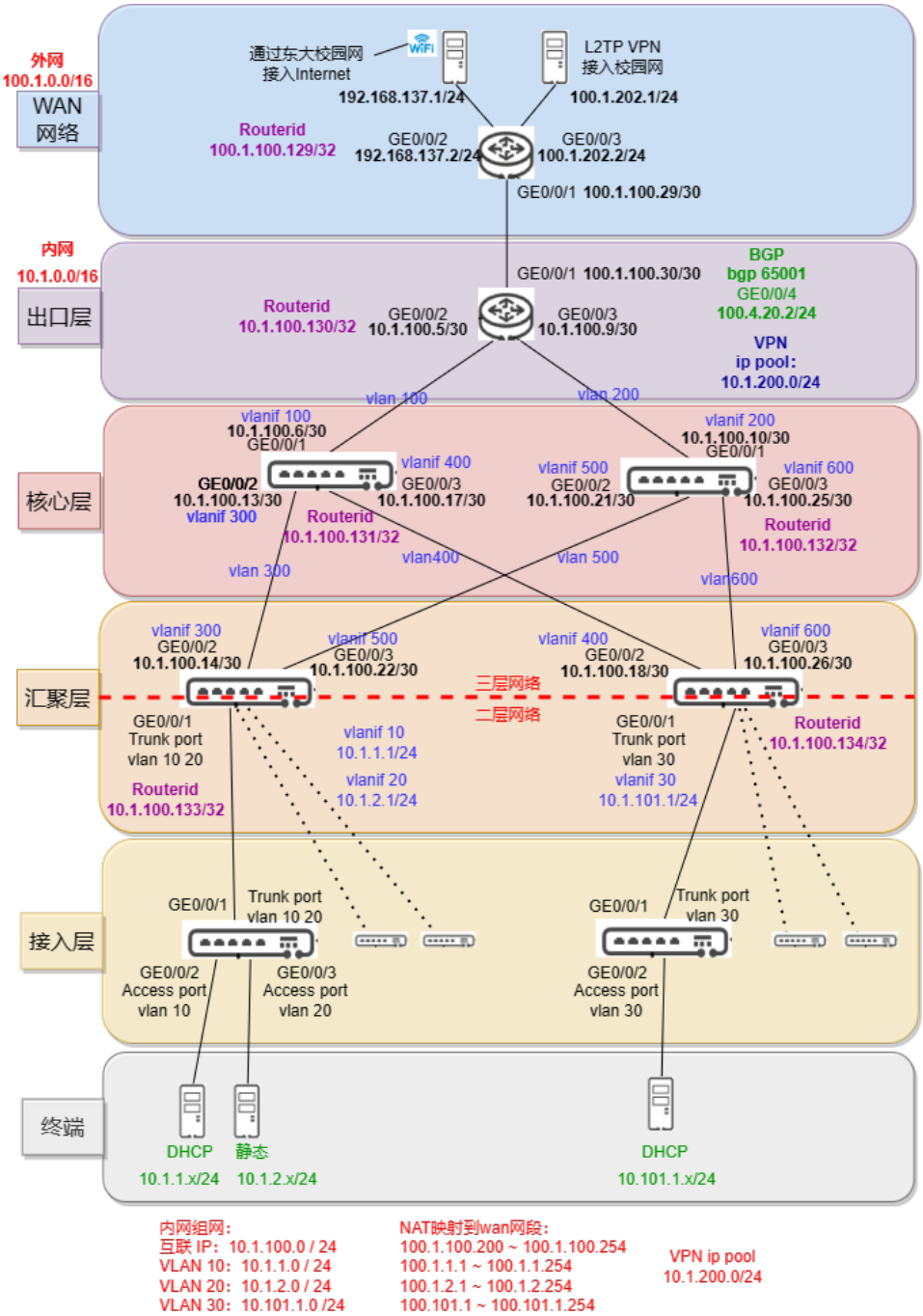


图 1: 网络拓扑图

2.1.2 IP 地址规划

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

2.1.3 各层设备配置注意事项

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。

2.1.4 效果检验规划

具体检验结果报告见附件。

- 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

- 接入层、汇聚层交换机联合调试：康镭、饶梓骞、何永麟
- 汇聚层、核心层交换机通路：黄锦峰、陈鑫、饶梓骞、何永麟
- 出口层、运营商路由器路由：黄锦峰、康镭
- 防火墙调试：何永麟、黄锦峰
- 共享网络调试：何永麟、黄锦峰、饶梓骞
- BGP 设置调试：黄锦峰、陈鑫

3 个人承担任务的实现

3.1 配置核心层 2 号交换机配置

- vlan 和 vlanif
- OSPF 发布路由
- 环路

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
```

3.2 出口层路由器配置

- 配置接口 IP
- OSPF
- 配置静态路由
- NAT
- firewall
- VPN
- BGP

接口 IP 配置

```
<> system-view
[] sysname ace_AR_out
[] interface gigabitethernet 0/0/1
[0/0/1] undo portswitch
[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

# 查看 ip 配置
[] display ip interface brief
```

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
```

3.2.1 静态路由

出口层路由器需要配置静态路由，实现与运营商及外网的通信，配置如下：

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

运营商路由器需要配置进入内网的路由信息，同时共享网络时需要配置到共享网络的缺省静态，配置如下：

```
# 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
# 通向共享网络的缺省路由
[ace_AR_wan]  ip route-static 0.0.0.0 0.0.0.0 192.168.137.1 //下一跳地址
[] ospf 1 router-id 10.1.100.129
[ospf-1] default-route-advertise always
```

3.2.2 NAT

对地址池的映射做了规定。在做防火墙测试时，需要模拟 ping 内网的地址，需要注意。

- 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

3.2.3 防火墙

设置安全区和非安全区后[1]，采用了 ACL 的方式进行防火墙的配置，ACL 的配置如下：其中允许了外界网络、BGP peer 和运营商路由器[2]访问动态主机。

```
[]acl 3102
[acl-adv-3102] rule permit ip source 100.1.0.0 0.0.255.255 destination 10.1.1.0
    0.0.0.255
[acl-adv-3102] rule permit ip source 100.1.0.0 0.0.255.255 destination 10.1.101.0
    0.0.0.255
# 共享网络
[acl-adv-3102] rule permit ip source 10.203.128.0 0.0.127.255 destination
    10.1.101.0  0.0.0.255
[acl-adv-3102] rule permit ip source 10.203.128.0 0.0.127.255 destination
    10.1.101.0  0.0.0.255
# BGP
[acl-adv-3102] rule permit ip source 10.4.0.0 0.0.255.255 destination 10.1.101.0
    0.0.0.255
[acl-adv-3102] rule permit ip source 10.4.0.0 0.0.255.255 destination 10.1.101.0
    0.0.0.255
```

