

中国矿业大学计算机学院

2019 级本科生课程报告

课程名称	网络系统与安全实践
报告时间	2022 年 6 月 24 日
学生姓名	叶文惠、李春阳、许万鹏、凌子健
学 号	03190867、10193657、05191643、08192888
专 业	信息安全
任课教师	王虎

分 工

姓名	完成工作情况
叶文惠	基础实验、综合大实验、报告撰写
李春阳	基础实验、综合大实验、报告撰写
许万鹏	基础实验、综合大实验、报告撰写、拓扑图绘制
凌子健	基础实验、综合大实验、报告撰写、拓扑图绘制

2021-2022 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 叶文惠 学号 03190867 班级 信息安全 2019-01 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: _____

2021-2022 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 李春阳 学号 10193657 班级 信息安全 2019-01 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: _____

2021-2022 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 许万鹏 学号 05191643 班级 信息安全 2019-01 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: _____

2021-2022 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 凌子健 学号 08192888 班级 信息安全 2019-01 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 实验设备	1
2 实验背景与要求	1
2.1 实验背景	1
2.2 实验网络要求	1
2.2.1 Site 1	1
2.2.2 Site 2	1
2.2.3 Tunnel	2
2.2.4 NATP	2
2.2.5 ACL	3
2.3 网络安全性要求	3
2.3.1 VRRP	3
2.3.2 IPSec	4
2.3.3 MAC 地址绑定	4
2.3.4 端口限速	5
3 网络拓扑	5
3.1 拓扑构建	5
3.2 拓扑仿真	6
4 网络配置	6
4.1 连通性配置	6
SW1	6
SW2	7
SW3	8
SW11	9
SW12	9
R1	10
R2	10
4.2 安全性配置——VRRP	11
SW2	11
SW3	12

4.3 安全性配置——IPSEC	12
R1	12
R2	13
4.4 安全性配置——Port Security	13
SW2/SW3	13
4.5 安全性配置——AAA	13
SW1	13
5 结果验证	14
5.1 各 PC 之间互通	14
5.1.1 PC1	14
5.1.2 PC2	15
5.1.3 PC3	15
5.1.4 PC4	16
5.2 各 PC 与 8.8.8.8 外网连通性	16
5.2.1 PC1	16
5.2.2 PC2	16
5.2.3 PC3	17
5.2.4 PC4	17
5.3 IPsec Tunnel 验证	18
5.3.1 PC1 到 PC3	18
5.3.2 PC2 到 PC4	18
5.3.3 PC3 到 PC1	19
5.3.4 PC4 到 PC1	19

1 实验设备

序号	设备	个数
1	RSR20 路由器	2 台
2	S3760E 三层交换机	3 台
3	S2628GI 二层交换机	2 台
4	Windows PC 机	4 台

2 实验背景与要求

2.1 实验背景

某一大型企业内部网络由母公司 Site1 和子公司 Site2 组成,其中母公司 Site1 下包含部门 Office 1 和 Office 2 子公司 Site2 下包含部门 Office 3 和 Office 4 总部与分公司间网络通过 Tunnel 打通路由。

2.2 实验网络要求

2.2.1 Site 1

①母公司 Site1 的部门 Office1 和 Office2 分别隶属于 VLAN10 和 VLAN20, 它们的网关分别指向 SW1 的 SVI10、SVI20 接口(交换机虚拟接口,Switch Virtual Interface, 代表一个由交换端口构成的 VLAN, 以便于实现系统中路由和桥接的功能);

②SW1 和边界路由器 R1 之间启用动态路由协议 OSPF(开放最短路径有限, Open Shortest Path First) ,并在 area0 中宣告所有本地路由。

③SW1 中开启 RSTP 协议(快速路由协议,Rapid Spanning Tree Protocol), 能够发现并生成局域网的一个最佳树型拓扑结构,在发现拓扑故障后随之进行恢复,自动更新网络拓扑结构,启用备份链路,同时保持最佳树型结构;同时能够有效避免环形网络中的报文增生和无限循环产生的广播风暴。

最终实现目标: 位于 Office1 中的主机(以 PC1 为代表)和位于 Office2 中的主机(以 PC2 为代表)能够实现互联互通,并且 R1 与 Switch1 建立路由邻居并收到 Vlan10 和 Vlan20 的路由明细。

2.2.2 Site 2

①子公司 Site 2 的部门 Office 3 和 Office 4 分别隶属于 vlan30、vlan40, 网关分别指向 Switch2 和 Switch3 各自的 svi 接口。

②SW2、SW3 之分别与边界路由器 R2 建立 OSPF 邻居,在区域 0 中宣告所有本地直连路由。

③SW2 和 SW3 之间启用 Trunk 放行 VLAN,并用了多生成树协议(MST),

能够通过 trunks 建立多个生成树，关联 VLANs 到相关的生成树进程，提供了多个数据转发路径和负载均衡，提高了网络容错能力。

最终实现目标：位于 Office3 中的主机（以 PC3 为代表）和位于 Office4 的主机（以 PC4 为代表）能实现互联互通，R2 与 SW2、SW3 建立 OSPF 邻居并收到 VLAN30、VLAN40 的路由明细。

2.2.3 Tunnel

隧道协议（英语：Tunneling Protocol）是一种网络协议，在其中，使用一种网络协议（发送协议），将另一个不同的网络协议，封装在负载部分。使用隧道的原因是在不兼容的网络上传输数据，或在不安全网络上提供一个安全路径。

隧道则是对比分层式的模型，如 OSI 模型或 TCP/IP。隧道协议通常（但并非总是）在一个比负载协议还高的层级，或同一层。要了解协议堆栈，负载和发送协议都须了解。传统的分层式协议，如 OSI 模型或 TCP/IP 模型，HTTP 协议，并不被认为是隧道协议。隧道是在相隔甚远的客户端和服务端两者之间进行中转，并保持双方通信连接的应用程序。

