

**计算机网络专题实验教程**

**张玉龙 朱利 魏恒义**

西安交通大学

2022年5月 （第二版）

知道事物应该是什么样，说明你是聪明的人；

知道事物实际是什么样，说明你是有经验的人；

知道怎样使事物变得更好，说明你是有才能的人。

------法国哲学家狄德罗

前 言

《计算机网络专题实验》是一门独立设置的实践课程，该课程是学生深入理解计算机网络工作机制、协议控制流程以及网络功能实现的有效途径，是对所学计算机网络知识全面、系统的总结、巩固和提高的一项课程实践活动。

在创新实践培养模式中，需要将创新意识、创新能力培养贯穿于人才培养的全过程和每个教学环节。在本课程的教学体系中将实验内容进行分层设计，在指导过程进行个性化互动，力图提高学生创新实践思维和能力。课程的内容设计中分为基础引导、进阶综合设计和师生互动讨论主题三部分。对基础引导阶段的内容尽可能简练、快速；进阶综合设计阶段尽可能让学生能基于刚刚完成的实验内容，在比较、分析、改进的基础上完成自主综合设计。师生互动讨论主题的设计主要有两个层次：覆盖全部同学的是实验结果质询与分析讨论，与每位同学的互动结果反映了该同学对实验原理、过程和结果的理解。对有时间进行进阶综合设计实验的同学，实验方法设计、实验结果的获得方法和结果分析是师生互动的主题。

完成本实践课程的同学，会在如下几个层次得到收获。一是设备配置与基本原理验证；二是网络协议分析；三是实验结果分析与拓展；四是进阶综合设计的创新。其中前三项是每位同学必然的收获。通过每个实验项目的实验结果分析与拓展延伸，培养学生的创新意识，提高学生自身的创新能力。

编者

二零二零年五月

实验注意事项

1. 实验包含7个网络设备实验和1个网络编程实验。
2. 参与同学须提前预习实验指导书，以便提高现场实验效率。
3. 在实验项目中每位同学的角色不同，现场检查单要反映本人工作特点，如实做好实验记录。
4. 每个实验项目过程中请及时截屏保存实验结果，作为现场检查单的素材。
5. 规范操作设备，实验完成后将网线等器材放入收纳盒。

现场实验检查单、师生互动结果是反映本实验效果的主要环节，也是成绩评定的主要依据，请如实记录。

# 

第一部分 实验环境与设备

# 实验设备及控制方式

## 设备配置方式

每实验组配备有4台计算机，编号为PC1-PC4。如1#组的PC1-4的IP地址根据实验设计要求自行配置（建议采用10网段，规则是10.**GN**.x.**PCN**，PCN为PC号，比如第2组的PC3，可以用10.2.2.3）。

用户使用putty登录到设备中，可以输入命令配置设备，建议固定一位同学对设备进行配置操作。

## 软件环境及工具

#### 台式计算机操作系统Windows/Win10

每台PC均安装了64位的Windows 7/10系统。

#### Wireshark

Wireshark是一个网络封包分析软件。网络封包分析软件的功能是捕获网络包，并尽可能详细的解析出报文资料。

#### TCP/UDP传输软件

提供TCP/UDP分析软件供传输协议分析实验用，可建立tcp或udp服务器或客户端，协助捕获报文。

# 设备配置

## 交换机配置

交换机是工作在OSI参考模型第二层的网络连接设备，它的基本功能是在多个计算机或者网段之间交换数据。交换机内部一般采用背板总线交换结构，为每个端口提供一个独立的共享介质，即每个冲突域只有一个端口。

以太网交换机在数据链路层进行数据转发时，根据数据包的MAC地址决定数据转发的端口，而不是简单地向所有端口转发，以便提高网络的利用率。当交换机接收到一个数据帧时，它首先会记录数据帧的源端口和源MAC地址的映射，然后将数据帧的目的MAC地址与系统内部的动态查找表进行比较，并根据比较结果将数据包发送给相应的目的端口。若数据包的目的MAC地址不在查找表中，则将包广播到每个端口（除了发送端口）。不同设备命令有所不同，下以H3C交换机为例。

### 交换机模式配置

<H3C> 默认用户视图，<H3C>

<H3C>display interface 查看交换机所有的端口的状态和配置

<H3C>system-view 进入系统视图，[H3C]，Ctrl+z返回用户视图

[H3C]interface Ethernet 1/0/1 进入以太网端口0/0/1

[H3C]vlan 1 进入vlan 1虚拟接口

#### 3）VLAN接口配置模式

[H3C]vlan 100 创建并进入vlan 100 接口配置模式

[H3C-vlan100] vlan 100 接口配置模式提示符

<H3C>display vlan 100 查看vlan 100的配置

#### 4）恢复交换机出厂设置

<H3C>reset saved-configuration 启动初始化

The saved configuration file will be erased. Are you sure [Y/N]:y 确认初始化

<H3C>reboot 重新启动交换机

Start to check configuration with next startup configuration file, please wait.........DONE!

This command will reboot the device. Current configuration will be lost, save current configuration? [Y/N]:N

This command will reboot the device. Continue? [Y/N]:Y

### 交换机主要命令列表

|  |  |  |
| --- | --- | --- |
| 状态 | 命令 | 作用 |
| <H3C> | system-view | 进入系统视图 [H3C] |
| [H3C] | Ctrl+z | 退出系统视图 |
|  | quit | 返回到上一级模式 |
| <H3C> | reset saved-configuration | 恢复出厂设置 |
| <H3C> | reboot | 热启动交换机 |
| <H3C> | Display current-configuration或者 dis cu | 显示目前生效的配置参数 |
| [H3C] | Interface enthernet 1/0/1 | 进入该端口配置模式 |
|  | ? | 显示当前模式可用的命令列表 |

1. 交换机VLAN配置命令

|  |  |  |
| --- | --- | --- |
| 状态 | 命令 | 作用 |
| [H3C] | vlan x | 划分Vlan x 进入该Vlan的配置模式switch(Config- vlanx)# |
| [H3C] | undo vlan x | 删除Vlan x |
| [H3C] | rip | 激活RIP进程，进入switch(Config-router)#模式 |
| [H3C] | network vlan x | 指定与RIP相关的valan号 |
| [H3C] | port interface 端口 | 将指定端口划分到vlan x |
| [H3C] | undo port interface 端口 | 从vlan x删除指定端口 |
| [H3C] | display vlan | 查看当前全部VLAN |
| [H3C] | ip address IP地址 子网掩码 | 为vlan x指定IP地址 |
| [H3C] | undo ip address IP地址 子网掩码 | 去掉vlan x的IP地址 |

## 路由器配置

路由器是工作在OSI参考模型第三层的网络连接设备，它的基本功能是根据数据包的IP地址选择发送路径，转发数据包到相应网络。路由器的数据转发是基于路由表实现的，每个路由器都会维护一张路由表，根据路由表决定数据包的转发路径。当路由器接收到一个数据包后，首先对数据包进行校验，对于发送给路由器的数据包，路由器就交给相应模块去处理，而大多数需要转发的数据包，路由器查询路由表，然后根据查询结果转发数据包到相应的端口和网络。下面以H3C MSR800为例。

#### 1）路由器配置模式转换

路由器和交换机一样，也有不同的配置模式：

<H3C> 默认用户视图，<H3C>

<H3C>display interface 查看交换机所有的端口的状态和配置

<H3C>system-view 进入系统视图，[H3C]，Ctrl+z返回用户视图

[H3C]interface Ethernet 1/0/1 进入以太网端口0/0/1

[H3C]vlan 1 进入vlan 1虚拟接口

命令“display interface”查看路由器所用端口的配置情况，路由器采用x/y的形式标识一个端口，其中x代表是第几个模块，y代表是该模块的第几个端口。

#### 2）路由端口配置

<H3C>system-view ！进入系统视图

[H3C-vlan1]name RouterA !修改路由名

[H3C-vlan1]interface vlan-interface1 !进入vlan-interface1接口配置

[H3C-vlan-interface1]ip address 10.1.2.1 255.255.255.0 !为路由端口设置IP

[H3C-vlan-interface1]quit !返回到上一个模式

[H3C]display interface vlan-interface1 !查看vlan-interface1接口信息

# 学生机的网络接口及配置

## 学生机的网络接口

### 学生机的网络接口

根据实验拓扑结构进行连接，为PC机指定角色，其IP地址根据实验设计要求自行配置（建议采用10网段，规则是10.**GN**.x.**PCN**，PCN为PC号，比如第2组的PC3，可以用10.2.2.3）。



图4-1 学生机网卡

### 学生机的网络接口配置

一般情况下，使用GUI（图形用户接口）界面配置Windows的网络接口。但在特殊情况下，Windows的网络接口及路由混乱，从GUI界面难以有效管理时，建议使用netsh和ipconfig等命令来管理学生机的网络接口。

#### GUI方式的网络接口配置方法

使用GUI方式修改，有多种方法。右键点击桌面的“网络”，或任务栏右下角的网络标记（如图4-2），选择“打开网络和共享中心”（图4-3）。请参见图4-4，选择点击“更改适配器设置”。



图4-2 任务栏右下角的网络标记

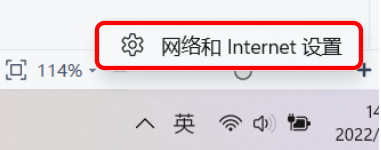


图4-3 右键点击网络标记并选择“打开网络和共享中心”



图4-4 Windows的“网络和共享中心”界面

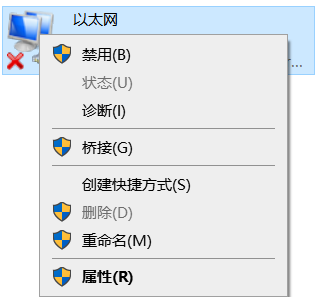


图4-5 Windows的网络接口右键菜单



图4-6 选择修改网卡的IPv4属性

通过右键可以禁用或启用，或者修改其属性（如图4-5）。现在假设我们来修改其IPv4属性。在图4-6中，双击“Internet协议版本4（TCP/IPv4）”，可以手工修改这个接口（这里是out）的IP地址、子网掩码和默认网关。有时候还需要进入“高级(V)…”中设置，比如删除一个IP地址或网关。

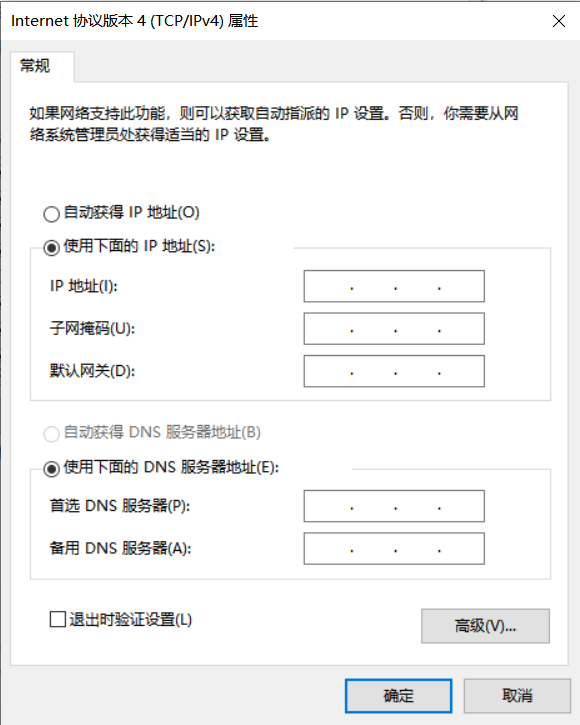


图4-7 网卡的IPv4属性修改

1. 命令行方式的网络接口配置

Windows的网络命令很多，这里主要介绍ipconfig 和 netsh。首先启动cmd窗口，方法如图4-8。点击Windows的左下角的“开始”按钮，在输入框中输入cmd，回车。

