



计算机网络实验 指导书

计算机科学与技术学院

2023 年 9 月

目 录

1 实验一 组网与接入认证	1
1.1 实验目的	1
1.2 实验内容	1
1.3 组网实验	1
1.4 802.1x 接入安全认证	2
1.5 互动讨论主题	8
1.6 进阶自设计	8
2 实验二 VLAN 的配置与协议分析	9
2.1 实验目的	9
2.2 实验内容	9
2.3 实验原理	9
2.4 VLAN 的组网实验	12
2.5 互动讨论主题	15
3 实验三 ARP 协议分析与欺骗防范	16
3.1 实验目的	16
3.2 实验内容	16
3.3 ARP 协议概述	16
3.4 实验环境与分组	17
3.5 实验网拓扑结构	17
3.6 ARP 协议分析	18
3.7 ARP 欺骗的原理	19
3.8 ARP 欺骗的安全危害	19
3.9 ARP 欺骗的防范	20
3.10 MAC 与 IP 绑定实验	20
3.11 互动讨论主题	21
3.12 进阶自设计	21
4 实验四 TCP 协议分析	22
4.1 实验目的	22
4.2 实验内容	22
4.3 实验原理	22
4.4 实验环境与分组	24
4.5 实验组网	24
4.6 实验过程及结果分析	24

4.7 TCP 协议脆弱性分析.....	26
4.8 针对 TCP 协议脆弱性的攻击.....	26
4.9 常见 TCP 攻击的解决方法.....	27
4.10 常见的 TCP 攻击工具.....	27
4.11 互动讨论主题.....	27
4.12 进阶自设计.....	28
5 实验五 应用层协议分析.....	29
5.1 实验目的.....	29
5.2 实验内容.....	29
5.3 HTTP 协议概述.....	29
5.4 FTP 协议概述.....	35
5.5 实验环境与分组.....	39
5.6 实验网拓扑结构.....	39
5.7 HTTP 协议分析.....	39
5.8 FTP 协议分析.....	40
5.9 互动讨论主题.....	41
5.10 进阶自设计.....	41
6 实验六 RIP 协议分析.....	42
6.1 实验目的.....	42
6.2 实验内容.....	42
6.3 实验原理.....	42
6.4 实验环境与分组.....	43
6.5 实验组网.....	43
6.6 RIP 启动与路由分析.....	43
6.7 RIP 报文结构及路由的更新.....	45
6.8 RIP 报文捕获及结果分析.....	47
6.9 互动讨论主题.....	48
6.10 进阶自设计.....	48
7 实验七 OSPF 路由协议分析.....	49
7.1 实验目的.....	49
7.2 实验内容.....	49
7.3 实验原理.....	49
7.4 实验环境与分组.....	52
7.5 实验组网.....	52
7.6 实验步骤.....	53
7.7 结果及分析.....	53

7.8 互动讨论主题	54
7.9 进阶自设计	54
8 实验八 防火墙与 SSLVPN 实验	55
8.1 实验方案及目的	55
8.2 SSL VPN 基础	55
8.3 实验规划及拓扑结构	56
8.4 实验主要步骤	57
8.5 进阶自设计	61
8.6 CISCO ASA5505 防火墙其它参考命令	61
9 选做实验	63
1 选做实验一：IPv6 与路由	64
2 选做实验二：QoS	70
3 选做实验三：WLAN 配置	79
4 选做实验四：校园园区网搭建	88

1 实验一 组网与接入认证

1.1 实验目的

①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；②网络接入安全方案设计与实现。

1.2 实验内容

- (1) 使用路由器和交换机进行组网，实现各 PC 间的互联互通；
- (2) 802.1x 认证服务器的构建；
- (3) 设计实现接入终端的认证；
- (4) 讨论接入认证的安全问题。

1.3 组网实验

1.3.1 实验环境与分组

路由器 1 台（DCR2626-1），交换机 2 台（DCR5650）；
每组 2-4 名同学，每人一台 PC，协同进行实验。

1.3.2 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。

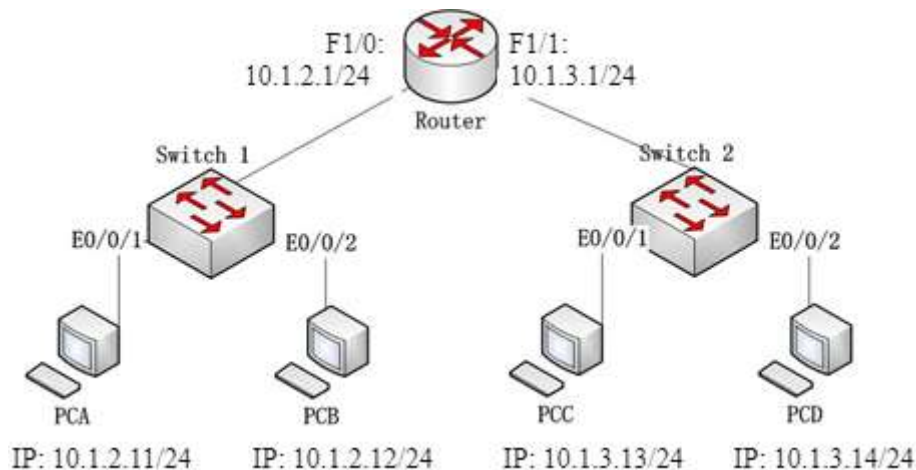


图 1-1 组网实验示意图

1.3.3 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 [2.4.3 实验过程及结果分析](#)

将交换机恢复为出厂设置，参考命令如下：

```
switch> enable !进入特权用户模式
switch# set default !启动初始化
Are you sure? [Y/N] = y ! 确认初始化，显示初始化信息
switch# write ! 写入初始化信息到启动文件
switch# reload ! 重新启动交换机
```

步骤 3: 配置路由器 Router 的接口 IP 地址, f0/0 接口的配置命令如下:

```
Router#config
Router_config#interface f0/0
Router_config_f0/0#ip address 10.1.2.1 255.255.255.0
Router_config_f0/0#no shutdown
Router#show interface f0/0
```

参照 f0/0 接口的配置命令配置 f0/3 接口的 IP 地址 10.1.3.1。

1.3.4 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 1#DCR2626-1) 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		

- 3) 用 show ip route 查看 R1 的路由表, 分析不同网段互通的原因, 体会网关的作用?

1.4 802.1x 接入安全认证

在组网实验基础上, 完成图 1-1 中部分 PC 的接入认证。主要工作和步骤有:

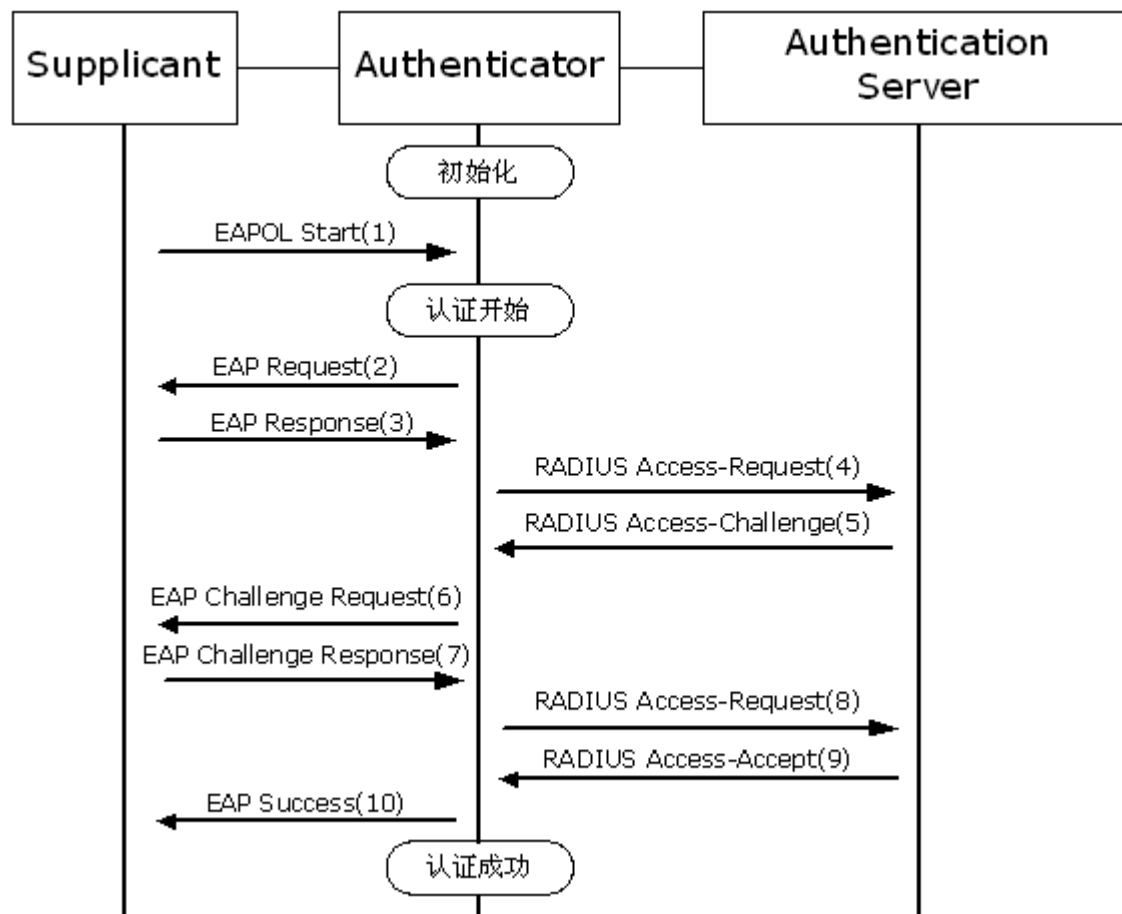
- ①理解并设计 802.1x 认证机制及方案;
- ②构建 802.1x 认证服务器(任选一台 PC);
- ③在 PC 的接入交换上配置认证参数;
- ④测试接入 PC 的认证效果。