通用路由封装是一种跑在 IP（IP 号码为 47）的协议，身为网络层上的网络层的例子，通常是用带有公开地址的 IP 数据包来携带带有 RFC 1918 私用地址的 IP 数据包来穿越互联网。在此例上，发送和负载协议是兼容的，但负载地址和发送网络是不兼容的。

隧道协议可能使用数据加密来发送不安全的负载协议。

① 母公司（Site 1）于子公司（Site 2）通过在 R1、R2 上通过 Tunnel 来打通路由，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。

最终实现目标：R1、R2 可以成功建立 OSPF 邻居，Site 1、Site 2 互传路由明细，PC1、PC2、PC3、PC4 四个部门可以相互通信。

2.2.4 NATP

由于 NAT 实现是私有 IP 和 NAT 的公共 IP 之间的转换，那么，私有网中同时与公共网进行通信的主机数量就受到 NAT 的公共 IP 地址数量的限制。为了克服这种限制，NAT 被进一步扩展到在进行 IP 地址转换的同时进行 Port 的转换，这就是网络地址端口转换 NAPT（Network Address Port Translation）技术。NAPT 也被称为“多对一”的 NAT，或者叫 PAT（Port Address Translations，端口地址转换）、地址超载（address overloading）。

NAPT 与 NAT 的区别在于，NAPT 不仅转换 IP 包中的 IP 地址，还对 IP 包中 TCP 和 UDP 的 Port 进行转换。这使得多台私有网主机利用 1 个 NAT 公共 IP 就可以同时和公共网进行通信。（NAPT 多了对 TCP 和 UDP 的端口号的转换）

私有网主机 192.168.1.2 要访问公网中的 Http 服务器 166.111.80.200。首先，要建立 TCP 连接，假设分配的 TCP Port 是 1010，发送了 1 个 IP 包（Des=166.111.80.200:80,Src=192.168.1.2:1010），当 IP 包经过 NAT 网关时，NAT 会将 IP 包的源 IP 转换为 NAT 的公共 IP，同时将源 Port 转换为 NAT 动态分配的

1 个 Port。然后，转发到公网，此时 IP 包（Des=166.111.80.200：80，Src=202.204.65.2:2010）已经不含任何私有网 IP 和 Port 的信息。由于 IP 包的源 IP 和 Port 已经被转换成 NAT 的公共 IP 和 Port，响应的 IP 包（Des=202.204.65.2:，Src=2010166.111.80.200:80）将被发送到 NAT。这时 NAT 会将 IP 包的目的 IP 转换成私有网主机的 IP，同时将目的 Port 转换为私有网主机的 Port，然后将 IP 包（Des=192.168.1.2:1010，Src=166.111.80.200:80）转发到私网。对于通信双方而言，这种 IP 地址和 Port 的转换是完全透明的

① 在 R2 的 lo 0 接口模拟公网 IP：8.8.8.8。

② R1 作为 Site 1 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。

③ R1 的 s2/0 口上开启端口复用 NAT 对所有来自 Site 1 内部访问外网（8.8.8.8）的流量进行地址转换。

最终实现目标：Site1 去往外部的流量能实现 NAT 转换，同时各主机也能够实现对公网地址的访问。

2.2.5 ACL

访问控制列表（Access Control Lists，ACL）是应用在路由器接口的指令列表。这些指令列表用来告诉路由器哪些数据包可以收、哪些数据包需要拒绝。至于数据包是被接收还是拒绝，可以由类似于源地址、目的地址、端口号等的特定指示条件来决定。

访问控制列表具有许多作用，如限制网络流量、提高网络性能；通信流量的控制，例如 ACL 可以限定或简化路由更新信息的长度，从而限制通过路由器某一网段的通信流量；提供网络安全访问的基本手段；在路由器端口处决定哪种类型的通信流量被转发或被阻塞，例如，用户可以允许 E-mail 通信流量被路由，拒绝所有的 Telnet 通信流量等。

① 编写标准 ACL 在 SW2 的入方向放行部门 Office 3 到所有目标地址的流量。

② 编写拓展 ACL 接口①下调用在 SW3 入方向只拒绝部门 Office 4 访问外网 8.8.8.8 的流量。

最终实现目标：四个部门的所有 PC 可以相互通信；除 PC4 之外，均能访问公网地址 8.8.8.8。

2.3 网络安全性要求

2.3.1 VRRP

虚拟路由冗余协议 VRRP（Virtual Router Redundancy Protocol）是一种用于提高网络可靠性的容错协议。它可以把一个虚拟路由器的责任动态分配到局域网上的 VRRP 路由器中的一台。控制虚拟路由器 IP 地址的 VRRP 路由器称为主路由器，它负责转发数据包到这些虚拟 IP 地址。一旦主路由器不可用，这种选择过程就提供了动态的故障转移机制，这就允许虚拟路由器的 IP 地址可以作为

终端主机的默认第一跳路由器。

VRRP 路由器是指运行 VRRP 的路由器,是物理实体;虚拟路由器是指 VRRP 协议创建的,是逻辑概念。一组 VRRP 路由器协同工作,共同构成一台虚拟路由器。该虚拟路由器对外表现为一个具有唯一固定的 IP 地址和 MAC 地址的逻辑路由器。处于同一个 VRRP 组中的路由器具有两种互斥的角色:主控路由器和备份路由器,一个 VRRP 组中有且只有一台处于主控角色的路由器,可以有一个或者多个处于备份角色的路由器。VRRP 协议从路由器组中选出一台作为主控路由器,负责 ARP 解析和转发 IP 数据包,组中的其他路由器作为备份的角色并处于待命状态,当由于某种原因主控路由器发生故障时,其中的一台备份路由器能在瞬间的时延后升级为主控路由器,由于此切换非常迅速而且不用改变 IP 地址和 MAC 地址,故对终端使用者系统是透明的。