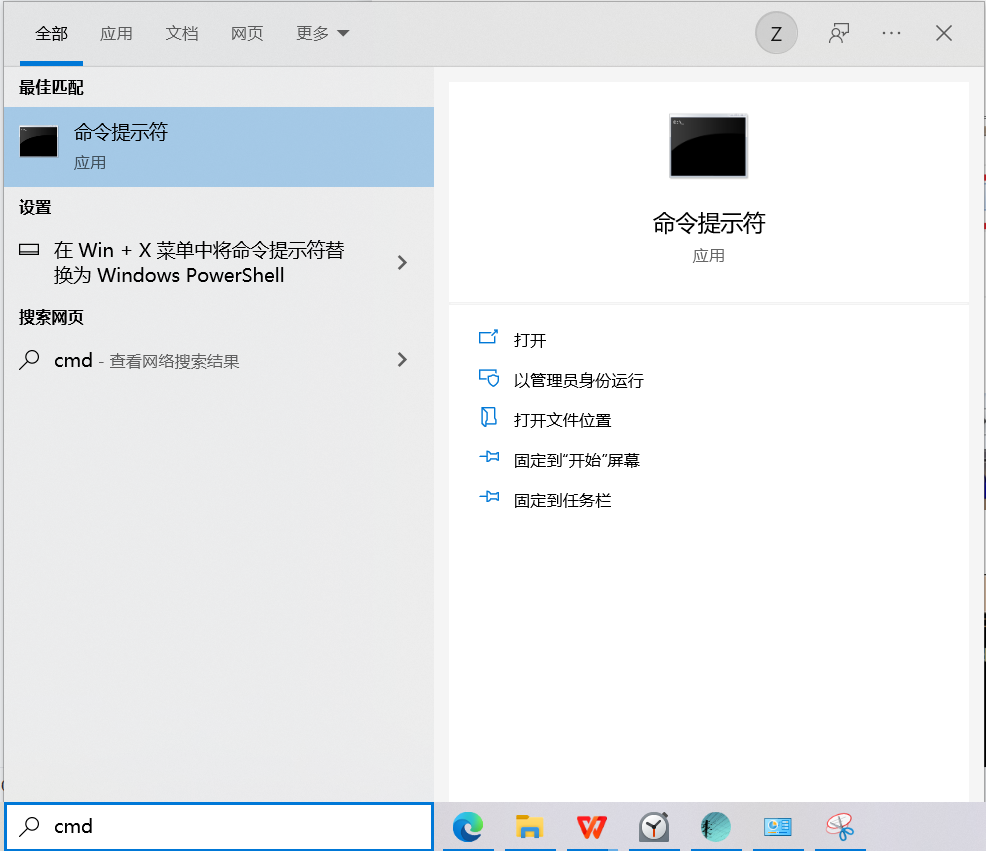


图4-8 Windows运行cmd命令

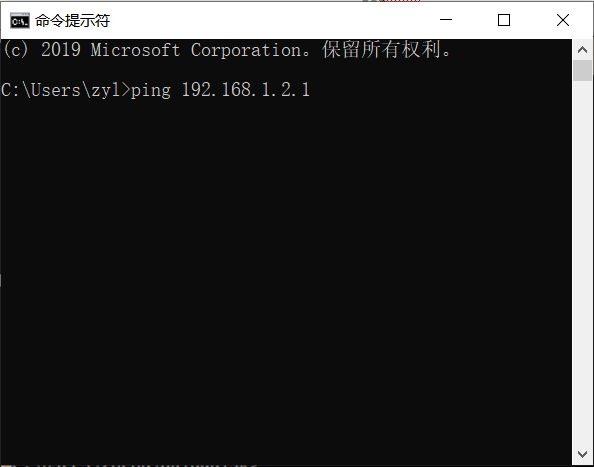


图4-9 cmd命令运行界面，在 **>**提示符下可以输入命令

cmd运行起来后，在其提示符 **>** 下（图4-9）可以输入命令。下面是ipconfig命令运行的例子，查看网络地址等信息。

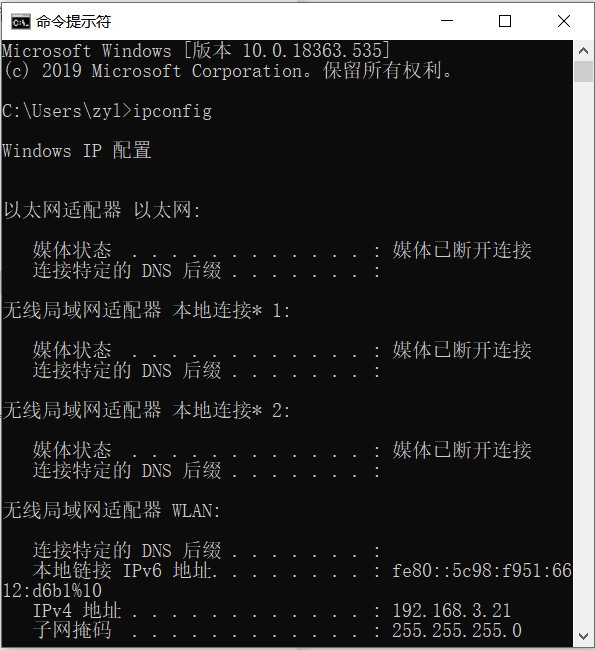


图4-10 cmd命令运行ipconfig界面

# 实验要求及考核

## 实验要求

（1）实验内容均在实验室完成，每次实验4小时，实验开始前指导教师讲授要点；

（2）根据实验内容，分2人小组或4人小组完成；

（3）每人填写实验现场检查单作为完成实验、提交验收的依据；

（4）指导教师按小组验收、与每位同学交流讨论；

（5）全部实验完成，按要求撰写综合实验报告，提交电子稿。

## 考核依据

（1）现场检查单及交流讨论记录；

（2）网络编程实现；

（3）考勤及其他。

## 注意事项

（1）注意截屏收集检查单素材。

（2）每次做完实验后应通过“display current- configuration”命令查看配置结果，并截获每个实验的主要结果图。

（3）注意PC机操作系统防火墙对测试的影响。

（4）对网络设备的配置是独享排它方式，确定专人通过PuTTY工具对网络设备进行配置。

（5）在捕获报文时，应关闭无关的应用程序运行窗口，减少无用报文产生；查阅报文时，灵活运用过滤器来查找实验所需报文。

# 实验中常见问题及解决方法

**实验经验**：

1. 实验开始前先画好网络拓扑图，并据此连接检查设备；
2. 实验过程中遇到ping不通的情况时，按以下顺序进行排查：
   1. 检查网络设备、PC接口的网线连接是否符合网络拓扑图；
   2. 检查各设备IP信息设置是符合网络拓扑图，包括IP地址、子网掩码、网关等；
   3. 根据由近到远的顺序ping各个节点，直至发现问题节点；
   4. 问题节点若是PC，利用ipconfig命令检查IP、网关是否正确，检查是否有多个网关同时存在，通过改为自动获取IP、禁用重启网卡、手动设置IP的方式重新配置IP；
   5. 问题节点若是网络设备，进入设备控制界面查看配置信息是否符合网络拓扑图，对错误配置进行更正。
3. 网络设备实验

# 实验一 组网

## 实验目的

掌握路由器、交换机进行简单组网的方法，理解交换机、路由器的工作原理；

## 实验内容

使用路由器和交换机进行组网，实现各PC间的互联互通；

## 实验原理

信息化已成为当前世界各国战略重点和优先发展方向，信息化首先从基础设施开始。

20 世纪 90 年代，我国尚未建立完整的网络通信技术自主研发体系，网络通信设备的研发及生产以国外大型通信设备公司为主。随着经济全球化程度的不断加深，欧美发达国家将产业重心转移到品牌及设计领域，大陆网络通信设备制造商开始承接欧美发达国家产业转移的生产业务，我国网络通信设备行业开始积累生产管理经验、管理人才及技术储备，行业正式起步发展。

进入 21 世纪以后，随着信息化时代的来临，国家对网络通信基础设施建设的重视程度不断提升，以华为、中兴为代表的中国通信企业依靠国家的政策支持、持续的高额研发投入、全球化的市场布局，在全球通信设备市场已经从追赶者逐渐变成了行业领跑者。同时，国内通信设备厂商积极利用资本市场，进行产业整合，壮大自身实力，以星网锐捷、烽火通信等为代表的国内网络通信设备厂商，在市场营销及品牌推广方面于全球网络通信设备市场上均有较好的表现，逐步发展为行业内知名品牌商。

近年来，随着云计算、物联网、视频应用、社交网络、网络直播等业务类型的发展，网络数据流量增长迅猛，激增的流量使骨干网和接入网对网络通信设备的需求也不断提高。随着国家对信息安全问题越来越重视，我国已有部分政府、军队、金融、电信、能源等重点领域及企业开始重新选择软硬件合作伙伴，以保障国内重点领域的信息安全。在多方面利好因素的影响下，我国网络通信设备企业实现了快速发展，未来发展趋势持续向好。随着国内品牌厂商的崛起，OEM/ODM 模式的国内网络通信设备制造商纷纷开始将事业重心转向国内，逐步摆脱对国外单一客户的依赖，实现国内外市场均衡发展，提升抗风险能力。

### 路由器

路由器是互联网的主要结点设备。路由器通过路由决定数据的转发。转发策略称为[路由选择](https://baike.baidu.com/item/%E8%B7%AF%E7%94%B1%E9%80%89%E6%8B%A9/10824858" \t "https://baike.baidu.com/item/%E8%B7%AF%E7%94%B1%E5%99%A8/_blank)（routing），这也是路由器名称的由来。作为不同网络之间互相连接的枢纽，路由器系统构成了基于TCP/IP的国际互联网络Internet 的主体脉络，也可以说，路由器构成了Internet的骨架。它的处理速度是网络通信的主要瓶颈之一，它的可靠性则直接影响着网络互连的质量。因此，在园区网、地区网、乃至整个Internet研究领域中，路由器技术始终处于核心地位，其发展历程和方向，成为整个Internet研究的一个缩影。

路由器通常位于网络层，因而路由技术也是与网络层相关的一门技术， 路由器与早期的网桥相比有很多的变化和不同。 通常而言，网桥的局限性比较大，它只能够连通[数据链路层](https://baike.baidu.com/item/%E6%95%B0%E6%8D%AE%E9%93%BE%E8%B7%AF%E5%B1%82/4329290" \t "https://baike.baidu.com/item/%E8%B7%AF%E7%94%B1%E5%99%A8/_blank)相同或者类似的网络，不能够连接数据链路层之间有着较大差异的网络。但是路由器却不同，它打破了这个局限，能够连接任意的两种不同的网络，但是这两种不同的网络之间要遵守一个原则，就是使用相同的网络层协议，这样才能够被路由器连接。 路由技术简单来说就是对网络上众多的信息进行转发与交换的一门技术，具体来说，就是通过互联网络将信息从源地址传送到目的地址。路由技术的发展，满足了人们对数据、语音和图像的综合应用，逐渐被大多数家庭网络所选择使用。

除此之外，这几年来，我国的路由技术越来越成熟，同时也结合了当代的智能化技术，使得人们在使用路由技术的过程中能够体会到快捷、快速的效果，从而推动和促进[互联网](https://baike.baidu.com/item/%E4%BA%92%E8%81%94%E7%BD%91/199186" \t "https://baike.baidu.com/item/%E8%B7%AF%E7%94%B1%E5%99%A8/_blank)和网络技术的发展。

### 交换机

“交换机”是一个外来词，源自英文“Switch”，原意是“开关”，中国技术界在引入这个词汇时，翻译为“交换”。在英文中，动词“交”和名词“交换机”是同一个词（注意这里的“交换”特指电信技术中的信号交换，与物品交换不是同一个概念）。

1993年，[局域网](https://baike.baidu.com/item/%E5%B1%80%E5%9F%9F%E7%BD%91" \t "https://baike.baidu.com/item/_blank)交换设备出现，1994年，国内掀起了交换[网络技术](https://baike.baidu.com/item/%E7%BD%91%E7%BB%9C%E6%8A%80%E6%9C%AF" \t "https://baike.baidu.com/item/_blank)的热潮。其实，交换技术是一个具有简化、低价、高性能和高端口密集特点的交换产品，体现了[桥接](https://baike.baidu.com/item/%E6%A1%A5%E6%8E%A5" \t "https://baike.baidu.com/item/_blank)技术的复杂交换技术在[OSI参考模型](https://baike.baidu.com/item/OSI%E5%8F%82%E8%80%83%E6%A8%A1%E5%9E%8B" \t "https://baike.baidu.com/item/_blank)的第二层操作。与[桥接器](https://baike.baidu.com/item/%E6%A1%A5%E6%8E%A5%E5%99%A8" \t "https://baike.baidu.com/item/_blank)一样，交换机按每一个包中的MAC地址相对简单地决策信息转发。而这种转发决策一般不考虑包中隐藏的更深的其他信息。与桥接器不同的是交换机转发延迟很小，操作接近单个局域网性能，远远超过了普通桥接[互联网](https://baike.baidu.com/item/%E4%BA%92%E8%81%94%E7%BD%91" \t "https://baike.baidu.com/item/_blank)网络之间的转发性能。

交换技术允许共享型和专用型的局域网段进行带宽调整，以减轻局域网之间信息流通出现的[瓶颈](https://baike.baidu.com/item/%E7%93%B6%E9%A2%88" \t "https://baike.baidu.com/item/_blank)问题。已有[以太网](https://baike.baidu.com/item/%E4%BB%A5%E5%A4%AA%E7%BD%91" \t "https://baike.baidu.com/item/_blank)、[快速以太网](https://baike.baidu.com/item/%E5%BF%AB%E9%80%9F%E4%BB%A5%E5%A4%AA%E7%BD%91" \t "https://baike.baidu.com/item/_blank)、[FDDI](https://baike.baidu.com/item/FDDI" \t "https://baike.baidu.com/item/_blank)和[ATM](https://baike.baidu.com/item/ATM" \t "https://baike.baidu.com/item/_blank)技术的交换产品。

类似传统的[桥接器](https://baike.baidu.com/item/%E6%A1%A5%E6%8E%A5%E5%99%A8" \t "https://baike.baidu.com/item/_blank)，交换机提供了许多[网络互联](https://baike.baidu.com/item/%E7%BD%91%E7%BB%9C%E4%BA%92%E8%81%94" \t "https://baike.baidu.com/item/_blank)功能。交换机能[经济](https://baike.baidu.com/item/%E7%BB%8F%E6%B5%8E" \t "https://baike.baidu.com/item/_blank)地将网络分成小的冲突网域，为每个[工作站](https://baike.baidu.com/item/%E5%B7%A5%E4%BD%9C%E7%AB%99" \t "https://baike.baidu.com/item/_blank)提供更高的[带宽](https://baike.baidu.com/item/%E5%B8%A6%E5%AE%BD" \t "https://baike.baidu.com/item/_blank)。协议的[透明性](https://baike.baidu.com/item/%E9%80%8F%E6%98%8E%E6%80%A7" \t "https://baike.baidu.com/item/_blank)使得交换机在[软件配置](https://baike.baidu.com/item/%E8%BD%AF%E4%BB%B6%E9%85%8D%E7%BD%AE" \t "https://baike.baidu.com/item/_blank)简单的情况下直接安装在多协议网络中；交换机使用现有的电缆、[中继器](https://baike.baidu.com/item/%E4%B8%AD%E7%BB%A7%E5%99%A8" \t "https://baike.baidu.com/item/_blank)、[集线器](https://baike.baidu.com/item/%E9%9B%86%E7%BA%BF%E5%99%A8" \t "https://baike.baidu.com/item/_blank)和工作站的[网卡](https://baike.baidu.com/item/%E7%BD%91%E5%8D%A1" \t "https://baike.baidu.com/item/_blank)，不必作高层的硬件升级；交换机对工作站是透明的，这样管理开销低廉，简化了[网络节点](https://baike.baidu.com/item/%E7%BD%91%E7%BB%9C%E8%8A%82%E7%82%B9" \t "https://baike.baidu.com/item/_blank)的增加、移动和网络变化的操作。

利用专门设计的集成电路可使交换机以[线路速率](https://baike.baidu.com/item/%E7%BA%BF%E8%B7%AF%E9%80%9F%E7%8E%87" \t "https://baike.baidu.com/item/_blank)在所有的端口并行转发信息，提供了比传统桥接器高得多的操作性能。[专用集成电路](https://baike.baidu.com/item/%E4%B8%93%E7%94%A8%E9%9B%86%E6%88%90%E7%94%B5%E8%B7%AF" \t "https://baike.baidu.com/item/_blank)技术使得交换器在更多端口的情况下得以实现上述性能，其端口造价低于传统型桥接器。

## 组网实验

### 实验环境与分组

路由器H3C MSR 800 一台，交换机H3C S3110 两台；

每组2-4名同学，每人一台PC，协同进行实验。

### 实验拓扑结构

图1-1给出了本实验的组网实验示意图，鼓励各小组灵活自定义IP分配。

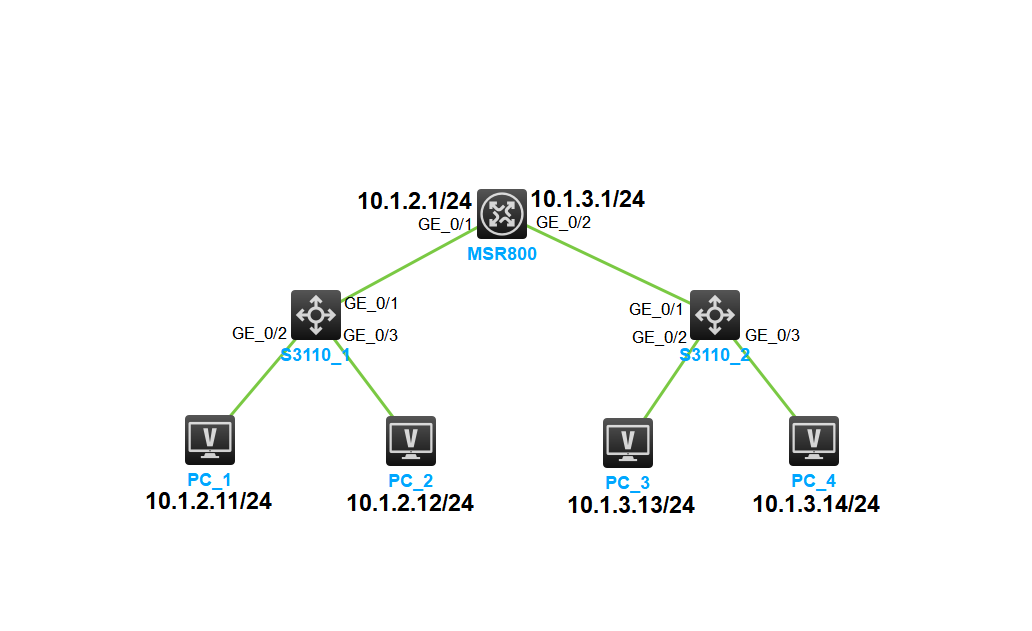


图1-1组网实验示意图

### 组网实验步骤

步骤1：按照图示连接好设备，设置各PC的IP地址和默认网关。

步骤2：将交换机恢复为出厂设置。具体方法参考2.1。

步骤3：配置路由器的接口IP地址，vlan 2接口的配置命令如下：

<H3C> system-view ！进入全局模式

[H3C]vlan 2 ！创建vlan2

[H3C-vlan2]port GigabitEthernet 0/3 ！将接口g0/3分配到vlan2

[H3C-vlan2]interface vlan 2 ！进入vlan接口配置模式

[H3C-Vlan-interface2]ip address 10.1.2.1 255.255.255.0

[H3C-Vlan-interface2]display interface vlan 2

参照vlan 2接口的配置命令配置vlan 3接口的IP地址10.1.3.1。

### 组网实验结果及分析

1. 在实验1的现场检查单上画出实验拓扑图，标明使用的设备（如H3C S3110等）及设置的接口及IP。
2. 在各台PC上使用ping命令检查网络连通情况，在现场检查单中按表6-1要求记录结果。

