

中国矿业大学
计算机科学与技术学院

2016 级本科生课程报告

课程名称 网络系统与安全实践

班 级 信息安全 2016-3 班

姓 名 骆信智、刘佳静

赵蓓蓓、黄雅文

报告时间 2019.07.06

任课教师 谢林

分 工

姓名	完成的工作情况
骆信智	设计网络互联与网络安全解决方案，设计拓展部分拓扑图并配置命令，绘制拓扑图。
刘佳静	设计网络互联与网络安全解决方案，设计拓展部分拓扑图并配置命令，撰写实验报告。
赵蓓蓓	设计网络互联与网络安全解决方案，设计综合实验主体拓扑图并配置命令，连接拓扑实验。
黄雅文	设计网络互联与网络安全解决方案，设计综合实验主体拓扑图并配置命令，连接拓扑实验。

2018-2019 学年 第二学期

《网络系统与安全实践》课程报告评分表

(小组成员每人单独一页)

姓名 骆信智 学号 08163337 班级 信息安全

2016-3 班

编号	课程教学目标	考查方式与考查点	占比	得分
1	(3.4) 目标 1: 根据指定场景, 独立设计网络互联与网络安全解决方案。	方案答辩; 解决方案的合理性、可行性和完备性, 文档规范性;	30%	
2	(4.2) 目标 2: 掌握网络互联设备网络安全设备的配置和使用, 能综合运用网络与安全的基本原理和技术, 解决网络互联与网络安全的具体实践问题, 具备设计与实施网络互联与网络安全工程的能力。	现场检查实验结果和配置文件, 问题提问;	40%	
3	(9.1) 目标 3: 通过分组实验, 锻炼合作团队意识, 锻炼组长的统筹协调能力。	分工情况是否合理, 各组员所完成任务情况;	10%	
4	(10.3) 目标 4: 能够就课程方案设计的过程撰写较为规范的课程报告, 在课程报告审查和方案答辩过程中清晰表达设计思路、出现的问题及解决方案。	课程报告; 课程报告的规范性和正确性;	20%	
	总分			

评阅人:

2018-2019 学年 第二学期

《网络系统与安全实践》课程报告评分表

(小组成员每人单独一页)

姓名 刘佳静 学号 08163340 班级 信息安

全 2016-3 班

编号	课程教学目标	考查方式与考查点	占比	得分
1	(3.4) 目标 1: 根据指定场景, 独立设计网络互联与网络安全解决方案。	方案答辩; 解决方案的合理性、可行性和完备性, 文档规范性;	30%	
2	(4.2) 目标 2: 掌握网络互联设备网络安全设备的配置和使用, 能综合运用网络与安全的基本原理和技术, 解决网络互联与网络安全的具体实践问题, 具备设计与实施网络互联与网络安全工程的能力。	现场检查实验结果和配置文件, 问题提问;	40%	
3	(9.1) 目标 3: 通过分组实验, 锻炼合作团队意识, 锻炼组长的统筹协调能力。	分工情况是否合理, 各组员所完成任务情况;	10%	
4	(10.3) 目标 4: 能够就课程方案设计的过程撰写较为规范的课程报告, 在课程报告审查和方案答辩过程中清晰表达设计思路、出现的问题及解决方案。	课程报告; 课程报告的规范性和正确性;	20%	
	总分			

评阅人:

2018-2019 学年 第二学期

《网络系统与安全实践》课程报告评分表

(小组成员每人单独一页)

姓名 赵蓓蓓 学号 08163275 班级 信息安

全 2016-3 班

编号	课程教学目标	考查方式与考查点	占比	得分
1	(3.4) 目标 1: 根据指定场景, 独立设计网络互联与网络安全解决方案。	方案答辩; 解决方案的合理性、可行性和完备性, 文档规范性;	30%	
2	(4.2) 目标 2: 掌握网络互联设备网络安全设备的配置和使用, 能综合运用网络与安全的基本原理和技术, 解决网络互联与网络安全的具体实践问题, 具备设计与实施网络互联与网络安全工程的能力。	现场检查实验结果和配置文件, 问题提问;	40%	
3	(9.1) 目标 3: 通过分组实验, 锻炼合作团队意识, 锻炼组长的统筹协调能力。	分工情况是否合理, 各组员所完成任务情况;	10%	
4	(10.3) 目标 4: 能够就课程方案设计的过程撰写较为规范的课程报告, 在课程报告审查和方案答辩过程中清晰表达设计思路、出现的问题及解决方案。	课程报告; 课程报告的规范性和正确性;	20%	
	总分			

评阅人:

2018-2019 学年 第二学期

《网络系统与安全实践》课程报告评分表

(小组成员每人单独一页)

姓名 黄雅文 学号 08163278 班级 信息安

全 2016-3 班

编号	课程教学目标	考查方式与考查点	占比	得分
1	(3.4) 目标 1: 根据指定场景, 独立设计网络互联与网络安全解决方案。	方案答辩; 解决方案的合理性、可行性和完备性, 文档规范性;	30%	
2	(4.2) 目标 2: 掌握网络互联设备网络安全设备的配置和使用, 能综合运用网络与安全的基本原理和技术, 解决网络互联与网络安全的具体实践问题, 具备设计与实施网络互联与网络安全工程的能力。	现场检查实验结果和配置文件, 问题提问;	40%	
3	(9.1) 目标 3: 通过分组实验, 锻炼合作团队意识, 锻炼组长的统筹协调能力。	分工情况是否合理, 各组员所完成任务情况;	10%	
4	(10.3) 目标 4: 能够就课程方案设计的过程撰写较为规范的课程报告, 在课程报告审查和方案答辩过程中清晰表达设计思路、出现的问题及解决方案。	课程报告; 课程报告的规范性和正确性;	20%	
	总分			

评阅人:

目 录

1 知识储备	1
2 拓扑图	1
2.1 主体拓扑文件	1
2.2 拓展拓扑示意图	2
3 网络描述	2
4 IP 地址表	7
5 配置文件	8
6 结论验证	19
6.1 Site1 验证	19
6.2 Site2 验证	20
6.3 Natp+acl 验证	21
6.4 VPN 验证	22
7 思考体会	22