在 SW3 和 SW4 上配置 VRRP, VLAN 30 的主虚拟网关位于 SW3, VLAN 40 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。

2.3.2 IPsec

联网安全协议(英语: Internet Protocol Security, 缩写为 IPsec), 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。IPsec 主要由以下协议组成:

- 认证头 (AH): 为 IP 数据报提供无连接数据完整性、消息认证以及防重放攻击保护。
- 封装安全载荷 (ESP): 提供机密性、数据源认证、无连接完整性、防重放和有限的传输流 (traffic-flow) 机密性。
- 安全关联 (SA): 提供算法和数据包, 提供 AH、ESP 操作所需的参数。
- 密钥协议 (IKE): 提供对称密码的密钥的生存和交换。

在该企业网络中, 为了保证母公司与子公司之间路由通信的安全, 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 AES-256 加密数据、Sha-HMAC 用于数据哈希校验。

2.3.3 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, 关闭掉端口或者拒绝服务。MAC 地址绑定就是利用三层交换机的安全控制列表将交换机上的端口与所对应的 MAC 地址进行捆绑。由于每个网络适配卡具有唯一的 MAC 地址, 为了有效防止非法用户盗用网络资源, MAC 地址绑定可以有效的规避非法用户的接入。以进行网络物理层面的安全保护。

在 SW2 和 SW3 交换口上设置端口安全自动 MAC 地址绑定, 如果检测到主机

MAC 改动立即关闭端口，从而严格控制了输入，防止了身份的伪造。

2.3.4 端口限速

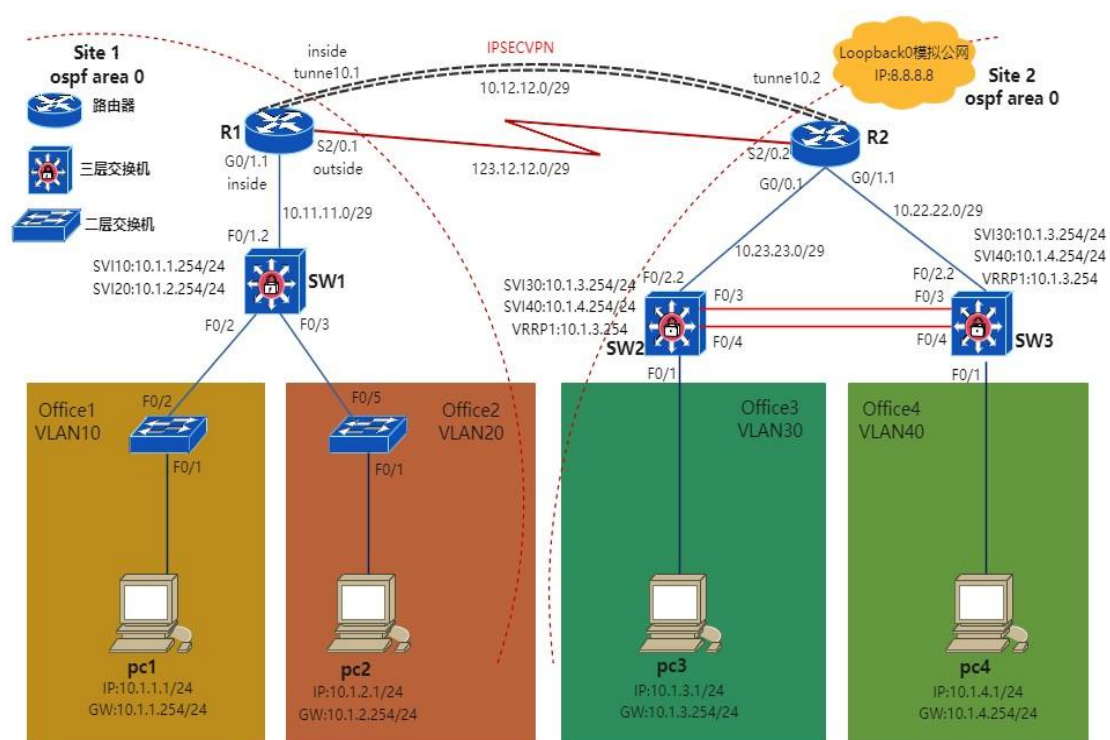
母公司部门 Office 1 的网络管理员最近收到很多员工的投诉，抱怨网络变得很慢，不论是收发邮件还是上网查资料都很慢，影响了工作效率。对此，网络管理员进行了调查，发现有交换机的某些端口的数据流量很大，严重影响了网络性能，于是决定对这个交换机端口进行速率限制，从而改进网络性能。

在 SW1 中定义分类映射图（class-map）和策略映射图（policy-map），设置带宽限制、猝发数据量限制，若用户使用超过此限制则直接丢弃数据包，在 f0/2 端口启用 QoS，并设置接口的 QoS 信任模式为 cos。