[1]详细见附件出口层B.4配置

[2]运营商路由器可用于测试外网对内网访问的测试

```
# 禁止其他访问
[acl-adv-3102] rule deny ip
[acl-adv-3102] quit
```

BGP 防止访问静态摄像头时也可以定义新的规则：

```
[] acl number 3103
[acl-adv-2000] rule deny ip source 10.1.2.0 0.0.0.255 destination any
[acl-adv-2000] rule permit ip
[acl-adv-2000] quit
```

防火墙中加入 ACL 规则

```
[] firewall interzone trust untrust
[interzone-trust-untrust] firewall enable
[interzone-trust-untrust] packet-filter 3102 inbound
[interzone-trust-untrust] packet-filter 3103 outbound // 添加 AC于出端口，酌情考虑
[interzone-trust-untrust] quit
```

3.2.4 出口层交换机 VPN 配置

VPN：L2TP 配置

```
# 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，参见：windows 10 启动 L2TP

3.2.5 出口层交换机 BGP

配置域间边界路由器接口 IP，标识自治系统号，引入路由。具体配置见下：
相关 BGP 过滤策略路由策略可见心得体会中：5.1.3BGP 过滤。

```
# 配置4号端口IP
[] interface gigabitethernet 0/0/4
[0/0/4] ip address 100.4.20.2 24
# 配置BGP
[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 100.4.20.1 as-number 65004

# 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
```

4 实现结果测试与分析

相关 IP 地址：

- 动态 PC：10.1.1.61
- 静态摄像头：10.1.2.2
- 动态 PC：10.101.230

4.1 核心层 2 号交换机配置查看

相关查看命令参照：2.1.4 各层设备配置检验

display vlan

```
[ace_Kernel_SW_2]disp vlan
The total number of VLANs is: 4
--------------------------------------------------------------------------------
U: Up;         D: Down;         TG: Tagged;         UT: Untagged;
MP: Vlan-mapping;               ST: Vlan-stacking;
#: ProtocolTransparent-vlan;    *: Management-vlan;
--------------------------------------------------------------------------------

VID  Type    Ports
--------------------------------------------------------------------------------
1    common  UT:GE0/0/4(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)
200  common  UT:GE0/0/1(U)
500  common  UT:GE0/0/2(U)
600  common  UT:GE0/0/3(U)

VID  Status  Property      MAC-LRN Statistics Description
--------------------------------------------------------------------------------
1    enable  default       enable  disable    VLAN 0001
200  enable  default       enable  disable    VLAN 0200
500  enable  default       enable  disable    VLAN 0500
600  enable  default       enable  disable    VLAN 0600
[ace_Kernel_SW_2]
```

display ip interface brief

```
[ace_Kernel_SW_2]display ip interface brief
*down: administratively down
^down: standby
(l): loopback
(s): spoofing
(E): E-Trunk down
The number of interface that is UP in Physical is 5
The number of interface that is DOWN in Physical is 1
The number of interface that is UP in Protocol is 5
The number of interface that is DOWN in Protocol is 1

Interface                         IP Address/Mask      Physical   Protocol
LoopBack0                         10.1.100.132/32      up         up(s)
NULL0                             unassigned           up         up(s)
Vlanif1                           unassigned           down       down
Vlanif200                         10.1.100.10/30       up         up
Vlanif500                         10.1.100.21/30       up         up
Vlanif600                         10.1.100.25/30       up         up
```

可见都配置了相应的 VLAN、VLANIF 和对应 IP 地址，接口显示为 up 状态，接口连接正常。下面检查相关路由：

display ospf peer

```
[ace_Kernel_SW_2]display ospf peer

        OSPF Process 1 with Router ID 10.1.100.132
                Neighbors

Area 0.0.0.0 interface 10.1.100.10(Vlanif200)'s neighbors
Router ID: 10.1.100.130     Address: 10.1.100.9
  State: Full  Mode:Nbr is  Slave  Priority: 1
  DR: 10.1.100.10  BDR: 10.1.100.9  MTU: 0
  Dead timer due in 33  sec
  Retrans timer interval: 5
  Neighbor is up for 02:25:40
  Authentication Sequence: [ 0 ]

                Neighbors

Area 0.0.0.0 interface 10.1.100.21(Vlanif500)'s neighbors
Router ID: 10.1.100.133     Address: 10.1.100.22
  State: Full  Mode:Nbr is  Master  Priority: 1
  DR: 10.1.100.22  BDR: 10.1.100.21  MTU: 0
  Dead timer due in 35  sec
  Retrans timer interval: 5
  Neighbor is up for 02:19:18
  Authentication Sequence: [ 0 ]

                Neighbors

Area 0.0.0.0 interface 10.1.100.25(Vlanif600)'s neighbors
Router ID: 10.1.100.134     Address: 10.1.100.26
  State: Full  Mode:Nbr is  Master  Priority: 1
  DR: 10.1.100.26  BDR: 10.1.100.25  MTU: 0
  Dead timer due in 38  sec
  Retrans timer interval: 2
  Neighbor is up for 02:21:32
  Authentication Sequence: [ 0 ]
```

显示了 OSPF 的相关检验效果。核心层 2 号交换机有三个邻居，它们的 State:Full 显示正常。

display ospf routing-table

