中国矿业大学
计算机科学与技术学院

2018 级本科生课程设计报告

课程名称： 网络系统与安全实践

班　　级： 信息安全 2018-2 班

姓　　名： 孙正雨、李徐庆

赵玉龙、李宏宇

报告时间： 2021 年 7 月 3 日

任课教师： 谢林

分　　工

姓名	完成工作情况
孙正雨	拓扑设计、搭建拓扑、配置设备、测试验证、撰写实验报告
李徐庆	拓扑设计、辅助配置、测试验证、visio 绘制拓扑图
李宏宇	拓扑设计、物理连线、测试验证、撰写实验告、整理错误命令
赵玉龙	拓扑设计、物理连线、测试验证、visio 绘制拓扑图

2020-2021 学年第二学期
《网络系统与安全实践》课程评分表

（小组成员每人单独一页）

姓名 孙正雨 学号 08183039 班级 信息安全 2018-2 班

编号	课程教学目标	考查方式及考查点	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：_____

2020-2021 学年第二学期
《网络系统与安全实践》课程评分表

（小组成员每人单独一页）

姓名 李徐庆 学号 08183024 班级 信息安全 2018-2 班

编号	课程教学目标	考查方式及考查点	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：_____

2020-2021 学年第二学期
《网络系统与安全实践》课程评分表

（小组成员每人单独一页）

姓名 李宏宇 学号 08183012 班级 信息安全 2018-2 班

编号	课程教学目标	考查方式及考查点	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：_____

2020-2021 学年第二学期
《网络系统与安全实践》课程评分表

（小组成员每人单独一页）

姓名 赵玉龙 学号 08183026 班级 信息安全 2018-2 班

编号	课程教学目标	考查方式及考查点	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 背景描述

- 某公司网络拓扑区域划分为母公司 Site1 和子公司 Site2，子母公司网络通过 Tunnel 隧道打通路由
- 母公司 Site1 分为 Office1 部门和 Office2 部门
- 子公司 Site2 分为 Office3 部门和 Office4 部门

2 实验目标

- 因特网投入和区域网分离
- 降低各子公司间的网络关联度
- 实现母子公司的各 Office 之间的互联互通
- 限制子公司的 Office4（即 PC4）访问 8.8.8.8

3 实验设备列表

设备	数量
路由器 RSR20	2 台
三层交换机 S3760E	3 台
二层交换机 S2628G-I	2 台
电脑 PC	4 台
物理接线	4 条（包括两路由器的 S 口）

4 关键技术手段

4.1 Tunnel

GRE（Generic Routing Encapsulation，通用路由封装）协议是对某些网络层协议（如 IP 和 IPX）的数据报文进行封装，使这些被封装的数据报文能够在另一个网络层协议（如 IP）中传输。GRE 采用了 Tunnel（隧道）技术，是 VPN（Virtual Private Network）的第三层隧道协议。

Tunnel 是一个虚拟的点对点的连接，提供了一条通路使封装的数据报文能够在这个通路上传输，并且在一个 Tunnel 的两端分别对数据报进行封装及解封装。

4.2 NATP

NAT（Network Address Translation，网络地址转换）是 1994 年提出的。当在专用网内部的一些主机本来已经分配到了本地 IP 地址（即仅在本专用网内使用的专用地址），但现在又想和因特网上的主机通信（并不需要加密）时，可使用 NAT 方法。

这种方法需要在专用网连接到因特网的路由器上安装 NAT 软件。装有 NAT 软件的路由器叫做 NAT 路由器，它至少有一个有效的外部全球 IP 地址。这样，所有使用本地地址的主机在和外界通信时，都要在 NAT 路由器上将其本地地址转换成全球 IP 地址，才能和因特网连接。

另外，这种通过使用少量的公有 IP 地址代表较多的私有 IP 地址

的方式，将有助于减缓可用的 IP 地址空间的枯竭。

NAPT（Network Address Port Translation），即网络端口地址转换，可将多个内部地址映射为一个合法公网地址，但以不同的协议端口号与不同的内部地址相对应，也就是<内部地址+内部端口>与<外部地址+外部端口>之间的转换。NAPT 普遍用于接入设备中，它可以将中小型的网络隐藏在一个合法的 IP 地址后面。

4.3 ACL

ACL（访问控制列表或访问列表）可以实现对流经路由器或交换机的数据包根据一定的规则进行过滤，从而可以提高网络可管理性和安全性。

4.4 VRRP

VRRP（虚拟路由器冗余协议）提供了局域网上的设备备份机制。VRRP 是一种容错协议，它保证当主机的下一跳路由器坏掉时，可以及时由另一台路由器来代替，从而保证通讯的连续性和可靠性。

VRRP 工作时会在网络中加入一个含有虚拟 IP 和虚拟 MAC 地址的虚拟路由器，该路由器充当网络用户的网关，使得网络上的主机与虚拟路由器通信无需了解这个网络上物理路由的任何信息。

4.5 IPSec

IPSec（Internet Protocol Security，互联网安全协议）是一个协议包，通过对 IP 协议的分组进行加密和认证来保护 IP 协议的网络传输

协议族（一些相互关联的协议的集合）。

提供访问控制、无连接消息完整性、认证和反重发保护的认证首部（Authentication Header，AH）以及同样支持这些服务再加上机密性的封装安全有效载荷（Encapsulating Security Payload，ESP）。