表6-1组网实验测试结果

|  |  |  |  |
| --- | --- | --- | --- |
|  |  | 所用命令 | 能否ping通 |
| 同一网段中 | PCA ping PCB |  |  |
| PCC ping PCD |  |  |
| 不同网段中 | PCB ping PCC |  |  |
| PCD ping PCA |  |  |

1. 用display ip routing-table查看路由器的路由表，分析不同网段互通的原因，体会网关的作用？
2. 在PCA上用tracert –d 10.1.3.14，查看PCA-PCD的路由连通路径。

## 互动讨论主题

1. 分析不同LAN中PC互通的原因及跨越的物理链路；
2. 路由表的形成及使用；

## 进阶自设计

1）采用Wireshark软件捕获计算机通信报表，分析网关的目的与作用；

# 实验二 VLAN的配置与协议分析

## 实验目的

了解VLAN的作用，掌握在一台交换机上划分VLAN的方法和跨交换机的VLAN的配置方法。掌握镜像端口的配置方法，了解VLAN数据帧的格式、VLAN标记添加和删除的过程。

## 实验内容

首先在一台交换机上划分VLAN，测试在同一VLAN和不同VLAN中设备的连通性。配置端口镜像，截获VLAN数据帧，分析VLAN数据帧的格式和VLAN标记添加与删除的过程。

## 实验原理

### 采用VLAN强化网络管理和网络安全

VLAN即虚拟局域网，通过将局域网划分为虚拟网络VLAN网段，可以强化网络管理和网络安全，控制不必要的数据广播，网络中工作组可以突破共享网络中的地理位置限制，而根据管理功能来划分子网。不同厂商的交换机对VLAN的支持能力不同，支持VLAN的数量也不同。

以太网交换机在数据链路层上基于端口进行数据转发，使得冲突域被缩小到交换机的每一个端口。但是交换机的所有端口都在同一个广播域，当网络内主机数量急剧增加时，大量的广播报文将引起网络性能恶化。为了将大的广播域隔离成多个较小的广播域，引入了VLAN技术。在VLAN技术中规定，凡是具有VLAN功能的交换机在转发数据报文时，都需要确认该报文属于某一个VLAN，并且该报文只能被转发到属于同一个VALN的端口或主机，不同VLAN间在链路层不能直接通信。VLAN的划分有很多种：按照[IP地址](http://www.qqread.com/z/tech/ip/index.html" \t "_blank)来划分，按照端口来划分、按照MAC地址划分或者按照协议来划分。其中基于端口划分的方法是最普遍使用的，也是目前所有交换机都支持的一种划分方法。

### 802.1q协议与三层交换

交换机可分为二层交换机、三层交换级和多层交换机。二层交换机按照接入设备的MAC地址进行数据帧的过滤和转发。802.1q协议定义了基于端口的VLAN模型。802.1q规范使第2层交换具有以优先级区分信息流的能力，完成动态多波过滤。802.1q标准主要用来解决如何将大型网络划分为多个小网络，如此广播和[组播](http://baike.baidu.com/view/492256.htm" \t "_blank)流量就不会占据更多带宽的问题。此外 802.1q 标准还提供更高的网络段间安全性。

三层[交换机](http://baike.baidu.com/view/1077.htm" \t "_blank)就是具有部分[路由器](http://baike.baidu.com/view/1360.htm" \t "_blank)功能的交换机，在同一个交换机划分的VLAN之间能够做到“一次[路由](http://baike.baidu.com/view/18655.htm" \t "_blank)，多次转发” 。对[路由](http://baike.baidu.com/view/18655.htm" \t "_blank)信息更新、[路由表](http://baike.baidu.com/view/149989.htm" \t "_blank)维护、路由计算、路由确定等功能都由[软件](http://baike.baidu.com/view/37.htm" \t "_blank)实现。[三层交换技术](http://baike.baidu.com/view/802.htm" \t "_blank)就是二层交换技术+三层转发技术。三层交换机都支持802.1q 标准。

#### 802.1q以太网帧格式

802.1Q标记过程修改原始的以太网帧。一个称为标记字段的4字节字段被插入原始的以太网帧中，并且原始帧的FCS(检验和)也根据这些变化而重新计算。插入4字节字段后以太网帧格式如下：

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 所占位 | 48 | 48 | 16 | 3 | 1 | 12 | 16 |  | 32 |
| 域名 | 目的地址 | 源地址 | 8100 | Priority | CFI | VLAN | 类型 | 数据 | FCS |

进行标记的目的是帮助其相连的交换机将帧置于源VLAN之中，插入得 4字节包含以下字段：

8100：16位恒定值域，指明这个帧包含802.1q标签。

Priority：3位，可定义8种用户优先级。支持802.1q规范的交换机可以使每一个输出端口具有使用多缓冲器排列能力，该能力可以选择信息传输的优先次序。该字段支持将数据包分组为各种流量种类。流量种类也可以定义为第二层服务质量（QoS）或服务类（CoS），并且在网络适配器和交换机上实现，而不需要任何预留设置。

CFI：规范格式指示，在以太网交换机中规范格式指示器总被设置为0。

VLAN：该字段为12位。支持4096个 VLAN的识别。

#### 以太网端口的三种链路类型

目前的主机都不支持带有tag域的帧，因此交换机要对连接主机的端口上的数据包执行封装和去封装操作。根据交换机处理VLAN数据帧的不同，可以将交换机端口分为三类：

（1）Access类型的端口

该类型的端口只能属于1个VLAN，一般用于连接计算机的端口。进入端口的数据，端口根据自己的缺省VLAN ID对帧进行封装，从Access端口转发出去的数据帧将它去掉封装，变成普通的以太网数据帧。

（2）Trunk类型的端口

该类型的端口可以属于多个VLAN，可以接收和发送多个不同VLAN的报文，一般用于连接两个交换机。进入Trunk端口的数据帧，对于已经携带tag域的数据，端口直接进行转发，而普通数据帧，端口用自己的缺省VLAN ID进行封装后再转发。

（3）Hybrid类型的端口

该类型的端口可以属于多个 VLAN，可以接收和发送多个不同VLAN的报文，可以用于交换机之间连接，也可以用于连接用户的计算机。Hybrid端口和Trunk端口的不同之处在于 Hybrid端口可以允许多个VLAN的报文发送时不打标签，而Trunk端口只允许缺省VLAN的报文发送时不打标签。

### 三层交换机实现VLAN之间的互通

三层交换机可以实现VLAN之间的互通，VLAN之间的互通是通过实现一个虚拟VLAN接口来实现的，即针对每个VLAN，交换机内部维护了一个与该VLAN对应的接口，该接口对外是不可见的，是一个虚拟的接口，但该接口有所有物理接口所具有的特性，比如有MAC地址，可配置IP地址、最大传输单元和传输的以太网帧类型等。当交换机接收到一个数据帧时，判断是不是发给自己的VLAN，判断的依据便是查看该MAC地址是不是针对接收数据帧所在VLAN的接口MAC地址，如果是，则进行三层处理，若不是，则进行二层处理。

### 端口镜像（port Mirroring)技术

以太网交换机在数据链路层上基于端口进行数据转发，使得冲突域被缩小到交换机的每一个端口。一般情况下，交换机每个端口只能得到与自己相关的数据包。

在网络数据包检测和安全监控中，就需要交换机把某一个端口接收或发送的数据帧完全相同的复制给另一个端口。其中被复制的端口称为镜像源端口，复制的端口称为镜像目的端口，镜像目的端口端口不能再传输数据。

端口镜像在不同的产品中通常有以下几种别名：

Port Mirroring；Monitoring Port ；Spanning Port ；SPAN port ；Link Mode port 。

## 实验环境与分组

交换机2台，每2-4人一组，共同配置2台交换机。

## 实验网拓扑

图2-1是在1个交换机上配置2个VLAN的组网图，图2-2是在2个交换机上配置2个VLAN的组网图。图中参数只作为参考，鼓励各小组灵活自定义IP等参数。

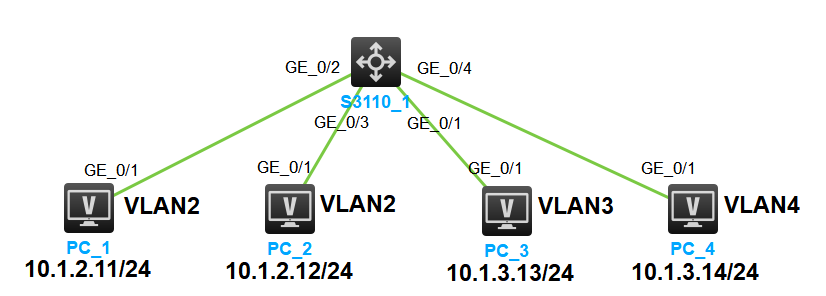


图2-1 同一交换设备上配置Vlan

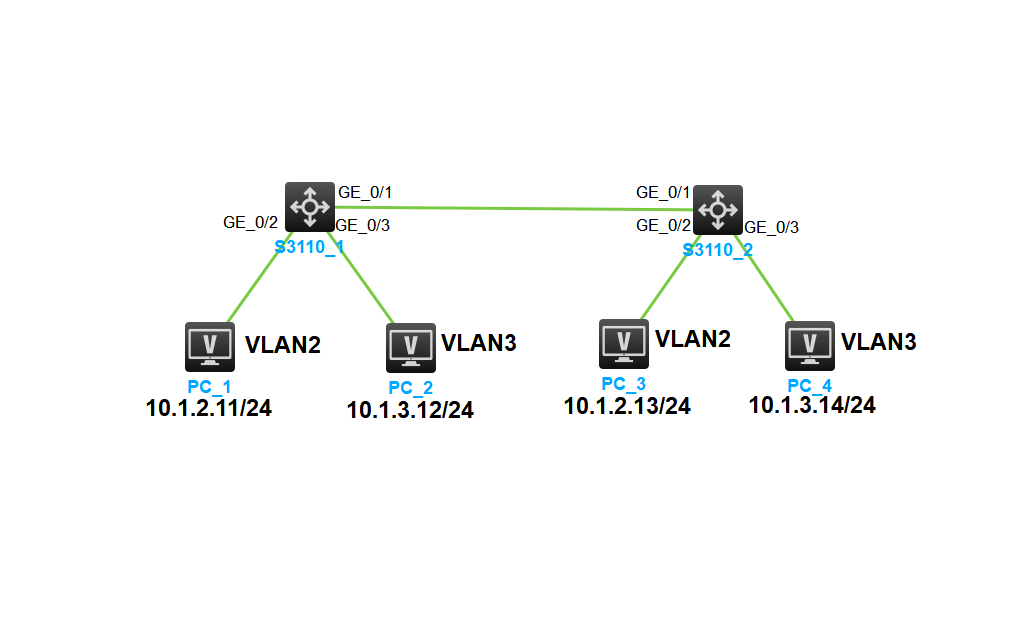


图2-2 利用trunk端口在2台设备上配置Vlan

## 实验过程及结果分析

#### VLAN的基本配置

首先**将交换机恢复为出厂设置。**具体方法参考2.1。然后按如下步骤进行实验。

步骤1：按图2-1所示连接好设备，为交换机划分VLAN，vlan 2的配置参考命令如下：

[H3C]vlan 2

[H3C-vlan2]port GigabitEthernet0/1 ！display interface命令查看设备端口

[H3C-vlan2]display vlan 2 ！查看vlan配置信息

同理配置vlan 3。

步骤2：设置各PC的IP地址。

步骤3：用ping命令验证同一VLAN的两台计算机能否通信，不同VLAN之间的计算机能否通信，记录结果。

#### Trunk端口配置

步骤4：按照图2-2连接好设备，配置各台计算机的IP地址。为交换机S1、S2各自划分VLAN2和VLAN3。配置命令同上。

步骤5：验证各PC机之间能否ping通。

步骤6：分别在两台交换机上配置Trunk端口，并且将trunk端口加入VLAN2和VLAN3中。参考配置命令如下：

[H3C]interface Ethernet 1/0/1 ！进入端口配置模式

[H3C-Ethernet1/0/1]port link-type trunk ！设置端口类型为trunk

[H3C-Ethernet1/0/1]port trunk permit vlan all ！允许所有VLAN通过

测试交换机S1、S2上相同VLAN和不同VLAN之间是否可以ping通，记录结果，分析原因。在PCA上用tracert -d 10.1.3.14，查看PCA-PCD的路由连通路径。

#### VLAN tag标记的分析

步骤7：在交换机上配置端口镜像，将E0/0/1端口镜像到端口E0/0/3，配置命令如下：

[H3C]mirroring-group 1 local ！创建本地镜像组

[H3C]mirroring-group 1 mirroring-port GigabitEthernet 0/3 both ！设置镜像源端口

[H3C]mirroring-group 1 monitor-port GigabitEthernet 0/4 ！设置目的端口

在4台PC上捕获报文，验证PCA ping PCC能否ping通。在PCB和PCD上截获含有802.1q标记的报文，对各PC上截获的报文进行比较分析，记录结果，并分析原因。

#### 网卡注册表的修改

如果在windows下无法捕获到含有802.1q标记的报文，就需要修改网卡的注册表项（在网络连接属性内可查看网卡类型，如Intel(R) 82579LM Gigabit Network Connection）。步骤如下：

（1）运行regedit程序。

（2）在这个项目（网卡接口对应的注册表配置）下进行修改（添加）：

HKEY\_LOCAL\_MACHINE\SYSTEM\ControlSet001\Control\Class{4D36E972-E325-11CE-BFC1-08002BE10318}\00nn

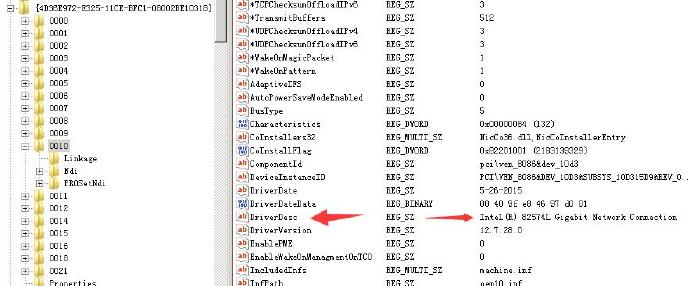
MonitorModeEnabled: 1

MonitorMode: 1

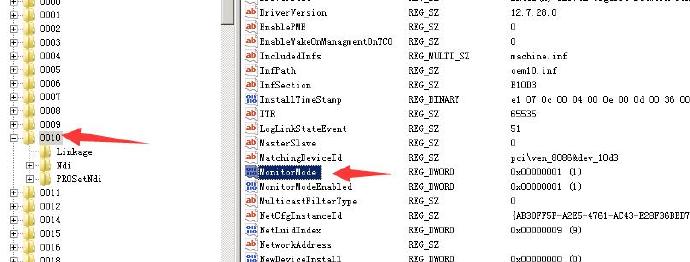
PriorityVLANTag: 0

SkDisableVlanStrip: 1

其中00XX指该项下有多个项，各向对应PC上不同的通讯端口，需要对应找到对应本地连接网卡的一项，此处为0010项对应本地连接网卡，具体为某项下的Driverdesc值为正确网卡型号的一项【注意：一般是0007】，如下图所示：