1.4.1 802.1x 接入安全认证概述

802.1x 协议 (RFC 3580) 是基于端口的访问控制和认证协议。该协议的认证体系结构中采用了“可控端口”和“不可控端口”的逻辑功能, 从而实现认证与业务的分离, 保证了网络传输的效率。它可以限制未经授权的用户或设备通过接入端口(access port)访问 LAN/WLAN。在获得交换机或 LAN 提供的各种服务之前, 802.1x 对连接到交换机端口上的用户或设备进行认证。在认证通过之前, 802.1x 只允许 EAPoL (基于局域网的扩展认证协议) 数据通过设备连接的交换机端口访问认证服务器。认证通过以后, 正常的数据可以顺利地通过以太网端口。

1.4.2 802.1x 接入安全认证方案

一个基于 802.1x 的认证系统主要包括三个重要部分：认证客户端、认证者和认证服务器。



EAPoL 协议是无 IP 层的通信（有什么好处？），而 Radius 协议则是基于 UDP/IP 的（有什么好处？）。请使用 Wireshark 抓取认证过程交互的协议数据分析其大概过程。

认证客户端是最终受控用户所扮演的角色，一般是个人计算机。它发起 802.1x 的协议认证过程。认证客户端必须运行符合 802.1x 客户端标准的软件，目前最典型的的就是 Windows 操作系统自带的 802.1x 客户端支持。另外，一些网络设备制造商也开发了自己的 802.1x 客户端软件。

认证者一般为交换机等接入设备。该设备的职责是根据认证客户端当前的认证状态控制其与网络的连接状态。扮演认证者角色的设备有两种类型的端口：受控端口（controlled Port）和非受控端口（uncontrolled Port）。其中，连接在受控端口的用户只有通过认证才能访问网络资源；而连接在非受控端口的用户无须经过认证便可以直接访问网络资源。把用户连接在受控端口上，便可以实现对用户的控制；非受控端口主要是用来连接认证服务器，以便保证服务器与交换机的正常通讯。

认证服务器通常称为 RADIUS 服务器。认证服务器在认证过程中与认证者配合，为用户提供认证服务。认证服务器保存了用户名及密码，以及相应的授权信息，一台认

证服务器可以对多台认证者提供认证服务，这样就可以实现对用户的集中管理。认证服务器还负责管理从认证者发来的审计数据。

1.4.3 构建 802.1x 认证服务器

1) 在 (PCB) 安装认证服务器软件

WinRadius14.zip 解压，有如下文件：

WinRadius.exe 认证管理主程序

WinRadius.mdb 认证数据库文件（可以不使用该数据库文件）

RadiusTest.exe 用于认证服务器测试

WinRadius.config 保存软件配置信息（配置生成）

2) 配置访问认证数据库连接

(1) 在认证服务器 (PCB) 直接打开 WinRadius.exe，进入图 1-2 的配置界面，在菜单栏中选择 设置->数据库。

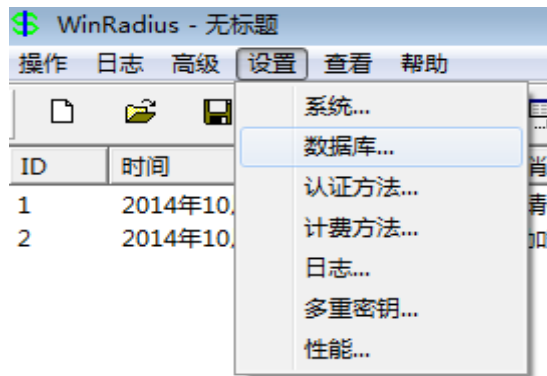


图 1-2 设置认证服务器数据库

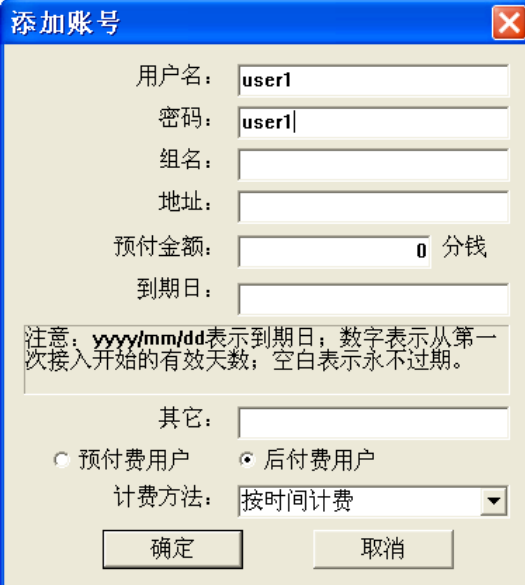
(2) 在图 1-3 弹出对话框中点击自动配置 ODBC，生成一个 ODBC 连接 WinRadius。



图 1-3 设置认证服务器数据库 ODBC 连接

3) 添加认证账户

在 WinRadius 菜单栏中选择 操作->添加账号，在图 1-4 的弹出对话框中填写账户信息，并点击确定，即可添加账户



添加账号

用户名: user1

密码: user1|

组名:

地址:

预付金额: 0 分钱

到期日:

注意: yyyy/mm/dd表示到期日; 数字表示从第一次接入开始的有效天数; 空白表示永不过期。

其它:

☐ 预付费用户 ☒ 后付费用户

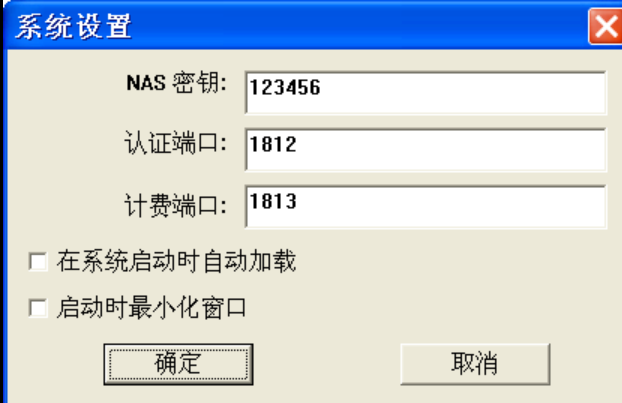
计费方法: 按时间计费

确定 取消

图 1-4 创建认证客户

4) 更改认证服务器的密钥

在 WinRadius 菜单栏中选择 设置->系统，在图 1-5 所示的弹出对话框中更改认证服务器的密钥为 WinRadius。



系统设置

NAS 密钥: 123456

认证端口: 1812

计费端口: 1813

☐ 在系统启动时自动加载

☐ 启动时最小化窗口

确定 取消

图 1-5 更改认证服务器的密钥为 WinRadius

5) 测试认证服务器是否能够工作

在这个文件夹中找到 RadiusTest.exe 程序，只修改用户名和口令，测试 WinRadius 服务器是否能够正常工作。

1.4.4 认证交换机配置

1) 配置认证交换机

登录 DCRS-5650 交换机，进入交换机命令行窗口。

```

DCRS-5650-28>enable          !进入特权配置模式
DCRS-5650-28#show run        !查看在用的交换机端口状态是否为非受控状
态，必要时初始化交换机
DCRS-5650-28(config)#interface vlan 1  !进入交换机缺省的 vlan 1
DCRS-5650-28(config-if-vlan1)#ip address 10.1.2.111 255.255.255.0 !配置 vlan1 并
设置 IP 和掩码
DCRS-5650-28(config-if-vlan1)#no shutdown  !激活 vlan 接口
DCRS-5650-28(config)#radius-server authentication host 10.1.2.11
！假定认证服务器为 PCB、IP 为 10.1.2.11
DCRS-5650-28(config)#radius-server key WinRadius  !设置通信密钥， winradius 服
务器的缺省密钥为 WinRadius
DCRS-5650-28(config)#aaa enable  !启用 AAA 认证
DCRS-5650-28(config)#dot1x enable  !启用 802.1x，注意必须在全局 config 模式中
设置启用 802.1x
DCRS-5650-28(config)#interface ethernet0/0/1 ！假定受控端口为 1，连接 PCA
DCRS-5650-28(config-ethernet0/0/1)#dot1x enable !在该端口或端口范围启用 802.1x
DCRS-5650-28(config-ethernet0/0/1)#dot1x port-control auto !设置端口的默认认证状
态为自动
DCRS-5650-28(config-ethernet0/0/1)#dot1x port-method portbased !设置基于端口的
认证方式
DCRS-5650-28(config-ethernet0/0/1)#show run  !查 ethernet0/0/1 端口状态

```

1.4.5 认证客户端配置

上面将 DCRS-5650-28 交换的 ethernet0/0/1 端口已配置为需要认证的受控端口，在该端口接入的 PCA,需要通过认证服务器的认证才能正常访问网络。



图 1-6 客户端认证软件窗口

在 PCA 上安装神州数码认证客户端软件 (setup.exe)，成功安装后双击桌面图标打开认证客户端 DigitalChinaSupplicant.exe，出现如图 1-6 所示的认证登录窗口。

点击属性按钮，选择认证服务器类型为 802.1x 认证服务器。

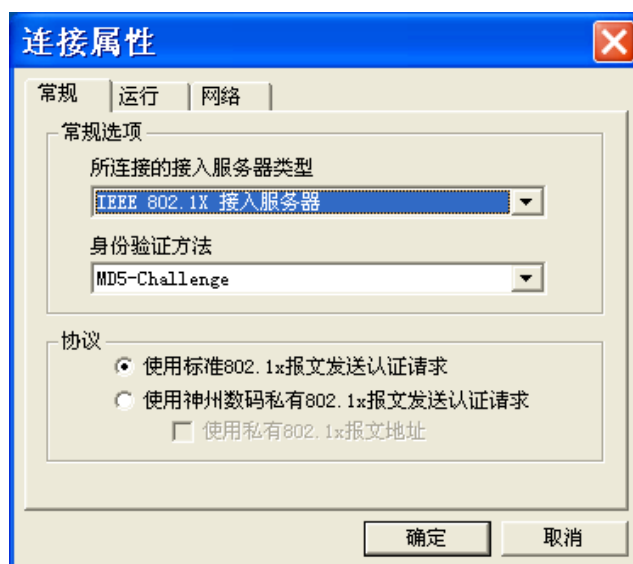


图 1-7 配置客户端认证服务器类型

在认证登录窗口。输入已 winradius 中添加的某个账户的用户名和密码，并点击连接，即可实现认证登陆。进入正常的网络访问，可以 ping 通其它 PC。

1.5 互动讨论主题

- 1) 分析不同 LAN 中 PC 互通的原因及跨越的物链路;
- 2) 理解网关的目的及作用;
- 3) 路由表的形成及使用;
- 4) 接入认证各组成部分的作用?
- 5) 接入认证能解决那些安全问题?
- 6) 802.1x 认证在网络的哪一层起作用?
- 7) 802.1x 认证与 PPPOE 和 Web+Portal 认证的区别?