```
[ace_Kernel_SW_2]display ospf routing

        OSPF Process 1 with Router ID 10.1.100.132
                Routing Tables

 Routing for Network
 Destination        Cost  Type       NextHop         AdvRouter       Area
 10.1.100.8/30      1     Transit    10.1.100.10     10.1.100.132    0.0.0.0
 10.1.100.20/30     1     Transit    10.1.100.21     10.1.100.132    0.0.0.0
 10.1.100.24/30     1     Transit    10.1.100.25     10.1.100.132    0.0.0.0
 10.1.1.0/24        2     Stub       10.1.100.22     10.1.100.133    0.0.0.0
 10.1.2.0/24        2     Stub       10.1.100.22     10.1.100.133    0.0.0.0
 10.1.100.4/30      2     Transit    10.1.100.9      10.1.100.131    0.0.0.0
 10.1.100.12/30     2     Transit    10.1.100.22     10.1.100.133    0.0.0.0
 10.1.100.16/30     2     Transit    10.1.100.26     10.1.100.134    0.0.0.0
 10.1.100.133/32    1     Stub       10.1.100.22     10.1.100.133    0.0.0.0
 10.1.101.0/24      2     Stub       10.1.100.26     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           10.1.100.9      10.1.100.13
0

 Total Nets: 11
 Intra Area: 10  Inter Area: 0  ASE: 1  NSSA: 0

[ace_Kernel_SW_2]
```

上图仅显示内网配置 OSPF 时的状态，考虑到实验完整的配置引入 BGP 后，OSPF 路由表项会有所更新。但在上图中也可以看到包含了内网所有网段的路由。

4.2 出口层交换机配置

对设备配置的检验同上

display ip interface brief

```
[ace_AR_out]disp ip inter b
*down: administratively down
^down: standby
(l): loopback
(s): spoofing
(E): E-Trunk down
The number of interface that is UP in Physical is 9
The number of interface that is DOWN in Physical is 6
The number of interface that is UP in Protocol is 6
The number of interface that is DOWN in Protocol is 9

Interface                         IP Address/Mask      Physical   Protocol
Cellular0/0/0                     unassigned           down       down
Ethernet0/0/0                     unassigned           down       down
GigabitEthernet0/0/1              100.1.100.30/30      up         up
GigabitEthernet0/0/2              10.1.100.5/30        up         up
GigabitEthernet0/0/3              10.1.100.9/30        up         up
GigabitEthernet0/0/4              100.4.20.2/24        down       down
GigabitEthernet0/0/5              unassigned           up         down
GigabitEthernet0/0/8              unassigned           down       down
GigabitEthernet0/0/9              unassigned           down       down
GigabitEthernet0/0/10             unassigned           up         down
LoopBack0                         10.1.100.130/32      up         up(s)
NULL0                             unassigned           up         up(s)
Virtual-Template1                 10.1.200.1/24        up         down
Vlanif1                           192.168.1.1/24       up         up
Vlanif4000                        192.10.50.5/24       down       down

[ace_AR_out]
```

查看有关 OSPF 的信息，确认配置无误，内网路由正常。

display ospf peer

```
[ace_AR_out]
[ace_AR_out]display ospf peer

        OSPF Process 1 with Router ID 10.1.100.130
                Neighbors

 Area 0.0.0.0 interface 10.1.100.5(GigabitEthernet0/0/2)'s neighbors
 Router ID: 10.1.100.131     Address: 10.1.100.6
   State: Full  Mode:Nbr is  Master  Priority: 1
   DR: 10.1.100.6  BDR: 10.1.100.5  MTU: 0
   Dead timer due in 39  sec
   Retrans timer interval: 4
   Neighbor is up for 02:30:36
   Authentication Sequence: [ 0 ]

                Neighbors

 Area 0.0.0.0 interface 10.1.100.9(GigabitEthernet0/0/3)'s neighbors
 Router ID: 10.1.100.132     Address: 10.1.100.10
   State: Full  Mode:Nbr is  Master  Priority: 1
   DR: 10.1.100.10  BDR: 10.1.100.9  MTU: 0
   Dead timer due in 39  sec
   Retrans timer interval: 0
   Neighbor is up for 02:36:56
   Authentication Sequence: [ 0 ]
```

display ospf routing-table

```
[ace_AR_out]display ospf routing

        OSPF Process 1 with Router ID 10.1.100.130
                Routing Tables

Routing for Network
Destination        Cost  Type       NextHop         AdvRouter       Area
10.1.100.4/30      1     Transit    10.1.100.5      10.1.100.130    0.0.0.0
10.1.100.8/30      1     Transit    10.1.100.9      10.1.100.130    0.0.0.0
10.1.1.0/24        3     Stub       10.1.100.10     10.1.100.133    0.0.0.0
10.1.1.0/24        3     Stub       10.1.100.6      10.1.100.133    0.0.0.0
10.1.2.0/24        3     Stub       10.1.100.10     10.1.100.133    0.0.0.0
10.1.2.0/24        3     Stub       10.1.100.6      10.1.100.133    0.0.0.0
10.1.100.12/30     2     Transit    10.1.100.6      10.1.100.133    0.0.0.0
10.1.100.16/30     2     Transit    10.1.100.6      10.1.100.134    0.0.0.0
10.1.100.20/30     2     Transit    10.1.100.10     10.1.100.133    0.0.0.0
10.1.100.24/30     2     Transit    10.1.100.10     10.1.100.134    0.0.0.0
10.1.100.133/32    2     Stub       10.1.100.10     10.1.100.133    0.0.0.0
10.1.100.133/32    2     Stub       10.1.100.6      10.1.100.133    0.0.0.0
10.1.101.0/24      3     Stub       10.1.100.10     10.1.100.134    0.0.0.0
10.1.101.0/24      3     Stub       10.1.100.6      10.1.100.134    0.0.0.0