在00XX下修改或创建DWORD类型键值：MonitorMode或MonitorModeEnabled值为1，没把握就两个全加上，如下图：



（3）修改完毕后关闭regedit，把网卡exp禁用后重新启用。重启 wireshark 。

（4）打开wireshark捕获PCA ping PCC的测试报文；

（5）分析802.1q标记的报文，对各PC上截获的报文进行比较分析，记录结果，并分析原因。

表7-1 跨交换机VLAN实验（PCA ping PCC）

|  |  |  |
| --- | --- | --- |
| 转发过程及方向 | VLAN标记值  （只填写观察到的值） | 标记出现与否的原因 |
| PCA - S1 |  |  |
| S1 - S2 |  |  |
| S2 - PCC |  |  |

#### VLAN间通信

步骤8：在4台计算机上都运行Wireshark截获报文，执行PCC ping PCD，观察能否ping通，对各计算机截获的报文进行综合分析，说明原因。

步骤9：**在交换机S1上**配置VLAN2和VLAN3的接口IP地址，VLAN2的IP为10.1.2.1/24，VLAN3接口的IP为10.1.3.1/24。VLAN2的IP配置参考命令如下：

[H3C]interface vlan 2

[H3C]ip address 10.1.2.1 255.255.255.0

同理配置VLAN3的IP地址。

步骤10：配置PCA和PCC的网关为10.1.2.1，配置PCB和PCD的网关为10.1.3.1。同时，在PCB上用Wireshark监听捕获报文；执行PCC ping PCD；观察能否ping通，说明原因。（如果ping不通，检查S2上镜像有没有关闭。）

## 互动讨论主题

（1）交换设备与Vlan配置；

（2）交换设备镜像口；

（5）Vlan标志出现与否的原因；

（6）Vlan技术可以防止那些网路安全问题。

## 进阶自设计

不同VLAN之间通信时VLAN标记的携带情况，解释其原因？

# 实验三 ARP协议分析与欺骗防范

## 实验目的

分析ARP协议报文首部格式，分析ARP协议在同一网段内和不同网段间的解析过程。分析ARP欺骗的基础和防范手段。

## 实验内容

（1）采用三层交换机分别搭建图3-1和图3-2网络拓扑结构；

（2）通过在位于同一网段和不同网段的主机之间执行ping命令，截获报文，分析ARP协议报文结构，并分析ARP协议在同一网段和不同网段间的解析过程。

（3）分析ARP欺骗的手段，**在H3C S5130 三层交换机上**构建基本防范功能。

## ARP协议概述

ARP即地址解析协议，它工作在数据链路层，在本层和硬件接口联系，同时对上层提供服务。IP数据包在以太网传送中，以太网设备并不识别IP地址，而是以48位以太网地址传输数据包。因此，必须把IP目的地址转换成以太网目的地址。

在以太网中，一个主机要和另一个主机进行直接通信，必须要知道目标主机的MAC地址。但这个目标MAC地址是通过地址解析协议ARP获得的。ARP协议用于将网络中的IP地址解析为的硬件地址（MAC地址），以保证通信的顺利进行。反向地址转换协议RARP则用MAC地址在RARP 服务器请求相应的 IP 地址。

### ARP的报文格式

下表是以太网上ARP报文的格式：

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 所占字节 | 2 | 2 | 1 | 3 | 1 | 6 | 4 | 6 | 4 |
| 域名 | 硬件类型 | 协议类型 | 硬件地址长度 | 协议长度 | OP | 发送者硬件地址 | 发送者IP | 目标硬件地址 | 目标IP |
|  | ARP首部 | | | | |  | | | |
|  |  | | | | |  | | | |

硬件类型字段指明了发送方想知道的硬件接口类型，以太网的值为1。协议类型字段指明了发送方提供的高层协议类型，IP为0800（16进制）。硬件地址长度和协议长度指明了硬件地址和高层协议地址的长度，这样ARP报文就可以在任意硬件和任意协议的网络中使用。操作字段OP用来表示这个报文的目的，ARP请求为1，ARP响应为2，RARP请求为3，RARP响应为4。

### ARP的工作原理

首先，每台主机都会在自己的ARP缓冲区 (ARP Cache)中建立一个 ARP列表，以表示IP地址和MAC地址的对应关系。

当源主机需要将一个数据包要发送到目的主机时，会首先检查自己 ARP列表中是否存在该IP地址对应的MAC地址，如果有，就直接将数据包发送到这个MAC地址；如果没有，就向本地网段发起一个ARP请求的广播包，查询此目的主机对应的MAC地址。此ARP请求数据包里包括源主机的IP地址、硬件地址、以及目的主机的IP地址。

网络中所有的主机收到这个ARP请求后，会检查数据包中的目的IP是否和自己的IP地址一致。如果不相同就忽略此数据包；如果相同，该主机首先将发送端的MAC地址和IP地址添加到自己的ARP列表中，如果ARP表中已经存在该IP的信息，则将其覆盖，然后给源主机发送一个 ARP响应数据包，告诉对方自己是它需要查找的MAC地址。

源主机收到这个ARP响应数据包后，将得到的目的主机的IP地址和MAC地址添加到自己的ARP列表中，并利用此信息开始数据的传输。如果源主机一直没有收到ARP响应数据包，表示ARP查询失败。

ARP在同一网段和不同网段解析过程有所不同，以上步骤说明了目的地址与源地址在同一网段时的解析过程。当不在同一网段时，主机首先查询的是它的默认网关的硬件地址，数据包也是先送到默认网关。

## 实验环境与分组

**H3C S5130三层交换机1台**。每2名同学一组，共同使用一台交换机，注意交换机上已经保存的设置，必要时进行设备初始化。

## 实验网拓扑结构

图3-1和图3-2给出本实验相同和不同网段的组网图，用于观察ARP在同一网段和不同网段解析过程。图中的参数只作为参考，鼓励各小组灵活自定义IP等参数。

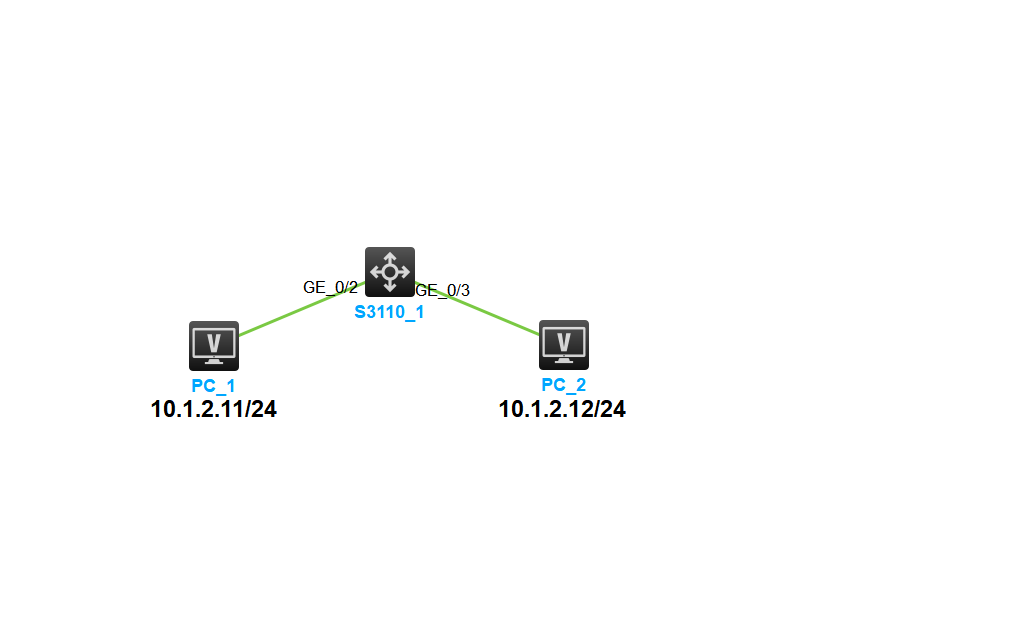


图3-1 ARP协议组网图（同一网段）

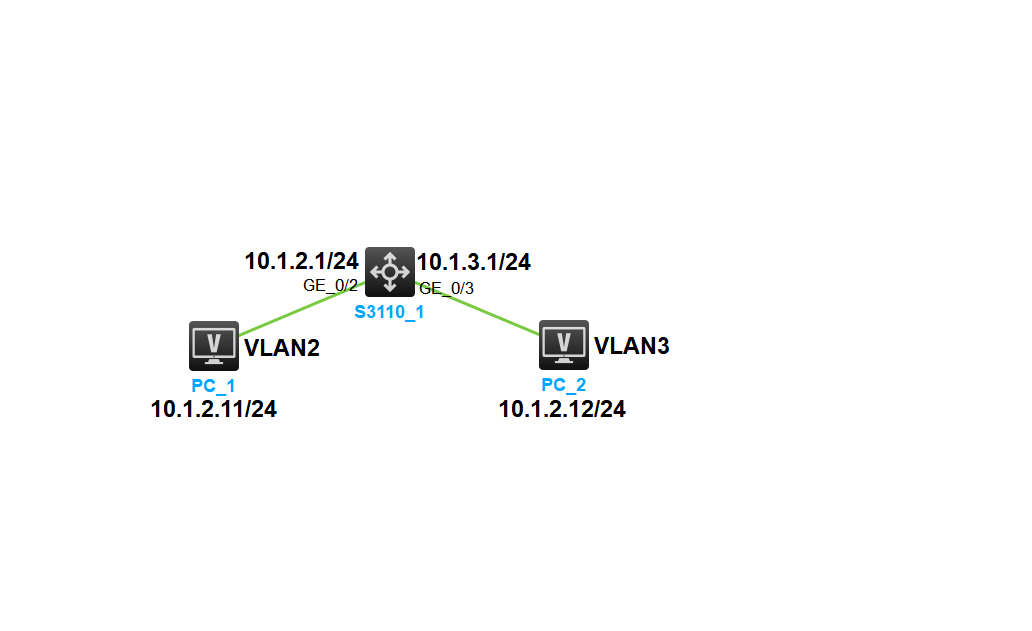


图3-2 ARP协议实验组网图（不同网段）

## ARP协议分析

### 同一网段的ARP协议分析

步骤1：按照图3-1所示连接设备，配置计算机的IP地址。

步骤2：在PCA、PCB的命令行窗口执行命令：

执行“arp –a”观察arp缓存；

执行“arp –d”命令清空arp缓存。需要以管理员身份运行cmd.exe。

步骤3：在PCA、PCB上运行wireshark截获报文；在PCA的命令行窗口执行“ping 10.1.2.12”。执行完之后，停止PCA、PCB上报文截获。分析截获的报文。

步骤4：在命令行窗口执行“arp –a”，记录结果。

### 不同网段的ARP协议分析

步骤5：按照图3-2所示连接设备，为交换机划分VLAN，为PC机配置IP地址和网关。

H3C S5130交换机配置

[H3C]display vlan ！查看设备Vlan现状

[H3C]vlan 2 ！创建Vlan 2

[H3C-vlan 2]port E0/0/2 ！将端口指派给Vlan 2

同理将 E0/0/3赋给vlan 3

[H3C]interface vlan 2 ！进入vlan 2

[H3C interface vlan 2 ]ip address 10.1.2.1 255.255.255.0 ！为vlan 2设定IP

同理为vlan 3设定IP10.1.2.1

[H3C]display ip routing-table ！查看路由表

PCA与PCB应能互通。

步骤6：首先在PCA、PCB上执行“arp –d”清空缓存，然后运行Wireshark捕获报文。在PCA上执行命令“ping 10.1.3.12”。

步骤7：执行“arp –a”命令，记录结果。

步骤8：比较PCA和PBB捕获的报文进行比较。在自己一端捕获的报文中选中第一条ARP请求报文和第一条应答报文，填写表3-1。

表3-1 ARP请求报文和应答报文的字段信息

|  |  |  |
| --- | --- | --- |
| 字段 | 请求报文的值 | 应答报文的值的值 |
| 以太网链路层Destination项 |  |  |
| 以太网链路层Source项 |  |  |
| ARP报文发送者硬件地址 |  |  |
| ARP报文发送者IP |  |  |
| ARP报文目标硬件地址 |  |  |
| ARP报文目标IP |  |  |

步骤9：比较ARP协议在不同网段和相同网段内解析过程的异同。

## ARP欺骗的原理

ARP协议是建立在信任局域网内所有节点的基础上，不会检查自己是否发送过ARP请求，也无法判定发给自己的ARP响应是否合法，只要ARP响应报文的目的MAC地址是自己，ARP协议都会接收并缓存到ARP列表。这种处理方式为ARP欺骗提供了可能。

ARP攻击者恶意发出大量ARP响应报文，使目标主机在ARP缓存保存大量的非真实的IP和MAC对应关系，使其发送的数据包无法到达真正的目的计算机，影响网络性能。

## ARP欺骗的安全危害

1）冒充主机的ARP欺骗

冒充主机的ARP欺骗由于冒充者不断的采取手段发出自己的ARP欺骗响应，用攻击对象的IP与自己的MAC地址配对，强迫与攻击对象正常通信的主机更新自己的ARP列表，将发给攻击对象的数据发给自己，窃取信息。

2）冒充网关的ARP欺骗

冒充网关的的ARP欺骗除了可以监听整个LAN的数据外，还可以用虚假的Web站点回答访问者的要求，进而在页面中植入带有病毒的网页，使整个LAN中毒，使其成为黑客手中的僵尸网络。

## ARP欺骗的防范

1）在本机利用arp –s命令制作一个批命令文件，静态设置网关的IP和MAC地址；

2）在接入的交换机或路由器上绑定各PC的IP和MAC地址，防范冒充主机的ARP欺骗；

3）利用一些特定的防范的工具和软件。

## 互动讨论主题

（1）PC、网关设备的MAC；

（2）链路层地址与ARP协议的地址区别；

（3）发送方与接收方arp与ICMP报文出现的次序成因；

## 进阶自设计

WinArpAttacker是一款ARP攻击软件。可以进行ARP机器列表扫描，还拥有基于ARP的各种攻击方法，如定时IP冲突、IP冲突洪水、禁止上网、禁止与其他机器通讯、监听与网关和其他机器的通讯数据、ARP代理等。此软件还可用于ARP攻击检测、主机状态检测、本地ARP表变化检测；检测到其他机器的ARP监听攻击后可进行防护，自动恢复正确的ARP表可发送手工定制ARP包等。WinArpAttacker的功能主要有：

1）Flood: 连续大量地发送“Ip Conflict”包，此功能有可能会导致对方DOWN机。

2）BanGateway: 发包欺骗网关，告诉网关错误的目标机MAC地址，导致目标机无法接收到网关发送的包。

3）Ip Conflict:发送IP相同、但Mac地址不一样的包至目标机，导致目标机IP冲突，频繁发送此包会导致机器断网。

4）Sniffgateway: 同时ARP欺骗网关和目标机，使你可以监听目标机的通信。

5）SniffHosts：欺骗多个主机，使你可以监听他们之间的通信。

6）SniffLan：欺骗局域网的所有机器，说是你才是网关，然后通过这个你可以监听整个网络。

利用WinArpAttacker软件监听目标机的通信。

# 实验四 TCP协议分析

## 实验目的

理解TCP报文首部格式和字段的作用，TCP连接的建立和释放过程，TCP数据传输中的编号与确认的过程。

## 实验内容

应用TCP应用程序传输文件，截取TCP报文，分析TCP报文首部信息、TCP连接的建立和释放过程、TCP数据的编号与确认机制。

## 实验原理

网络协议指的是计算机网络中互相通信的对等实体之间交换信息时所必须遵守的规则的集合。对等实体通常是指计算机网络体系结构中处于相同层次的信息单元。一般系统网络协议包括五个部分：通信环境，传输服务，词汇表，信息的编码格式，时序、规则和过程。1969年美国国防部建立最早的网络——阿帕计算机网络时，发布了一组计算机通信协议的军用标准，它包括了五个协议，习惯上以其中的TCP和IP两个协议作为这组协议的通称。