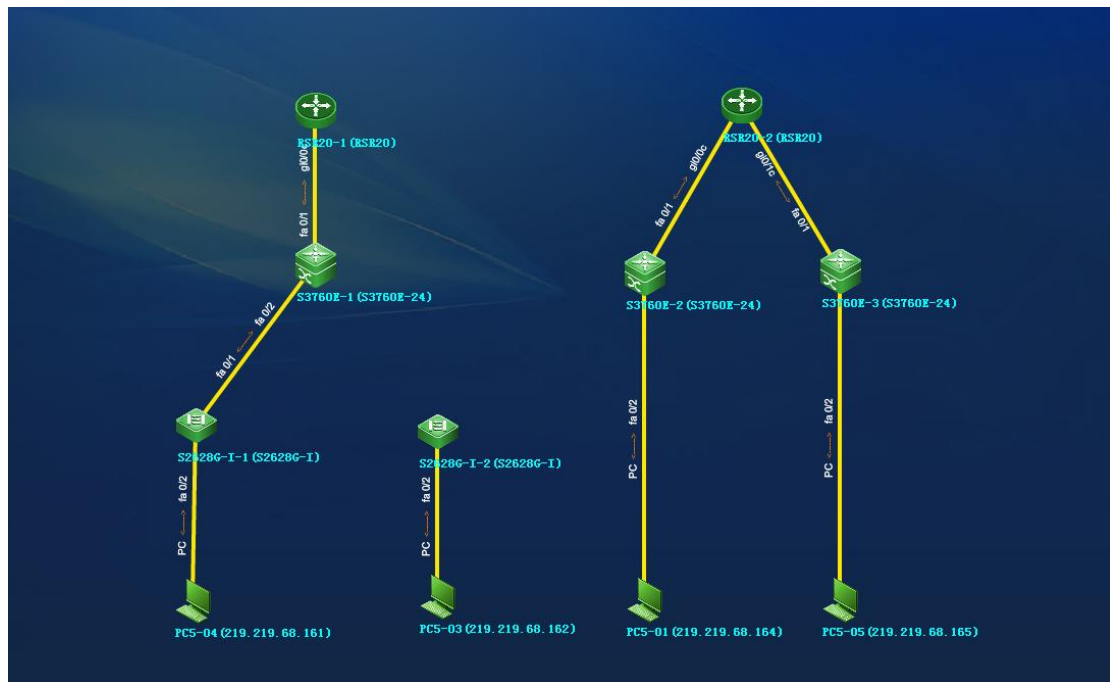
3 网络拓扑

3.1 拓扑构建

根据企业网络架构，设计出的网络拓扑图如下：



3.2 拓扑仿真



除了上图中通过平台连线之外,下面这些线直接在机柜中进行物理线路的连接:

- RSR20-1 的 s2/0 口与 RSR20-2 的 s2/0 口
- S3760E-1 的 3 口与 S2628G-1-2 的 5 口
- S3760E-2 与 S3760E-3 的 3 口
- S3760E-2 与 S3760E-3 的 4 口

4 网络配置

4.1 连通性配置

SW1

```
enable ! 修改主机名
configure terminal
hostname SW1
spanning-tree enable ! 开启生成树
! 该指令错误, 修正为: spanning-tree
spanning-tree enable mode rstp
! 该指令错误, 修正为: spanning-tree mode rstp
vlan 10 ! 创建 vlan
vlan 20
interface f0/24 ! 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 area0 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 10.1.2.0/24
network 10.11.11.0 0.0.0.7 area 0      ! 宣告网段 10.11.11.0/29
```

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
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
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 hostnet 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

```

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
instance 2 vlan 40
instance 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 extenbled 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
```

SW11

```
enable
configure terminal    ! 特权模式
hostname SW11         ! 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
```

SW12

```
enable    ! 进入特权模式修改主机名
configure terminal
hostname SW12
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
```

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
    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
    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
```

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 源地址
    tunnel destination 123.12.12.1 ! 设置 tunnel 目的地址
    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

```

4.2 安全性配置——VRRP

SW2

```

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 vlan40
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

```

SW3

```

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

```

4.3 安全性配置——IPSEC

R1

```

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
! 该指令错误, 修正为: crypto isakmp police 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
! 该指令错误, 修正为: crypto isakmp 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
! 该指令错误, 修正为: crypto map VPN 1 ipsec-isakmp
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

```

R2

```

ip access-list extend 100    ! 同上
per ip 10.0.0.0 0.0.0.255
crypto iskamp police 10
! 该指令错误, 修正为: crypto isakmp police 10
encry 3des
authen preshare
group 2
crypto iskamp key 7 ruijie add 10.12.12.1
! 该指令错误, 修正为: 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-iskamp
! 该指令错误, 修正为: crypto map VPN 1 ipsec-isakmp
set transform-set IPSEC
set peer 10.12.12.1
match add 100
int tunnel0
crypto map VPN

```

4.4 安全性配置——Port Security

SW2/SW3

```

interface f0/1
    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