4.6 MAC 地址绑定

交换机的端口安全，是一种交换机的过滤策略，即为交换机的某个端口绑定一个固定的 MAC 地址，使其他的 MAC 地址访问的时候触发策略，关闭端口或者拒绝服务。

4.6 AAA

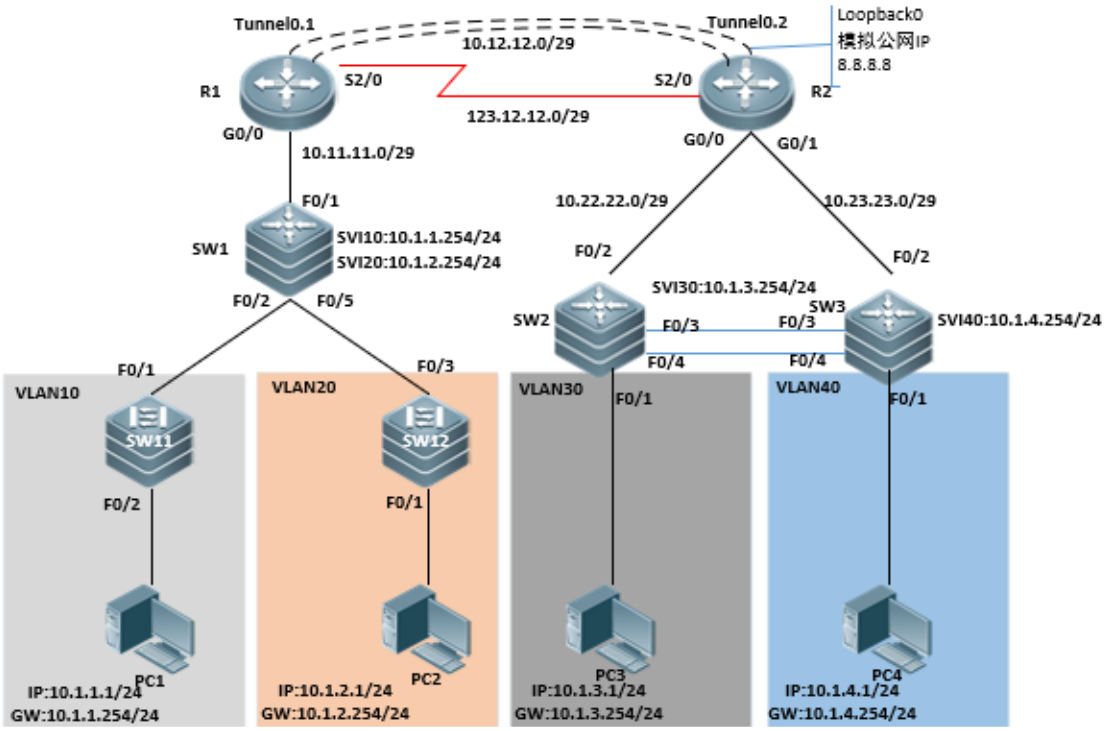
（AAA 是验证、授权和记账（Authentication、Authorization、Accounting）三个英文单词的简称，是一个能够处理用户访问请求的服务器程序，提供验证授权以及帐户服务，主要目的是管理用户访问网络服务器，对具有访问权的用户提供服务。

AAA 服务器通常同网络访问控制、网关服务器、数据库以及用户信息目录等协同工作。同 AAA 服务器协作的网络连接服务器接口是“远程身份验证拨入用户服务 （RADIUS）”。