互联网的顶级域名解析服务由根服务器完成，根服务器对网络安全、运行稳定至关重要，被称为互联网的“中枢神经”。根服务器主要用来管理互联网的主目录，最早是IPV4，全球只有13台（这13台IPv4根域名服务器名字分别为“A”至“M”），1个为主根服务器在美国，由美国互联网机构Network Solutions运作。其余12个均为辅根服务器，其中9个在美国，2个在欧洲(位于英国和瑞典)，1个在亚洲(位于日本)。

在与现有[IPv4](https://baike.baidu.com/item/IPv4/422599" \t "https://baike.baidu.com/item/%E6%A0%B9%E5%9F%9F%E5%90%8D%E6%9C%8D%E5%8A%A1%E5%99%A8/_blank)根服务器体系架构充分兼容基础上，由我国下一代互联网工程中心领衔发起，联合WIDE机构（现国际互联网M根运营者）、互联网域名工程中心（ZDNS）等共同创立了“[雪人计划](https://baike.baidu.com/item/%E9%9B%AA%E4%BA%BA%E8%AE%A1%E5%88%92/17915851" \t "https://baike.baidu.com/item/%E6%A0%B9%E5%9F%9F%E5%90%8D%E6%9C%8D%E5%8A%A1%E5%99%A8/_blank)”，于2016年在全球16个国家完成25台[IPv6根服务器](https://baike.baidu.com/item/IPv6%E6%A0%B9%E6%9C%8D%E5%8A%A1%E5%99%A8/52239399" \t "https://baike.baidu.com/item/%E6%A0%B9%E5%9F%9F%E5%90%8D%E6%9C%8D%E5%8A%A1%E5%99%A8/_blank)架设，事实上形成了13台原有根加25台[IPv6](https://baike.baidu.com/item/IPv6" \t "https://baike.baidu.com/item/%E6%A0%B9%E5%9F%9F%E5%90%8D%E6%9C%8D%E5%8A%A1%E5%99%A8/_blank)根的新格局，为建立多边、民主、透明的国际互联网治理体系打下坚实基础。中国部署了其中的4台，由1台[主根服务器](https://baike.baidu.com/item/%E4%B8%BB%E6%A0%B9%E6%9C%8D%E5%8A%A1%E5%99%A8/9678400" \t "https://baike.baidu.com/item/%E6%A0%B9%E5%9F%9F%E5%90%8D%E6%9C%8D%E5%8A%A1%E5%99%A8/_blank)和3台辅根服务器组成，打破了中国过去没有根服务器的困境。

### TCP协议报文格式

TCP协议工作在网络层之上，是一个面向连接的、端到端的、可靠的传输层协议。TCP的报文格式如图4-1，详细地规范参阅RFC 793。

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 0 16 31 | | | | | | | | |
| 源端口Source port | | | | | | | | 目的端口Destination port |
| 顺序号Sequence number | | | | | | | | |
| 确认号Acknowledgement number | | | | | | | | |
| Data Offset | Resrvd | **U**  **R**  **G** | **A**  **C**  **K** | **P**  **S**  **H** | **R**  **S**  **T** | **S**  **Y**  **N** | **F**  **I**  **N** | 窗口大小Window |
| 校验和Checksum | | | | | | | | 紧急指针Urgent pointer |
| 选项和填充Option + Padding | | | | | | | | |
| 数据Data | | | | | | | | |

图4-1 The TCP header structure

1）源端口号，标识主机上发起传送的应用程序；目的端口标识主机上传送要到达的应用程序。源端和目的端的端口号，用于寻找发端和收端应用进程。这两个值加上I P包首部中的源端I P地址和目的端I P地址唯一确定一个T C P连接。

2）顺序号字段：占32比特。用来标识从TCP源端向TCP目标端发送的数据字节流，它表示在这个报文段中的第一个数据字节序号。

3）确认号字段：占32比特。只有ACK标志为1时，确认号字段才有效。它包含目标端所期望收到源端发送的下一个数据字节号。

4）Data Offset字段：占4比特。给出头部占32比特的数目，同时也指出数据的开始位置。没有任何选项字段的TCP头部长度为20字节；最多可有60字节的TCP头部。

5）Resrvd预留：由跟在数据偏移字段后的6位构成，预留位通常为0.

6）控制标志位（U、A、P、R、S、F）：占6比特。各比特的含义如下：

URG：紧急指针（urgent pointer）值有效；

ACK：确认号Acknowledgement number值有效；

PSH：接收方应该尽快将这个报文段交给应用层；

RST：重建连接；

SYN：发起一个连接；

FIN： 释放一个连接。

7）窗口大小字段：占16比特。此字段用来进行流量控制。单位为字节数，这个值是本机期望一次接收的字节数。

8）TCP校验和字段：占16比特。对整个TCP报文段，即TCP头部和TCP数据进行校验和计算，并由目标端进行验证。

9）紧急指针字段：占16比特。URG设置时有效，它是一个正偏移量，和序号字段中的值相加指向数据包中的第一个重要数据字节。

10）选项字段：占32比特。可能包括"窗口扩大因子"、"时间戳"等选项。

### TCP连接的建立与撤销

TCP连接的建立采用了三次握手方式，连接的撤销则是四次握手，TCP连接的建立和撤销的过程如图4-2所示：



图4-2 TCP 连接的建立的三次握手

## 实验环境与分组

1）路由器1台，交换机1台。

2）每2名同学一组，共同配置1台路由器。

3）使用TCP协议测试软件和报文捕获软件。

## 实验组网

图4-3是本实验的组网图，图中参数仅供参考，鼓励各小组灵活自定义IP等参数。

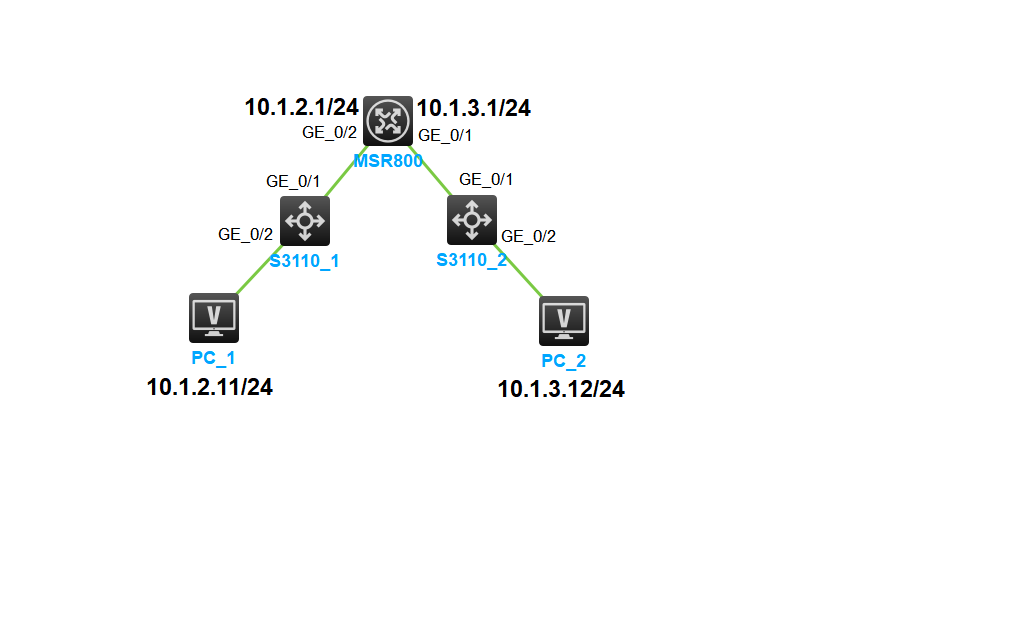


图4-3 TCP协议分析组网图

## 实验过程及结果分析

步骤1：按图4-3所示连接设备，为PC和路由器接口配置IP。路由器e1/0接口的配置命令如下：

[H3C]interface e1/0

[H3C interface e1/0]port link-mode route ！设置接口模式为路由

[H3C interface e1/0]ip address 10.1.2.1 255.255.255.0

[H3C interface e1/0]display interface e1/0

路由器e1/1接口的配置同上。

步骤2：在PCA和PCB上开始截获报文。

步骤3：在PCA和PCB上分别运行TCP协议测试软件，以客户机/服务器模式通信，发送和接收一个约800KB的文件。文件传输完成后，停止报文截获。

步骤4：观察截获的报文，分析TCP协议的建立过程的三个报文并填写表4-1。

表4-1 TCP连接建立过程的三个报文信息

|  |  |  |  |
| --- | --- | --- | --- |
| 字段名称 | 第1条报文的值及含义 | 第2条报文的值及含义 | 第3条报文的值及含义 |
| 报文序号NO. |  |  |  |
| Seq # |  |  |  |
| Ack # |  |  |  |
| ACK |  |  |  |
| SYN |  |  |  |

步骤5：分析TCP连接的释放过程，选择TCP连接撤销的四个报文并填写表4-2。

表4-2 TCP连接撤销的四个报文信息

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 字段名称 | 首条报文的值及含义 | 二条报文的值及含义 | 三条报文的值及含义 | 四条报文的值及含义 |
| 报文捕获序号NO. |  |  |  |  |
| Seq # |  |  |  |  |
| Ack # |  |  |  |  |
| ACK |  |  |  |  |
| FIN |  |  |  |  |

步骤6：TCPDebug软件，调整发送时间间隔等参数，“发送缓冲长度”不得小于2000，使得接收方的窗口有明显变化。

步骤7：分析TCP数据传送阶段的报文，填写现场检查单。

表4-3 记录TCP数据传送阶段的前12个报文

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 报文序号 | 报文种类 (数据/确认) | 序号字段Seq Number | 确认号Ack Number | 数据长度 | 确认到哪条报文（填序号） | 窗口大小 |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

步骤8、观察数据发送方和接收方的报文数据长度，推测原因。

步骤9、在交换机上设置端口镜像，用Wireshark捕获报文进行分析，确定双方TCP数据长度不同的原因所在。

步骤10、修改发送方的Realtek PCIe GBE网卡（如果是其他网卡，则作为接收方），网卡属性-> 配置->高级 ->“大量发送减负”为“关闭”。重新发送。

## TCP协议脆弱性分析

TCP协议是网络模型中的传输层协议，主要为两台主机上的应用程序提供端到端的通信。在提供大量信息服务的同时也存在着安全隐患。这种隐患源于TCP协议脆弱性。

1）不能提供可靠身份验证

TCP中的每个报文都含有一个标识本报文在整个通信流中位置的32位二进制序列号，通信双方通过序列号来确认数据的有效性。由于TCP涉及三次握手过程本身并不是为了身份验证，只是提供同步确认和可靠信息，虽然这也能够提供一定的身份验证的支持，但这种支持很薄弱。首先，由于TCP/IP不能对节点上的用户进行有效的身份验证，服务器无法鉴别登陆用户的身份有效性，攻击者可以冒充某个可信节点的IP地址，进行IP地址欺骗攻击。其次，由于某些系统的TCP序列号是可以预测的，攻击者可以构造一个TCP数据包，对网络中的某个可信节点进行攻击。

2）不能有效防止信息泄漏

在TCP中没有对数据进行加密，现在大部分协议都是以明文方式在网络上传输，如TELNET，FTP，SMTP，HTTP等。攻击者可通过某些监控软件或网络分析仪等进行窃听。

3）没有提供可靠的信息完整性验证手段

在TCP协议中对数据完整性的保护是比较弱的。虽然每个报文都经过校验和检查，保证数据的可靠传输，但事实上，绝大部分基于TCP的应用都假设TCP传输是可靠的，而这种数据完整性的检查是不够的。另外，校验算法中没有涉及加密和密码验证，很容易对报文内容进行修改，再重新计算校验和。最后，TCP的序列号也可以任意的修改，从而可在原数据流中添加和删除数据。

4）没有提供控制资源占有和分配手段

在传统的网络中，有两种控制资源占有和分配的手段：资源限额和计费。然而，在TCP/IP中却没有提供相应的机制，参加TCP通信的一方发现上次发送的数据报丢失，则主动将通信速率降至原来的一半。这样，也给恶意的网络破坏者提供了机会。如网络破坏者可以大量地发送IP数据报，造成网络阻塞，也可以向一台主机发送大量SYN包，从而占用该主机大量的资源。

## 针对TCP协议脆弱性的攻击

危害是比较大的主要有以下几种：

1）SYN泛洪

SYN泛洪攻击指通过发送大量的TCP SYN连接请求，填满目的主机的连接队列，使目的主机不能对正常用户的TCP连接请求产生响应。

2）TCP序号攻击

TCP序号攻击是基于建立TCP连接时所用的“三次握手”过程基础之上的，它是通过预测初始序号，构造TCP报文，以假冒信任主机。此种攻击就是“会话劫持”，主要有“中间人攻击”和“注射式攻击”

3）RST和FIN攻击

RST标志位用来复位一个连接，FIN标志位表示没有数据要发送了。冒充者产生一个带有RST位设置的TCP段，将其发往主机B，主机B收到该TCP段后就关闭与主机A的连接。利用FIN位的攻击与利用RST位的攻击很相似，攻击者预测到正确的序列号后，冒充A创建一个带FIN位的TCP分段，然后发送给主机B，制造主机A没有数据要发送了的假象。这样，由主机A随后发出的TCP段都会被主机B认为是网络错误而忽略。

## 常见TCP攻击的解决方法

1）对系统设定相应的内核参数，使得系统强制对超时的SYN请求连接数据包复位，同时通过缩短超时常数和加长等待队列使得系统能迅速处理无效的SYN请求数据包。

2）建议在该网段的路由器上调整配置，主要包括限制SYN半开数据包的流量和个数。

3）建议在路由器的前端做必要的TCP拦截，使得只有完成TCP三次握手的数据包才能进入该网段，这样可以有效的保护本网段内的服务器不受此类攻击。

4）加密TCP的会话过程；

5）在配置防火墙时，限制尽可能少量的外部许可连接的IP地址；

6）加强对网络系统的检测和审计，如果发现ACK包明显增加，网络系统就有可能受到劫持攻击。

## 常见的TCP攻击工具

常用有Juggernaut，它可以进行TCP会话劫持的网络Sniffer程序；TTY Watcher，而它是针对单一主机上的连接进行会话劫持。还有如Dsniff这样的工具包也可以实现会话劫持。Linux和一些Unix平台下的Hunt工具能将会话劫持发挥得淋漓尽致。

## 互动讨论主题

1）TCP握手和链接解除报文的理解；

2）传输层窗口值变化的成因；

3）传输层与与上下相邻层的关系；

4）报文的传输与确认对应关系。

## 进阶自设计

在上面实验结果的基础上，利用一个TCP攻击工具对正常地TCP通信进行会话劫持，观察报文序列。

# 实验五 RIP协议分析

## 实验目的

1. 理解路由协议的分类，掌握静态路由和RIP协议的配置方法；
2. 分析掌握RIP报文结构及各字段的含义；

3）分析两个路由设备之间RIP报文的交换及路由表的构建过程。

## 实验内容

1）在路由器、三层交换机上依次配置静态路由、缺省路由和RIP协议，然后分别用ping命令测试网络的连通性。

2）在路由器和三层交换机上配置RIP协议，在计算机上使用报文分析软件截获RIP报文，分析RIP报文各字段的含义。

3）采用镜像技术，捕获两个路由设备之间交换的RIP报文，分析两个设备中路由表的构建情况。

## 实验原理

路由器以两种基本方式构建非直连路由。一是可以使用预设值的静态路由，二是使用通过任何一种动态路由协议来动态计算路由。路由器使用动态路由协议发现路由，并通过这些路由来转发报文。