1.6 进阶自设计

- 1) 采用 Wireshark 软件捕获接入认证的报文, 分析 802.1x 认证交互过程。
- 2) 如果 Radius 服务器连接在另外一台交换机上, 该如何正确配置交换机才能正确地完成 802.1x 认证。将组网拓扑和测试结果写在现场检查单背面, 并说明理由。

2 实验二 VLAN 的配置与协议分析

2.1 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。掌握镜像端口和 Trunk 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。

2.2 实验内容

首先在一台交换机上划分 VLAN，用 ping 命令测试连通性。然后在交换机上配置 Trunk 端口，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。

2.3 实验原理

2.3.1 路由器和交换机

以太网交换机实际是一个基于网桥技术的多端口第二层网络设备，它为数据帧从一个端口到另一个任意端口的转发提供了低时延、低开销的通路。而交换机技术的发展，还出现了集成了三层路由功能的三层交换机，这时交换机又“变成”了一个路由器。交换机工作在数据链路层，可以用来隔离冲突域，按 MAC 地址寻址。交换机通过自学习来建造一个 MAC 地址和端口的对照表（知道某个 MAC 在哪个端口上连着），通过这张表进行数据帧的转发。

路由器是网络层中的分组交换设备，基本功能是把 IP 报文传送到正确的网络，包括：

1. IP 数据报的转发，包括数据报的寻径和传送；
2. 子网隔离，抑制广播风暴；
3. 维护路由表，并与其他路由器交换路由信息，这是 IP 报文转发的基础。
4. IP 数据报的差错处理及简单的拥塞控制；
5. 实现对 IP 数据报的过滤和记帐。

路由器的 IP 数据报转发是通过路由表进行的，寻址的依据是目标 IP 地址。而路由表的建造是通过路由协议自动完成，或管理员的人工设置。

2.3.2 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 VLAN 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。

2.3.3 802.1q 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。

三层交换机就是具有部分路由器功能的交换机,在同一个交换机划分的 VLAN 之间能够做到“一次路由,多次转发”。对路由信息更新、路由表维护、路由计算、路由确定等功能都由软件实现。三层交换技术就是二层交换技术+三层转发技术。三层交换机都支持 802.1q 标准。

1) 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。

2) 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。

2.3.4 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。

2.3.5 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 。

2.4 VLAN 的组网实验

2.4.1 实验环境与分组

DCRS-5650 交换机 2 台，每 4 人一组，共同配置 2 台交换机。

2.4.2 实验网络拓扑

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。

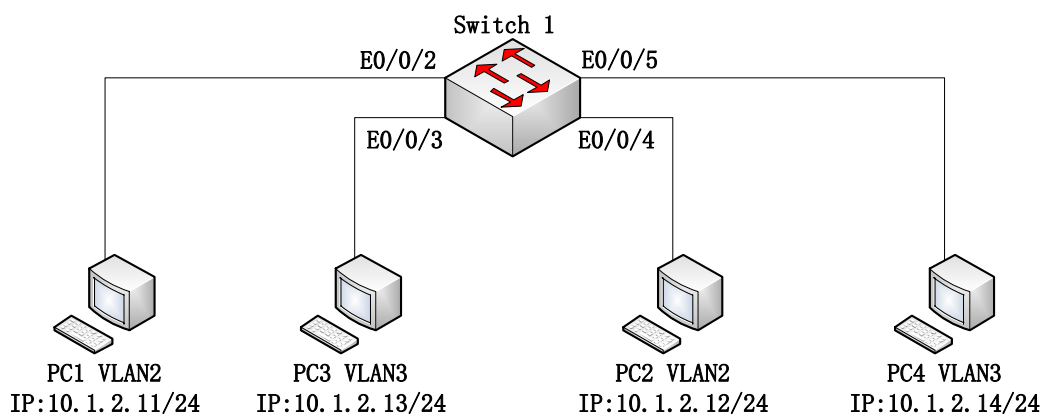


图 2-1 同一交换设备上配置 Vlan

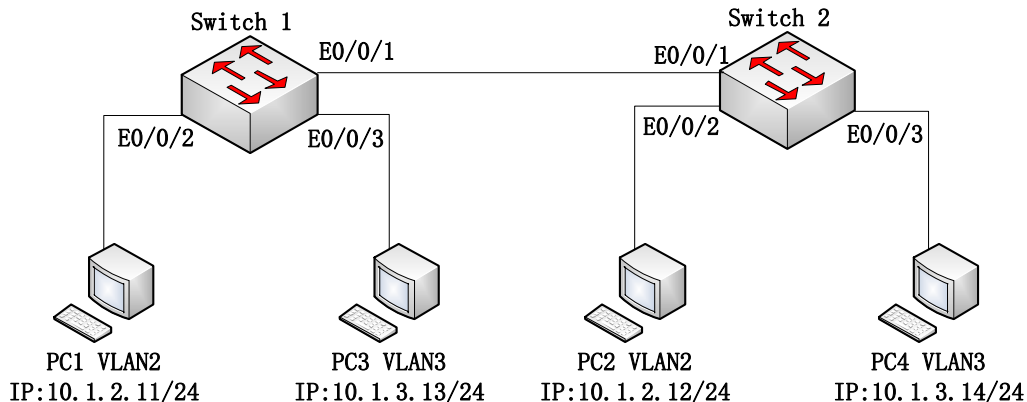


图 2-2 利用 trunk 端口在 2 台设备上配置 Vlan

2.4.3 实验过程及结果分析

将交换机恢复为出厂设置，参考命令如下：

```
switch> enable !进入特权用户模式
switch# set default !启动初始化
Are you sure? [Y/N] = y ! 确认初始化，显示初始化信息
switch# write ! 写入初始化信息到启动文件
switch# reload ! 重新启动交换机
```


1) VLAN 的基本配置

步骤 1: 按照图 2-1 连接好设备, 设置各 PC 的 IP 地址和默认网关。测试各台 PC 之间能否 ping 通, 记录结果。

步骤 2: 为交换机划分 VLAN, vlan 2 的配置参考命令如下: 同理配置 vlan 3。

```
switch> enable
switch# config                ! 进入全局配置模式
switch(Config)#vlan 2
switch(Config-vlan2)#switchport interface Ethernet 0/0/2
switch(Config-vlan2)#switchport interface Ethernet 0/0/4
switch(Config-vlan2)#exit
switch#show vlan              ! 查看 vlan 配置信息
```

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, 记录结果并分析原因。

2) Trunk 端口配置

步骤 4: 按照图 2-2 连接好设备, 设置各 PC 的 IP 地址和默认网关。

步骤 5: 为交换机 S2 划分 VLAN2 和 VLAN3, 配置命令同上。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, 参考配置命令如下:

```
switch(Config)#interface ethernet 0/0/1
switch(Config-Ethernet0/0/1)#switchport mode trunk
switch(Config-Ethernet0/0/1)#switchport trunk allowed vlan all
switch(Config-Ethernet0/0/1)#exit
switch#show vlan
```

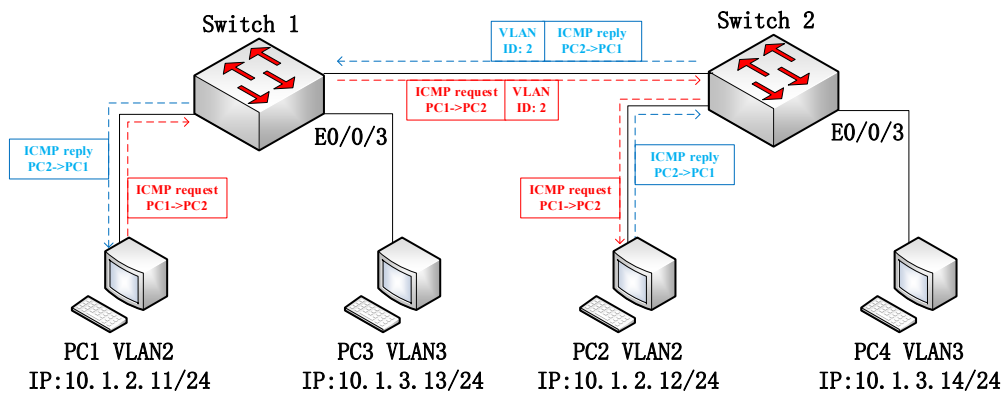
将 trunk 端口加入 VLAN2 和 VLAN3 中。

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。

步骤 7: 分别在交换机 S1 和 S2 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:

```
switch(Config)#monitor session 1 source interface ethernet 0/0/1 both
switch(Config)#monitor session 1 destination interface ethernet 0/0/3
```

在 4 台 PC 上捕获报文, 验证 PC1 ping PC2 能否 ping 通, 对各 PC 上截获的 ICMP 报文进行分析 (观测是否含有 802.1q 标记), 记录结果并分析原因。