1 知识储备

路由器：连接两个或多个网络的硬件设备，在网络间起网关的作用，读取每一个数据包中的地址然后决定如何传送的专用智能性的网络设备。

网关：网关(Gateway)又称网间连接器、协议转换器。网关在网络层以上实现网络互连，是最复杂的网络互连设备，仅用于两个高层协议不同的网络互连。与网桥只是简单地传达信息不同，网关对收到的信息要重新打包，以适应目的系统的需求。

交换机：交换机(Switch)意为“开关”是一种用于电(光)信号转发的网络设备。它可以为接入交换机的任意两个网络节点提供独享的电信号通路。最常见的交换机是以太网交换机。其他常见的还有电话语音交换机、光纤交换机等。

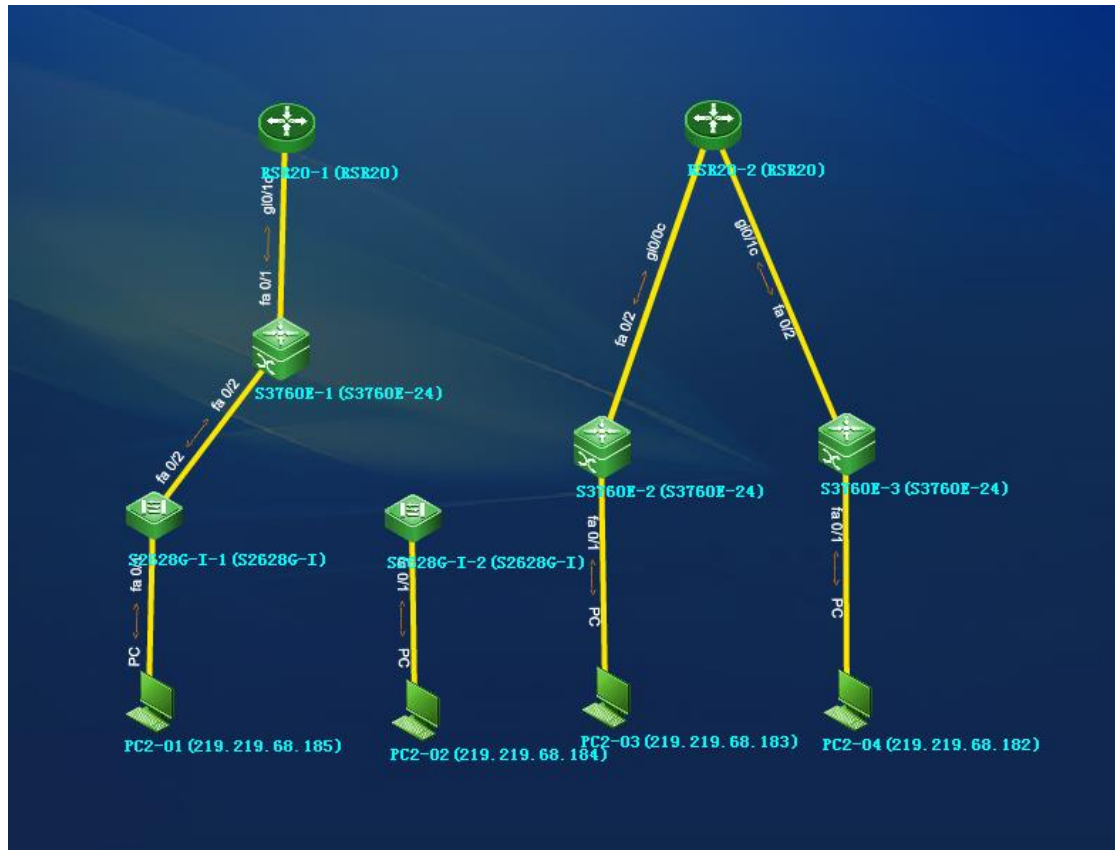
ospf：开放式最短路径优先(Open Shortest Path First, OSPF)是目前广泛使用的一种动态路由协议，它属于链路状态路由协议，具有路由变化收敛速度快、无路由环路、支持变长子网掩码(VLSM)和汇总、层次区域划分等优点。

防火墙：防火墙技术是通过有机结合各类用于安全管理与筛选的软件和硬件设备，帮助计算机网络于其内、外网之间构建一道相对隔绝的保护屏障，以保护用户资料与信息安全性的一种技术。

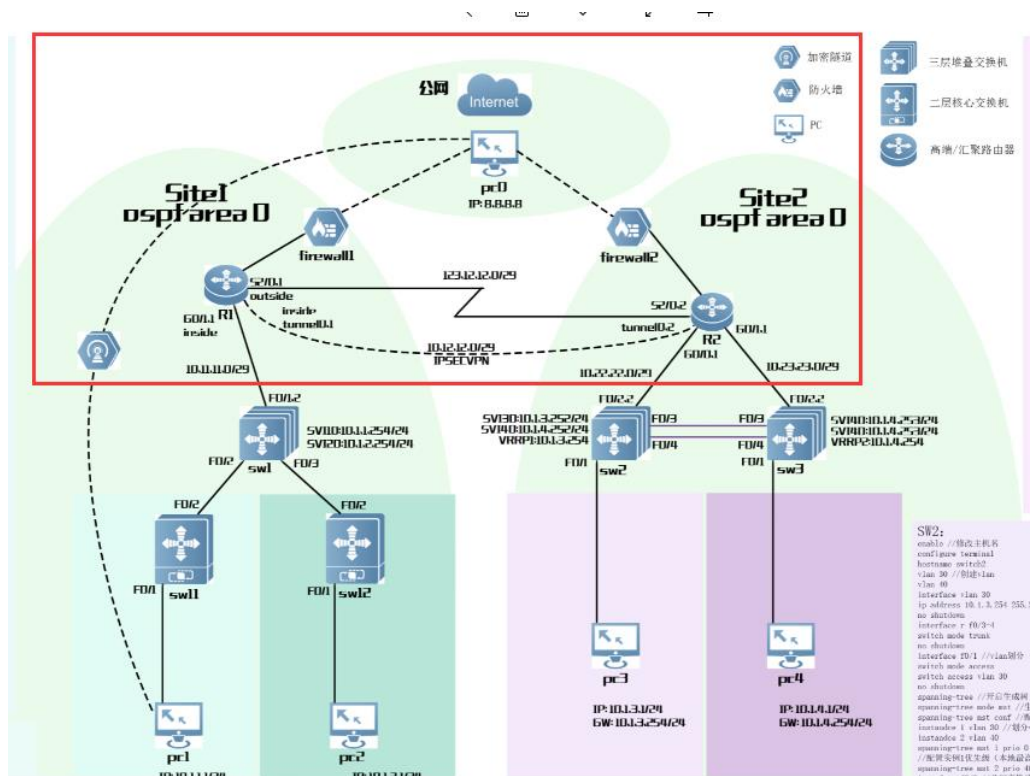
VPN：在公用网络上建立专用网络，进行加密通讯。在企业网络中有广泛应用。VPN 网关通过对数据包的加密和数据包目标地址的转换实现远程访问。VPN 有多种分类方式，主要是按协议进行分类。VPN 可通过服务器、硬件、软件等多种方式实现。