```

4.5 安全性配置——AAA

SW1

```

enable
configure terminal
ip access-list standard qoslimit1    ! 定义访问控制列表
    permit host 10.1.1.254            ! 定义需要限速的数据流
    exit
class-map classmap1                  ! 设置分类映射图
    match access-group qoslimit1      ! 匹配访问控制列表
    exit
policy-map policymap1                ! 设置策略映射图

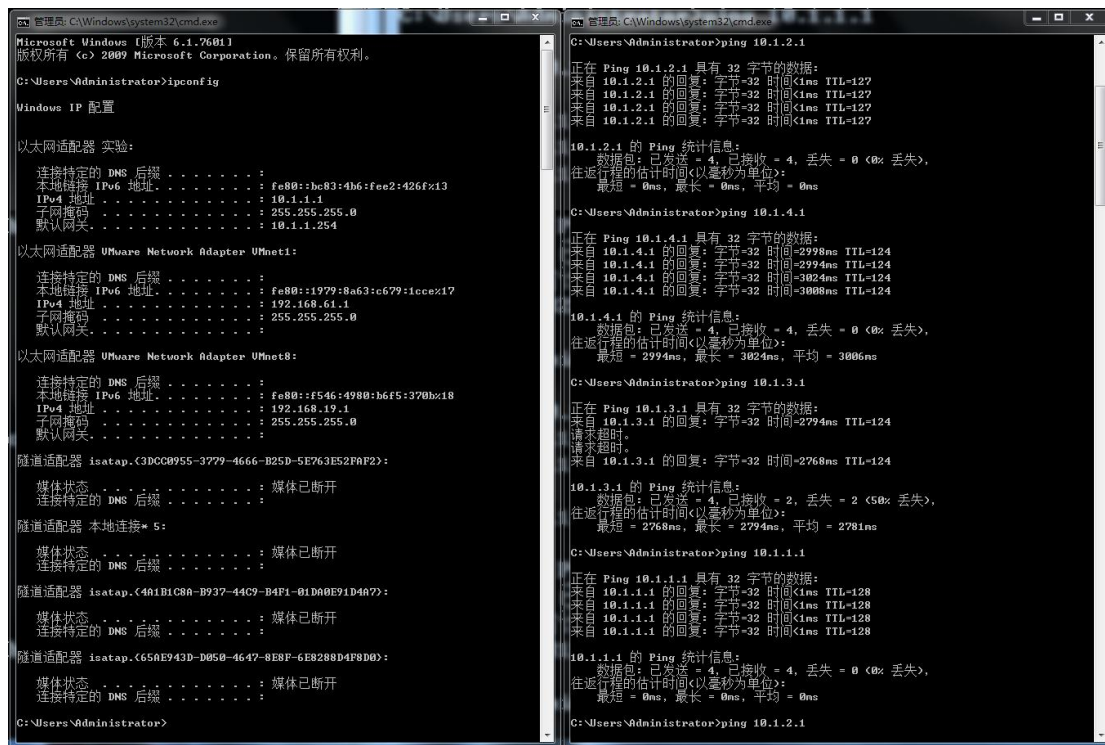
```

```
class classmap1 ! 匹配分类映射图
police 1000000 65536 exceed-action drop ! 带宽限制为 1Mbps, 突发数据量为 64k/sec
exit
interface fa0/2
mls qos trust cos ! 启动 Qos, 并且设置信任模式为 cos
service-policy input policymap1 ! 应用策略
```

5 结果验证

5.1 各 PC 之间互通

5.1.1 PC1



The image shows two side-by-side Windows command prompt windows. The left window displays the output of the 'ipconfig' command for three network adapters: '以太网适配器 实验:', '以太网适配器 VMware Network Adapter VMnet1:', and '以太网适配器 VMware Network Adapter VMnet8:'. Each adapter shows its IPv4 address, IPv6 address, and default gateway. The right window shows the output of several 'ping' commands: 'ping 10.1.2.1', 'ping 10.1.4.1', 'ping 10.1.3.1', 'ping 10.1.1.1', and 'ping 10.1.2.1'. Each ping command shows the results of four requests, including the number of bytes, time, TTL, and statistics for the round-trip time.

```
Microsoft Windows [版本 6.1.7601]
版权所有 (c) 2009 Microsoft Corporation。保留所有权利。

C:\Users\Administrator>ipconfig

Windows IP 配置

以太网适配器 实验:

    连接特定的 DNS 后缀 . . . . . :
    本地链接 IPv6 地址. . . . . : fe80::bc83:4b6:fee2:426f::13
    IPv4 地址. . . . . : 10.1.1.1
    子网掩码. . . . . : 255.255.255.0
    默认网关. . . . . : 10.1.1.254

以太网适配器 VMware Network Adapter VMnet1:

    连接特定的 DNS 后缀 . . . . . :
    本地链接 IPv6 地址. . . . . : fe80::1979:8a63:c679:1cce::17
    IPv4 地址. . . . . : 192.168.61.1
    子网掩码. . . . . : 255.255.255.0
    默认网关. . . . . :

以太网适配器 VMware Network Adapter VMnet8:

    连接特定的 DNS 后缀 . . . . . :
    本地链接 IPv6 地址. . . . . : fe80::f546:4980:b6f5:370b::18
    IPv4 地址. . . . . : 192.168.19.1
    子网掩码. . . . . : 255.255.255.0
    默认网关. . . . . :

隧道适配器 isatap.{3DC8955-3779-4666-B25D-5E763E52F8F2}:

    媒体状态 . . . . . : 媒体已断开
    连接特定的 DNS 后缀 . . . . . :

隧道适配器 本地连接* 5:

    媒体状态 . . . . . : 媒体已断开
    连接特定的 DNS 后缀 . . . . . :

隧道适配器 isatap.{401B1C8A-B937-44C9-B4F1-01D00E91D4A7}:

    媒体状态 . . . . . : 媒体已断开
    连接特定的 DNS 后缀 . . . . . :

隧道适配器 isatap.{65AE943D-D050-4647-8E8F-6E8288D4F8D0}:

    媒体状态 . . . . . : 媒体已断开
    连接特定的 DNS 后缀 . . . . . :

C:\Users\Administrator>

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=2998ms TTL=124
来自 10.1.4.1 的回复: 字节=32 时间=2994ms TTL=124
来自 10.1.4.1 的回复: 字节=32 时间=3024ms TTL=124
来自 10.1.4.1 的回复: 字节=32 时间=3006ms 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 = 2994ms, 最长 = 3024ms, 平均 = 3006ms

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=2794ms TTL=124
请求超时。
请求超时。
来自 10.1.3.1 的回复: 字节=32 时间=2768ms TTL=124

10.1.3.1 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 2, 丢失 = 2 (50% 丢失),
    往返行程的估计时间(以毫秒为单位):
        最短 = 2768ms, 最长 = 2794ms, 平均 = 2781ms

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<1ms TTL=128
来自 10.1.1.1 的回复: 字节=32 时间<1ms TTL=128
来自 10.1.1.1 的回复: 字节=32 时间<1ms TTL=128
来自 10.1.1.1 的回复: 字节=32 时间<1ms TTL=128

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 = 0ms, 最长 = 0ms, 平均 = 0ms

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

5.1.2 PC2