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

4.3 缺省静态路由及路由表

display ip routing-table

```
[ace_Kernel_SW_2]display ip routing-table
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   10.1.100.9      Vlanif200
       10.1.1.0/24  OSPF    10   2           D   10.1.100.22     Vlanif500
       10.1.2.0/24  OSPF    10   2           D   10.1.100.22     Vlanif500
     10.1.100.4/30  OSPF    10   2           D   10.1.100.9      Vlanif200
     10.1.100.8/30  Direct  0    0           D   10.1.100.10     Vlanif200
    10.1.100.10/32  Direct  0    0           D   127.0.0.1       Vlanif200
    10.1.100.12/30  OSPF    10   2           D   10.1.100.22     Vlanif500
    10.1.100.16/30  OSPF    10   2           D   10.1.100.26     Vlanif600
    10.1.100.20/30  Direct  0    0           D   10.1.100.21     Vlanif500
    10.1.100.21/32  Direct  0    0           D   127.0.0.1       Vlanif500
    10.1.100.24/30  Direct  0    0           D   10.1.100.25     Vlanif600
    10.1.100.25/32  Direct  0    0           D   127.0.0.1       Vlanif600
   10.1.100.132/32  Direct  0    0           D   127.0.0.1       LoopBack0
   10.1.100.133/32  OSPF    10   1           D   10.1.100.22     Vlanif500
     10.1.101.0/24  OSPF    10   2           D   10.1.100.26     Vlanif600
      10.4.10.0/24  O_ASE   150  1           D   10.1.100.9      Vlanif200
      10.4.20.0/24  O_ASE   150  1           D   10.1.100.9      Vlanif200
      10.4.30.0/24  O_ASE   150  1           D   10.1.100.9      Vlanif200
      10.4.40.0/24  O_ASE   150  1           D   10.1.100.9      Vlanif200
     10.4.100.4/30  O_ASE   150  1           D   10.1.100.9      Vlanif200
     10.4.100.8/30  O_ASE   150  1           D   10.1.100.9      Vlanif200
    10.4.100.12/30  O_ASE   150  1           D   10.1.100.9      Vlanif200
    10.4.100.16/30  O_ASE   150  1           D   10.1.100.9      Vlanif200
    10.4.100.20/30  O_ASE   150  1           D   10.1.100.9      Vlanif200
    10.4.100.24/30  O_ASE   150  1           D   10.1.100.9      Vlanif200
     10.4.220.0/24  O_ASE   150  1           D   10.1.100.9      Vlanif200
     100.4.10.0/24  O_ASE   150  1           D   10.1.100.9      Vlanif200
     100.4.30.0/24  O_ASE   150  1           D   10.1.100.9      Vlanif200
      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_Kernel_SW_2]
```

由该路由表项可以看出，出口层的缺省路由配置成功且已发布到内网。

4.4 内网路由：核心层 2 号交换机 ping 测试

```
[ace_Kernel_SW_2]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=127 time=1 ms
    Reply from 10.1.2.2: bytes=56 Sequence=2 ttl=127 time=1 ms
    Reply from 10.1.2.2: bytes=56 Sequence=3 ttl=127 time=1 ms
    Reply from 10.1.2.2: bytes=56 Sequence=4 ttl=127 time=1 ms
    Reply from 10.1.2.2: bytes=56 Sequence=5 ttl=127 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 10.1.2.2

```
[ace_Kernel_SW_2]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=127 time=1 ms
    Reply from 10.1.1.61: bytes=56 Sequence=2 ttl=127 time=1 ms
    Reply from 10.1.1.61: bytes=56 Sequence=3 ttl=127 time=1 ms
    Reply from 10.1.1.61: bytes=56 Sequence=4 ttl=127 time=1 ms
    Reply from 10.1.1.61: bytes=56 Sequence=5 ttl=127 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 10.1.1.61

```
[ace_Kernel_SW_2]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=63 time=1 ms
    Reply from 10.1.101.230: bytes=56 Sequence=2 ttl=63 time=1 ms
    Reply from 10.1.101.230: bytes=56 Sequence=3 ttl=63 time=1 ms
    Reply from 10.1.101.230: bytes=56 Sequence=4 ttl=63 time=1 ms
    Reply from 10.1.101.230: bytes=56 Sequence=5 ttl=63 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
```

ping 10.1.101.230

可见，内网路由正常，核心层 2 号交换机 ping 通所有内网主机。

4.5 VPN 连接路由测试

VPN 连接测试

ping 10.1.1.61

```
C:\Users\75677>ping 10.1.1.61

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=2ms TTL=125
来自 10.1.1.61 的回复: 字节=32 时间=2ms TTL=125

10.1.1.61 的 Ping 统计信息:
    数据包: 已发送 = 2, 已接收 = 2, 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
```

ping 10.1.2.2

```
正在 Ping 10.1.2.2 具有 32 字节的数据:
Control-C
^C
C:\Users\75677>ping 10.1.2.2

正在 Ping 10.1.2.2 具有 32 字节的数据:
请求超时。
请求超时。

10.1.2.2 的 Ping 统计信息:
    数据包: 已发送 = 2, 已接收 = 0, 丢失 = 2 (100% 丢失),
Control-C
^C
C:\Users\75677>
```

ping 10.1.101.230

```
C:\Users\75677>ping 10.1.101.230

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=61
来自 10.1.101.230 的回复: 字节=32 时间=2ms TTL=61
来自 10.1.101.230 的回复: 字节=32 时间=3ms TTL=61
来自 10.1.101.230 的回复: 字节=32 时间=2ms TTL=61

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 = 3ms, 平均 = 2ms
```

可见 VPN 连接正常，VPN 连接的主机可以 ping 通内网动态主机，但不能访问静态的摄像头。

同时，这也验证了防火墙的设置，防火墙只允许外部网络访问内网的动态主机，不允许访问静态主机。

4.6 BGP 路由和过滤

我们作为 group1，邻接的 group2 访问我们的内网：

group2：ping 10.1.1.61

```
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
```

group2：ping 10.1.2.2

```
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
```

group2：ping 10.1.101.230

```
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
```