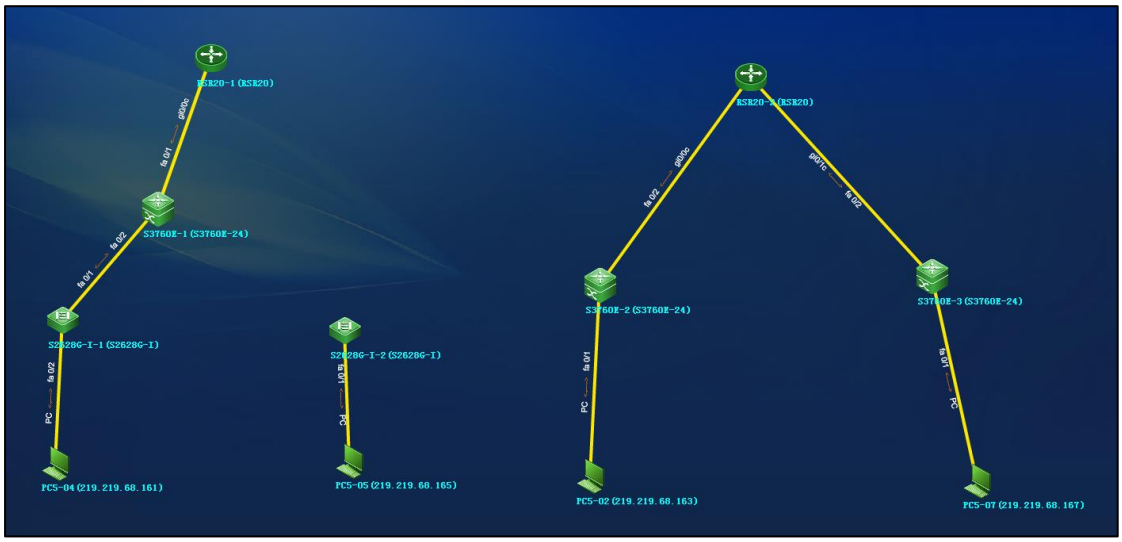
5 基本配置

5.1 拓扑图及物理接线

5.1.1 网络拓扑图

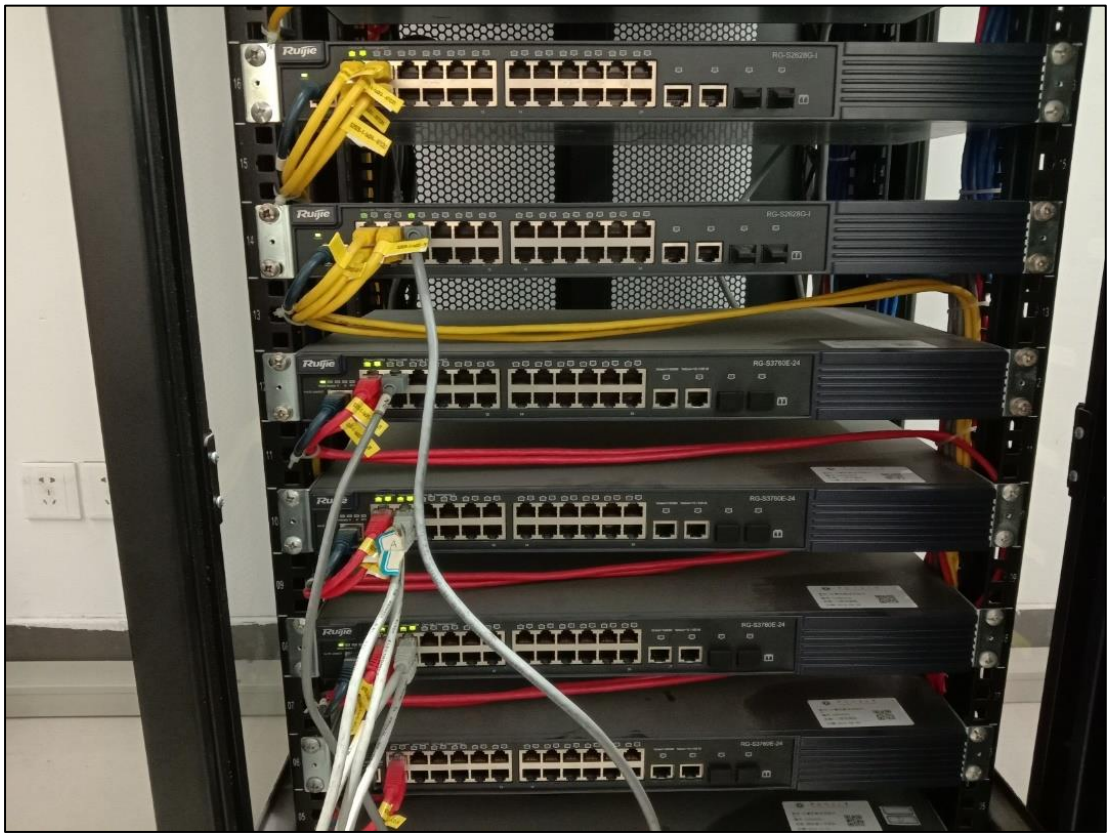


5.1.2 仿真拓扑图



5.1.3 物理接线

- RSR20-1(RSR20) 的 s2/0 口与 RSR20-2(RSR20) 的 s2/0 //设备本身就已经连接好
- S3760E-1(S3760E-24) 的 3 口与 S2628G-1-2(S2628G-I) 的 5 口
- S3760E-2(S3760E-24) 与 S3760E-3(S3760E-24) 的 3 口
- S3760E-2(S3760E-24) 与 S3760E-3(S3760E-24) 的 4 口//两个三层交换机连接两条线是为了在一条线路出问题时，流量可以从另外一条线路走，保证整个系统的稳定性



5.2 配置过程

本次实验的网络拓扑图与之前做的实验相比更加复杂，不能简单的将所有命令全部输入的设备中（出错不好排查），为了能够正确配置和快速排除设备中出现的错误，采用的是从左到右，从下到上的方法对设备进行配置。（SW11、SW12、SW1; SW2 和 SW3; R1 和 R2）

首先配置 SW11 和 SW12(vlan10 和 vlan20 的二层交换机)，再配置 SW1（三层交换机），实现跨 vlan 通信和配置通向外网的通信接口，当配置完 SW1 时，此时 vlan10 和 vlan20 中的主机通过三层交换的路由功能进行通信，即 PC1 和 PC2 可以互相 ping 通。（若无法 ping 通则配置有问题，可以通过 ping 网关 10.1.1.254 或 10.1.2.254 的方法检测在哪一段中存在问题，减少工作量）

其次配置 SW2 和 SW3，二者将 PC3 和 PC4 分开在两个 vlan 中，通过将 f0/3 和 f0/4 设置为 trunk 模式，实现 PC3 和 PC4 跨 vlan 通信，此时 PC3 和 PC4 可以互相 ping 通。在 SW3 中拒绝了 PC4 访问 8.8.8.8 的流量，在后续测试中的效果就是 PC4 ping 不通 8.8.8.8。（若 PC3 和 PC4 无法 ping 通，同样可以使用 ping 网关的方法去排查出错位置。）