2 拓扑图

2.1 主体拓扑文件



2.2 拓展拓扑示意图



3 网络描述

某公司网络拓扑区域划分为母公司 Site1，子公司 Site2。

PC1 和 PC2 分属 VLAN10 和 VLAN20，其中 SW11 连接 PC1，SW12 连接 PC2，SW11 和 SW12 再统一连接到交换机 SW1 上，通向路由 R1。

PC3 和 PC4 分属 VLAN30 和 VLAN40，其中 SW2 连接 PC3，SW3 连接 PC4，SW2、SW3 通向路由 R2。R1、R2 之间通过建立 tunnel0 建立连接。

在公网和内网搭建防火墙并进行配置，过滤恶意流量。公网有主机 PC0，IP 地址为 8.8.8.8，分别经过 Firewall 1 和 Firewall 2 与 Site1、site2 连通，保证与外网通信。

在公网 PC0 和 site1 间建立加密隧道连接，使公网用户能安全地直接访问内网。公网 PC0 与 site1 的 VLAN10 之间增设 VPN，可直接访问。

在 SW1 上连接到 radius 服务器，开启用户远程登陆的认证、授权、审计功能。

在 SW3\4 上配置 VRRP(虚拟路由冗余网关)，vlan30 的主虚拟网关位于 SW3，VLAN40 的主虚拟网关位于 SW4。当交换机检测上行链路转发故障时自动降低本地 vrrp 进程优先级，虚拟网关身份切换到 peer 端。

用 IPSEC 加密 Tunnel 隧道，模式为隧道模式。规定 IKE 第一阶段采用预共享密钥的方式建立安全关联，IKE 第二阶段采用 256 位 aes 加密数据、sha 用于数据哈希校验。

在 SW3\4 交换口上启用 mac 地址绑定，若检测到主机 mac 改动立即关闭端口。

为简化以后的网络维护和方便管理公司中计算机的 IP 地址，需要配置 DHCP 服务，使计算机能自动获取 IP 地址；为防止网络中可能出现的链路回路问题，需要开启交换机的链路冗余功能；在传输链路的主干上配置端口聚合，提高干道的传输速率。在设备配置中，对交换机进行了 VLAN 的划分，配置了静态路由和动态路由，对路由器进行了 NAT 地址转换配置。

Site1

1、site1 的部门 Office1 属于 VLAN10，网关指向 SW1 的 svi10 接口，部门 Office2 属于 VLAN20，网关指向 SW1 的 svi20 接口。

2、SW1 和边界路由器 R1 之间启用动态路由协议 OSPF。

验证：位于 VLAN10 和 VLAN20 的 PC1、PC2 互通，R1 与 SW1 建立路由邻居并收到 VLAN10、20 的路由明细。

Site2

1、site2 的部门 Office3 属于 VLAN30，网关指向 SW2 的 svi30 接口，部门 Office4 属于 VLAN40，网关指向 SW3 的 svi40 接口。

2、SW2、SW3 起 Trunk 放行 VLAN，并分别与边界路由器 R2 建立 ospf 邻居，在区域 0 中宣告所有本地直连路由。

验证：位于 VLAN30 和 VLAN40 的 PC3、PC4 互通，R2 与 SW2、SW3 建立 ospf 邻居并收到 VLAN30、40 的路由明细。

Tunnel 10

1、在 R1、R2 上建立 tunnel10，源目的地址分别为自己和对端的串口。

2、R1、R2 通过 tunnel 隧道建立 ospf 邻居。

验证：tunnel 口创建成功，r1、r2 建立 ospf 邻居，PC1、PC2、PC3、PC4 四个部门互通。

Natp+acl

1、R1 作为 site1 唯一网络出口默认路由指向外网接口 s2/0，并下发默认路由。

2、R1 的 s2/0 上开启端口复用 nat 对所有来自 site1 内部访问外网 PC0 的流量进行地址转换。

3、编写标准 acl 在 SW2 入方向放行 pc3 到所有目标地址的流量。

4、编写拓展 acl 应用在 SW3 入方向只拒绝 PC4 访问 PC0 的流量。

验证：所有 pc 互通；除 PC4 均能访问公网 PC0 8.8.8.8；site1 去往外部的流量实现 natp 转换。

防火墙

1、在外网主机 PC0 与路由器 R1 间设置防火墙 Firewall 1，源目的地址分别为自己和对端的串口。

2、在外网主机 PC0 与路由器 R2 间设置防火墙 Firewall 2，源目的地址分别为自己和对端的串口。

3、R1、R2 通过 Firewall 1、Firewall 2 与外网建立通信联系。

验证：在符合防火墙规定标准之下，满足安全性能以及类型才可以进行信息的传递，而一些不安全的因素则会被防火墙过滤、阻挡。

防火墙具体配置

1、Web 登录设备

用网线将 pc 网卡连接设备 MGMT(或者 internal, switch)口, 并设置网卡 ip 地址。进入浏览器, 登录设备。

输入用户名 admin, 密码 firewall (设备默认为网关模式), 网关模式下默认用户名和密码 admin/firewall。

2、选择运行模式, 默认为 NAT(路由) 模式

固件版本	V5.2-R5.08.3900(p0) [更新]
系统配置	最后一次备份: N/A [备份] [恢复]
运行模式	NAT [修改]
虚拟域	停用 [启用]
当前管理员	1 [细节]
当前用户	admin [修改密码]