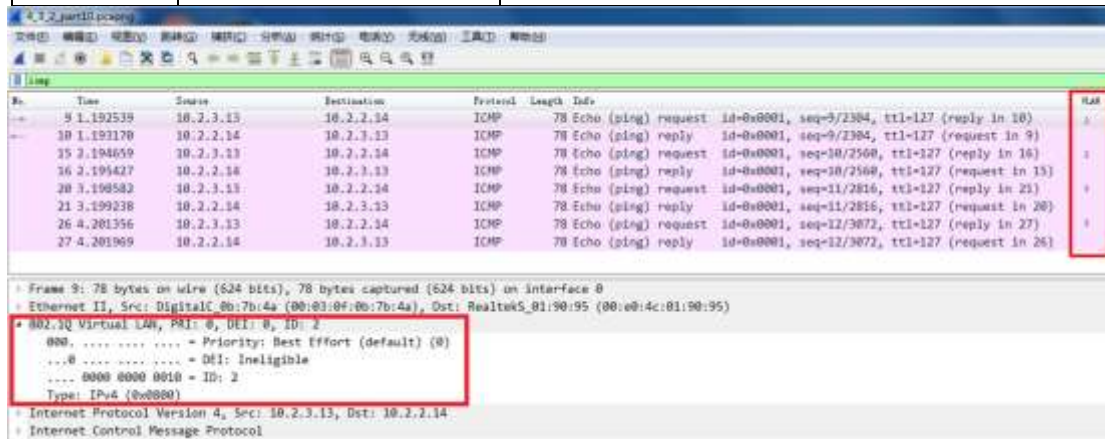


注:

- 1、新网卡默认过滤掉了 802.1q 标记，如果抓不到含有标记的报文，如实记录即可，在原因分析中填写预期能观测到的值，分析标记未出现可能的原因；
- 2、结合抓到的报文，尝试分析交换机在处理端口镜像和 VLAN 标记时的先后顺序。

表 2-1 跨交换机 VLAN 实验（PC1 ping PC2）

转发过程	802.1Q VLAN ID	标记出现与否的原因分析
PC1 - S1	Request 报文:	
	Reply 报文:	
S1 - S2	Request 报文:	
	Reply 报文:	
S2 - PC2	Request 报文:	
	Reply 报文:	



3) VLAN 间通信

关闭 S2 上的镜像，配置参考命令如下：

```
switch(Config)# no monitor session 1 source interface ethernet 0/0/1
switch(Config)# no monitor session 1 destination interface ethernet 0/0/3
```

步骤 8: 执行 PC2 ping PC4，观察能否 ping 通，分析原因。

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：

```
switch(Config)#interface vlan 2
switch(Config-If-Vlan2)#ip address 10.1.2.1 255.255.255.0
switch(Config-If-Vlan2)#no shutdown
switch(Config-If-Vlan2)#exit
```

同理配置 VLAN3 的 IP 地址。

步骤 10：在 4 台 PC 上捕获报文，验证 PC2 ping PC4 能否 ping 通，对各 PC 上截获的 ICMP 报文进行分析，填写表 5-3，分析观测到的过程和 VLAN ID 是否与预期相符。

注：如果监听机（PC3）抓不到带标记的报文，在组内另找一台可以抓到的 PC，与 PC3 更换 IP 配置和连线后，再进行测试。

表 2-2 跨 VLAN 通信（PC2 ping PC4）

转发过程	802.1Q VLAN ID	标记出现与否的原因分析
PC2 -- S2	Request 报文:	
	Reply 报文:	
S1 -- S2	Request 报文:	
	Reply 报文:	
S2 -- PC4	Request 报文:	
	Reply 报文:	

如果 ping 不通： 1、检查 PC 机和交换机的 IP 地址、子网掩码和**网关**设置是否正确，设备接口连接是否与拓扑图相符； **2、断开无线网卡，只保留 exp 网卡。**

2.5 互动讨论主题

- 8) 交换设备工作原理、端口类型和端口镜像工作原理；
- 9) Vlan 的配置与工作原理。

3 实验三 ARP 协议分析与欺骗防范

3.1 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。

3.2 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 Cisco3560 三层交换机上构建基本防范功能。

3.3 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。

3.3.1 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的目的，ARP 请求为 1，ARP 响应为 2，RARP 请求为 3，RARP 响应为 4。

3.3.2 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。

网络中的所有主机收到这个 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。

3.4 实验环境与分组

Cisco 3560 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。

3.5 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。

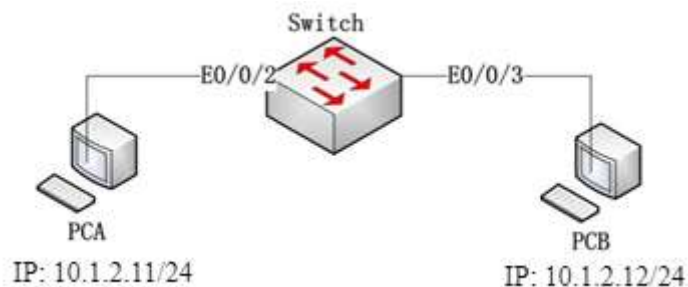


图 3-1 ARP 协议组网图（同一网段）

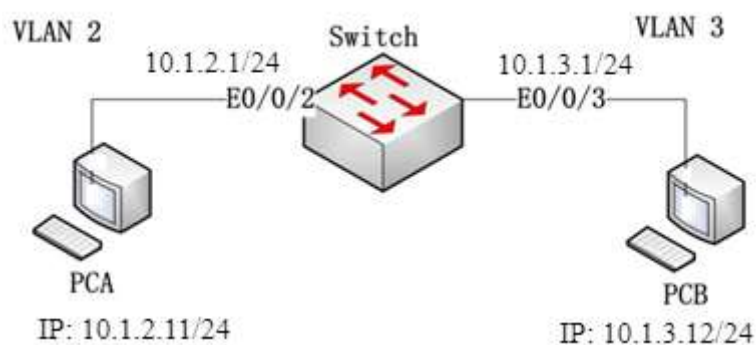


图 3-2 ARP 协议实验组网图（不同网段）

3.6 ARP 协议分析

3.6.1 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。

步骤 3：在 PCA、PCB 上截获报文；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。

3.6.2 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。

Cisco3560 交换机配置

```
Switch#show vlan          ! 查看设备 Vlan 现状
Switch#config t          ! 进入配置状态
Switch(config)#vlan 2     ! 创建 Vlan 2
Switch(config)#vlan 3
Switch(config)#interface fa0/2    ! 进入端口
Switch(config-if)#switchport access vlan 2    ! 将端口指派给 Vlan 2
同理将 fa0/3 赋给 vlan 3
Switch(config)#interface vlan 2    ! 进入 vlan 2
Switch(config-if)#ip address 10.1.2.1 255.255.255.0    ! 为 vlan 2 设定 IP
同理为 vlan 3 设定 IP 10.1.3.1
Switch(config)#ip routing    ! 开启交换机路由功能
Switch#show ip route        ! 查看路由表
```

PCA 与 PCB 应能互通

步骤 6: 首先执行“arp -d”清空缓存。在 PCA、PCB 上捕获报文, 执行命令“ping 10.1.2.22”。

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。

3.7 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。

3.8 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。

3.9 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。

3.10 MAC 与 IP 绑定实验

MAC 与 IP 绑定是在交换机内建立 MAC 地址和 IP 地址对应的映射表。端口获得的源 IP 和 MAC 地址将匹配该表，不符合则丢弃该端口发送的数据包。

Cisco3560 交换机上进行 MAC 与 IP 绑定

下面是在 Cisco3560 交换机上利用访问控制列表技术 ACL 进行 MAC 与 IP 绑定的实验：

步骤 1：在图 3-2 基础上，定义与 PCA 对应的 MAC 地址访问控制列表 `mac1`。

查看 PCA 对应的 MAC 地址，假设为 00:19:e0:2c:86:40。

```
Switch(config)#mac access-list extended mac1
```

定义 `mac1` 的访问策略：如 MAC 地址为 0019.e02c.8640 的主机可以访问任意主机，所有主机可以访问 MAC 地址为 0019.e02c.8640 的主机

```
Switch(config-ext-macl)#permit host 0019.e02c.8640 any
```

```
Switch(config-ext-macl)#permit any host 0019.e02c.8640
```

步骤 2：定义与 PCA 对应的 IP 地址访问控制列表 `ipac1`。

```
Switch(config)#ip access-list extended ipac1
```

定义 `ipac1` 的访问策略：如 IP 地址为 10.1.2.11 的主机可以访问任意主机，所有主机可以访问 IP 地址为 10.1.2.11 的主机

```
Switch(config-ext-nacl)#permit ip 10.1.2.11 0.0.0.0 any
```

```
Switch(config-ext-nacl)#permit ip any 10.1.2.11 0.0.0.0
```

步骤 3：在 fa0/2 端口启用 MAC 的访问列表 `mac1` 和 IP 访问列表 `ipac1`（定义的访问策略）

```
Switch(config)#interface fa0/2
```

```
Switch(config-if)#mac access-group mac1 in
```

```
Switch(config-if)#ip access-group ipac1 in
```

```
Switch#show access-lists
```

！ 查看当前访问列表

步骤 4：进行如下连通性测试，通过报文分析原因，记录结果。

- (1) 更换 PCA 的 IP 地址，如 10.1.2.13，接入端口仍为 fa0/2；

- (2) 为 Vlan2 添加端口 fa0/1, 接入 PCA, IP 地址不变, 即 10.1.2.11;
- (3) 将 PCC 替换 PCA 接入 fa0/2, 使用 10.1.2.11 地址;
- (4) 将 PCC 替换 PCA 接入 fa0/2, 使用 10.1.2.13 地址。

访问控制列表 ACL 使用包过滤技术, 读取第三层及第四层包头中的信息, 不仅仅用来提供网络安全访问的基本手段, 还可以限制网络流量、提高网络性能。在路由器端口处还可以决定哪种类型的通信流量被转发或被阻塞。

3.11 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;
- (4) MAC 与 IP 绑定后交换机的变化有哪些?

