**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、visio绘图 |
| 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 1](#_Toc76288943)

[2 实验目标 1](#_Toc76288944)

[3 实验设备列表 1](#_Toc76288945)

[4 关键技术手段 2](#_Toc76288946)

[4.1 Tunnel 2](#_Toc76288947)

[4.2 NATP 2](#_Toc76288948)

[4.3 ACL 3](#_Toc76288949)

[4.4 VRRP 3](#_Toc76288950)

[4.5 IPSec 3](#_Toc76288951)

[4.6 MAC地址绑定 4](#_Toc76288952)

[4.6 AAA 4](#_Toc76288953)

[5 基本配置 5](#_Toc76288954)

[5.1 拓扑图及物理接线 5](#_Toc76288955)

[5.1.1 网络拓扑图 5](#_Toc76288956)

[5.1.2 仿真拓扑图 5](#_Toc76288957)

[5.1.3 物理接线 6](#_Toc76288958)

[5.2 配置过程 7](#_Toc76288959)

[5.3 Site1 8](#_Toc76288960)

[5.3.1 S11 —— S2628G-I-1(S2628G-I) 8](#_Toc76288961)

[5.3.1 S12 —— S2628G-I-2(S2628G-I) 9](#_Toc76288962)

[5.3.3 S1 —— S3760E-1 (S3760E-24) 9](#_Toc76288963)

[5.3.4 R1 —— RSR20-1(RSR20) 11](#_Toc76288964)

[5.4 Site2 12](#_Toc76288965)

[5.4.1 S2 —— S3760E-2 (S3760E-24) 12](#_Toc76288966)

[5.4.2 S3 —— S3760E-3 (S3760E-24) 13](#_Toc76288967)

[5.4.3 R2 —— RSR20-2(RSR20) 15](#_Toc76288968)

[5.5 Tunnel —— Site1和Site2之间 16](#_Toc76288969)

[5.6 NATP + ACL —— 模拟公网 16](#_Toc76288970)

[6 安全配置 16](#_Toc76288971)

[6.1 VRRP（虚拟路由冗余网关） 17](#_Toc76288972)

[6.1.1 S2 —— S3760E-2 (S3760E-24) 17](#_Toc76288973)

[6.1.2 S3 —— S3760E-3 (S3760E-24) 17](#_Toc76288974)

[6.2 IPSec（Internet 协议安全） 18](#_Toc76288975)

[6.2.1 R1 —— RSR20-1(RSR20) 18](#_Toc76288976)

[6.2.2 R2 —— RSR20-2(RSR20) 19](#_Toc76288977)

[6.3 Port-security(交换机端口安全) 20](#_Toc76288978)

[6.3.1 S2 + S3 20](#_Toc76288979)

[6.4 AAA 20](#_Toc76288980)

[6.4.1 SW1 20](#_Toc76288981)

[7 连通性结果验证 21](#_Toc76288982)

[7.1 PC1(10.1.1.1) 连通性 22](#_Toc76288983)

[7.2 PC2(10.1.2.1) 连通性 23](#_Toc76288984)

[7.3 PC3(10.1.3.1) 连通性 24](#_Toc76288985)

[7.4 PC4(10.1.4.1) 连通性 25](#_Toc76288986)

[7.5 IPsec Tunnel 验证 26](#_Toc76288987)

[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） 26](#_Toc76288988)

[8.1 S1 —— SW1.docx 26](#_Toc76288989)

[8.2 R1 + R2 —— 安全配置.docx 27](#_Toc76288990)

[9 实验总结 27](#_Toc76288991)