可见可以 goup2 可以 ping 通内网动态主机，但不能访问静态的摄像头。

我们将用于 BGP 路由的接口设置在防火墙的非安全区中，使用 ACL 过滤规则对数据包进行过滤。

5 心得体会

5.1 问题及解决方法

5.1.1 汇聚层和核心层形成环路

问题：形成环路之后导致直连的路由 ping 不通，相关环路知识见：5.2.5环路

解决方案：需要关闭核心层交换机的 stp，在核心层交换机上执行以下命令：

```
    undo stp enable
```

5.1.2 共享网络，路由配置

问题：共享网络时，数内网数据包到达运营商网络后丢弃

解决方案：需要在运营商网络的路由器上配置静态路由到共享网络 PC；共享网络 PC 需要设置正确的路由。

运营商路由器配置静态路由：

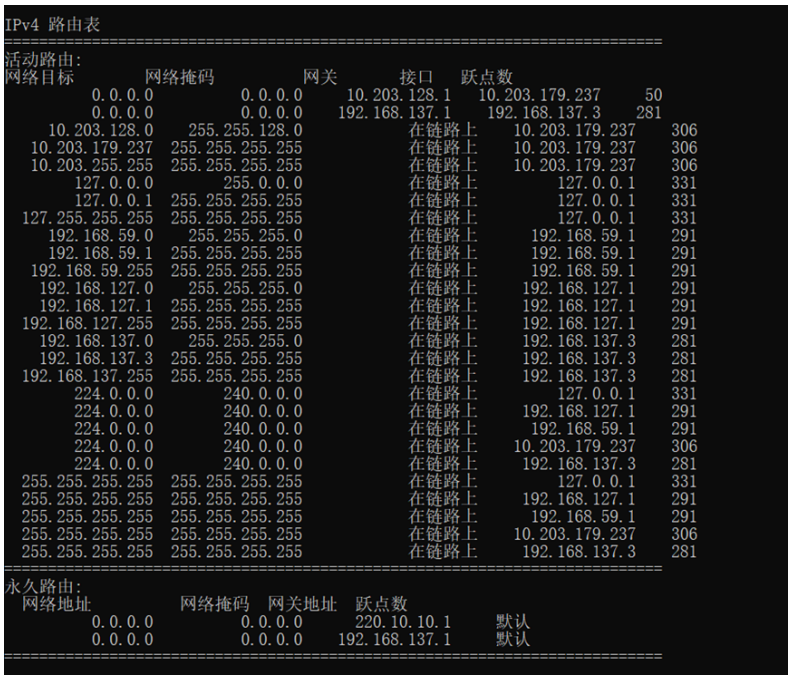
```
# 运营商配置一个缺省的静态路由到共享网络
[ace_AR_wan] ip route-static 0.0.0.0 0.0.0.0 192.168.137.1   # 下一跳地址
[ace_AR_wan] ospf 1 router-id 10.1.100.129
[ospf-1] default-route-advertise always
```

共享网络 PC 配置路由：参见：Windows：配置多网卡路由表（规则）

```
[windows] route print -4

命令: route delete 0.0.0.0
作用: 将默认路由规则清空。

命令: route add 0.0.0.0 mask 0.0.0.0 <访问外网的网关>
作用: 添加默认路由规则，指向外网网关。【访问外网】
```

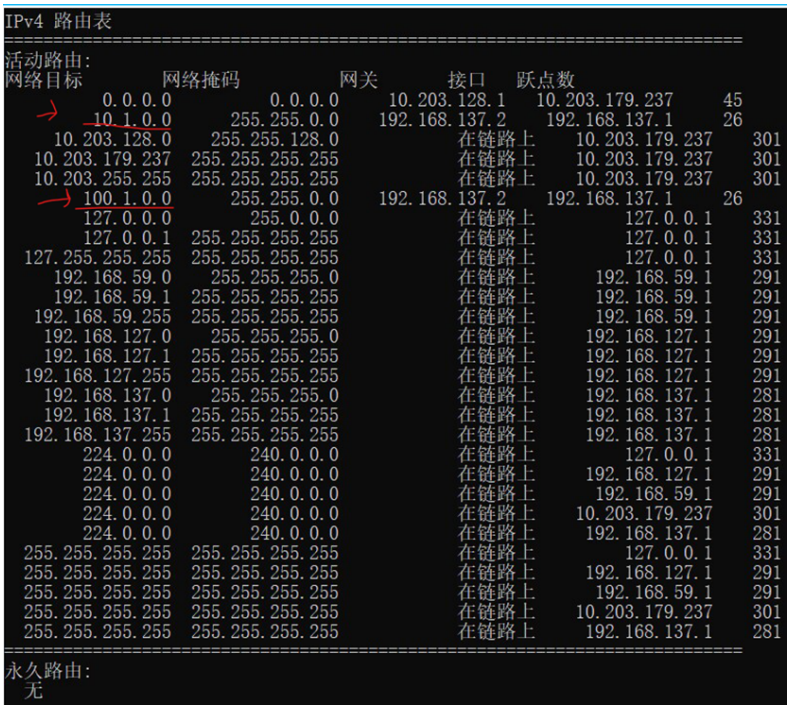
```
命令：route add 10.1.0.0 mask 255.255.0.0 192.168.137.1
作用：添加普通路由规则，指向内网网关。【访问内网】

命令：route add 100.1.0.0 mask 255.255.0.0 192.168.137.1
作用：添加普通路由规则，指向内网网关。【访问内网】
```

共享 PC 路由表中出现的问题



发现有有两条默认路由，一条指向外网，一条指向内网，这样就会导致数据包无法到达外网。依据上述解决方案和代码，修改路由表。

共享 PC 路由表中问题的解决



5.1.3 BGP 过滤

使用 BGP 策略过滤不符合规则路由

- 两校区间 PC 机间可以互访
- 两校区间摄像头间不能互访

在防火墙上设置 ACL 过滤规则，过滤掉不符合规则的路由。除此之外还可以尝试以下方法：

- 配置地址前缀列表

  当需要根据路由的目的地址控制路由的发布和接收时，配置地址前缀列表。

  配置 IPv4 地址前缀列表

```
ip ip-prefix _ip-prefix-name_ [ index _index-number_ ] { **permit** | **deny**
     } _ipv4-address_ _mask-length_ [match-network] [ **greater-equal** _
    greater-equal-value_ ] [ less-equal  _less-equal-value_ ]
```

```
# 使用地址前缀来进行过滤
[] ip ip-prefix myfilter deny 10.1.2.0 24
[] ip ip-prefix myfilter permit 0.0.0.0 0 less-equal 32
[] peer [ipB] as-number [65002]  # 对端 IP 地址，对端自治系统号
[bgp] ipv4-family unicast myprefix import
```

- 配置邻居按需发布路由

```
1. 执行命令**bgp** { _as-number-plain_ | _as-number-dot_ }，进入BGP视图。
2. 执行命令**ipv4-family** **unicast**，进入IPv4单播地址族视图。
3. 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。
4. 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。
5. 缺省情况下，未使能BGP对等体（组）基于地址前缀的ORF功能。
```