最后配置 R1 和 R2，也是最重要的一步。R1 与 R2 中间属于公网网端（123.12.12.0/29），同时为了保证安全同时开启了 tunnel 接口实现安全通信；在 R2 的 loopback0 模拟公网 8.8.8.8；R1 上存在 NAT 功能，将内网地址转化为外网地址，可以保证内网的安全。当 PC1 和 PC2 访问 8.8.8.8 时（验证时，使用 PC1, ping 8.8.8.8 -t），R1 的 nat 转换表会出现 ip 地址转换记录；R1 和 R2 最基本的功能是实现来自两个 site

的流量转发，从而实现四台主机可以互相通信。

针对 R1 和 R2 配置完无法通信的错误排查方法（在其他设备正常工作情况下）：每个路由器配置都涉及三个接口，若出错时都重新配的话，工作量很大，通过排查找到出错接口可以提高效率。这里以 R1 为例，R2 同理。若 PC1 无法 ping 通 R2 的 s2/0(123.12.12.2),此时尝试 ping R1 的 s2/0（123.12.12.1）,如果无法 ping 通 123.12.12.1 则是 R1 的 s2/0 接口或 Gi0/1 配置存在问题，如果可以 ping 通 123.12.12.1 则是 R2 的 s2/0 接口存在的问题，通过简单判断可以将修正的工作量大大减小。出现其他的错误情况，也可以通过这样的方法。

5.3 Site1

- Site1 的部门 Office1 和 Office2 分别隶属于 vlan10、vlan20，网关分别指向 Switch1 的 svi10、svi20 接口
- Switch1 和边界路由器 R1 之间启用动态路由协议 OSPF，并在区域 0 中宣告所有本地路由

5.3.1 S11 —— S2628G-I-1(S2628G-I)

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 sh // 开始端口

5.3.1 S12 —— S2628G-I-2(S2628G-I)

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

5.3.3 S1 —— S3760E-1 (S3760E-24)

enable //修改主机名

configure terminal hostname switch1

spanning-tree //开启生成树，原指令出错，本处为修正过的指令

spanning-tree mode rstp//原指令出错，本处为修正过的指令

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 ospfpf 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

5.3.4 R1 —— RSR20-1(RSR20)

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 hostnamet 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

exi //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

5.4 Site2

- Site2 的部门 Office3 和 Office4 分别隶属于 vlan30、vlan40
- Switch2、Switch3 开启 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

5.4.1 S2 —— S3760E-2 (S3760E-24)

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

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

instance 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

outer ospf 1 //开启 ospfpf 进程并在 areaa 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 hostnamet 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 ACL10 接口下调用在接口的入方向

5.4.2 S3 —— S3760E-3 (S3760E-24)

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

instance 2 vlan 40

instance 1 vlan 30

spanning-tree mst 2 prio 0

spanning-tree mst 1 prio 4096

nterface 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 ospfpf 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 extenabled 100 //拓展访问控制列表 100

deny ip hostnamet 10.1.4.1 host 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

5.4.3 R2 —— RSR20-2(RSR20)

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

5.5 Tunnel —— Site1 和 Site2 之间

- 在 R1、R2 上起 Tunnel0，源目的地址分别为自己和对端的串口
- R1、R2 通过 Tunnel 隧道建立 OSPF 邻居

5.6 NATP + ACL —— 模拟公网

- 在 R2 上 lo0 口模拟公网 IP：8.8.8.8
- 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
- R1 的 s2/0 上开启端口复用 NAT 对所有来自 Site1 内部访问外网 8.8.8.8 的流量进行地转换
- 编写标准 ACL 在 Switch2 入方向放行 PC3 到所有目标地址的流量
- 编写拓展 ACL 接口下调用在 Switch3 入方向只拒绝 PC4 访问 8.8.8.8 的流量

6 安全配置

所有的设备的配置截图放在另外一个文件夹中。

6.1 VRRP（虚拟路由冗余网关）

在 SW2 和 SW3 上配置 VRRP（虚拟路由冗余网关），vlan30 的主虚拟网关位于 SW2，vlan40 的主虚拟网关位于 SW3。当交换机检测上行链路转发故障时自动降低本地 VRRP（路由冗余协议）优先级，虚拟网关身份切换到 peer（对等）端。

6.1.1 S2 —— S3760E-2 (S3760E-24)

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
interface vlan40//进入 vlan 40 的接口
ip add 10.1.4.252 255.255.255.0 //为 vlan 40 设置 ip
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

6.1.2 S3 —— S3760E-3 (S3760E-24)

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

6.2 IPSec（Internet 协议安全）

用 IPSec（Internet 协议安全）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。

6.2.1 R1 —— RSR20-1(RSR20)

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

access-list 100 permit ip 10.0.0.0 0.0.0.255 any // conf 模式，改后的命令

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

6.2.2 R2 —— RSR20-2(RSR20)

ip access-list extend 100 //同上

access-list 100 permit ip 10.0.0.0 0.0.0.255 any // conf 模式，改后的命令

crypto iskamp police 10

encry 3des

authen preshare

group 2

crypto iskamp 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-iskamp

set transform-set IPSEC

set peer 10.12.12.1

match add 100

int tunnel0

crypto map VPN

6.3 Port-security(交换机端口安全)

在 SW2 和 SW3 交换口上启用 mac 地址绑定，如果检测到主机 mac 改动立即关闭端口。

6.3.1 S2 + S3

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

6.4 AAA

6.4.1 SW1

aaa new-mode //开启 AAA

radius-server hostnamest 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 authenticaton 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 authostnamerization exec execauth group radius local