3、配置接口 ip 地址和子网掩码

名称	wan1
别名	<input type="text"/>
连接状态	Up
类型	物理接口

地址模式	<input checked="" type="radio"/> 自定义 <input type="radio"/> DHCP <input type="radio"/> PPPoE
IP/子网掩码	<input type="text" value="202.1.1.10/30"/>

管理访问	<input checked="" type="checkbox"/> HTTPS <input checked="" type="checkbox"/> PING <input type="checkbox"/> HTTP <input type="checkbox"/> SSH <input type="checkbox"/> SNMP <input type="checkbox"/> TELNET
------	--

4、配置默认路由

新建静态路由	
目的IP/子网掩码	<input type="text" value="0.0.0.0/0.0.0.0"/>
设备	<input type="text" value="wan1"/>
网关	<input type="text" value="202.1.1.9"/>
路径长度	<input type="text" value="10"/> (1-255)
优先级	<input type="text" value="0"/> (0-4294967295)
注释	<input type="text"/>
<div>确定 取消</div>	

5、配置上网策略

编辑输出策略

源接口/区

internal

源地址

all

多个

目的接口/区

wan1

目的地址

all

多个

时间表

always

服务

ALL

多个

动作

ACCEPT

记录允许流量

NAT

不使用 NAT

启用 NAT

使用中央NAT表

动态IP地址池

Session TTL

0

(300-604800)

6、开启反病毒功能

动作

ACCEPT

记录允许流量

NAT

不使用 NAT

启用 NAT

使用中央NAT表

动态IP地址池

Session TTL

0

(300-604800)

启用基于用户认证的策略

UTM

代理选项

default

启用病毒检测

default

启用IPS

请选择

启用Web过滤器

请选择

启用email过滤器

请选择

启用DLP传感器

请选择

启用应用控制

请选择

7、流控功能

使用中央NAT表

Session TTL (300-604800)

☐ 启用基于用户认证的策略

☒ UTM

☒ 代理选项

default

▼

☒ 启用病毒检测

default

▼

☐ 启用IPS

[请选择]

▼

☐ 启用Web过滤器

[请选择]

▼

☐ 启用email过滤器

[请选择]

▼

☐ 启用DLP传感器

[请选择]

▼

☐ 启用应用控制

default

▼

☐ 启用VoIP

[请选择]

▼

☐ 启用SSL/SSH检测

[请选择]

▼

☐ 流量控制

low-priority

▼

☐ 反向流量控制

[请选择]

▼

☒ 针对每个IP的流量整形

1M

▼

名称

1M

☒ 最大带宽

1024

(1-16776000 Kbps)

☒ 最大并发连接数

300

x (1-2097000)

☐ 正向差分服务代码点

000000

(000000 - 111111)

☐ 反向差分服务代码点

000000

(000000 - 111111)

确定

取消

VPN

1、公网 PC0 可通过 VPN 访问 site1 的 PC1，建立连接。

验证：VPN 创建成功，PC0 通过 VPN，输入账号密码，可访问 PC1，PC0 与 PC1 互通。

(具体配置命令见 5 配置文件说明)

4 IP 地址表

设备名	IP 地址	子网掩码	网关地址	备注
PC0	8. 8. 8. 8	/	/	公网
PC1	10. 1. 1. 1	255. 255. 255. 0	10. 1. 1. 254	VLAN10
PC2	10. 1. 2. 1	255. 255. 255. 0	10. 1. 2. 254	VLAN20
PC3	10. 1. 3. 1	255. 255. 255. 0	10. 1. 3. 254	VLAN30
PC4	10. 1. 4. 1	255. 255. 255. 0	10. 1. 4. 254	VLAN40

5 配置文件

（VPN 安全隧道配置包含于各设备命令之后）

配置 SW1

```
enable //修改主机名
```

```
configure terminal
```

```
hostname switch1
```

```
spanning-treeenableing-tree //开启生成树
```

```
spanning-treeenableing-tree mode rstp
```

```
vlan 10 //创建 vlan
```

```
vlan 20
```

```
interface f0/2 //划分 vlan
```

```
switch mode access
```

```
switch access vlan 10
```

```
no shutdown
```

```
interface f0/3
```

```
switch mode access
```

```
switch access vlan 20
```

```
no shutdown
```

```
interface vlan 10 //进入 svi 口
```

```
ip address 10.1.1.254 255.255.255.0 //设置 svi 的 ip 地址
```

```
no shutdown //打开接口
```

```
interface vlan 20 //设置 svi 口
```

```
ip address 10.1.2.254 255.255.255.0
```

```
no shutdown
```

```
interface f0/1 //进入接口
```

```
no switch //关闭交换功能（打开路由功能）
ip address 10.11.11.2 255.255.255.248 //配置 ip
no shutdown //开启接口

router ospf 1 //开启 ospf 进程 1
network 10.1.1.0 0.0.0.255 area 0 //在 area 0 中宣告网段 10.1.1.0/24
network 10.1.2.0 0.0.0.255 area 0 //宣告网段 10.1.1.0/24
network 10.11.11.0 0.0.0.7 area 0 //宣告网段 10.11.11.0/29

aaa new-mode //开启 AAA
radius-server hostname 150.1.1.1 //AAA 服务器 ip
radius-server key ruijie //用于连接 radius 服务器的密钥 ruijie

aaa authentication login ruijie group radius local
//登录方法认证列表 ruijie，优先采用 radius 组认证其次本地组
aaa local authentication attempts 3 //允许 3 次登录失败
aaa local authentication lockout-time 1 //连续 3 次输错密码锁定账户 1 小时

username admin password ruijie //创建本地用户 admin 密码 ruijie
username admin privilege 15 //用户权限 15 级

aaa authentication exec execauth group radius local
//登陆授权列表 execauth，优先采用 radius 组认证其次本地组
aaa authentication commands 15 commauth group radius local
//命令授权列表 commauth，优先采用 radius 组认证其次本地组
aaa accounting exec execaccount start-stop group radius local
//登入登出审计列表 execaccount，优先采用 radius 组认证其次本地组
aaa accounting commands 15 commaccount start-stop group radius local
//命令审计列表 commaccount，优先采用 radius 组认证其次本地组

line vty 0 4 //进入接口 vty
login authentication ruijie //接口下调用认证列表
login authentication exec execauth //接口下调用登陆授权列表
login authentication commands commauth //接口下调用命令授权列表
```