3.12 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。

4 实验四 TCP 协议分析

4.1 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。

4.2 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。

4.3 实验原理

4.3.1 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									
32																	
源端口 Source port								目的端口 Destination port									
顺序号 Sequence number																	
确认号 Acknowledgement number																	
Data Offset		Resrvd		URG		ACK		PSH		RST		SYN		FIN		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 IP 包首部中的源端 IP 地址和目的端 IP 地址唯一确定一个 TCP 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，这个值是本地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。

4.3.2 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：

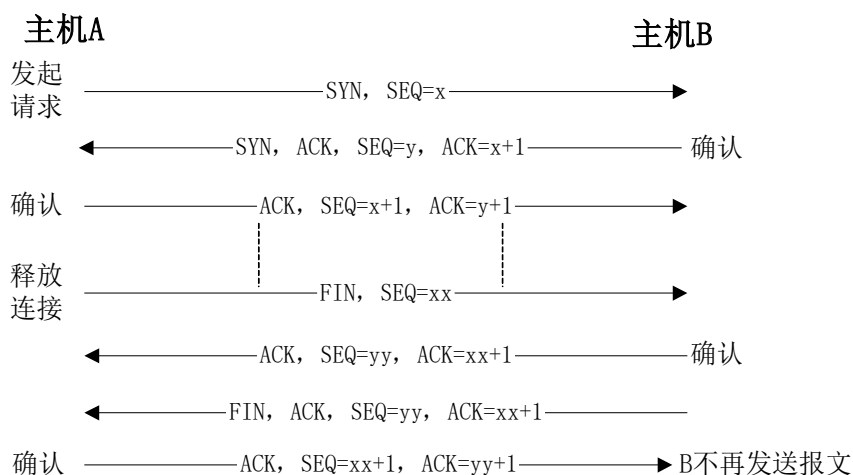


图 4-2 TCP 连接的建立的三次握手

4.4 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。

4.5 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。

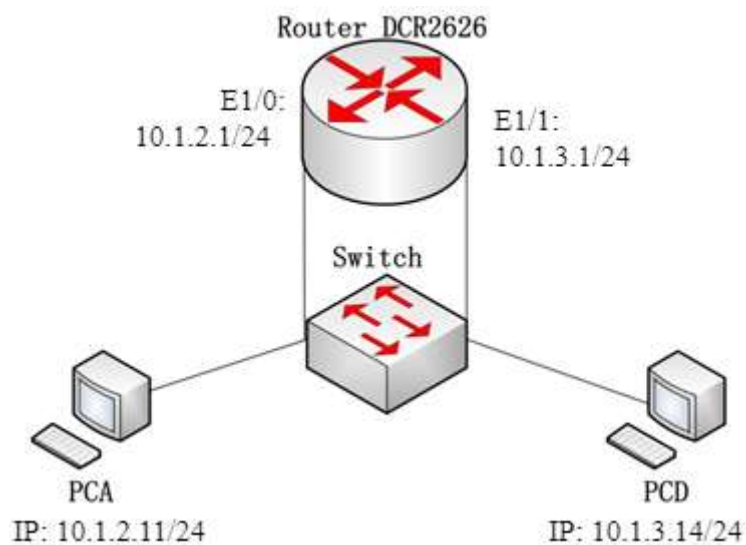


图 4-3 TCP 协议分析组网图

4.6 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：

```

Router#config
Router_config#interface e1/0
Router_config_e1/0#ip address 10.1.2.1 255.255.255.0
Router#show 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，发送和接收一个约 300KB 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: 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 7、TCPDebug 软件, 减小发送时间间隔 (如改为 0), 增大“发送缓冲长度”, 使得接收方的窗口有明显变化。

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。

4.7 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,从而占用改主机大量地资源。

4.8 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。

4.9 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。

4.10 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。

4.11 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) 传输层与上下相邻层的关系；

4) 报文的传输与确认对应关系。

4.12 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。

5 实验五 应用层协议分析

5.1 实验目的

分析应用层协议（如 FTP，HTTP）的工作过程，理解应用层与传输层及下层协议的关系。

5.2 实验内容

- （1）每组同学利用现有实验室网络及云服务器搭建内网、外网环境；
- （2）用 Wireshark 截获 HTTP 报文，分析报文结构及浏览器和服务器的交互过程；分析 HTTP 协议的缓存机制。分析应用层协议跟 TCP/DNS 等协议的交互关系。
- （3）用 Wireshark 截获 FTP 的报文，分析 FTP 协议的连接；分析被动模式，普通模式的区别；分析 NAT 对 FTP 的影响。使用 netcat 工具模拟 FTP 的客户端。

注：HTTP 和 FTP 两个协议二选一。

5.3 HTTP 协议概述^①

超文本传输协议（HyperText Transfer Protocol，HTTP）是一种用于分布式、协作式和超媒体信息系统的应用层协议。HTTP 是 WWW 的数据通信基础。

HTTP 的发展是由蒂姆·伯纳斯-李于 1989 年在欧洲核子研究组织（CERN）所发起。HTTP 的标准制定由万维网协会（World Wide Web Consortium，W3C）和互联网工程任务组（Internet Engineering Task Force，IETF）进行协调，最终发布了一系列的 RFC，其中最著名的是 1999 年 6 月公布的 RFC 2616，定义了 HTTP 协议中现今广泛使用的一个版本——HTTP 1.1。

2014 年 12 月，互联网工程任务组（IETF）的 Hypertext Transfer Protocol Bis（httpbis）工作小组将 HTTP/2 标准提议递交至 IESG 进行讨论，于 2015 年 2 月 17 日被批准。HTTP/2 标准于 2015 年 5 月以 RFC 7540 正式发表，取代 HTTP 1.1 成为 HTTP 的实现标准。

5.3.1 HTTP 协议概况

HTTP 是一个客户端终端（用户）和服务器端（网站）请求和应答的标准。客户端通常是浏览器，发起一个 HTTP 请求到服务器上指定端口（默认 80）。客户端称为用户代理（user agent）。应答服务器上存储着一些资源，比如 HTML 文件和图像。称

^①这部分内容参考了 CSDN 博主「有抱负的小狮子」的[原创文章](#)，有改动。

为源服务器（origin server）。在用户代理和源服务器中间可能存在多个“中间层”，比如代理服务器、网关或者隧道（tunnel）。

尽管 TCP/IP 协议是互联网上最流行的应用，HTTP 协议中，并没有规定必须使用它或它支持的层。事实上，HTTP 可以在任何互联网协议上，或其他网络上实现。HTTP 假定其下层协议提供可靠的传输。因此，任何能够提供这种保证的协议都可以被其使用。

通常，HTTP 客户端发起一个请求，创建一个到服务器指定端口（默认 80）的 TCP 连接。HTTP 服务器则在该端口监听客户端的请求。一旦收到请求，服务器会向客户端返回一个状态，比如"HTTP/1.1 200 OK"，以及返回的内容，如请求的文件、错误消息、或者其它信息。HTTP 协议的特点是无状态，就是说 HTTP 协议本身不会对请求和响应之间的通信状态做保存。建立在 HTTP 协议之上的应用如果需要状态，可以使用 cookie 来完成。

5.3.2 HTTP 协议的请求

HTTP 协议由 HTTP 请求和 HTTP 响应组成，当在浏览器中输入网址访问某个网站（或点击链接）时，你的浏览器会将你的请求封装成一个 HTTP 请求发送给服务器站点，服务器接收到请求后会组织响应数据封装成一个 HTTP 响应返回给浏览器。

HTTP 请求包括请求行、请求头、请求体，HTTP 响应包括响应行、响应头、响应体。

HTTP 请求的例子如下图所示：



请求行必须在 http 请求格式的第一行。请求头从第二行开始，到第一个空行结束。请求头和请求体之间存在一个空行（如图中 Cookie 行和 name 行之间）。请求体是可选的，可以为空。

请求头是后面几行（直到 Cookie 行），

请求行的格式：请求方式 资源路径 协议/版本，例如：POST /chapter17/user.html HTTP/1.1。**请求方式**很多，如 GET，POST，HEAD 等等。

GET 请求将请求参数追加在 URL 后面，很简单，没有请求体。但 URL 长度限制 GET 请求方式数据的大小。一般的 HTTP 请求大多都是 GET。常见 GET 请求:地址栏直接访问、、等。

POST 请求：请求参数在请求体处，请求数据大小没有限制，只有表单设置为 method=“POST”才是 POST 请求，其他大都是 GET 请求。

HEAD 请求：跟 GET 相似，不过服务端接收到 HEAD 请求时只返回响应头，不发送响应内容。所以，如果只需要查看某个页面的状态时，用 HEAD 更高效，因为省去了传输页面内容的时间。

其他还有 DELETE，OPTIONS，PUT，TRACE，CONNECT 请求等。

请求头从第二行开始，通常以键值对 key:value 方式传递数据。例如：