动态路由协议按照其所执行的算法不同，可以分为距离矢量路由协议、链路状态路由协议，以及混合型路由协议。

RIP协议的全称是路由信息协议（Routing Information Protocol），它是一种内部网关协议，用于一个自治系统内的路由信息的传递。RIP协议是基于距离矢量（Distance Vector）算法的，它使用“跳数”，即metric来衡量到达目标地址的路由距离。RIP协议用于使用同种技术的中型网络，对于更复杂的环境，一般不使用RIP协议。

RIP进程运行于路由器中，负责从网络中的其它路由器接收路由信息，从而对本地IP路由表进行动态维护，保证IP层发送报文时选择正确的路由，同时广播本路由器的路由信息，通知相邻路由器作相应的修改。RIP协议使用UDP通信，所接收的路由信息都封装在UDP的数据报中，RIP 在520号端口上接收来自远程路由器的路由修改信息，并对本地的路由表做相应的修改，同时通知其它路由器。通过这种方式，达到全局路由的有效。

## 实验环境与分组

1）H3C S5130三层交换机1台(简称S1)，H3C MSR800路由器1台(简称R1)，其它交换设备1台(简称S2)。

2）每2人一组，共同配置设备，完成实验。

## 实验组网

图5-1是本实验的组网图，图中的参数只作为参考，鼓励各小组灵活自定义IP等参数。

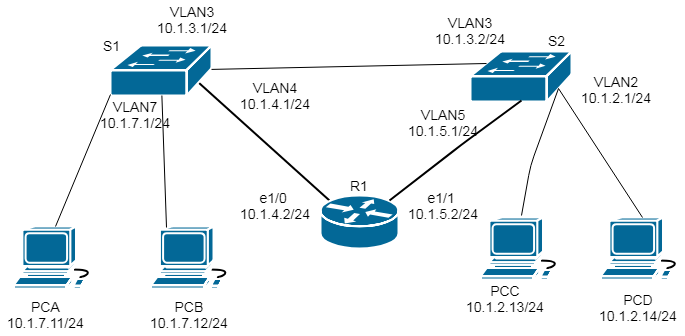


图5-1 RIP协议配置组网拓扑图

## . RIP启动与路由分析

步骤1：按照图5-1所示连接好设备，配置各PC的IP地址、子网掩码和网关。配置交换机和路由器各接口的IP地址。参考命令如下：

配置交换机S1：

[H3C]vlan 3

[H3C]port GigabitEthernet 1/0/1-2

[H3C]interface vlan 3

[H3C interface vlan 3]ip address 10.1.3.1 255.255.255.0

同理配置其他所有vlan。

配置路由器R1：

[H3C]interface e1/0

[H3C interface e1/0]port link-mode route ！开启端口路由功能

[H3C interface e1/0]ip address 10.1.4.2 255.255.255.0 ！配置端口IP

同理配置接口e1/1的地址。

此时，测试2台PC和S1、R1和S1之间是否可以互相通信。

[H3C]display ip routing-table ！查看路由表

在R1上ping各台PC，看能否ping通，通过路由表分析原因。

步骤2：在R1上配置10.1.7.0/24 的静态路由。命令如下：

[H3C]ip route-static 10.1.7.0 255.255.255.0 10.1.4.1

在R1上ping各PC看能否ping通，查看路由表，分析原因。

步骤3：删除步骤2配置的静态路由：

[H3C] undo ip route-static 10.1.7.0 255.255.255.0 10.1.4.1

步骤4：在S1和R1分别启动RIP协议。命令如下：

在交换机S1启动RIP协议命令：

[H3C] rip ！激活RIP进程

[H3C-rip-1]version 2 ！指定RIP版本2

[H3C-rip-1]network 10.1.3.0 ！指定与RIP相关的网络号

[H3C-rip-1]network 10.1.4.0

[H3C-rip-1]network 10.1.7.0

在路由器R1启动RIP协议：

[H3C] rip ！激活RIP进程

[H3C-rip-1]version 2 ！指定RIP版本2

[H3C-rip-1]network 10.1.4.0

[H3C-rip-1]network 10.1.5.0

测试连通性，查看S1和R1的路由表信息，将路由表信息填入检查单的表5-1中，分析原因，回答相关问题。

表5-1路由表信息

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 设备 | Destination/Mask | Protocol | Pref | Cost | Nexthop | Interface |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

Pref：路由表项优先级；Cost：路由表项代价。

步骤5：在S2上配置各个接口地址，并启动RIP协议。命令略。并测试连通性。在PCA上用tracert -d 10.1.2.14，查看PCA-PCD的路由连通路径。

## RIP报文结构及路由的更新

### RIP报文结构

RIP报文可分为请求信息的报文（Request报文）和应答信息报文（Response报文），格式相同，由固定的首部和可选的网络的IP地址和到该网络的跳数组成，RIP版本1（RFC 1058）的结构如图5-2所示，图5-3是RIP版本2（RFC 2453）的报文格式：

|  |  |  |
| --- | --- | --- |
| 0 8 16 32 | | |
| 命令Command | 版本Version | 必须为0 |
| 地址类型标志符Address family identifier | |  |
| IP地址 | | |
| 必须为0 | | |
| 必须为0 | | |
| metric | | |

图5-2 RIP（版本1）报文的格式

命令Command字段为1时表示RIP请求，为2时表示RIP应答。地址类型标志符在实际应用中总是为2，即地址类型为IP地址。“IP地址”字段表明目的网络地址，“Metric”字段表明了到达目的网络所需要的“跳数”。距离度量值用跳数来衡量，取值范围是1－16，其中16表示无限远（不可达路由）。路由器每经过30秒发送一次Response报文，这种报文用广播方式传播。

RIP版本1对RIP报文中“版本”字段的处理：

“版本”字段为0，忽略该报文；版本”字段为1表示是RIP版本1报文，检查报文中“必须为0”的字段，若不符合规定，忽略该报文。

“版本”字段>1时，不检查报文中“必须为0”的字段，仅处理RFC 1058中规定的有意义的字段。因此，运行RIP版本1的机器能够接收处理RIP版本2的报文，但会丢失其中的RIP版本2新规定的那些信息。

RIP版本1不能识别子网网络地址，因为在其传送的路由更新报文中不包含子网掩码，因此RIP路由信息要么是主机地址，用于点对点链路的路由；要么是A、B、C类网络地址，用于以太网等的路由；另外，还可以是0.0.0.0，即缺省路由信息。

|  |  |  |
| --- | --- | --- |
| 0 8 16 32 | | |
| 命令Command | 版本Version | 必须为0 |
| 地址类型标志符Address family identifier | | 路由标签Route Tag |
| IP地址 | | |
| 子网掩码Subnet mask | | |
| 下一跳Next Hop | | |
| metric | | |

图5-3 RIP（版本2）报文的格式

RIP版本2使用了版本1中“必须为0”的字段，增加了一些对于路由的有用信息，其主要新添的特性有①报文中包含子网掩码，可以进行子网路由；②支持明文/MD5验证；③报文中包含了下一跳IP，为路由的选优提供了更多的信息。路由标签Route Tag用于区分或者过滤路由。

### RIP路由表的更新

路由器最初启动时只包含了其直连网络的路由信息，并且其直连网络的metric值为1，然后它向周围的邻居路由器发出完整路由表的RIP请求。路由器根据接收到的RIP应答来更新其路由表。若接收到与已有表项的目的地址相同的路由信息，则分别对待①已有表项的来源端口与新表项的来源端口相同，那么无条件根据最新的路由信息更新其路由表；②已有表项与新表项来源于不同的端口，那么比较它们的metric值，将metric值较小的一个最为自己的路由表项；③新旧表项的metric值相等，普遍的处理方法是保留旧的表项。

路由器每30秒发送一次自己的路由表（以RIP应答的方式广播出去）。针对某一条路由信息，如果180秒以后都没有接收到新的关于它的路由信息，那么将其标记为失效，即metric值标记为16。在另外的120秒以后，如果仍然没有更新信息，该条失效信息被删除。

## RIP报文捕获及结果分析

步骤1：按照图5-1完成配置；

步骤2：将交换机S1上与R相连接端口镜像到E0/0/1端口；

步骤3：停止交换机S1上的RIP协议；

[H3C]undo rip

步骤4：在PCA上运行Ethereal截获报文，然后在S1上启动RIP协议。观察截获的请求报文和应答报文，选择一条RIP应答报文填写在表5-2中并理解其含义。

表5-2 RIP协议的应答报文

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 观察点： | | 字段 | 值 | 含义 |
| IP | | 目的地址 |  |  |
| UDP | | 端口号 |  |  |
| RIP | 头部 | 命令字段 |  |  |
| 版本号 |  |  |
| 路由信息 | 地址族标识 |  |  |
| 网络地址 |  |  |
| 跳数 |  |  |

## 互动讨论主题

1）缺省路由、直连路由、静态路由与动态路由；

2）RIP构建路由的条件与好处；

3）理解RIP构建的路由表及其使用；

4）RIP报文如何构建路由表；

5）RIP报文的结构；

6）RIP报文的启动与报文形成次序的关系；

7）RIPv1与RIPv2的比较。

## 进阶自设计

在上述实验结果的基础上，设法得到S1和R1之间交互的完整RIP报文，用此报文解释S1和R1中RIP类型路由表项是如何形成的。

# 实验六 OSPF路由协议分析

## 实验目的

详细分析OSPF的5种报文结构，掌握OSPF邻居建立及报文交换过程。

## 实验内容

在路由器上启动OSPF协议，同时在计算机上运行Ethereal截获报文，然后详细分析OSPF邻居建立和报文交换过程。

## 实验原理

### OSPF简介

OSPF(Open Shortest Path First开放式最短路径优先)是一个内部网关协议，用于在单一自治系统内决策路由。与RIP相对，OSPF是链路状态路由协议，而RIP是距离向量路由协议。链路是路由器接口的另一种说法，因此OSPF也称为接口状态路由协议。

OSPF是基于链路状态的路由协议。在OSPF路由协议的定义中，可以将一个路由域或（自治系统）划分为几个区域。在OSPF中，由按照一定的OSPF路由法则组合在一起的一组网络或路由器的集合称为区域（AREA）。每一个区域都有着该区域独立的网络拓扑数据库及网络拓扑图。对于每一个区域，其网络拓扑结构在区域外是不可见的。

在OSPF路由协议中存在一个骨干区域（Backbone），该区域包括属于这个区域的网络及相应的路由器，骨干区域必须是连续的，同时也要求其余区域必须与骨干区域直接相连。骨干区域一般为区域0，其主要工作是在其余区域间传递路由信息。

### OSPF邻接关系建立的4个阶段

1）邻居发现阶段 。

2）双向通信阶段：Hello报文都列出了对方的RouterID，则邻接关系建立完成。

3）数据库同步阶段。

4）完全邻接阶段: full adjacency。

邻居关系的建立和维持是靠Hello包完成的，在一般的网络类型中，Hello包是每经过1个Hello Interval以组播的方式发送给224.0.0.5一次。

当一个OSPF路由器初始化时，首先初始化路由器自身的协议数据库，然后等待低层次协议（数据链路层）提示端口是否处于工作状态。如果低层协议得知一个端口处于工作状态时，OSPF会通过其Hello协议数据包与其余的OSPF路由器建立交互关系。一个OSPF路由器向其相邻路由器发送Hello数据包，如果接收到某一路由器返回的Hello数据包，则在这两个OSPF路由器之间建立起OSPF邻居关系。

一个OSPF路由器会与其新发现的相邻路由器建立OSPF邻居关系，并且在一对OSPF路由器之间作链路状态数据库的同步。OSPF的数据库同步是通过OSPF数据库描述数据包（Database Description Packets）来进行的。OSPF路由器周期性地产生与其相联的所有链路的状态信息，有时这些信息也被称为链路状态广播LSA（Link State Advertisement）。当路由器相联接的链路状态发生改变时，路由器也会产生链路状态广播信息，所有这些广播数据是通过Flood的方式在某一个OSPF区域内进行的。

### OSPF协议报文结构

OSPF用IP报文直接封装协议报文，协议号为89（回忆TCP和UDP的协议号各是多少？）。表6-1是OSPF报文结构。

表6-1 OSPF报文结构

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| IP Header | OSPF Packet Header | Number of LSAs | LAS Header | LSA Data |

OSPF邻居建立及数据库同步过程中会用到OSPF的五种协议报文，这五种报文有相同的OSPF报文头（OSPF Packet Header），共24字节。图6-1是OSPF的头部结构。

0 7 15 31

|  |  |  |
| --- | --- | --- |
| Version | Type | Packet Length |
| Router ID | | |
| Area ID | | |
| Checksum | | AuType |
| Authentication | | |

图6-1 OSPF 头部结构

第一个字节为OSPF版本号，目前为2。第二个字节为OSPF报文类型，用来确定该报文是五种报文的哪一种，数值为1-5分别标识Hello报文、DD报文、LSR报文、LSU报文和LSAck报文。接下来两个字节为报文长度。跟着的四个字节为此报文源的Router ID，OSPF协议用此唯一标识一台路由器，RouterID一般是手工配置的路由器某个接口的IP地址。接下来的4个字节为此报文所在的OSPF区域信息。接下来为2字节的OSPF校验和，用来判断报文是否损坏。接下来AuType为2字节的验证类型字段和8字节的验证数据字段，这些字段允许路由器验证报文是否确实由报头中Router ID所标识的路由器所发，以及报文内容是否被修改过。

### OSPF报文类型

1）Hello报文：用于发现及维持邻居关系，选举DR，BDR。除去报文头后Hello报文还有20字节，其中前4个字节是发送接口的子网掩码，接下来两个字节是发送Hello报文的周期。路由器周期性地发送Hello报文以发现新的邻居和维持已有的邻居关系。接下来是选项字段，用于协商报文发送方式，接着是1字节的路由器优先级字段，用于选举DR和BDR。然后是4字节的Dead Interval字段，缺省为40秒，表示一台路由器如果在40秒内没有收到从邻居来的Hello报文，则认为此邻居的连接已经发生故障。剩下的是DR接口地址和BDR接口地址，都为4字节，对于第一个Hello报文，此时网段中没有选举出DR和BDR，两字段值都为0。

2）DD报文：用于描述整个数据库，该数据包仅在OSPF初始化时发送。其主要作用是描述本地LSDB的LSA摘要信息，并通过交换DD报文来确定哪些LSA需要交换。第一个DD报文用于确定路由器的主从关系，报文中的Flags标志位有三个字段，分别是I、M和MS。I为1表示是第一个DD报文；M为1表示这不是最后一个DD报文；MS为1表示发送者在DD报文交换过程中为Master，为0则是Slave。路由器一般根据Router ID来决定主从关系。主从关系确定后，路由器就通过DD报文交换LSA信息，当发现邻居的LSDB中有些LSA信息自己没有时，路由器会发送LSR报文向邻居要求这些LSA信息。

3）LSR报文：用于向相邻的OSPF路由器请求部分或全部的数据，这种数据包是在当路由器发现其数据已经过期时才发送的。LSR报文的主体部分为12字节，前4个字节为LSA的类型，接着为链路状态ID，用于在本地路由器上唯一标识一条LSA。最后4个字节为发送路由器的Router ID。路由器在收到邻居发送的LSR报文后，会将要求的LSA的具体内容用LSU报文发送给对方。

4）LSU报文：这是对LSA数据包的响应。LSU报文包含了所请求LSA信息的具体细节，当路由器收到LSU报文后，会以flooding的方式发送出去。

5）LSAck报文：是对LSA数据包的响应。路由器收到LSU报文后，都会以组播地址224.0.0.5发送LSAck报文表示自己已经收到相应的LSA信息。

### [LSA类型](http://blog.chinaunix.net/u/30306/showart_495072.html)及报文结构

有11种链路状态广播LSA（Link State Advertisement），本实验关注的主要有如下几种：

类型1：Router LSA：每个路由器都将产生Router LSA，这种LSA只在本区域内传播，描述了路由器所有的链路和接口，状态和开销。

类型2：Network LSA：在每个多路访问网络中，DR都会产生这种Network LSA，它只在产生这条Network LSA的区域泛洪描述了所有和它相连的路由器（包括DR本身）。