使用下面的代码，不让内网网段的数据流出:

```
[huawei] ip ip-prefix myfilter deny 10.1.2.0 24
[huawei] route-policy mypolicy deny node 10
[huawei-route-policy-mypolicy-10] apply ip-prefix myfilter
[huawei-route-policy-mypolicy-10] quit
[huawei] bgp 65001
[huawei-bgp] peer 100.4.20.1 route-policy mypolicy export
[huawei-bgp] quit
```

5.2 知识积累与问答

5.2.1 互联 IP 地址为何使用 30 位掩码网段？

在互联网中，使用 30 位掩码的网段可以提供更多的 IP 地址。一个 30 位掩码的 IP 地址可以支持 4 个主机地址，因为有两个主机地址必须保留（一个用于网络地址，另一个用于广播地址）。这种 IP 地址结构通常用于连接两个网络设备之间的点对点连接，如路由器之间的连接。使用 30 位掩码的网段可以使网络管理员更有效地使用 IP 地址，同时提高网络的安全性和性能。

5.2.2 接入层技术分析

1. VLAN 与 VLANIF 的关系
2. VLANIF 与物理端口的关系
3. 为何接入层部署二层技术，而不直接三层终结？

- access 端口：
  通过 access 端口的数据包都是不带 VLAN tag 的，且只属于一个 VLAN；在 access 端口进方向，交换机接收到数据包后，先判断是否带 VLAN tag，有则丢弃数据包，没有则打上该端口已配置的 VLAN tag；在 access 端口出方向，交换机将打了与端口相同 VLAN tag 的数据包转发出去，并且去掉 VLAN tag 变成普通数据包。
- trunk 端口：
  通过 trunk 端口的数据包都必须带上 VLAN tag；在 trunk 端口进方向，交换机接收到数据包后，先判断是否带 VLAN tag，没有则丢弃数据包，有则按照对应 VLAN 进行转发；在 trunk 端口出方向，交换机将带 VLAN tag 的数据包原封不动转发出去，没有带 VLAN tag 数据包不会从 trunk 端口转发出去。
- VLANIF：
  VLANIF 是基于 VLAN 技术创建的虚拟接口。通过 VLANIF 接口，可以将不同 VLAN 中的设备进行通信，实现跨 VLAN 的互通。
- 二层技术，而不直接三层终结？
  当我们考虑在网络中部署二层技术还是三层技术时，主要是因为这些技术各自有不同的优缺点，需要根据具体的应用场景来选择。
  二层技术主要指的是使用 MAC 地址进行通信和转发的技术:
  - 优点: 转发速度快、网络拓扑简单、不需要配置 IP 地址等。因此，在需要高速转发、对网络拓扑要求不高、或者需要简单部署的场景下，使用二层技术是比较合适的选择。
  - 缺点: 由于二层通信只使用 MAC 地址进行转发，因此不支持跨子网通信。此外，二层技术的广播和组播功能容易引起网络拥塞，而且很难进行流量控制和故障隔离。

  相比之下，三层技术主要指的是使用 IP 地址进行通信和转发的技术
  - 优点: 支持跨子网通信、可以进行流量控制和故障隔离、支持广播和组播控制等。在需要进行跨子网通信、需要进行路由控制、需要进行故障隔离等场景下，使用三层技术是比较合适的选择

  总的来说，当我们需要在网络中部署二层技术还是三层技术时，需要根据具体的应用场景来选择。在一些小型的、不需要进行跨子网通信和路由控制的网络中，使用二层技术可能更加合适；而在一些大型的、需要进行跨子网通信和路由控制的网络中，使用三层技术可能更加合适。同时，也可以结合二层和三层技术的优点，采用混合的网络架构，来更好地满足不同的需求。

5.2.3 路由冗余保护原理

RRP 协议的原理是：在网络中存在多个路由器时，每个路由器都会通过 RRP 协议发送 RRP 报文，向其它路由器宣告自己的存在。路由器之间通过 RRP 报文交互，从而发现所有的邻居路由器，并维护一个 RRP 邻居表。如果某个路由器失效，其它路由器可以通过 RRP 邻居表快速地发现该路由器失效，并重新计算路由表，从而保证网络的连通性。

5.2.4 数据面如何实现多个冗余路径

在数据通信中实现多个冗余路径通常需要使用一种叫做“多路径传输”（Multipath Transport）的技术。多路径传输是指在数据通信中同时利用多条不同的通信路径，以提高数据传输的可靠性和效率

在多路径传输中，数据被分成多个数据包，并且这些数据包可以通过不同的路径进行传输。在接收端，这些数据包被重新组合成原始的数据。如果其中一条路径出现了问题，数据包可以通过其他路径重新传输，以保证数据的完整性和可靠性

5.2.5 环路

路由器间出现环路时，报文将在环路中不断循环转发，这可能导致网络出现拥塞、延迟和丢包等问题。

当路由器收到一个报文时，它会查找转发表以确定报文的下一个路由器。如果转发表中指定的下一个路由器是一个在环路上的路由器，那么该报文将被发送到该路由器，该路由器也会将报文继续转发到下一个路由器，从而形成一个循环。

1. 使用动态路由协议：动态路由协议可以动态地计算最短路径，从而避免环路的产生。当网络中某个路由器发生故障或链路状态改变时，动态路由协议可以及时地重新计算最短路径，从而保证网络的正常运行。
2. 使用 Spanning Tree Protocol(STP)：STP 是一种链路层协议，它可以自动建立一个无环树形拓扑结构，从而避免环路的产生。当网络中发生故障时，STP 可以及时地重新计算最短路径，从而保证网络的正常运行。
3. 手动配置路由器转发表：管理员可以手动配置路由器转发表，从而避免将报文发送到在环路上的路由器。这需要管理员具有一定的网络知识和技能，同时也需要对网络进行持续的监控和维护，以确保网络的正常运行。

在本次的实践设计中，汇聚层和核心层交换机形成了环路。

```
undo stp enable
```

5.2.6 缺省路由的作用及其转发原理

缺省路由（Default Route）是指当路由表中没有匹配的目标网络时，路由器所采用的默认路由。它的作用是将数据包发送到一个预定的网关，以使其能够到达目的网络。