# 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

电脑萤幕画面

已生成高可信度的说明

### 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

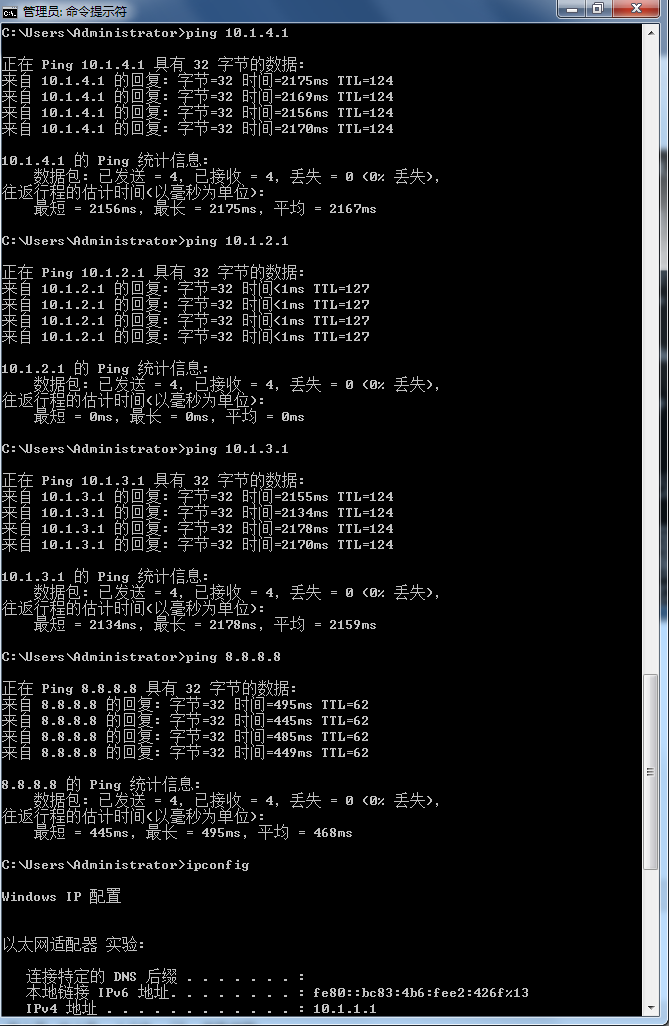
accouting commands 15 commaccout //接口下调用命令登出审计列表

# 7 连通性结果验证

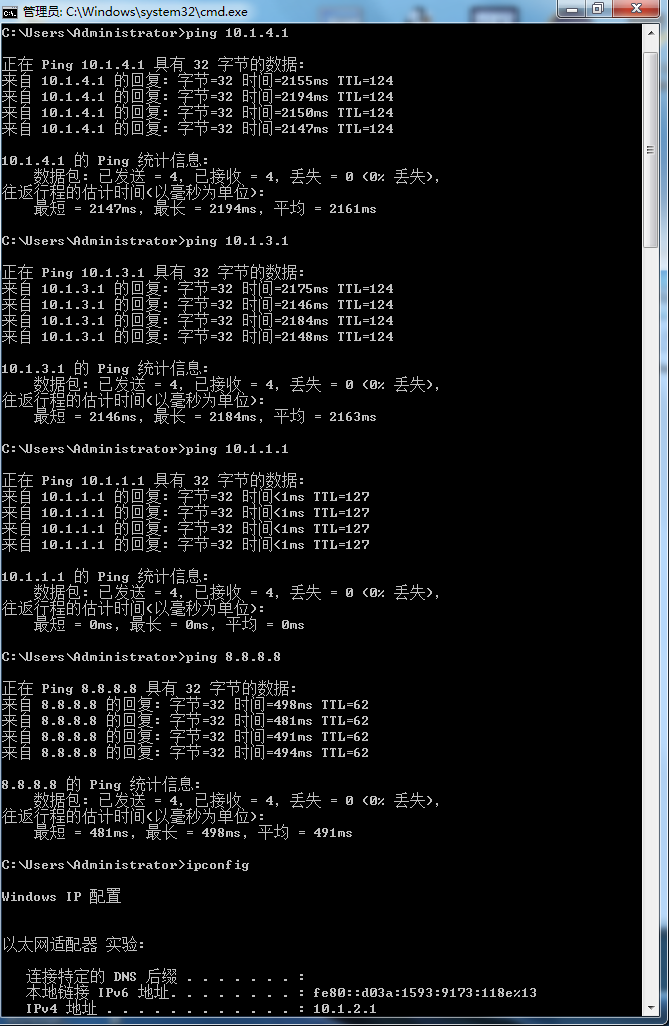
* PC1(10.1.1.1)与PC2、PC3、PC4、外网（8.8.8.8）互通
* PC2(10.1.2.1)与PC1、PC3、PC4、外网（8.8.8.8）互通
* PC3(10.1.3.1)与PC1、PC2、PC4、外网（8.8.8.8）互通
* PC4(10.1.4.1)与PC1、PC2、PC3互通，但ping不通外网（8.8.8.8）