accounting exec execaccout //接口下调用登入登出审计列表

accounting commands 15 commaccout //接口下调用命令登出审计列表

```
Sw1(config-if-FastEthernet 0/2)#no shutdown
Sw1(config-if-FastEthernet 0/2)#int vlan 10
Sw1(config-if-VLAN 10)#*Jul  4 15:15:54: %LINEPROTO-5-UPDOWN: Line protocol on I
nterface VLAN 10, changed state to up.

Sw1(config-if-VLAN 10)#ip add 10.1.1.254 255.255.255.0
Sw1(config-if-VLAN 10)#no shutdown
Sw1(config-if-VLAN 10)#int fa0/1
Sw1(config-if-FastEthernet 0/1)#no sw
Sw1(config-if-FastEthernet 0/1)#ip add 10.11.11.2 255.255.255.248
Sw1(config-if-FastEthernet 0/1)#no shutdown
Sw1(config-if-FastEthernet 0/1)#router os 1
Sw1(config-router)#net 10.1.1.0 0.0.0.255 are 0
Sw1(config-router)#net 10.1.2.0 0.0.0.255 are 0
Sw1(config-router)#net 10.11.11.0 0.0.0.7 are 0
Sw1(config-router)#
```

配置 SW2

enable //修改主机名

configure terminal

hostname switch2

vlan 30 //创建 vlan

vlan 40

interface vlan 30

ip address 10.1.3.254 255.255.255.0

no shutdown

interface r f0/3-4

switch mode trunk

no shutdown

interface f0/1 //vlan 划分

switch mode access

switch access vlan 30

no shutdown

spanning-tree //开启生成树

spanning-tree mode mst //生成树模式 mst

spanning-tree mst conf //配置 mst

instandce 1 vlan 30 //划分 vlan30 到 mst 实例 1

instandce 2 vlan 40

spanning-tree mst 1 prio 0

//配置实例 1 优先级（本地最高）

spanning-tree mst 2 prio 4096 //配置实例 2 优先级

interface f0/2 //关闭交换功能配置三层 ip

```
no switch
ip address 10.22.22.2 255.255.255.248
no shutdown
router ospf 1
//开启 ospf 进程并在 area 0 中宣告路由
network 10.22.22.0 0.0.0.7 area 0
network 10.1.3.0 0.0.0.255 area 0
network 10.1.4.0 0.0.0.255 area 0
ip access-list stand 10 //标准的访问控制列表 10
permit host 10.1.3.1
//放行源地址是 10.1.3.1 的所有流量
interface f0/1 //进入接口
ip access-group 10 in
//将 ACL 10 接口下调用在接口的入方向
int vlan 30
ip address 10.1.3.252 255.255.255.0
vrrp 1 version 2 //vrrp 进程 1 版本 2
vrrp 1 ip 10.1.3.254 //虚拟网关 10.1.3.254
vrrp 1 prio 100 //本地进程优先级 100（主）
vrrp 1 preempt
//开启抢占，进程优先级高的会抢占成为主设备
vrrp 1 track f0/2 20
//监控 f0/2 状态，如果异常优先级降低 20
int vlan 40
ip add 10.1.4.252 255.255.255.0
vrrp 2 version 2 //进程 1 版本 2
vrrp 2 ip 10.1.4.254 //虚拟网关 10.1.4.254
vrrp 2 prio 99 //本地进程优先级 99（备）
vrrp 2 preempt //开启抢占
vrrp 2 track f0/2 20
//监控 f0/2 口状态，异常降低优先级
interface f0/2
sw port-security mac-address sticky //端口安全自动绑定 mac
sw port-security violation shutdown //发生违规自动关闭端口
```

```
Sw2(config-mst)#span mst 2 prio 4096
Sw2(config)#int f0/2
Sw2(config-if-FastEthernet 0/2)#no sw
Sw2(config-if-FastEthernet 0/2)#ip add 10.22.22.2 255.255.255.248
Sw2(config-if-FastEthernet 0/2)#no shut
Sw2(config-if-FastEthernet 0/2)#router os 1
Sw2(config-router)#net 10.22.22.0 0.0.0.7 are 0
Sw2(config-router)#net 10.1.3.0 0.0.0.255 are 0
Sw2(config-router)#ip access-list stan 10
Sw2(config-std-nacl)#per host 10.1.3.1
Sw2(config-std-nacl)#int f0/1
Sw2(config-if-FastEthernet 0/1)#ip access-group 10 in
Sw2(config-if-FastEthernet 0/1)#
```