```
POST /vk/app/rest/ddp/findModelByType HTTP/1.1
User-Agent: Fiddler
Host: 39.108.107.149:8080
Content-Length: 11
```

name=城市

key 为规范的固定值，value 为 key 对应的取值，通常是一个值，可能是一组。

HTTP 请求报文头属性

常见请求头

Referer：表示这个请求是从哪个 url 跳过来的。通过百度来搜索淘宝网，那么在进入淘宝网的请求报文中，Referer 的值就是 www.baidu.com。如果是直接访问就不会有这个头。常用于防盗链。

Accept：告诉服务端该请求所能支持的响应数据类型，即 MIME 类型。

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8

MIME 格式：大类型/小类型[:参数]

例如:text/html, text/css, text/javascript, image/*等。

If-Modified-Since:浏览器通知服务器，本地缓存的最后变更时间。与另一个响应头组合控制浏览器页面的缓存。

Cookie：客户端的 Cookie 通过这个属性传给服务端。

User-Agent:浏览器通知服务器，客户端浏览器与操作系统相关信息

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/69.0.3497.100 Safari/537.36

Connection:表示客户端与服务连接类型; Keep-Alive 表示持久连接, close 已关闭。

Host:请求的服务器主机名

Content-Length:请求体的长度

POST /vk/app/rest/ddp/iModelServiceImpl/findModelByType HTTP/1.1

User-Agent: Fiddler

Host: 39.108.107.149:8080

Content-Length: 11

name=城市

Content-Type:请求的与实体对应的 MIME 信息。如果是 post 请求,会有这个头,默认值为 application/x-www-form-urlencoded, 表示请求体内容使用 url 编码。

Accept-Encoding: 浏览器通知服务器, 浏览器支持的数据压缩格式。如 GZIP 压缩

Accept-Encoding: gzip, deflate

Accept-Language: 浏览器通知服务器, 浏览器支持的语言。各国语言(国际化 i18n)

Accept-Language: zh-CN,zh;q=0.9

Cache-Control: 指定请求和响应遵循的缓存机制

对缓存进行控制, 如一个请求希望响应返回的内容在客户端要被缓存一年, 或不希望被缓存就可以通过这个报文头达到目的。

Cache-Control: no-cache

请求体

当请求方式是 POST 时, 请求体有请求的参数, 格式如下:

username=zhangsan&password=123

5.3.3 HTTP 协议的应答

HTTP 应答 (也称响应) 也由三部分组成 (响应行+响应头+响应体)。



响应行：

① 报文协议及版本：

例如：HTTP/1.1 200 OK

② 状态码及状态描述：

状态码：由 3 位数字组成，第一个数字定义了响应的类别

1xx：指示信息，表示请求已接收，继续处理

2xx：成功，表示请求已被成功接受，处理。

200 OK：客户端请求成功

204 No Content：无内容。服务器成功处理，但未返回内容。一般用在只是客户端向服务器发送信息，而服务器不用向客户端返回什么信息的情况。不会刷新页面。

206 Partial Content：服务器已经完成了部分 GET 请求（客户端进行了范围请求）。响应报文中包含 Content-Range 指定范围的实体内容

3xx：重定向

301 Moved Permanently：永久重定向，表示请求的资源已经永久的搬到了其他位置。

302 Found：临时重定向，表示请求的资源临时搬到了其他位置

303 See Other：临时重定向，应使用 GET 定向获取请求资源。303 功能与 302 一样，区别只是 303 明确客户端应该使用 GET 访问

307 Temporary Redirect：临时重定向，和 302 有着相同含义。POST 不会变成 GET

304 Not Modified：表示客户端发送附带条件的请求(GET 方法请求报文中的 IF...)时，条件不满足。返回 304 时，不包含任何响应主体。虽然 304 被划分在 3XX，但和重定向没有关系。

4xx：客户端错误

400 Bad Request：客户端请求有语法错误，服务器无法理解。

401 Unauthorized: 请求未经授权, 这个状态代码必须和 WWW-Authenticate 报头域一起使用。

403 Forbidden: 服务器收到请求, 但是拒绝提供服务

404 Not Found: 请求资源不存在。比如, 输入了错误的 url

415 Unsupported media type: 不支持的媒体类型

5xx: 服务器端错误, 服务器未能实现合法的请求。

500 Internal Server Error: 服务器发生不可预期的错误。

503 Server Unavailable: 服务器当前不能处理客户端的请求, 一段时间后可能恢复正常,

响应头:

③响应头, 也是由多个属性组成; 也是用键值对 k: v 表示。

服务器通过响应头来控制浏览器的行为, 不同的头浏览器操作不同。

常见响应头	描述
Location	指定响应的路径, 需要与状态码 302 配合使用, 完成跳转。
Content-Type	响应正文的类型 (MIME 类型) 取值: text/html;charset=UTF-8
Content-Disposition	通过浏览器以下载方式解析正文 取值: attachment;filename=xx.zip
Set-Cookie	与会话相关技术。服务器向浏览器写入 cookie
Content-Encoding	服务器使用的压缩格式 取值: gzip
Content-length	响应正文的长度
Refresh	定时刷新, 格式: 秒数;url=路径。url 可省略, 默认值为当前页。 取值: 3;url=www.itcast.cn //三秒刷新页面到 www.itcast.cn
Server	服务器名称
Last-Modified	服务器通知浏览器, 文件的最后修改时间。与 If-Modified-Since 一起使用。
Cache-Control	响应输出到客户端后, 服务端通过该报文头告诉客户端如何控制响应内容的缓存。常见的取值有 private、public、no-cache、max-age, no-store, 默认为 private。缓存时间为 31536000 秒 (365 天)

响应体:

④响应体, 就是服务器发送给浏览器的正文, 即我们真正要的内容 (如网页, 图片等);

响应体, 响应体是服务器回写给客户端的页面正文, 浏览器将正文加载到内存, 然后解析渲染显示页面内容

5.4 FTP 协议概述

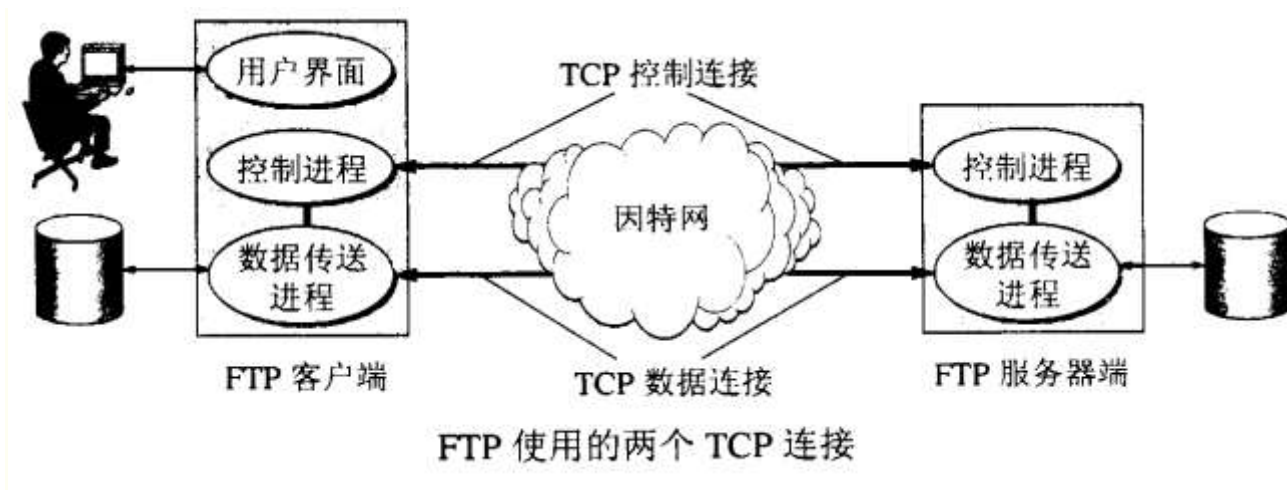
文件传输协议 FTP(File Transfer Protocol)是 Internet 早期使用最广泛的文件传输协议。FTP 使用交互式的访问,允许客户指定文件的类型和格式(如指明是否使用 ASCII 码),并允许文件具有存取权限(如访问文件的用户必须经过授权,并输入有效的口令)。

5.4.1 FTP 基本原理

FTP 只提供文件传送的一些基本服务,它使用 TCP 可靠地运输服务。FTP 使用客户端-服务器模型,一个 FTP 服务器进程可以为多个客户进程提供服务。通常 FTP 服务器有两大组成部分:一个主进程,负责接受新的请求;还有若干从属进程,负责处理单个请求。主进程工作步骤:

1. 打开熟知端口(21),使客户进程能够连接上
2. 等待客户进程发送连接请求
3. 启动子进程处理客户进程发送的连接请求,子进程处理完请求后结束。子进程在运行期间可能根据需要可创建其他一些子进程
4. 回到等待状态,继续接受其他客户进程发起的请求,主进程与子进程的处理是并发进行的

典型的 FTP 应用会用到两种连接:控制连接和数据连接。FTP 控制连接在整个会话期间都保持打开,只用来发送 FTP 命令及其应答。当客户进程向服务器发送连接请求时,连接服务器进程的熟知端口 21,就是一个控制连接。当双方需要交换数据(如传文件,列表文件等)时,这些数据的交换要在数据连接中传输。所以双方还要协商建立一个数据连接。



5.4.2 FTP 的数据表示

FTP 协议规定了控制协议传送与存储的多种选择,在以下 4 个方面必须做出一个选择。

- 文件类型: ASCII 码文件(默认的)/ 二进制的文件类型

- 格式控制：该选项针对 ASCII 类型文件适用，非打印(默认选择，文件中不包含垂直格式信息)/ 远程登录格式控制
- 结构：文件结构(默认选择，文件被认为是一个连续的字节流)/ 记录结构
- 传输方式：流方式(模式选择，文件以字节流方式传输，对于文件结构，发方在文件尾提示关闭数据连接，对于记录结构，有专用的两字节序列码记录结束和文件结束)/ 块方式(文件以一系列块来传送，每块前面有一个或多个首部字节)/ 压缩方式

5.4.3 FTP 的命令和应答

FTP 协议的命令和应答在客户和服务器的控制连接上以 ASCII 码形式传送。这就要求在每行结尾都要返回 CR、LF 对（也就是每个命令或每个应答）。这些命令都是 3 或 4 个字节的大写 ASCII 字符，其中一些带选项参数。从客户向服务器发送的 FTP 命令超过 30 种。下图是比较常用的几种命令：