```
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>ipconfig

Windows IP 配置

以太网适配器 实验:

    连接特定的 DNS 后缀 . . . . . :
    本地链接 IPv6 地址. . . . . : fe80::c0d6:2f:8b14:a4b72:13
    IPv4 地址. . . . . : 10.1.2.1
    子网掩码. . . . . : 255.255.255.0
    默认网关. . . . . : 10.1.2.254

以太网适配器 VMware Network Adapter VMnet1:

    连接特定的 DNS 后缀 . . . . . :
    本地链接 IPv6 地址. . . . . : fe80::1979:8a63:c679:1ccc:17
    IPv4 地址. . . . . : 192.168.61.1
    子网掩码. . . . . : 255.255.255.0
    默认网关. . . . . :

以太网适配器 VMware Network Adapter VMnet8:

    连接特定的 DNS 后缀 . . . . . :
    本地链接 IPv6 地址. . . . . : fe80::f546:4980:b6f5:370b:18
    IPv4 地址. . . . . : 192.168.19.1
    子网掩码. . . . . : 255.255.255.0
    默认网关. . . . . :

隧道适配器 isatap.{3DC08955-3779-4666-B25D-5E763E52FAF2}:

    媒体状态. . . . . : 媒体已断开
    连接特定的 DNS 后缀. . . . . :

隧道适配器 本地连接* 5:

    媒体状态. . . . . : 媒体已断开
    连接特定的 DNS 后缀. . . . . :

隧道适配器 isatap.{4A1B1C8A-B937-44C9-B4F1-01D0A0E91D407}:

    媒体状态. . . . . : 媒体已断开
    连接特定的 DNS 后缀. . . . . :

隧道适配器 isatap.{65AE943D-D050-4647-8E8F-6E8288D4F8D0}:

    媒体状态. . . . . : 媒体已断开
    连接特定的 DNS 后缀. . . . . :

C:\Users\Administrator>

管理员: C:\Windows\system32\cmd.exe
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<1ms TTL=127
来自 10.1.1.1 的回复: 字节=32 时间<1ms TTL=127
来自 10.1.1.1 的回复: 字节=32 时间<1ms TTL=127
来自 10.1.1.1 的回复: 字节=32 时间<1ms TTL=127

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 = 0ms, 最长 = 0ms, 平均 = 0ms

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=128
来自 10.1.2.1 的回复: 字节=32 时间<1ms TTL=128
来自 10.1.2.1 的回复: 字节=32 时间<1ms TTL=128
来自 10.1.2.1 的回复: 字节=32 时间<1ms TTL=128

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 10.1.3.1

正在 Ping 10.1.3.1 具有 32 字节的数据:
请求超时。
来自 10.1.3.1 的回复: 字节=32 时间=3211ms TTL=124
来自 10.1.3.1 的回复: 字节=32 时间=3194ms TTL=124
来自 10.1.3.1 的回复: 字节=32 时间=3183ms TTL=124

10.1.3.1 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 3, 丢失 = 1 (25% 丢失),
    往返行程的估计时间(以毫秒为单位):
        最短 = 3183ms, 最长 = 3211ms, 平均 = 3169ms

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=3131ms TTL=124
请求超时。
来自 10.1.4.1 的回复: 字节=32 时间=3087ms TTL=124
来自 10.1.4.1 的回复: 字节=32 时间=3052ms TTL=124

10.1.4.1 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 3, 丢失 = 1 (25% 丢失),
    往返行程的估计时间(以毫秒为单位):
        最短 = 3052ms, 最长 = 3131ms, 平均 = 3090ms

C:\Users\Administrator>
```

5.1.3 PC3

```
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>ipconfig

Windows IP 配置

以太网适配器 实验:

    连接特定的 DNS 后缀 . . . . . :
    本地链接 IPv6 地址. . . . . : fe80::8cef:8456:b38e:b825:13
    IPv4 地址. . . . . : 10.1.3.1
    子网掩码. . . . . : 255.255.255.0
    默认网关. . . . . : 10.1.3.254

以太网适配器 VMware Network Adapter VMnet1:

    连接特定的 DNS 后缀 . . . . . :
    本地链接 IPv6 地址. . . . . : fe80::1979:8a63:c679:1ccc:17
    IPv4 地址. . . . . : 192.168.61.1
    子网掩码. . . . . : 255.255.255.0
    默认网关. . . . . :

以太网适配器 VMware Network Adapter VMnet8:

    连接特定的 DNS 后缀 . . . . . :
    本地链接 IPv6 地址. . . . . : fe80::f546:4980:b6f5:370b:18
    IPv4 地址. . . . . : 192.168.19.1
    子网掩码. . . . . : 255.255.255.0
    默认网关. . . . . :

隧道适配器 isatap.{3DC08955-3779-4666-B25D-5E763E52FAF2}:

    媒体状态. . . . . : 媒体已断开
    连接特定的 DNS 后缀. . . . . :

隧道适配器 本地连接* 5:

    媒体状态. . . . . : 媒体已断开
    连接特定的 DNS 后缀. . . . . :

隧道适配器 isatap.{4A1B1C8A-B937-44C9-B4F1-01D0A0E91D407}:

    媒体状态. . . . . : 媒体已断开
    连接特定的 DNS 后缀. . . . . :

隧道适配器 isatap.{65AE943D-D050-4647-8E8F-6E8288D4F8D0}:

    媒体状态. . . . . : 媒体已断开
    连接特定的 DNS 后缀. . . . . :