配置 SW3

enable //修改主机名

configure terminal

hostname switch3

vlan 30 //

vlan 40 //创建 vlan40 并设置 svi40 接口

interface vlan 40

ip address 10.1.4.254 255.255.255.0

no shutdown

interface r f0/3-4

switch mode trunk

no shutdown

interface f0/1 //vlan 划分

switch mode access

switch access vlan 40

no shutdown

spanning-tree //配置 mst 生成树

spanning-tree mode mst

spanning-tree mst conf

instandce 2 vlan 40

instandce 1 vlan 30

spanning-tree mst 2 prio 0

spanning-tree mst 1 prio 4096

interface f0/2 //关闭交换功能，打开路由功能

no switch

ip address 10.23.23.2 255.255.255.248

no shutdown

router ospf 1 //开启 ospf 进程 1 并宣告网段

```
network 10.23.23.0 0.0.0.7 area 0
network 10.1.4.0 0.0.0.255 area 0
network 10.1.3.0 0.0.0.255 area 0
ip access-list extenabed 100
//拓展访问控制列表 100
deny ip hostnamet 10.1.4.1 hostnamet 8.8.8.8
//拒绝主机 10.1.4.1 访问主机 8.8.8.8
permit ip any any //放行所有流量
interface f0/1
//进入接口 f0/1 并在入方向接口下调用 ACL100
ip access-group 100 in

int vlan 30
ip address 10.1.3.253 255.255.255.0
vrrp 1 version 2 //版本
vrrp 1 ip 10.1.3.254 //虚拟网关
vrrp 1 prio 99 //优先级（备）
vrrp 1 pre //抢占
vrrp 1 track f0/2 20 //监控端口
int vlan 40
ip add 10.1.4.253 255.255.255.0
vrrp 2 version 2 //版本
vrrp 2 ip 10.1.4.254 //虚拟网关
vrrp 2 prio 100 //优先级（主）
vrrp 2 pre //抢占
vrrp 2 track f0/2 20 //监控端口
interface f0/2
sw port-sec mac-address sticky
//端口安全自动绑定 mac
sw port-sec violation shutdown
//发生违规自动关闭端口
```

```
Sw3(config-if-FastEthernet 0/1)#no shut
Sw3(config-if-FastEthernet 0/1)#int f0/2
Sw3(config-if-FastEthernet 0/2)#no sw
Sw3(config-if-FastEthernet 0/2)#ip add 10.23.23.2 255.255.255.248
Sw3(config-if-FastEthernet 0/2)#no shut
Sw3(config-if-FastEthernet 0/2)#router os 1
Sw3(config-router)#net 10.23.23.0 0.0.0.7 are 0
Sw3(config-router)#net 10.1.4.0 0.0.0.255 are 0
Sw3(config-router)#ip access-list extend 100
Sw3(config-ext-nacl)#deny ip host 10.1.4.1 host 8.8.8.8
Sw3(config-ext-nacl)#per ip any any
Sw3(config-ext-nacl)#int f0/1
Sw3(config-if-FastEthernet 0/1)#ip access-group 100 in
Sw3(config-if-FastEthernet 0/1)#
```

配置 SW11

enable

configure terminal //特权模式

hostname switch11 //命名

vlan 10 //创建 vlan10

spanning-tree //开启生成树

spanning-tree mode rstp //设置生成树模式 rstp

interface f0/1 //进入接口

switch mode access //设置接口模式

switch access vlan 10 //给接口划分 vlan

no shutdown //打开接口

interface f0/2 //划分 vlan

switch mode access

switch access vlan 10

no shutdown

配置 SW12

enable //进入特权模式修改主机名

configure terminal

hostname switch12

vlan 20 //创建 vlan

```
spanning-tree //开启生成树
spanning-tree mode rstp
```

```
interface f0/1 //划分 vlan
switch mode access
switch access vlan 20
no shutdown
```

```
interface f0/2 //划分 vlan
switch mode access
switch access vlan 20
no shutdown
```

```
Sw12(config)#spanning-tree mode rstp
Sw12(config)#int F0/1
Sw12(config-if-FastEthernet 0/1)#switch mode access
Sw12(config-if-FastEthernet 0/1)#sw acc vlan 20
Sw12(config-if-FastEthernet 0/1)#no shutdown
Sw12(config-if-FastEthernet 0/1)#exit
Sw12(config)#int F0/5
Sw12(config-if-FastEthernet 0/5)#switch mode access
Sw12(config-if-FastEthernet 0/5)#switch access vlan 20
Sw12(config-if-FastEthernet 0/5)#no shutdown
Sw12(config-if-FastEthernet 0/5)#end
```

配置 R1

```
enable
configure terminal
hostname R1
```

```
interface gi0/1 //给接口配置 ip
ip address 10.11.11.1 255.255.255.248
no shutdown
```

```
interface s2/0
ip address 123.12.12.1 255.255.255.248
no shutdown
interface tunnel 0 //
```

配置 tunnel 口，设置模式、协议、IP 地址、源目

```
tunnel mode gre ip
tunnel source 123.12.12.1
tunnel destination 123.12.12.2
ip address 10.12.12.1 255.255.255.248
no shutdown

router ospf 1 //ospf进程 1

network 10.11.11.0 0.0.0.7 area 0 //宣告接口
network 10.12.12.0 0.0.0.7 area 0
default-info originate //给邻居下发默认路由

ip route 0.0.0.0 0.0.0.0 ser2/0 //配置静态默认路由

ip access-list extend NAT //拓展 ACL NAT
permit ip 10.1.0.0 0.0.255.255 host 8.8.8.8 //
允许源自 10.1.0.0/16 的 ip 层流量访问主机 8.8.8.8

exit //退出

ip nat inside source list NAT interface s2/0 overload //
动态 nat 在 s2/0 接口端口复用

interface s2/0
ip nat outside //nat 流量为出方向

interface tunnel0
ip nat inside //nat 流量进方向

interface gi0/1
ip nat inside //nat 流量进方向

ip access-list extend 100 //
拓展 ACL 抓取加密感兴趣流
```

per ip 10.0.0.0 0.0.0.255

crypto iskamp police 10 //ike 第一阶段 策略 10

encry 3des //加密算法 3des

authen preshare //协商方法预共享密钥

group 2 //密钥长度 1024

crypto iskamp key 7 ruijie add 10.12.12.2 //

加密的共享密钥 ruijie, 对端 ip10.12.12.2

crypto ipsec transform-set IPSEC esp-aes-256 esp-sha-hmac

//ike 第二阶段 设置传输集 IPSEC, 约定 esp 协议封装数据包、加

密算法 256 位 aes、哈希算法 sha

mode tunnel //加密模式位传输

crypto map VPN 1 ipsec-iskamp //配置加密映射表 VPN 策略 1

set transform-set IPSEC //设定传输集 IPSEC

set peer 10.12.12.2 //设置对端 ip10.12.12.2

match add 100 //匹配感兴趣流量

int tunnel0

crypto map VPN //接口下调用加密策略


```
[Message : Hello, welcome to lookon experiment.]

[Message : Device is RSR20-1]
enable
Ruijie#config
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)#hostname R1
R1(config)#int gi0/1
R1(config-if-GigabitEthernet 0/1)#ip add 10.11.11.1 255.255.255.248
R1(config-if-GigabitEthernet 0/1)#no shutdown
R1(config-if-GigabitEthernet 0/1)#int s2/0
R1(config-if-Serial 2/0)#ip add 123.12.12.1 255.255.255.248
R1(config-if-Serial 2/0)#no shutdown
R1(config-if-Serial 2/0)#exit
R1(config)#int tun 0
R1(config-if-Tunnel 0)#tunnel mode gre ip
R1(config-if-Tunnel 0)#tun so 123.12.12.1
R1(config-if-Tunnel 0)#tun dest 123.12.12.2

R1(config-if-Tunnel 0)#ip add 10.12.12.1 255.255.255.248
R1(config-if-Tunnel 0)#no shutdown
R1(config-if-Tunnel 0)#exit
R1(config)#router os 1
R1(config-router)#net 10.11.11.0 0.0.0.7 area 0
R1(config-router)#net 10.12.12.0 0.0.0.7 area 0
R1(config-router)#default-info ori
R1(config-router)#ip route 0.0.0.0 0.0.0.0 ser2/0
R1(config)#ip access-list extend NAT
R1(config-ext-nacl)#per ip 10.1.0.0 0.0.255.255 host 8.8.8.8
R1(config-ext-nacl)#exit
R1(config)#ip nat inside source list NAT int s2/0 overload
R1(config)#int s2/0
R1(config-if-Serial 2/0)#ip nat outside
R1(config-if-Serial 2/0)#int tunnel 0
R1(config-if-Tunnel 0)#ip nat inside
R1(config-if-Tunnel 0)#int gi0/1
R1(config-if-GigabitEthernet 0/1)#ip nat inside
R1(config-if-GigabitEthernet 0/1)#exit
R1(config)#show run
```