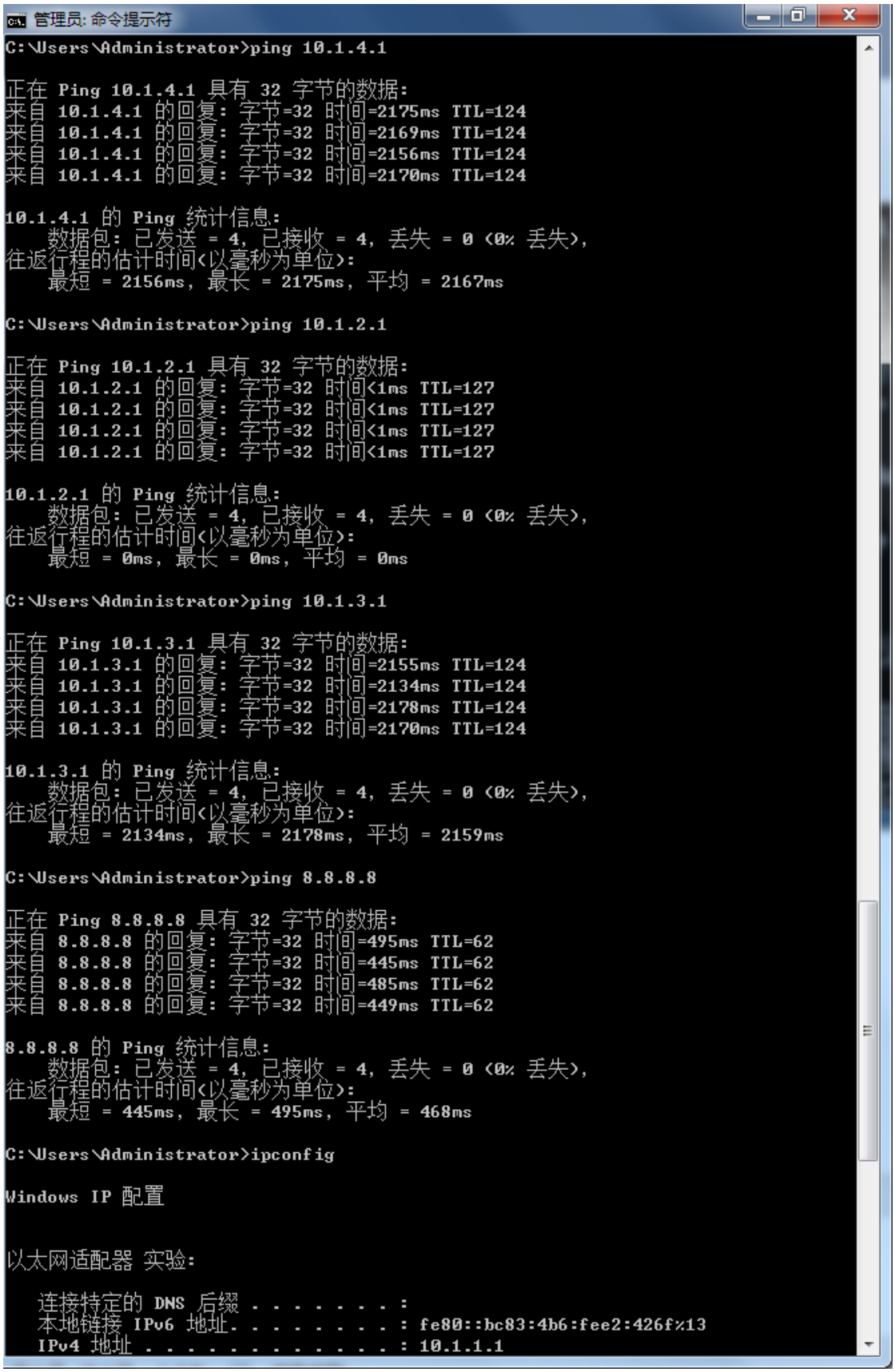
//登陆授权列表 execauth，优先采用 radius 组认证其次本地组
aauthostnamerization commands 15 commauth group radius local
//命令授权列表 commauth，优先采用 radius 组认证其次本地组
aaa accounting exec execaccount start-stop group radius local
//登入登出审计列表 execaccount，优先采用 radius 组认证其次本地组
aaa accounting commands 15 commaccount start-stop group 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 authostnamerization exec execauth　//接口下调用登陆授权列表
login authostnamerization commands commauth　//接口下调用命令授权列表
accouting exec execaccout　//接口下调用登入登出审计列表
accouting commands 15 commaccout　//接口下调用命令登出审计列表