类型3：Network Summary LSA ：由ABR (Area Border Router区域边界路由器)路由器始发，用于通告该区域外部的目的地址.当其他的路由器收到来自ABR的Network Summary LSA以后，它不会运行SPF算法，它只简单的加上到达那个ABR的开销和Network Summary LSA中包含的开销，通过ABR，到达目标地址的路由和开销一起被加进路由表里，这种依赖中间路由器来确定到达目标地址的完全路由(full route)实际上是距离矢量路由协议的行为。

0 15 23 31

|  |  |  |
| --- | --- | --- |
| LS 年龄 | 选项 | LS类型 |
| 链路状态ID | | |
| 通告路由器 | | |
| LS序列号 | | |
| LS校验和 | 长度 | |

图6-2 LSA头部

图6-2给出了LSA头部的结构，LS 年龄（LS Age）表明该LSA产生了多少秒；选项字段请求附加特性；LS类型字段标识LSA数据包类型；链路链路状态ID（Link-States ID）根据LS类型字段的不同代表不同含义，表6-2给出了部分LSA类型及对应的链路链路状态ID；通告路由器字段表明生成该LSA的路由器ID。

表6-2 LSA类型及对应的链路链路状态ID

|  |  |
| --- | --- |
| LSA类型 | 链路链路状态ID |
| 1 | 生成LSA的路由器ID |
| 2 | 该网路中DR的路由器ID |
| 3 | 目标网路的IP地址 |

## 实验环境与分组

1）H3C S5130三层交换机2台，路由器1台。

2）每4位同学一组，共同配置交换机、路由器等设备。

## 实验组网

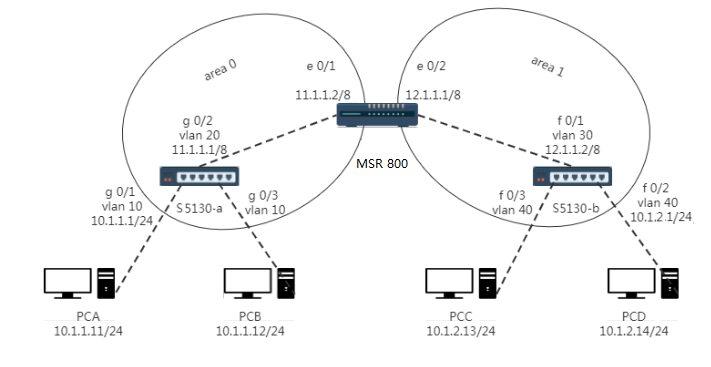


图6-3 OSPF邻居建立和报文交换过程组网图

图6-3是本实验的组网图，图中参数仅供参考，鼓励各小组灵活自定义IP等参数。

## 实验步骤

步骤1：按图连接好各实验设备，配置IP地址。

步骤2：将路由器的端口镜像到其中一台PC连接的端口上。

例：若路由器使用25、26口，PCA连接在1口，将25、26口的流量镜像到1端口的命令如下：

[H3C]mirroring-group 1 local ！创建本地镜像组

[H3C]mirroring-group 1 mirroring-port ethernet 0/0/25 both ！设置镜像源端口

[H3C]mirroring-group 1 mirroring-port ethernet 0/0/26 both ！设置镜像源端口

[H3C]mirroring-group 1 monitor-port ethernet 0/0/1 ！设置目的端口

步骤3：在每台PC上运行Ethereal软件，开始截获报文。

步骤4：配置两台路由器，启动OSPF协议，并在接口上指定相应的OSPF区域，S3110-a 配置接口g 0/1的参考命令如下：

<H3C>system-view

[H3C]vlan 10 ！配置vlan10

[H3C vlan 10] port g 0/1 g 0/3

[H3C vlan 10]q

[H3C]interface vlan 10

[H3C interface vlan 10]ip address 10.1.1.1 24

同理配置vlan 20

[H3C]ospf !开启ospf功能

[H3C ospf-1]area 0 ！划分区域0

[H3C-ospf-1-area-0.0.0.0]network 10.1.1.0 255.255.255.0 ！划分接口至区域0

[H3C-ospf-1-area-0.0.0.0]network 11.0.0.0 255.0.0.0

同理配置其他交换机、路由器。

步骤5：“display ip routing-table”查看路由表，如果出现了ospf路由，则说明两台路由器成功建立了邻居关系并交换了路由信息。在PC上停止报文截获。

## 结果及分析

1）分析所截获的报文，找出ospf的5种协议报文，描述ospf协议邻居建立和数据库同步的过程。

2）说明路由器中产生的OSPF路由项的含义？

3）选择封装在OSPF分组中的任一种链路状态广播Router-LSA，说明各字段的含义与作用。

## 互动讨论主题

1）OSPF报文与Lsa报文的关系；

2）如何选举DR和BDR；

3）LSR、LSU、Lsack等报文的关联关系；

4）R1、 R2路由表的形成与作用。

## 进阶自设计

在本实验的基础上，利用实验环境中的3台交换机构建一个支持OSPF协议的网络。在配置好OSPF路由后，从PCA能够ping通PCD。

# 防火墙与SSLVPN实验

## 实验方案及目的

通过不可靠的公共网建立一条加密通道，使企业内部员工能访问企业内部局域网的敏感资源。这对全球办公室的建立非常必要。本实验的目的是利用防火墙设备解决企业内部资源的安全访问问题。

## 实验内容

配置防火墙的安全策略，通过路由表信息分析外部 PC 如何通过VPN安全访问内网上的资源。

## 实验原理

随着计算机技术的飞速发展，信息网络已经成为社会发展的重要保证。有很多是敏感信息，甚至是国家机密，难免会吸引来自世界各地的各种人为攻击（例如信息泄露、信息窃取、数据篡改、数据删添、计算机病毒等）。网络安全性问题关系到未来网络应用的深入发展，它涉及安全策略、移动代码、指令保护、密码学、操作系统、软件工程和网络安全管理等内容。一般专用的内部网与公用的互联网的隔离主要使用“防火墙”技术。

SSL VPN 提供增强的远程安全接入功能。 IPSec VPN 通过在两站点间创建隧道提供直接（非代理方式）接入，实现对整个网络的透明访问。SSL VPN的特点主要有：① SSL VPN 提供安全、可代理连接，只有经认证的用户才能对资源进行访问；②SSL VPN 能对加密隧道进行细分，从而使得终端用户能够同时接入 Internet 和访问内部企业网资源，也就是说它具备可控功能；③SSL VPN 还能细化接入控制功能，易于将不同访问权限赋予不同用户，实现伸缩性访问。④SSL VPN 基本上不受接入位置限制，可以从众多 Internet 接入设备、任何远程位置访问网络资源。

SSL VPN 通信基于标准 TCP/UDP 协议传输，因而能遍历所有 NAT 设备、基于代理的防火墙和状态检测防火墙。这使得用户能够从任何地方接入，无论是处于其他公司网络中基于代理的防火墙之后，或是宽带连接中。

SSL VPN 不需要复杂的客户端支撑，广泛支持SSL的浏览器就可以使Internet上的远程机计算机如同在自己企业内部LAN 中一样。

## 实验环境与分组

1. 交换机3台，路由器1台，防火墙1台。
2. HSF（Http File Server）软件
3. 每4位同学一组，共同配置交换机、路由器、防火墙等设备。

## 实验网络拓扑

如图7[-1](#_bookmark0) 所示，SSL VPN 网关设备连接公网用户和企业私有网络。用户通过 SSL VPN 网关设备、采用Web 接入方式能够安全地访问位于私有网络内的Server A 和Server B。其中，Server A 和Server B 均为Web 服务器，使用HTTP 协议、端口号 80。具体需求如下：

1）SSL VPN 网关设备对用户进行本地认证和本地授权。

2）用户能访问 Server A 和 Server B。

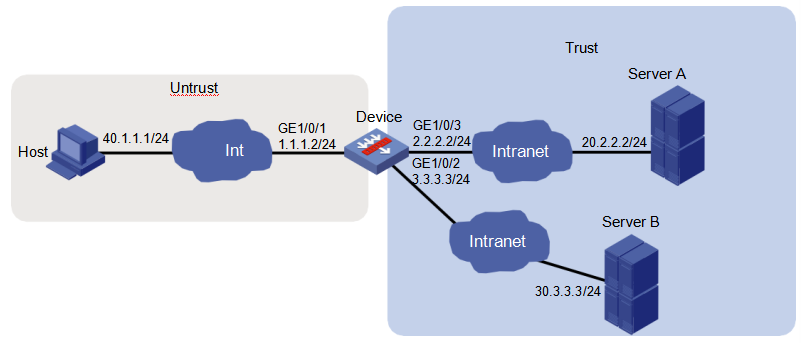
****

图7-1 Web 接入方式配置组网图（缺省证书）

## 实验过程及结果分析

登录防火墙，进入配置页面：

步骤 1：配置 PCA 的IP 为 192.168.0.2，并将其网线连接防火墙接g0/0，打开浏览器输入 [https://192.168.0.1](http://192.168.0.1/)，用户名和密码均为 admin。

步骤 2：配置防火墙的接口、用户等；

步骤 3：配置防火墙的安全策略:添加策略，untrust、local、trust域连通（双向），服务等选择 any；

全部配置完成后，参考路由表信息，分析外部 PC 如何通过VPN安全访问内网上的资源。分别在内网PC 和外网PC 同时访问内网 Web 资源服务器上的同一个资源并捕获报文，分析两种报文的差别。解释外部PC 通过VPN 访问内网的安全性。

详细配置步骤如下：

### 配置接口 IP 地址和安全域

步骤4：选择“网络 > 接口 > 接口”，进入接口配置页面。

步骤5：单击接口 GE1/0/1 右侧的<编辑>按钮，参数配置如下：

A.选择“基本配置”页签，添加到安全域：Untrust

B.选择“IPV4 地址”页签，配置 IP 地址/掩码长度：1.1.1.2/24

C.其他配置项使用缺省值

步骤6：单击<确定>按钮，完成接口 IP 地址和安全域的配置。

步骤7：单击接口 GE1/0/2 右侧的<编辑>按钮，参数配置如下：

A.选择“基本配置”页签，添加到安全域：Trust

B.选择“IPV4 地址”页签，配置 IP 地址/掩码长度：3.3.3.3/24

C.其他配置项使用缺省值

步骤8：单击<确定>按钮，完成接口 IP 地址和安全域的配置。

步骤9：单击接口 GE1/0/3 右侧的<编辑>按钮，参数配置如下：

A.选择“基本配置”页签，添加到安全域：Trust

B.选择“IPV4 地址”页签，配置 IP 地址/掩码长度：2.2.2.2/24

C.其他配置项使用缺省值

步骤10：单击<确定>按钮，完成接口 IP 地址和安全域的配置。

### 配置安全策略，参照步骤3。

### 配置SSL VPN 网关

步骤11：选择“网络> SSL VPN > 网关”，进入 SSL VPN 网关页面，单击<新建>按钮，创建 SSL VPN 网关，参数配置如下图所示。



图7-2 配置SSL VPN 网关

步骤12：单击<确定>按钮，完成配置。

### 配置SSL VPN 访问实例

步骤13：选择“网络 > SSL VPN > 访问实例”，进入 SSL VPN 访问实例页面，单击<新建>按钮，创建 SSL VPN 访问实例，参数配置如下图所示，未显示的部分，采用默认配置即可。



图7-3 配置SSL VPN 访问实例

步骤14：单击<下一步>，不配置 URI ACL，继续单击<下一步>，在跳转的页面选择“Web 业务”，单击<下一步>。配置所需的 Web 接入资源，配置结果如下图所示。