配置 R2

enable

configure terminal

hostname R2

interface gi0/0 //打开接口配置 ip

ip address 10.22.22.1 255.255.255.248

no shutdown

interface gi0/1

ip address 10.23.23.1 255.255.255.248

no shutdown

interface s2/0

ip address 123.12.12.2 255.255.255.248

no shutdown

interface tunnel 0 //进入 tunnel 口 0

tunnel mode gre ip //tunnel 模式为 gre, ip 支持 ipv4

```
tunnel source 123.12.12.2 //设置 tunnel 源
tunnel destination 123.12.12.1 //设置 tunnel 目的
ip address 10.12.12.2 255.255.255.248 //给 tunnel 口配置 ip 地址
no shutdown //开启接口

interface lo 0 //进入环回接口 loopback0
ip address 8.8.8.8 255.255.255.255 //配置 ip

router ospf 1 //ospf 进程 1
network 10.22.22.0 0.0.0.7 area 0 //在 area 0 宣告路由
network 10.23.23.0 0.0.0.7 area 0
network 10.12.12.0 0.0.0.7 area 0

ip access-list extend 100 //同 R1
per ip 10.0.0.0 0.0.0.255
crypto isakmp police 10
encr 3des
authen preshare
group 2
crypto isakmp key 7 ruijie add 10.12.12.1
crypto ipsec transform-set IPSEC esp-aes-256 esp-sha-hmac mode tunnel
crypto map VPN 1 ipsec-isakmp
set transform-set IPSEC
set peer 10.12.12.1
match add 100
int tunnel0
crypto map VPN
```

6 结论验证

6.1 Site1 验证

PC1 可 ping 通 PC2

```
C:\Users\Administrator>ping 10.1.2.1

正在 Ping 10.1.2.1 具有 32 字节的数据:
来自 10.1.2.1 的回复: 字节=32 时间<1ms TTL=127
来自 10.1.2.1 的回复: 字节=32 时间<1ms TTL=127
来自 10.1.2.1 的回复: 字节=32 时间<1ms TTL=127
来自 10.1.2.1 的回复: 字节=32 时间<1ms TTL=127

10.1.2.1 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
```

PC2 可 ping 通 PC1

```
C:\Users\Administrator>ping 10.1.1.1

正在 Ping 10.1.1.1 具有 32 字节的数据:
来自 10.1.1.1 的回复: 字节=32 时间=1838ms TTL=124
来自 10.1.1.1 的回复: 字节=32 时间=1786ms TTL=124
来自 10.1.1.1 的回复: 字节=32 时间=1801ms TTL=124
来自 10.1.1.1 的回复: 字节=32 时间=1833ms TTL=124

10.1.1.1 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 = 1786ms, 最长 = 1838ms, 平均 = 1814ms
```

6.2 Site2 验证

PC3 可 ping 通 PC4

```
C:\Users\Administrator>ping 10.1.4.1

正在 Ping 10.1.4.1 具有 32 字节的数据:
来自 10.1.4.1 的回复: 字节=32 时间=1688ms TTL=124
来自 10.1.4.1 的回复: 字节=32 时间=1708ms TTL=124
来自 10.1.4.1 的回复: 字节=32 时间=1703ms TTL=124
来自 10.1.4.1 的回复: 字节=32 时间=1639ms TTL=124

10.1.4.1 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 = 1639ms, 最长 = 1708ms, 平均 = 1684ms
```