C:\Users\Administrator>

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 10.1.1.1

正在 Ping 10.1.1.1 具有 32 字节的数据:
请求超时。
来自 10.1.1.1 的回复: 字节=32 时间=3235ms TTL=124
来自 10.1.1.1 的回复: 字节=32 时间=3238ms TTL=124
来自 10.1.1.1 的回复: 字节=32 时间=3225ms TTL=124

10.1.1.1 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 3, 丢失 = 1 (25% 丢失),
    往返行程的估计时间(以毫秒为单位):
        最短 = 3225ms, 最长 = 3238ms, 平均 = 3232ms

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=3221ms TTL=124
来自 10.1.2.1 的回复: 字节=32 时间=3153ms TTL=124
来自 10.1.2.1 的回复: 字节=32 时间=3119ms TTL=124

10.1.2.1 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 3, 丢失 = 1 (25% 丢失),
    往返行程的估计时间(以毫秒为单位):
        最短 = 3119ms, 最长 = 3221ms, 平均 = 3164ms

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=128
来自 10.1.3.1 的回复: 字节=32 时间<1ms TTL=128
来自 10.1.3.1 的回复: 字节=32 时间<1ms TTL=128
来自 10.1.3.1 的回复: 字节=32 时间<1ms TTL=128

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

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<1ms TTL=125
来自 10.1.4.1 的回复: 字节=32 时间<1ms TTL=125
来自 10.1.4.1 的回复: 字节=32 时间<1ms TTL=125
来自 10.1.4.1 的回复: 字节=32 时间<1ms TTL=125

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 = 0ms, 最长 = 0ms, 平均 = 0ms

C:\Users\Administrator>
```


5.1.4 PC4

```
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>ipconfig

Windows IP 配置

以太网适配器 实验:

    连接特定的 DNS 后缀 . . . . . :
    本地链接 IPv6 地址. . . . . : fe80::d03a:1593:9173:118e%13
    IPv4 地址. . . . . : 10.1.1.1
    子网掩码 . . . . . : 255.255.255.0
    默认网关. . . . . : 10.1.1.254

以太网适配器 VMware Network Adapter VMnet1:

    连接特定的 DNS 后缀 . . . . . :
    本地链接 IPv6 地址. . . . . : fe80::1979:8a63:c679:1cce%17
    IPv4 地址. . . . . : 192.168.61.1
    子网掩码 . . . . . : 255.255.255.0
    默认网关. . . . . :

以太网适配器 VMware Network Adapter VMnet8:

    连接特定的 DNS 后缀 . . . . . :
    本地链接 IPv6 地址. . . . . : fe80::f546:4980:b6f5:370b%18
    IPv4 地址. . . . . : 192.168.19.1
    子网掩码 . . . . . : 255.255.255.0
    默认网关. . . . . :

隧道适配器 isatap.{3DC08955-3779-4666-B25D-5E763E52F8F2}:

    媒体状态 . . . . . : 媒体已断开
    连接特定的 DNS 后缀 . . . . . :

隧道适配器 本地连接* 5:

    媒体状态 . . . . . : 媒体已断开
    连接特定的 DNS 后缀 . . . . . :

隧道适配器 isatap.{401B1C80-B937-44C9-B4F1-01D00E91D407}:

    媒体状态 . . . . . : 媒体已断开
    连接特定的 DNS 后缀 . . . . . :

隧道适配器 isatap.{65AE943D-D050-4647-8E8F-6E8288D4F8D0}:

    媒体状态 . . . . . : 媒体已断开
    连接特定的 DNS 后缀 . . . . . :

C:\Users\Administrator>

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 10.1.1.1

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=321ms TTL=124
来自 10.1.1.1 的回复: 字节=32 时间=317ms TTL=124
来自 10.1.1.1 的回复: 字节=32 时间=319ms TTL=124
来自 10.1.1.1 的回复: 字节=32 时间=310ms 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 = 310ms, 最长 = 321ms, 平均 = 317ms

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=309ms TTL=124
来自 10.1.2.1 的回复: 字节=32 时间=306ms TTL=124
来自 10.1.2.1 的回复: 字节=32 时间=304ms TTL=124
请求超时。

10.1.2.1 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 3, 丢失 = 1 (25% 丢失),
    往返行程的估计时间(以毫秒为单位):
        最短 = 304ms, 最长 = 309ms, 平均 = 306ms

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

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<1ms TTL=128
来自 10.1.4.1 的回复: 字节=32 时间<1ms TTL=128
来自 10.1.4.1 的回复: 字节=32 时间<1ms TTL=128
来自 10.1.4.1 的回复: 字节=32 时间<1ms TTL=128

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 = 0ms, 最长 = 0ms, 平均 = 0ms

C:\Users\Administrator>
```

5.2 各 PC 与 8.8.8.8 外网连通性

5.2.1 PC1

```
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=432ms TTL=62
来自 8.8.8.8 的回复: 字节=32 时间=481ms 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=454ms 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 = 432ms, 最长 = 481ms, 平均 = 454ms

C:\Users\Administrator>

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>ipconfig

Windows IP 配置

以太网适配器 实验:

    连接特定的 DNS 后缀 . . . . . :
    本地链接 IPv6 地址. . . . . : fe80::bc83:4b6:fee2:426f%13
    IPv4 地址. . . . . : 10.1.1.1
    子网掩码 . . . . . : 255.255.255.0
    默认网关. . . . . : 10.1.1.254
```

5.2.2 PC2

```
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 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=575ms TTL=62
来自 8.8.8.8 的回复: 字节=32 时间=538ms TTL=62
来自 8.8.8.8 的回复: 字节=32 时间=620ms TTL=62
来自 8.8.8.8 的回复: 字节=32 时间=580ms 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 = 538ms, 最长 = 620ms, 平均 = 578ms

C:\Users\Administrator>

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>ipconfig

Windows IP 配置

以太网适配器 实验:

    连接特定的 DNS 后缀 . . . . . :
    本地链接 IPv6 地址. . . . . : fe80::c9d6:2f:8b14:a4b7%13
    IPv4 地址. . . . . : 10.1.2.1
    子网掩码 . . . . . : 255.255.255.0
    默认网关. . . . . : 10.1.2.254

以太网适配器 VMware Network Adapter VMnet1:

    连接特定的 DNS 后缀 . . . . . :
    本地链接 IPv6 地址. . . . . : fe80::1979:8a63:c679:1cce%17
    IPv4 地址. . . . . : 192.168.61.1
    子网掩码 . . . . . : 255.255.255.0
    默认网关. . . . . :
```


5.2.3 PC3

```
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>ipconfig

Windows IP 配置

以太网适配器 实验:

    连接特定的 DNS 后缀 . . . . . :
    本地连接 IPv6 地址. . . . . : fe80::8cef:8456:b38e:b825%13
    IPv4 地址 . . . . . : 10.1.3.1
    子网掩码 . . . . . : 255.255.255.0
    默认网关. . . . . : 10.1.3.254

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<1ms TTL=63
来自 8.8.8.8 的回复: 字节=32 时间<1ms TTL=63
来自 8.8.8.8 的回复: 字节=32 时间<1ms TTL=63
来自 8.8.8.8 的回复: 字节=32 时间<1ms TTL=63

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 = 0ms, 最长 = 0ms, 平均 = 0ms

C:\Users\Administrator>
```

5.2.4 PC4

```
C:\Windows\system32\cmd.exe
C:\Users\Administrator>ipconfig

Windows IP 配置

以太网适配器 实验:

    连接特定的 DNS 后缀 . . . . . :
    本地连接 IPv6 地址. . . . . : fe80::d83a:1593:9173:118e%13
    IPv4 地址 . . . . . : 10.1.4.1
    子网掩码 . . . . . : 255.255.255.0
    默认网关. . . . . : 10.1.4.254

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),

C:\Users\Administrator>
```

5.3 IPsec Tunnel 验证

5.3.1 PC1 到 PC3



The first screenshot shows the output of the `ipconfig` command in an administrator command prompt. It displays the network configuration for the Ethernet adapter, including the IPv6 address `fe80::bc83:4b6:fee2:426f%13`, the IPv4 address `10.1.1.1`, the subnet mask `255.255.255.0`, and the default gateway `10.1.1.254`.

The second screenshot shows the output of the `tracert 10.1.3.1` command. It displays the route from the local host to the destination IP address `10.1.3.1`. The route consists of five hops: 1. `10.1.1.254` (1 ms), 2. `10.11.11.1` (<1 ms), 3. `10.12.12.2` (2899 ms), 4. `10.22.22.2` (2919 ms), and 5. `WL21-04 [10.1.3.1]` (2917 ms). The traceroute is completed successfully.

5.3.2 PC2 到 PC4



The first screenshot shows the output of the `ipconfig` command in an administrator command prompt. It displays the network configuration for the Ethernet adapter, including the IPv6 address `fe80::c0d6:2f:8b14:a4b7%13`, the IPv4 address `10.1.2.1`, the subnet mask `255.255.255.0`, and the default gateway `10.1.2.254`.

The second screenshot shows the output of the `tracert 10.1.4.1` command. It displays the route from the local host to the destination IP address `10.1.4.1`. The route consists of five hops: 1. `10.1.2.254` (1 ms), 2. `10.11.11.1` (<1 ms), 3. `10.12.12.2` (2787 ms), 4. `10.23.23.2` (2745 ms), and 5. `WL21-05 [10.1.4.1]` (2757 ms). The traceroute is completed successfully.

5.3.3 PC3 到 PC1

```
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>ipconfig

Windows IP 配置

以太网适配器 实验:

    连接特定的 DNS 后缀 . . . . . :
    本地链接 IPv6 地址. . . . . : fe80::8cef:8456:b38e:b825%13
    IPv4 地址 . . . . . : 10.1.3.1
    子网掩码 . . . . . : 255.255.255.0
    默认网关. . . . . : 10.1.3.254

C:\Users\Administrator>tracert 10.1.1.1

通过最多 30 个跃点跟踪
到 WL21-01 [10.1.1.1] 的路由:

 1    1 ms    1 ms    1 ms  10.1.3.254
 2    <1 毫秒  <1 毫秒  <1 毫秒  10.22.22.1
 3   2813 ms  2786 ms  2651 ms  10.12.12.1
 4   2448 ms  2465 ms  2463 ms  10.11.11.2
 5   2438 ms  2462 ms  2585 ms  WL21-01 [10.1.1.1]

跟踪完成。

C:\Users\Administrator>
```

5.3.4 PC4 到 PC1

```
管理员: C:\Windows\system32\cmd.exe
C:\Users\Administrator>ipconfig

Windows IP 配置

以太网适配器 实验:

    连接特定的 DNS 后缀 . . . . . :
    本地链接 IPv6 地址. . . . . : fe80::d03a:1593:9173:118e%13
    IPv4 地址 . . . . . : 10.1.4.1
    子网掩码 . . . . . : 255.255.255.0
    默认网关. . . . . : 10.1.4.254

C:\Users\Administrator>tracert 10.1.2.1

通过最多 30 个跃点跟踪
到 WL21-02 [10.1.2.1] 的路由:

 1    1 ms    1 ms    1 ms  10.1.4.254
 2    <1 毫秒  <1 毫秒  <1 毫秒  10.23.23.1
 3    *       2794 ms  2741 ms  10.12.12.1
 4   2726 ms  2697 ms  2691 ms  10.11.11.2
 5   2719 ms  2679 ms  2672 ms  WL21-02 [10.1.2.1]

跟踪完成。

C:\Users\Administrator>
```