7 连通性结果验证

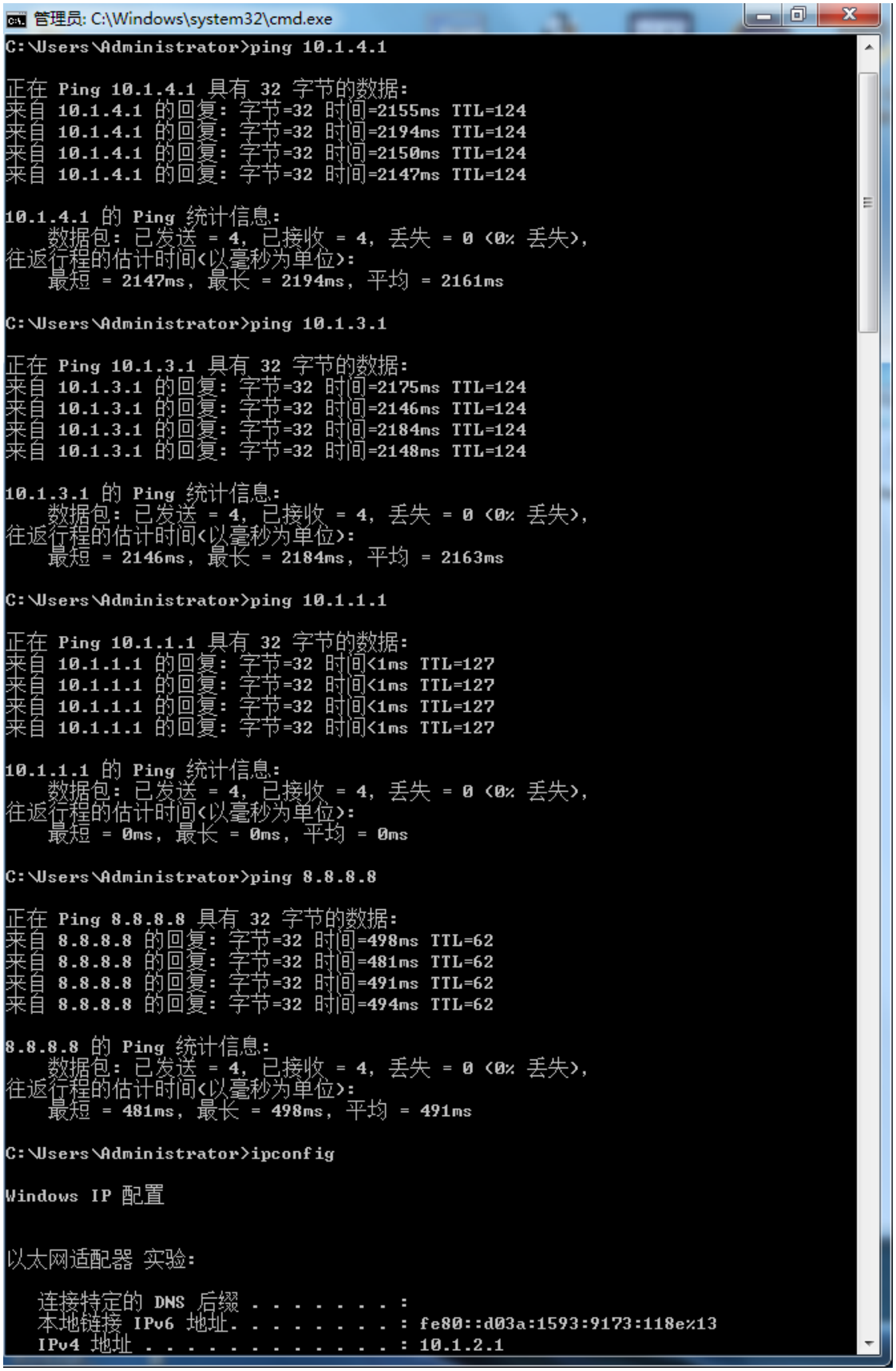
- PC1(10.1.1.1)与 PC2、PC3、PC4、外网（8.8.8.8）互通
- PC2(10.1.2.1)与 PC1、PC3、PC4、外网（8.8.8.8）互通
- PC3(10.1.3.1)与 PC1、PC2、PC4、外网（8.8.8.8）互通
- PC4(10.1.4.1)与 PC1、PC2、PC3 互通，但 ping 不通外网（8.8.8.8）