（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）

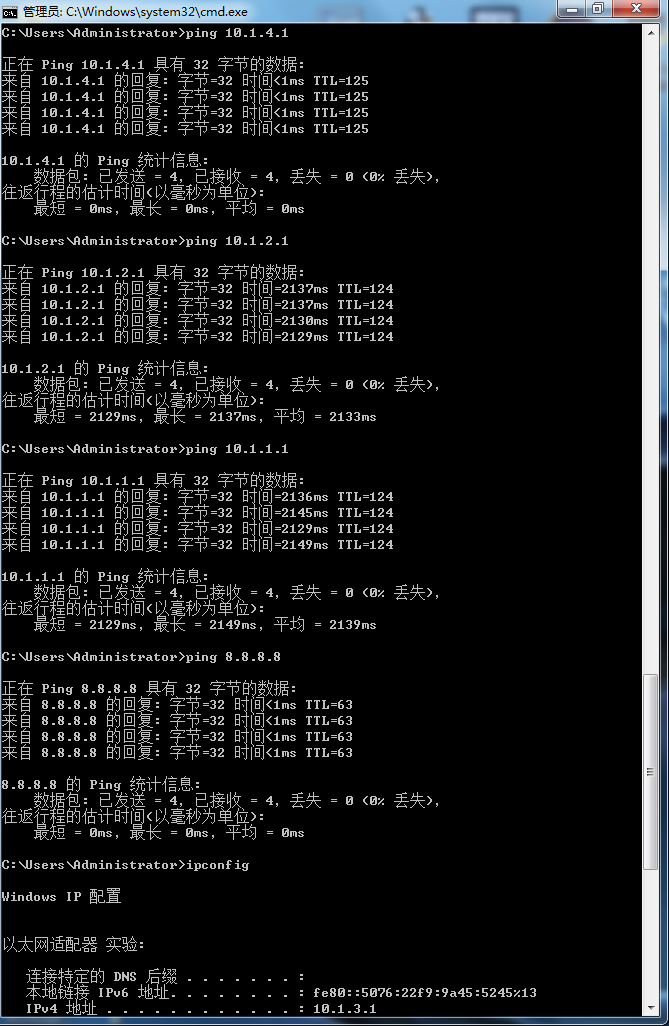
## 7.1 PC1(10.1.1.1) 连通性



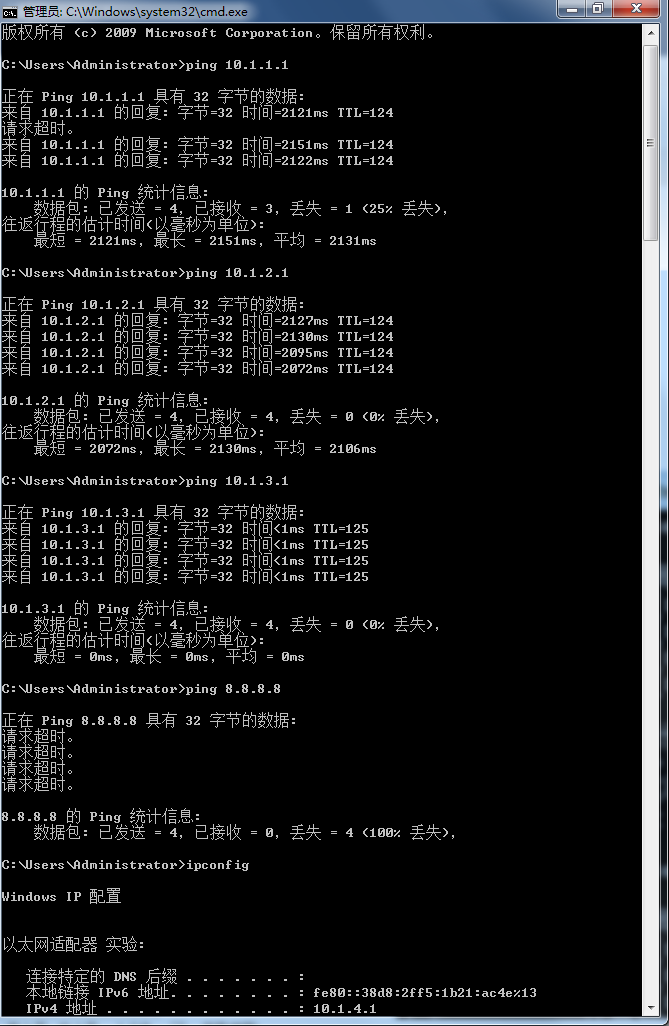
## 7.2 PC2(10.1.2.1) 连通性



## 7.3 PC3(10.1.3.1) 连通性

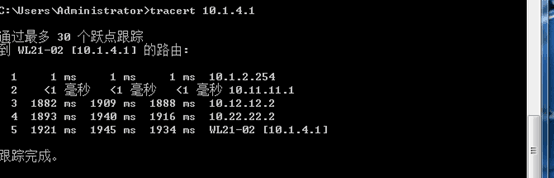
****

## 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。