PC4 可 ping 通 PC3

```
C:\Users\Administrator>ping 10.1.3.1

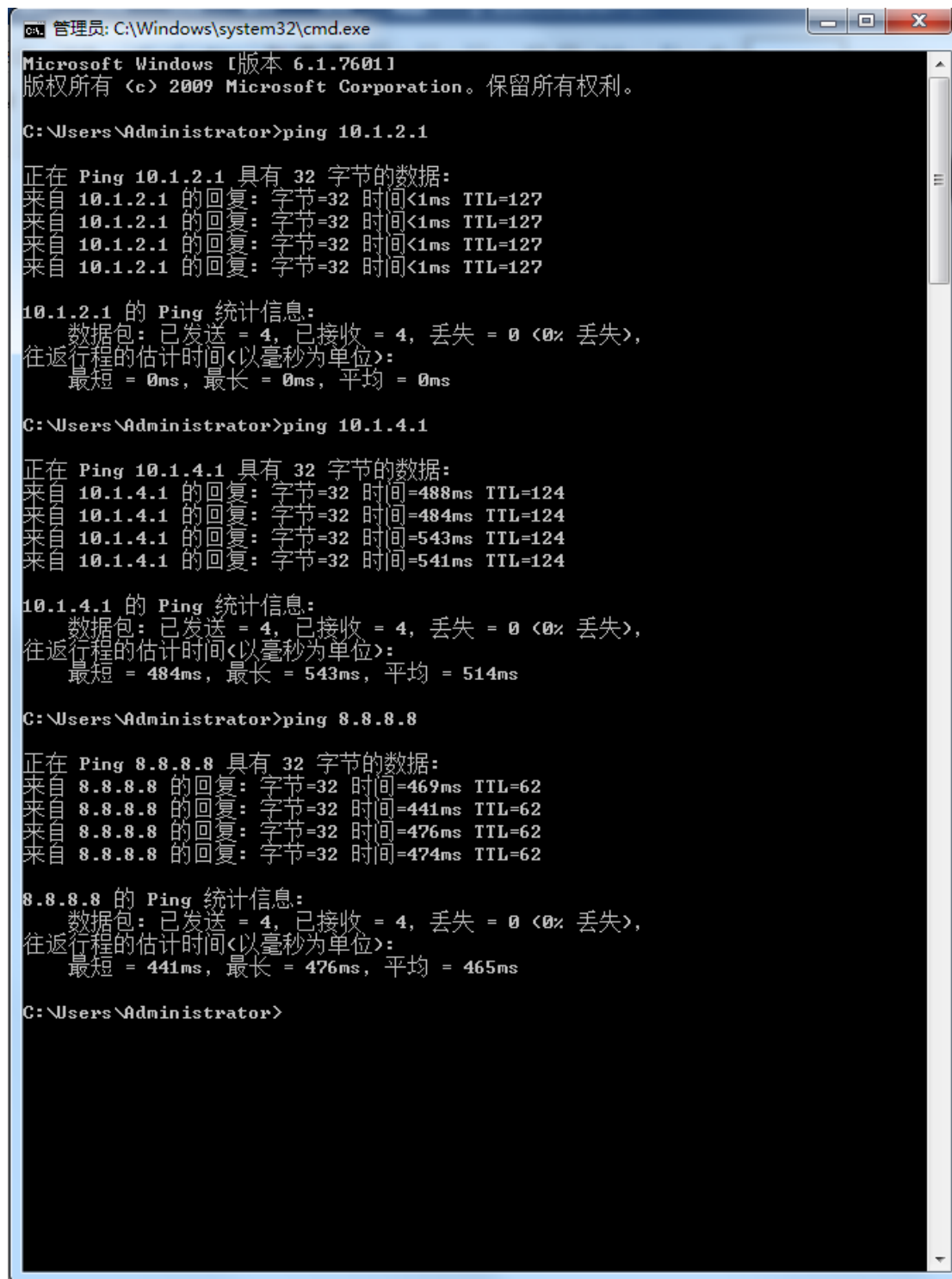
正在 Ping 10.1.3.1 具有 32 字节的数据:
来自 10.1.3.1 的回复: 字节=32 时间<1ms TTL=125
来自 10.1.3.1 的回复: 字节=32 时间<1ms TTL=125
来自 10.1.3.1 的回复: 字节=32 时间<1ms TTL=125
来自 10.1.3.1 的回复: 字节=32 时间<1ms TTL=125

10.1.3.1 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
```

6.3 Natp+acl 验证

所有 PC 均可互通。除 PC4 外，都可 ping 通 PC0 8.8.8.8

(下图为 PC1 ping 的情况)



```
管理员: C:\Windows\system32\cmd.exe
Microsoft Windows [版本 6.1.7601]
版权所有 (c) 2009 Microsoft Corporation。保留所有权利。

C:\Users\Administrator>ping 10.1.2.1

正在 Ping 10.1.2.1 具有 32 字节的数据:
来自 10.1.2.1 的回复: 字节=32 时间<1ms TTL=127
来自 10.1.2.1 的回复: 字节=32 时间<1ms TTL=127
来自 10.1.2.1 的回复: 字节=32 时间<1ms TTL=127
来自 10.1.2.1 的回复: 字节=32 时间<1ms TTL=127

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

C:\Users\Administrator>ping 10.1.4.1

正在 Ping 10.1.4.1 具有 32 字节的数据:
来自 10.1.4.1 的回复: 字节=32 时间=488ms TTL=124
来自 10.1.4.1 的回复: 字节=32 时间=484ms TTL=124
来自 10.1.4.1 的回复: 字节=32 时间=543ms TTL=124
来自 10.1.4.1 的回复: 字节=32 时间=541ms TTL=124

10.1.4.1 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 = 484ms, 最长 = 543ms, 平均 = 514ms

C:\Users\Administrator>ping 8.8.8.8

正在 Ping 8.8.8.8 具有 32 字节的数据:
来自 8.8.8.8 的回复: 字节=32 时间=469ms TTL=62
来自 8.8.8.8 的回复: 字节=32 时间=441ms TTL=62
来自 8.8.8.8 的回复: 字节=32 时间=476ms TTL=62
来自 8.8.8.8 的回复: 字节=32 时间=474ms TTL=62

8.8.8.8 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 = 441ms, 最长 = 476ms, 平均 = 465ms

C:\Users\Administrator>
```

pc4 不能 ping 通 PC0 8.8.8.8

```
C:\Users\Administrator>ping 8.8.8.8

正在 Ping 8.8.8.8 具有 32 字节的数据:
请求超时。
请求超时。
请求超时。
请求超时。

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

6.4 VPN 验证

PC0 可 ping 通 PC1

```
C:\Users\Administrator>ping 10.1.1.1

正在 Ping 10.1.1.1 具有 32 字节的数据:
来自 10.1.1.1 的回复: 字节=32 时间=2070ms TTL=124
来自 10.1.1.1 的回复: 字节=32 时间=2053ms TTL=124
来自 10.1.1.1 的回复: 字节=32 时间=2073ms TTL=124
来自 10.1.1.1 的回复: 字节=32 时间=2045ms TTL=124

10.1.1.1 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 = 2045ms, 最长 = 2073ms, 平均 = 2060ms
```

PC1 可 ping 通 PC0

```
C:\Users\Administrator>ping 8.8.8.8

正在 Ping 8.8.8.8 具有 32 字节的数据:
来自 8.8.8.8 的回复: 字节=32 时间=512ms TTL=62
来自 8.8.8.8 的回复: 字节=32 时间=459ms TTL=62
来自 8.8.8.8 的回复: 字节=32 时间=491ms TTL=62
来自 8.8.8.8 的回复: 字节=32 时间=474ms TTL=62

8.8.8.8 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 = 459ms, 最长 = 512ms, 平均 = 484ms
```

7 思考体会

通过本次课程的学习，我们组对网络系统的安全有了更多认识，尤其是防火墙技术和 VPN 技术，防火墙具有一定的抗攻击能力，对于外部攻击具自我保护的作用。本门课程锻炼了我们的动手实践能力，巩固了以前学过的知识，并拓展了新的知识领域。尤其这门课程可以结合我们一起以前学过的计算机网络相关知识深入学习，受益匪浅。本组分工情况比较合理，各组员都完成了相应任务，也锻炼了我们的团队协作能力。