当路由器接收到一个数据包时，它会首先检查该数据包的目的 IP 地址，然后查询路由表以确定下一跳的地址。如果路由表中没有与目的 IP 地址匹配的网络，则路由器将查找缺省路由。缺省路由是一个预先定义的路由，它告诉路由器将数据包发送到预设的网关。这个网关可以是另一个路由器，也可以是一个特殊的设备，如网关路由器或防火墙。

在转发数据包时，路由器会根据最长匹配原则进行路由选择。它会查找路由表中与目的 IP 地址最长匹配的网络，并将数据包发送到相应的下一跳。如果没有匹配的网络，路由器就会将数据包转发到缺省路由指定的网关。

缺省路由通常用于连接不同的自治系统或互联网。在这些情况下，路由器可能会收到大量的外部数据包，这些数据包的目的 IP 地址不在本地网络中。如果路由器没有缺省路由，则这些

数据包将被丢弃，从而导致通信中断。通过设置缺省路由，路由器可以将这些数据包转发到指定的网关，以便它们可以到达目的网络。

5.2.7 两个私网终端 P2P 流量如何穿透 NAT

建立 VPN 隧道是一种实现 NAT 穿透的有效方法。通过 VPN 隧道，可以将两个私有网络之间建立一个安全的、加密的通道，以便在不同的 NAT 网络中实现直接通信。

5.2.8 BGP 与 OSPF 应用场景的差别

BGP 是一种自治系统（AS）之间的路由协议，主要用于在不同 AS 之间交换路由信息，例如在互联网中不同 ISP 之间交换路由信息。BGP 可以实现非常复杂的路由策略，例如路径选择、路由筛选和路由汇聚。因此，BGP 适用于需要管理和控制多个自治系统之间路由的场景，例如互联网服务提供商（ISP）之间的路由管理、多个数据中心之间的路由管理等。

相比之下，OSPF 是一种在同一个自治系统内部的路由协议，它主要用于在一个自治系统内部交换路由信息。OSPF 使用开放式最短路径优先算法，可以实现快速且可靠的路由计算。因此，OSPF 适用于需要在同一个自治系统内部进行路由管理的场景，例如企业内部的网络管理、数据中心内部的网络管理等。

5.2.9 关于 ARP 攻击

ARP 协议是将 IP 地址转换成物理地址（MAC 地址）的一种协议，通常在局域网内使用。ARP 攻击者利用 ARP 协议的“请求响应”机制，发送虚假的 ARP 响应包或 ARP 请求包，以欺骗目标主机或路由器，让其将网络流量发送到攻击者所指定的 MAC 地址。常见的 ARP 攻击方式包括以下几种：

1. ARP 欺骗攻击（ARP Spoofing）：攻击者发送虚假的 ARP 响应包，欺骗目标主机或路由器将网络流量发送到攻击者所指定的 MAC 地址。
2. 中间人攻击（Man-in-the-Middle，MitM）：攻击者通过 ARP 欺骗攻击，将自己伪装成网络中的一个合法设备，从而可以获取目标主机或路由器的网络流量，并对其进行篡改或监听。
3. ARP 病毒攻击（ARP Virus）：攻击者通过广播大量的虚假 ARP 请求包，使网络中的所有主机和路由器都认为攻击者的 MAC 地址对应于某个 IP 地址，从而导致网络拥塞或崩溃。

为了防止 ARP 攻击，可以采取以下几种措施：

1. 静态 ARP 绑定（Static ARP Binding）：管理员可以手动配置 ARP 表项，将 IP 地址与 MAC 地址绑定在一起，从而避免虚假 ARP 响应包的欺骗。
2. 使用网络安全设备：如防火墙、入侵检测系统等，可以检测和阻止 ARP 攻击。
3. 安全网络架构设计：合理的网络架构设计可以有效地防止 ARP 攻击，如采用 VLAN 分隔、物理隔离等方式，限制网络攻击的范围和影响。

在实验攻防的过程中，不妨在别的组上配置一条错误的静态 arp 表项

```
在别人的汇聚层交换机上，开始 arp 攻击
所有访问静态PC，都失灵，packet 因为汇聚层交换机的叛变

在静态PC上
# 查看IP地址
ipconfig    //查看IP地址
```

```
在汇聚层交换机上
# 查看arp 映射表
disp display arp all
清除静态ARP表项
reset arp all
配置一条假的 arp 表项
arp static 10.1.2.2 5489-9868-0ec2 vid 20 interface gigabitethernet 0/0/1
# vid 表示 vlan

# arp static
# 在接入层交换机上
[] arp static <ip地址> <改成自己端口的mac,欺骗一下> vlan20 gigabitethernet 0/0/1

就把中间的Mac地址改变一下
arp static 10.1.2.2 5489-9868-0ec2 vid 10 interface gigabitethernet 0/0/1
```

5.3 体会与收获

在本次实践中，我们小组齐心合力，通过学习和查阅相关资料，较为圆满的完成了所有的实践任务。

- 知识架构和实践层面：
  我深刻体会到了分层思想的高妙之处，这不仅仅是一种思想，而是一种思维方式。在实践中，我们通过分层思想，将复杂的网络拆分成多个子网络，每个子网络只负责处理自己的事情，这样就大大简化了网络的管理和维护工作，有利于我们小组成员的并行开发。同时，分层思想也使得网络的扩展性得到了很好的保证，只要在合适的层次上添加新的设备，就可以很方便地扩展网络的功能。
- 组织协调层面：
  作为组长，我在组织协调方面做了很多工作，例如制定了实践计划、分配了任务、组织了会议等。在实践过程中，我还积极与其他组员沟通，及时解决了遇到的问题，使得我们小组的实践顺利进行。在实践结束后，我还积极与其他组员分享了自己的实践经验，帮助他们更好地完成实践任务。

最后，感谢李伟老师和叶言飞老师对本小组实践过程中的指导和帮助，感谢老师们为我们答疑解惑。通过本次实践，使得我对计算机网络知识有了更深刻的理解，同时也积累了宝贵的实践经验。