图7-4 Web 接入资源

步骤15：单击<下一步>，不配置快捷方式，继续单击<下一步>，在跳转的页面单击<新建>按钮，配置资源组，参数配置如下图所示。

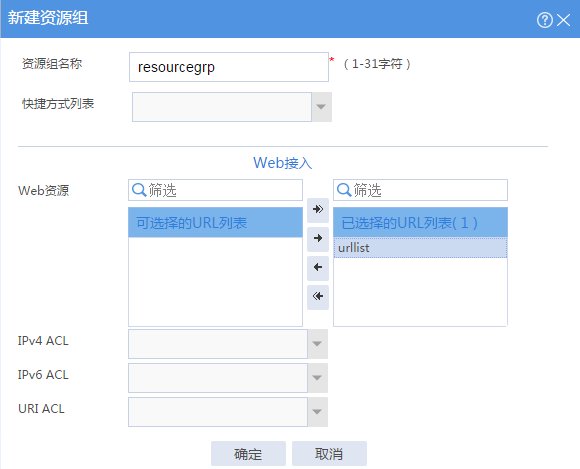


图7-5 配置资源组

步骤16：单击<确定>按钮，如下图所示。

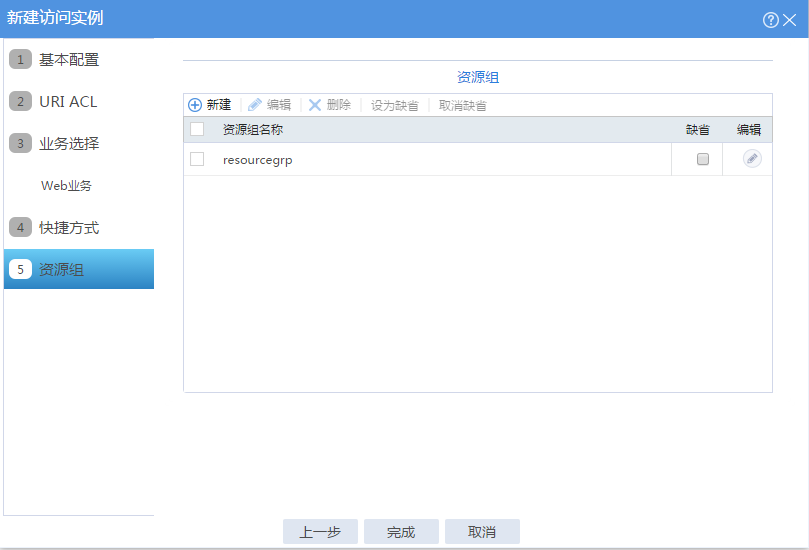


图7-6 资源组

步骤17：单击<完成>按钮，完成配置。

步骤18：在<使能>按钮的选择框上挑勾，使能配置的访问实例，如下图所示。

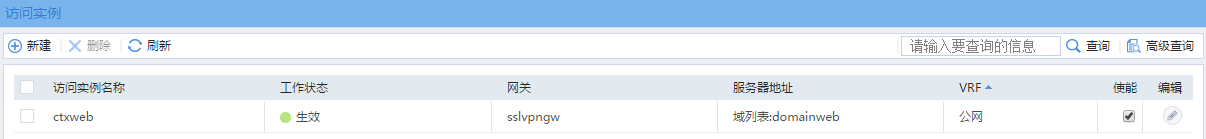


图7-7 使能访问实例

### 创建SSL VPN 用户

步骤19：选择“对象 > 用户 > 用户管理 > 本地用户”，进入用户界面，点击<新建>按钮，创建 SSL VPN用户，参数配置如下图所示。

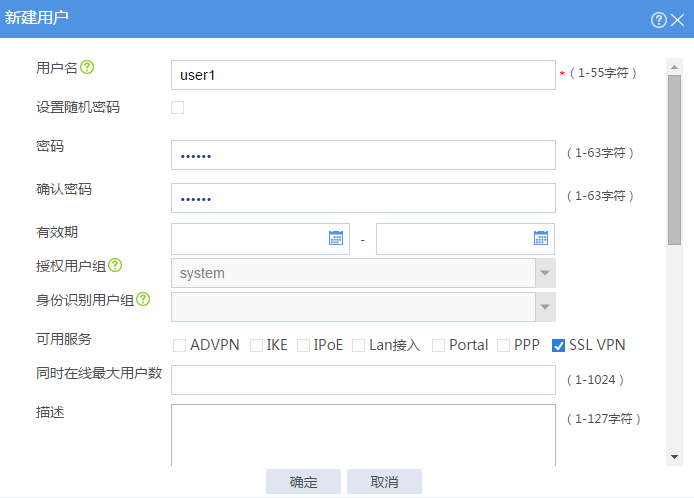


图7-8 创建SSL VPN 用户

步骤20：为该用户授权SSL VPN 策略组，参数配置如下图所示。



图7-9 授权属性

步骤21：单击<确定>按钮，完成配置。

### Host 的配置

步骤22：配置 IP 地址、网关，保证到 SSL VPN 网关的路由可达。

### 验证配置

步骤23：在浏览器地址栏输入 https://1.1.1.2，回车确认之后跳转到域列表选择界面，如下图所示。

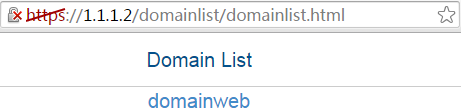


图7-10 域列表

步骤24：单击“domainweb”，跳转到SSL VPN登录界面，输入用户名密码（用户名user1， 密码123456），如下图所示。



图7-11 SSL VPN 登录界面

步骤25：单击<登录>按钮，成功登录后可看到如下图所示的资源列表。

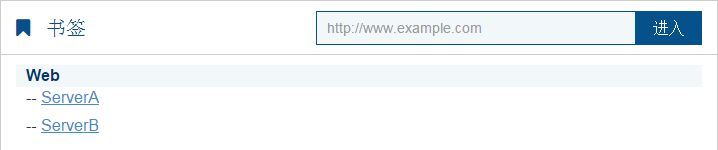


图7-12 Web 接入资源列表

步骤26：单击链接名为ServerA 的链接，可以成功访问 Web 服务器 ServerA 对应的资源，如下图所示。



图7-13 成功访问ServerA

步骤27：单击链接名为ServerB 的链接，可以成功访问 Web 服务器 ServerB 对应的资源，如下图所示。



图7-14 成功访问ServerB

# 实验八 Socket网络编程实验

## 实验目的

1) 掌握Sockets的相关基础知识，学习Sockets编程的基本函数和数据类型

2) 掌握UDP、TCP Client/Server模式的通信原理。

3) 掌握socket编程命令

## 实验内容

1) 实现一个简单的客户机/服务器程序，基于TCP和UDP协议分别实现。

2) 应用场景为一个验证用户登录的程序。

## 实验原理

下面简单介绍互联网的Client/Server模式的工作原理，以TCP服务器为例说明，UDP服务器略有不同。客户端也是如此。

1）服务器

服务器先创建一个套接字（Socket），并将该套接字和特定端口绑定，然后服务器开始在此套接字上监听，直到收到一个客户端的连接请求，然后服务器与客户端建立连接，连接成功后和该客户端进行通信（相互接收和发送数据），进行用户信息验证，并返回验证信息。最后，服务器和客户端断开连接，继续在端口上监听。

2）客户端

客户端创建一个套接字，里面包含了服务器的地址和端口号，客户端的端口号由系统自动分配，不需要指明。和服务器建立连接，如果连接成功则socket创建成功。然后客户端发送用户名和密码，等待验证。通信结束后主动断开连接，释放资源。

## 实验要求

1）比较TCP DUP两种协议的不同，在实验报告中写出自己的理解；

2）可用多种语言实现，建议 C/C++，JAVA或 Python。

## 实验环境和分组

1）每2位同学一组，共编写程序（一人客户端，服务）。

2）编程时请自备电脑编程调试。验收时电脑1台。

## 实验步骤

步骤 1：编写server端程序

步骤 2：编写client端程序

步骤 3：client端和 server端实现互联通信， 验证用户登录验证用户登录信息。例如，客户端发送用户名和密码，如若信息正确服务器端返回：送用户名和密码，如若信息正确服务器端返回：送用户名和密码，如若信息正确服务器端返回：“*信息正确*”；否则，服务器端返回：“*用户名或密码错误请再次输入*”。（提示信息不唯一，可自由改变）

## 结果分析

1) 如何服务器能实现循环监听？

2) 比较两种协议在代码层面的区别。

## 互动讨论主题

1) TCP协议和 HTTP协议的区别和联系；

## 进阶自设计

1. 在服务器端实现多线程的好处是什么？如何在服务端实现多线程？

计算机网络专题实验现场检查单1（共1页）

实验名称：组网与接入认证 时间： 年 月 日 早□ 午□ 晚□

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **班 级** |  | | **学号** |  | | **姓 名** |  | |
| **E-Mail** |  | | | | | **联系电话** |  | |
| 使用设备组别  G1 G2  G3 G4  G5 G6  G7 G8  实验组网图  （设备编号、端口号、IP地址、  认证角色等） |  | | | | | | | |
| 组 网  实 验  结 果 | 1.网络连通测试结果：   |  |  |  |  | | --- | --- | --- | --- | |  |  | 所用命令 | 能否ping通 | | 同一网段中 | PC□ ping PC□ |  |  | | PC□ ping PC□ |  |  | | 不同网段中 | PC□ ping PC□ |  |  | | PC□ ping PC□ |  |  |   2.用display ip routing-table查看R1的路由表，分析不同网段互通的原因？ | | | | | | | |
| 本人机位（图中标识） | |  | | | 同组人（只填一人） | | |  |
| 本人主要工作 | |  | | | | | | |
| 师生互动交流 | |  | | | | | | |
| 验收教师签名 | |  | | | 本实验成绩 | | |  |

计算机网络专题实验现场检查单2（共2页）

实验名称：VLAN的配置与协议分析 时间： 年 月 日 早□ 午□ 晚□

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 班 级 |  | | 学号 |  | | 姓 名 |  | |
| E-Mail |  | | | | | 联系电话 |  | |
| 使用设备组别  G1 G2  G3 G4  G5 G6  G7 G8  实验组网图  （标明设备编号、端口号、vlan号、IP地址） |  | | | | | | | |
| 实 验  结 果 | 1．验证同一VLAN的两台计算机能否通信，不同VLAN之间的计算机能否通信，记录结果并解释原因（步骤3）。  2．步骤6（完成Trunk端口配置）完成后，测试同一VLAN和不同VLAN中计算机的互通情况，记录测试结果并解释原因。  3. 填写步骤7中的表格并解释原因（设置镜像端口后）。   |  |  |  | | --- | --- | --- | | Ping发起： | Source: | Destination: | | 观查点 |  | |  |  |  |  |  | | --- | --- | --- | --- | | 转发过程（标明方向） | 报文类型（请求/响应） | VLAN标记（只填写观察到的） | 标记出现与否的原因 | | PCA — S1 |  |  |  | | S1 — S2 |  |  |  | | S2 — PCC |  |  |  |   4. 完成实验步骤10后，解释不同Vlan 间可以通信的原因？ | | | | | | | |
| 本人机位（图中标识） | |  | | | 同组人（只填一人） | | |  |
| 本人主要工作 | |  | | | | | | |
| 师生互动交流 | |  | | | | | | |
| 验收教师签名 | |  | | | 本实验成绩 | | |  |

计算机网络专题实验现场检查单3（共2页）

实验名称：ARP协议分析与欺骗防范 时间： 年 月 日 早□ 午□ 晚□

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 班 级 |  | | 学号 |  | | 姓 名 |  | |
| E-Mail |  | | | | | 联系电话 |  | |
| 使用设备组别  G1 G2  G3 G4  G5 G6  G7 G8  实验组网图  （标明设备编号、端口号、vlan号、IP地址） |  | | | | | | | |
| 实 验  结 果 | 1. 记录步骤4中“arp –a”的结果，写出其含义。 2. 观察同一网段的arp包格式，记录结果。  |  |  |  | | --- | --- | --- | | 字段 | 请求报文 | 应答报文 | | 以太网链路层Destination项 |  |  | | 以太网链路层Source项 |  |  | | ARP报文发送者硬件地址 |  |  | | ARP报文发送者IP |  |  | | ARP报文目标硬件地址 |  |  | | ARP报文目标IP |  |  |  1. 完成步骤7后，分析不同网段的ARP请求和响应报文，填写下表。  |  |  |  | | --- | --- | --- | | 字段 | 请求报文 | 应答报文 | | 以太网链路层Destination项 |  |  | | 以太网链路层Source项 |  |  | | ARP报文发送者硬件地址 |  |  | | ARP报文发送者IP |  |  | | ARP报文目标硬件地址 |  |  | | ARP报文目标IP |  |  |  1. 完成3.10节步骤4后，测试结果及原因是： | | | | | | | |
| 本人机位（图中标识） | |  | | | 同组人（只填一人） | | |  |
| 本人主要工作 | |  | | | | | | |
| 师生互动交流 | |  | | | | | | |
| 验收教师签名 | |  | | | 本实验成绩 | | |  |

计算机网络专题实验现场检查单4（共2页）

实验名称：TCP协议分析 时间： 年 月 日 早□ 午□ 晚□

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 班 级 |  | | 学号 |  | | 姓 名 |  | |
| E-Mail |  | | | | | 联系电话 |  | |
| 使用设备组别  G1 G2  G3 G4  G5 G6  G7 G8  实验组网图 |  | | | | | | | |
| 实 验  结 果 | 1. 分析截获的报文，记录TCP连接建立过程的三个报文和连接撤销过程的四个报文。   （1）TCP连接建立报文信息：  报文捕获计算机：   |  |  |  |  | | --- | --- | --- | --- | | 字段名称 | 第1条报文值及含义 | 第二条报文值及含义 | 第三条报文值及含义 | | 报文发出计算机 |  |  |  | | 捕获的报文序号 |  |  |  | | Sequence Number |  |  |  | | Acknowledgement Number |  |  |  | | ACK标志 |  |  |  | | SYN标志 |  |  |  |   （2）TCP连接撤销报文信息：  报文捕获计算机：   |  |  |  |  |  | | --- | --- | --- | --- | --- | | 字段名称 | 第一条报文值及含义 | 第二条报文值及含义 | 第三条报文值及含义 | 第四条报文值及含义 | | 报文发出计算机 |  |  |  |  | | 捕获的报文序号 |  |  |  |  | | Sequence Number |  |  |  |  | | Acknowledgement Number |  |  |  |  | | ACK标志 |  |  |  |  | | FIN标志 |  |  |  |  |  1. 记录TCP数据传送阶段的前12个报文。  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | | 报文序号 | 报文种类 (数据/确认) | 序号字段Seq Number | 确认号Ack Number | 数据长度 | 确认到哪条报文（填序号） | 窗口大小 | |  |  |  |  |  |  |  | |  |  |  |  |  |  |  | |  |  |  |  |  |  |  | |  |  |  |  |  |  |  | |  |  |  |  |  |  |  | |  |  |  |  |  |  |  | |  |  |  |  |  |  |  | |  |  |  |  |  |  |  | |  |  |  |  |  |  |  | |  |  |  |  |  |  |  | |  |  |  |  |  |  |  | |  |  |  |  |  |  |  |  1. 如何确定那条捕获的报文已被确认？窗口值大小何时、何因由谁调整？ | | | | | | | |
| 本人机位（图中标识） | |  | | | 同组人（只填一人） | | |  |
| 本人主要工作 | |  | | | | | | |
| 师生互动交流 | |  | | | | | | |
| 验收教师签名 | |  | | | 本实验成绩 | | |  |

计算机网络专题实验现场检查单5（共2页）

实验名称： RIP协议分析 时间： 年 月 日 早□ 午□ 晚

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 班 级 |  | | 学号 |  | | 姓 名 |  | |
| E-Mail |  | | | | | 联系电话 |  | |
| 使用设备组别  G1 G2  G3 G4  G5 G6  G7 G8  实验组网图  （标明设备编号、端口号、vlan号、IP地址） |  | | | | | | | |
| RIP协议配置与启动实验结果 | * 1. 步骤1之后在R1上ping各台PC，看能否ping通，分析路由表并写出原因。   2. 步骤2之后在R1上ping各台PC，看能否ping通，分析路由表并写出原因。   3. 步骤4之后。   4. 测试连通性（在R1上ping各台PC，看能否ping通），记录连通性结果，写出原因。   5. 查看路由填写下表。  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | | 设备 | Destination/Mask | Protocol | Pref | Cost | Nexthop | Interface | |  |  |  |  |  |  |  | |  |  |  |  |  |  |  | |  |  |  |  |  |  |  | |  |  |  |  |  |  |  | |  |  |  |  |  |  |  | |  |  |  |  |  |  |  | | | | | | | | |
| RIP协议分析结果 | * 1. 完成7.8节步骤4之后，分析所截获的报文，理解所截获的请求报文和应答报文的含义，将应答报文之一的各字段值填入下表：  |  |  |  |  |  | | --- | --- | --- | --- | --- | | 观察点： | | 字段 | 值 | 含义 | | IP | | 目的地址 |  |  | | UDP | | 端口号 |  |  | | RIP | 头部 | 命令字段 |  |  | | 版本号 |  |  | | 路由信息 | 地址族标识 |  |  | | 网络地址 |  |  | | 跳数 |  |  |  * 1. 进阶自设计实验结果写在背面（选），要求祥见实验指导书。 | | | | | | | |
| 本人机位（图中标识） | |  | | | 同组人（只填一人） | | |  |
| 本人主要工作 | |  | | | | | | |
| 师生互动交流 | |  | | | | | | |
| 验收教师签名 | |  | | | 本实验成绩 | | |  |

计算机网络专题实验现场检查单6（共2页）

实验名称OSPF路由协议分析 时间： 年 月 日 早□ 午□ 晚□

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 班 级 |  | | 学号 |  | | 姓 名 |  | |
| E-Mail |  | | | | | 联系电话 |  | |
| 使用设备组别  G1 G2  G3 G4  G5 G6  G7 G8  实验组网图  （标明设备编号、端口号、vlan号、IP地址） |  | | | | | | | |
| 实 验  结 果 | * + 1. 针对自己截获的报文，写出其包含的ospf报文的的含义（每类挑选一条）；结合实验获得的报文，简要描述ospf协议邻居建立和数据库同步的过程。 | | | | | | | |
|  | * + 1. 说明路由器R1、R2中产生的OSPF路由表项的含义？     2. 选择封装在OSPF分组中的任一种链路状态广播Router-LSA，说明各字段的涵义与作用。     3. 进阶自设计实验（选）结果写在背面，要求详见实验指导书8.9节。 | | | | | | | |
| 本人机位（图中标识） | |  | | | 同组人（只填一人） | | |  | |
| 本人主要工作 | |  | | | | | | |
| 师生互动交流 | |  | | | | | | |
| 验收教师签名 | |  | | | 本实验成绩 | | |  |

计算机网络专题实验现场检查单7（共1页）

实验名称：防火墙与SSLVPN实验 时间： 年 月 日 早□ 午□ 晚□

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 班 级 |  | | 学号 |  | | 姓 名 |  | |
| E-Mail |  | | | | | 联系电话 |  | |
| 使用设备组别  G1 G2  G3 G4  G5 G6  G7 G8  实验组网图  （标明设备编号、端口号、IP地址等） |  | | | | | | | |
| 实 验  结 果 | 1. 创建的SSL VPN用户名是： 2. 分析完成捕获的报文，分析两台PC上报文的差别。 | | | | | | | |
| 本人机位（图中标识） | |  | | | 同组人（只填一人） | | |  |
| 本人主要工作 | |  | | | | | | |
| 师生互动交流 | |  | | | | | | |
| 验收教师签名 | |  | | | 本实验成绩 | | |  |