（当可以 ping 通以下节点时，其他网络中的节点都可以 ping 通，无需验证）

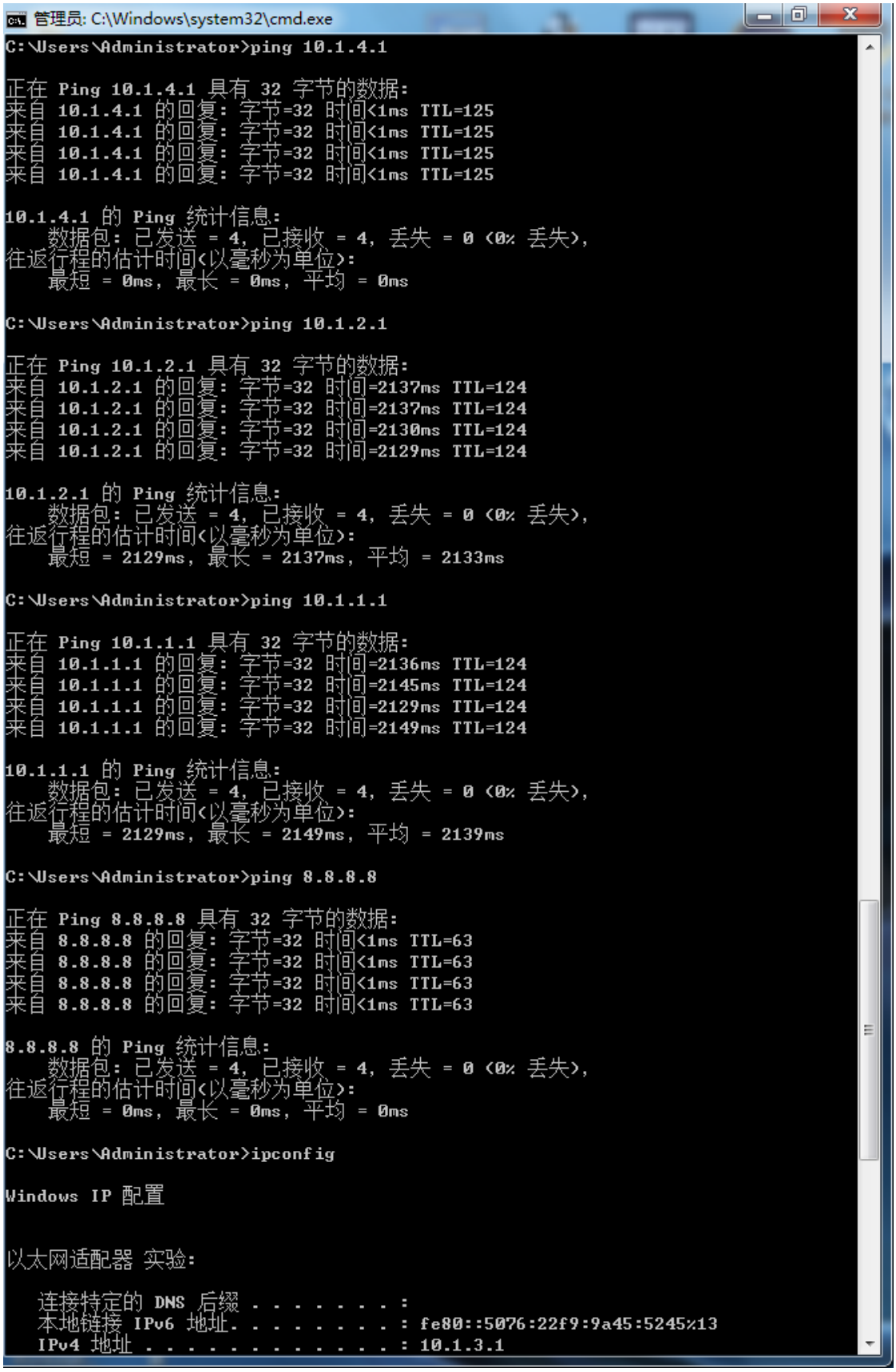
7.1 PC1(10.1.1.1) 连通性



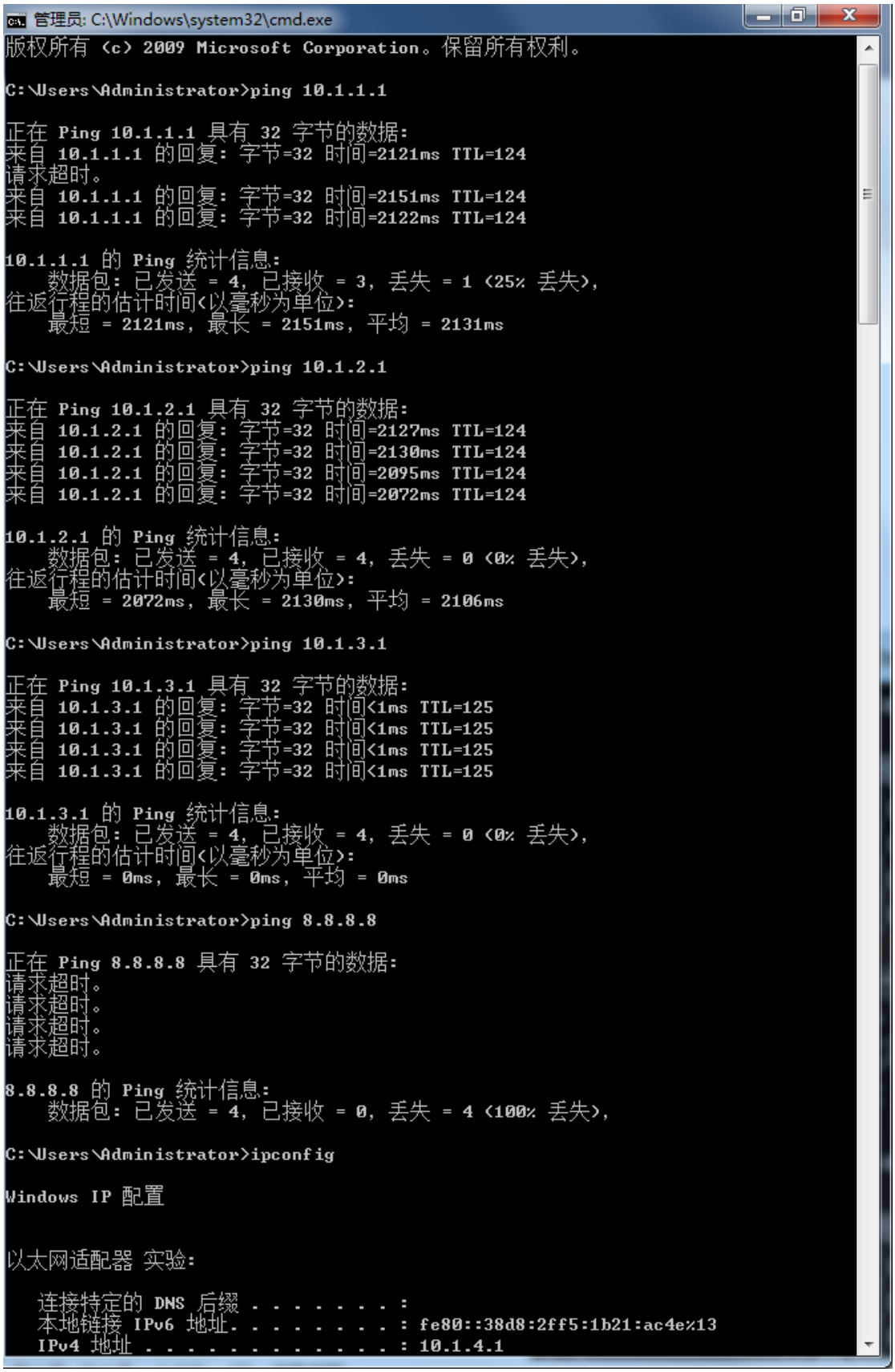
7.2 PC2(10.1.2.1) 连通性



7.3 PC3(10.1.3.1) 连通性

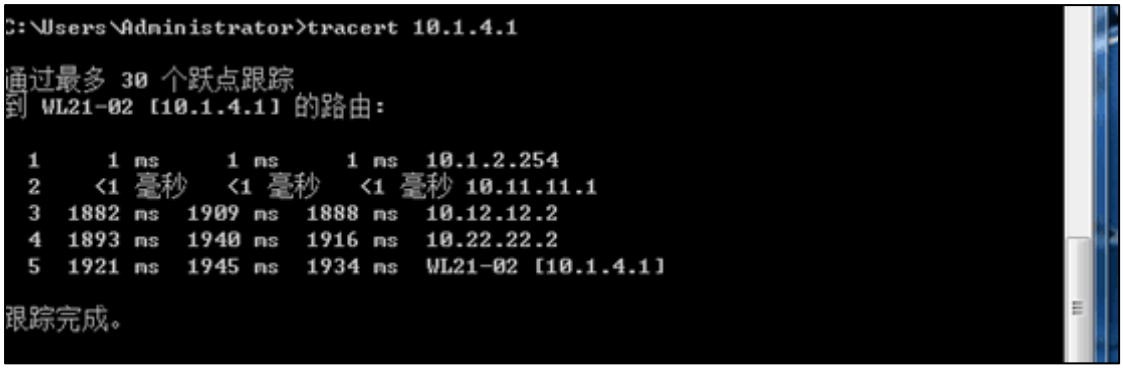


7.4 PC4(10.1.4.1) 连通性



7.5 IPsec Tunnel 验证

7.5.1 PC2 → PC4



7.5.2 PC3 → PC1

8 促进实验可持续发展（基于大实验中给出的疑似错误指令的修正）

8.1 S1 —— SW1.docx

■ 文件《SW1.docx》中第 3、4 行：

spanning-treenableing-tree //开启生成树，可能是版本问题，这个命令不能用

spanning-treenableing-tree mode rstp

■ 应改为：

spanning-tree //开启生成树

spanning-tree mode rstp

8.2 R1 + R2 —— 安全配置.docx

■ 文件《安全配置.docx》中第 2 行 和 第 28 行：

per ip 10.0.0.0 0.0.0.255 //可能是设备版本不一样