附录

A 联系作者 & 项目仓库

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。

项目 Github 地址：CN Practice

Email:756778953@qq.com

B 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.cfg
<HUAWEI> copy 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
```

B.1 接入层

- VLAN 配置 access, trunk

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
[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
```

B.2 汇聚层

- vlan & vlanif
- DHCP
- OSPF

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

[] interface gigabitethernet 0/0/3
[0/0/3] port link-type access
[0/0/3] port default vlan 500
```

```
[0/0/3] quit

# trunk 配置
[] interface gigabitethernet 0/0/1
[0/0/1] port link-type trunk
[0/0/1] port trunk allow-pass vlan 10 20
[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。
[Vlanif10] dhcp server dns-list 114.114.114.114  # 可尝试
```

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
```

B.3 核心层

- vlan & vlanif
- OSPF
- 环路

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
```

B.4 出口层

- 接口 IP 配置
- 出口路由器内网网段发布 OSPF
- 缺省静态路，并发布
- NAT
- 共享网络
- firewall
- VPN：L2TP

ace_AR_out

ip 配置

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

缺省静态路由

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

运营商路由器需要配置进入内网的路由信息，同时共享网络时需要配置到共享网络的缺省静态，配置如下：

```
# 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
# 通向共享网络的缺省路由
[ace_AR_wan]  ip route-static 0.0.0.0 0.0.0.0 192.168.137.1 //下一跳地址
[] ospf 1 router-id 10.1.100.129
[ospf-1] default-route-advertise always
```

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
- 设置有线网卡 ip 地址，选择以太网，右键属性->internet 协议版本 4(TCP/IPV4)-> 属性，配置 ip，子网掩码 DNS 服务器，地址选择 WLAN 中的 DNS 服务器 ip 地址，否则无法打开网页。双击 WLAN- DNS 服务器，地址选择 WLAN 中的 DNS 服务器 ip 地址，否则无法打开网页。双击 WLAN-> 详细信息来查看 DNS 服务器地址。
- 设置另一台电脑有线网卡的 ip 地址，过程同上。ip 地址要在同一局域网内 192.128.137.xxx (xxx 为 1 到 255 的任意数值)，默认网关选择共享网卡的 ip 地址 192.168.137.1，DNS 服务器 ip 地址同共享网卡 ip 地址

运营商网络需要进行同步的配置, 运营商路由器需要配置缺省静态路由

```
# 运营商配置一个缺省的静态路由到共享网络
[AR_wan] ip route-static 0.0.0.0 0.0.0.0 192.168.137.1   # 下一跳地址
[] ospf 1 router-id 10.1.100.129
[ospf-1] default-route-advertise always
```

在做共享的 Windows 电脑上也要配置路由规则，不然这里会出现一些问题：

共享网络 PC 配置路由，参见：Windows：配置多网卡路由表（规则）

```
[windows] route print -4

命令: route delete 0.0.0.0
作用: 将默认路由规则清空。

命令: route add 0.0.0.0 mask 0.0.0.0 <访问外网的网关>
作用: 添加默认路由规则, 指向外网网关。【访问外网】

命令: route add 10.1.0.0 mask 255.255.0.0 192.168.137.1
作用: 添加普通路由规则, 指向内网网关。【访问内网】

命令: route add 100.1.0.0 mask 255.255.0.0 192.168.137.1
作用: 添加普通路由规则, 指向内网网关。【访问内网】
```

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 安全
[0/0/2] zone trust
[0/0/2] quit

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

[] interface gigabitethernet 0/0/1 # 1 号接口 非安全
[0/0/1] ip address 100.1.100.30 30
[0/0/1] zone untrust
[0/0/1] quit
```

在 router 上配置 ACL 过滤规则对外网网段 100.1.0.0 /16 和校园网，BGP，VPN 等进行过滤
外部主机可以到达的地方为：10.1.1.0/24，10.1.101.0/24
注意反掩码

```
[]acl 3102
[acl-adv-3102] rule permit ip source 100.1.0.0 0.0.255.255 destination 10.1.1.0
    0.0.0.255
[acl-adv-3102] rule permit ip source 100.1.0.0 0.0.255.255 destination 10.1.101.0
    0.0.0.255

[acl-adv-3102] rule permit ip source 10.4.0.0 0.0.255.255 destination 10.1.101.0
    0.0.0.255
[acl-adv-3102] rule permit ip source 10.4.0.0 0.0.255.255 destination 10.1.101.0
    0.0.0.255

[acl-adv-3102] rule permit ip source 10.203.128.0 0.0.127.255 destination
    10.1.101.0  0.0.0.255
[acl-adv-3102] rule permit ip source 10.203.128.0 0.0.127.255 destination
    10.1.101.0  0.0.0.255

[acl-adv-3102] rule permit ip destination 100.1.1.0  0.0.0.255
[acl-adv-3102] rule permit ip destination 100.1.101.0  0.0.0.255

[acl-adv-3102] rule deny ip
[acl-adv-3102] quit
```

BGP 策略

- 我们 group1 的自治系统号 65001 与第 group4 相连，65004，
- 连接线路 IP，对端：100.4.20.1/24
- 配置 g0/0/4 ip：100.4.20.2/24

```
[] interface gigabitethernet 0/0/4
[0/0/4] ip address 100.4.20.2 24
```

```
# 标识自己
```

```
[AR_1] bgp 65001  # 自治系统号，我们是第一组
[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 100.4.20.1 as-number 65004  # 对端 IP 地址，对端自治系统号

# 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

```
计算机\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\RasMan\Parameters
注意：隧道接口的 ip 地址为 100.1.100.30
```

B.5 WAN 层

在配置出口层路由器时，需要同步配置运营商路由器，配合实现功能。

- IP 配置
- 相关的静态路由

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
```

缺省静态路由：指向出口层路由器

```
# 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

```
# 运营商配置一个缺省的静态路由到共享网络
[AR_wan] ip route-static 0.0.0.0 0.0.0.0 192.168.137.1   # 下一跳地址
[] ospf 1 router-id 10.1.100.129
[ospf-1] default-route-advertise always
```

C 效果检验

- 各层设备配置检验
- 内网路由测试
- 内网上网测试
- 防火墙测试
- VPN 连接测试
- BGP 域间测试

详情请见 Github 项目中的《效果检验》文档：Github 项目: 效果检验