■ 应改为：

access-list 100 permit ip 10.0.0.0 0.0.0.255 any // conf 模式

9 实验总结

经连通性配置后，可验证：

■ 位于不同部门的 PC1、PC2 互通，R1 与 Switch1 建立路由邻居并收到 vlan10、20 的路由明细

■ 位于不同部门的 PC3、PC4 互通，R2 与 Switch2、Switch3 建立 OSPF 邻居并收到 vlan30、40 的路由明细

■ tunnel 口创建成功，R1、R2 建立 OSPF 邻居，Site1、Site2 互传路由明细，PC1、PC2、PC3、PC4 四个部门互通

■ 所有 PC 互通；除 PC4 均能访问公网地址 8.8.8.8；Site1 去往外部的流量实现 NATP 转换

经安全配置后，实现了：

- VRRP 安全配置
- IPSec 安全配置
- Port-security 安全配置
- 对 AAA 的安全配置的理解

总结部分：

- 对本次实验出现的疑似错误指令进行了总结

实验体会

综合性实验更能考验对整个网络环境和各个协议的理解；选择合理的配置顺序可以提高配置的准确性，提高效率；在配置完某个设备后可以清楚的知道各个节点间的状态如何；遇到错误知道如何排查，而不是一味的推翻重来，这是对我们能力和思维的锻炼；同时，完成整个综合实验需要队友的配合，锻炼了团结协作的能力。