命 令	说 明
ABOR	放弃先前的FTP命令和数据传输
LIST <i>filelist</i>	列表显示文件或目录
PASS <i>password</i>	服务器上的口令
PORT <i>n1,n2,n3,n4,n5,n6</i>	客户端IP地址（ <i>n1.n2.n3.n4</i> ）和端口（ $n5 \times 256 + n6$ ）
QUIT	从服务器注销
RETR <i>filename</i>	检索（取）一个文件
STOR <i>filename</i>	存储（放）一个文件
SYST	服务器返回系统类型
TYPE <i>type</i>	说明文件类型：A表示ASCII码，I表示图像
USER <i>username</i>	服务器上用户名

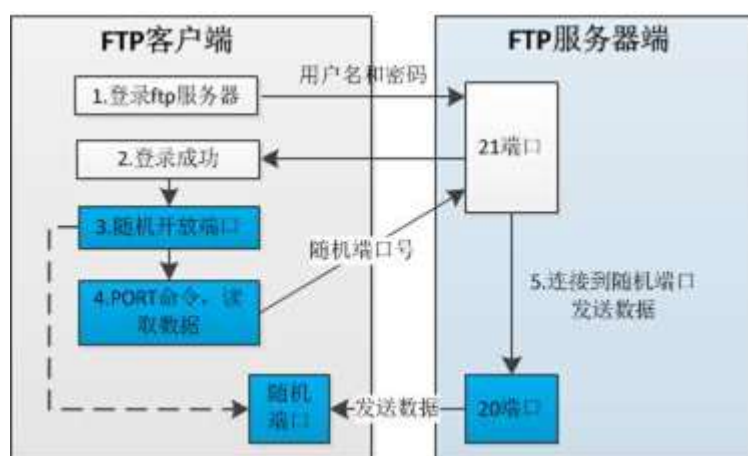
应答都是 ASCII 码形式的 3 位数字，并跟有报文选项。其原因是软件系统需要根据数字代码来决定如何应答，而选项串是面向人工处理的。由于客户通常都要输出数字应答和报文串，一个可交互的用户可以通过阅读报文串（而不必记忆所有数字回答代码的含义）来确定应答的含义。

应答	说 明
1yz	肯定预备应答。它仅仅是在发送另一个命令前期待另一个应答时启动
2yz	肯定完成应答。一个新命令可以发送
3yz	肯定中介应答。该命令已被接受，但另一个命令必须被发送
4yz	暂态否定完成应答。请求的动作没有发生，但差错状态是暂时的，所以命令可以过后再发
5yz	永久性否定完成应答。命令不被接受，并且不再重试
x0z	语法错误
x1z	信息
x2z	连接。应答指控制或数据连接
x3z	鉴别和记帐。应答用于注册或记帐命令
x4z	未指明
x5z	文件系统状态

5.4.4 FTP 数据连接的工作模式

FTP 有两种工作模式，分别是主动模式(PORT)和被动模式(PASV)两种模式，这两种模式是按照 FTP 服务器的“角度”来说的，更通俗一点说就是：在传输数据时，如果是服务器主动连接客户端，那就是主动模式；如果是客户端主动连接服务器，那就是被动模式。

PORT 中文称为主动模式，工作的原理：FTP 客户端连接到 FTP 服务器的 21 端口，发送用户名和密码登录，登录成功后要 list 列表或者读取数据时，客户端随机开放一个端口（1024 以上），发送 PORT 命令到 FTP 服务器，告诉服务器客户端采用主动模式并开放端口；FTP 服务器收到 PORT 主动模式命令和端口号后，通过服务器的 20 端口和客户端开放的端口连接，发送数据，原理如下图：

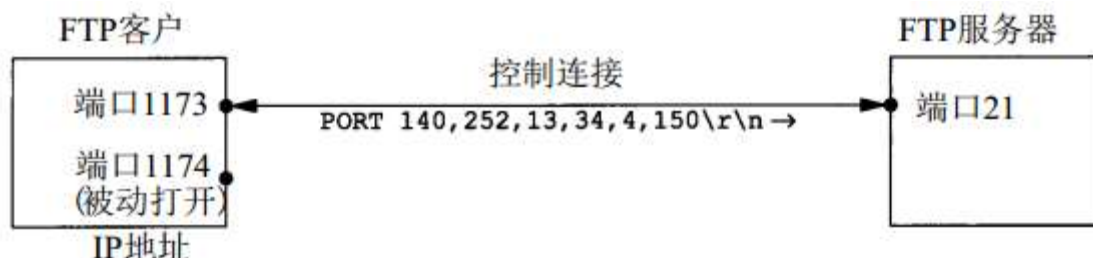


主动模式其一般过程如下：

1. 客户端监听在一个临时端口号，使用 PORT 命令从控制连接上把端口号发向服

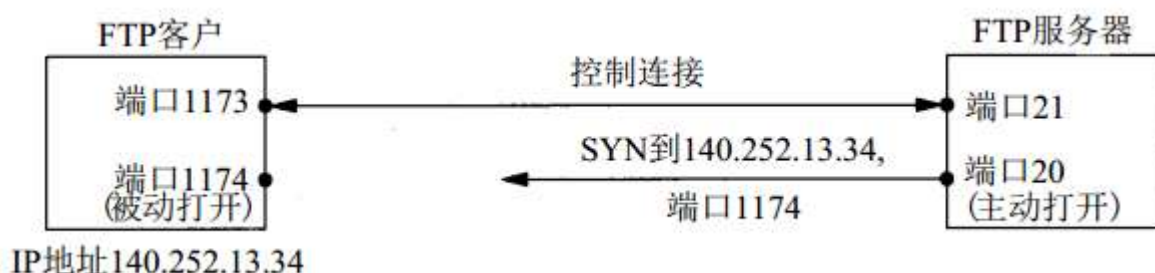
务器。

2. 服务器接收到端口号，使用端口 20 向客户端的这个端口发送一个连接请求，建立起数据连接。

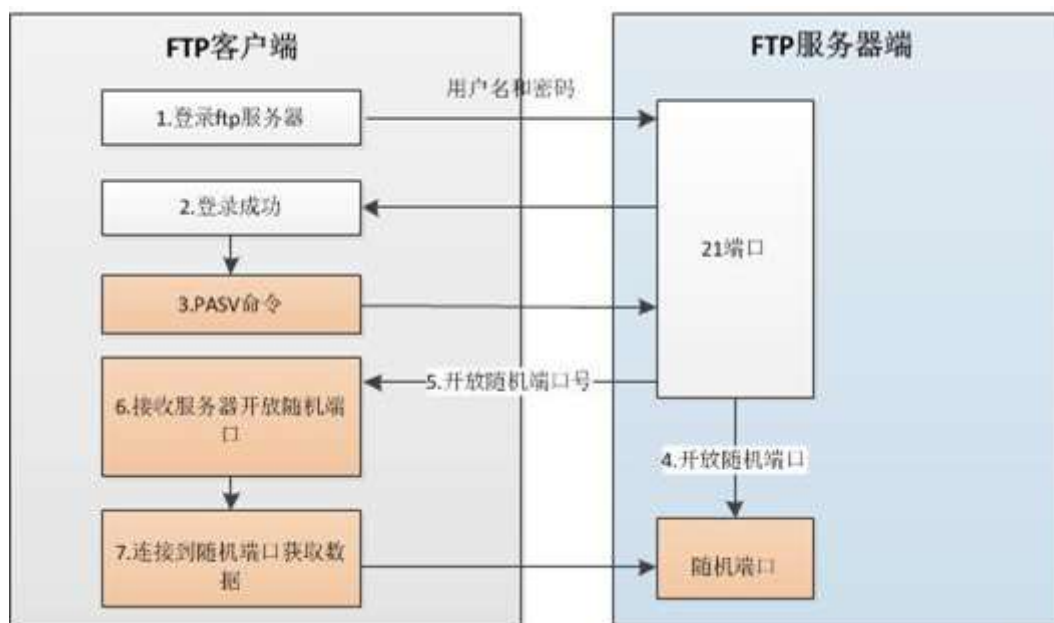


上图给出了第 1 步执行时的连接状态。假设客户用于控制连接的临时端口是 1173，客户用于数据连接的临时端口是 1174。客户发出的 PORT 命令，其参数是 6 个 ASCII 编码的十进制数字，它们之间由逗号隔开。前面 4 个数字指明客户上的 IP 地址，服务器将向它发出主动打开（本例是 140.252.13.34），而后两位指明 16 bit 端口地址。由于 16 bit 端口地址是从这两个数字中得来，所以其值在本例中就是 $4 \times 256 + 150 = 1174$ 。

下图给出了服务器向客户所在数据连接端发起主动打开时的连接状态。服务器的端点是端口 20。



被动模式其一般过程如下（参考下图）：



1. 客户端使用 **PASV** 命令从控制连接上告诉服务器，希望用被动模式传输数据。
2. 服务器接收到 **PASV** 命令，监听在某个随机的端口上，并以应答（比如 227 Entering Passive Mode (202,117,1,2,172,17).）告诉客户端该端口号（比如 44049）。
3. 客户端新建一个 TCP 连接到服务器的 44049 端口。

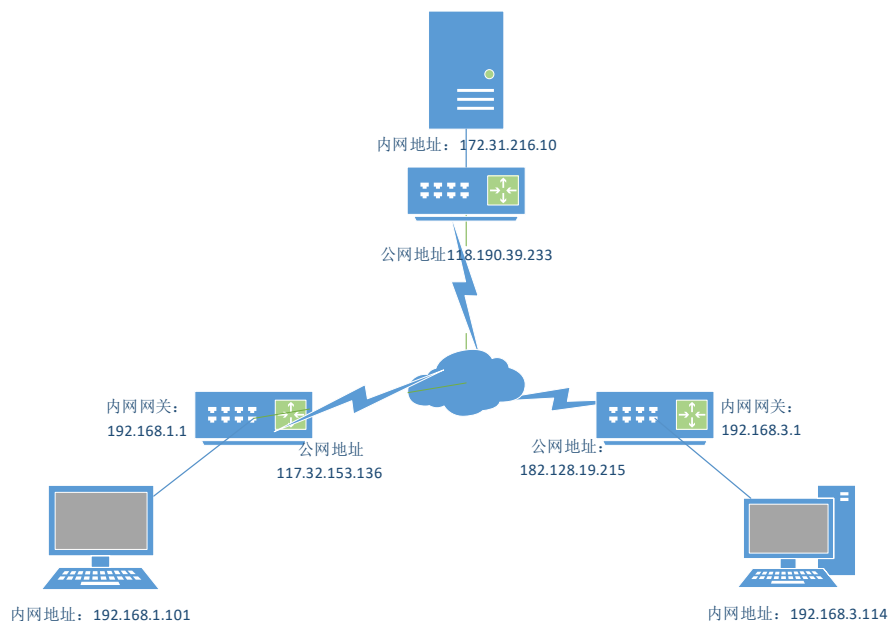
今天的互联网中大部分客户端机器都藏在 NAT 和防火墙后，所以主动模式通常不能工作，需要使用被动模式来建立连接。如果服务器也是在 NAT 盒子后面，那么还需要扩展的被动模式（命令是 **EPSV**）来完成数据连接建立。

5.5 实验环境与分组

每 2 名同学一组，以现有校园网络环境及云服务器搭建内网、外网网络。

5.6 实验网拓扑结构

以各组现有网络实际情况为准，标注内网、公网地址。



5.7 HTTP 协议分析

5.7.1 清空缓存后的 ARP, DNS 和 HTTP 协议分析

步骤 1：在计算机终端上运行 Wireshark 截获所有的报文。

步骤 2：清空 ARP, DNS 和 HTTP 浏览器的缓存：

浏览器缓存的清除以 Chrome 浏览器为例，地址栏中输入 `chrome://settings/`，找到高级选项中的“隐私设置和安全性”，清除浏览数据。

执行“ipconfig /flushdns”清除本地 DNS 缓存。

执行“arp -d”命令清空 arp 缓存。

步骤 3：在浏览器中访问 3 个网址，比如 www.xjtu.edu.cn, www.github.com, www.unb.br;

步骤 4：执行完之后，Wireshark 停止报文截获，分析截获的报文。

观察几个协议的配合使用，注意访问的延迟情况。特别分析 HTTP 的请求和应答。注意一个网址的访问中，用了几个连接，取了几个对象（HTML，CSS，JS，图片等），有几次 DNS 解析，有没有 Cookie 等。

5.7.2 带缓存的 ARP，DNS 和 HTTP 协议分析

照着 1.7.1 中的步骤 1-4 再次执行一遍，但不执行步骤 2。观察缓存的使用和带来的好处。

5.7.3 使用 ncat 工具访问 HTTP 服务

参考 1.7.1 中的步骤 1-4 和分析结果，在命令窗口执行 `ncat -C xxx.xxx.xxx.xxx 80`，ncat 连接上 HTTP 服务器后，根据协议输入合适的请求。其中 xxx.xxx.xxx.xxx 为服务器地址。

例：

ncat -C 202.117.1.13 80

GET / HTTP/1.1

Host: www.xjtu.edu.cn

（命令输入完毕后，需要敲两次回车键）

5.8 FTP 协议分析

5.8.1 FTP 协议的分析

步骤 1：在远程的云服务器上开启 ftp 服务，并在云服务器控制台把 21 端口开放。在云服务器上运行报文截获工具（如 Linux 的 tcpdump，Windows 的 Wireshark）截获 FTP 报文。

步骤 2：在计算机终端上运行 Wireshark 截获报文，使用 IE 浏览器来访问该 FTP 服务器。比如在地址栏输入 <ftp://xxx.xxx.xxx.xxx/> 其中 xxx.xxx.xxx.xxx 是该云服务器的 IP 地址。

步骤 3：进入 FTP 服务器中的某个目录中，下载一个文件。结束后，停止报文截获。

分析该 FTP 的过程。注意对照服务器和客户端的一起分析，注意 NAT 的影响。观察是否使用了被动模式，如果是主动模式并且工具允许，使用被动模式再做一次下载，

并分析。

如果 FTP 不能正常工作,请仔细抓包并分析原因。NAT 穿越问题可能是原因之一。

5.8.2 使用 ncat 工具来访问 FTP 服务

步骤 1: 提前把用到的 FTP 命令准备好(写在 notepad++中)。

步骤 2: 在云服务器上运行报文截获工具准备截获 FTP 报文。在命令窗口执行 `ncat -C xxx.xxx.xxx.xxx 21`, ncat 连接上 FTP 服务器后,根据协议输入合适的命令。其中 `xxx.xxx.xxx.xxx` 为云服务器地址。

步骤 3: 解析完毕后停止报文截获。把过程整理记录到报告中。

在 ncat 模拟 FTP 客户端的过程中,请查看服务器的文件列表,并下载一个不大的文本文件。过程中,必要时用 `netstat` 命令观察双方的(新开)端口监听情况。

5.9 互动讨论主题

- (1) HTTP 协议的缓存, DNS 的缓存;缓存对网络访问速度的影响。
- (2) NAT 对 FTP 传输的影响,比较 HTTP 与 FTP 的特点;

5.10 进阶自设计

观察缓存的更新和失效:在云服务器上搭建 Apache2(或其他 WEB 服务器),测试修改 HTML 或图片文件,看客户端能否及时访问到更新的内容,注意抓包分析。

6 实验六 RIP 协议分析

6.1 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。

6.2 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**。

6.3 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。

6.4 实验环境与分组

- 1) DCR5650 三层交换机 2 台(S1, S2), DCR2626 路由器 1 台(R1)。
- 2) 每 4 人一组, 共同配置设备, 完成实验。

6.5 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 地址、端口等参数。

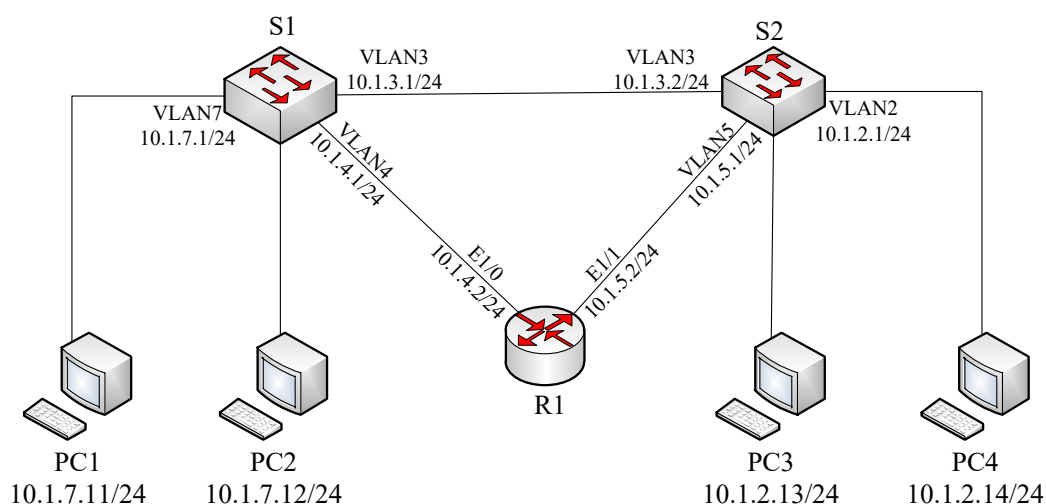


图 5-1 RIP 协议配置组网拓扑图

6.6 RIP 启动与路由分析

将交换机、路由器恢复为出厂设置, 参考命令如下:

交换机:

```
Switch> enable    !进入特权用户模式
Switch# set default !启动初始化
Are you sure? [Y/N] = y ! 确认初始化, 显示初始化信息
Switch# write     ! 写入初始化信息到启动文件
Switch# reload    ! 重新启动交换机
```

路由器:

```
Router>enable     !进入特权用户配置模式
Router#delete      !恢复出厂设置
Router#reboot      !重启路由设备
```


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：

```
switch(Config)# hostname S1      ! 改名以方便配置操作
S1(Config)# vlan 3
S1(Config-vlan3)# switchport interface ethernet 0/0/1
S1(Config-vlan3)# exit
S1(Config)# interface vlan 3
S1(Config-If-Vlan3)# ip address 10.1.3.1 255.255.255.0
```

同理配置交换机 S1 其他 vlan。

配置路由器 R1：

```
Router#config
Router(Config)# hostname R1 ! 改名以方便配置操作
R1(config)# interface e1/0
R1(config-if)#ip address 10.1.4.2 255.255.255.0
```

同理配置 R1 的接口 e1/1。

此时，测试 PC1、PC2 和 S1 之间是否可以互相通信，测试 R1 和 S1 之间是否可以互相通信。在 R1 上 ping 两台机器 PC1 和 PC2，看能否 ping 通，通过各自的路由表分析原因。

```
R1# show ip route      ! 查看路由表
```

步骤 2: 在 R1 上配置 10.1.7.0/24 的静态路由。命令如下：

```
R1(config)# ip route 10.1.7.0 255.255.255.0 10.1.4.1
```

在 R1 上 ping 各个 PC 看能否 ping 通，查看各自的路由表，分析原因。

步骤 3: 删除步骤 2 配置的静态路由：

```
R1(config)# no ip route 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：

```
S1(Config)# router rip      ! 激活 RIP 进程
S1(Config-router)#version 2    ! 指定 RIP 版本
S1(Config-router)#network vlan3 ! 指定 RIP 相关网络号
S1(Config-router)#network vlan4
S1(Config-router)#network vlan7
```


在路由器 R1 启动 RIP 协议命令：

```
R1(config)# router rip
R1(config-rip)# version 2      ! 指定 RIP 版本
R1(config-rip)# network 10.1.4.0 255.255.255.0
R1(config-rip)# network 10.1.5.0 255.255.255.0
```

测试 R1 和各个 PC 的连通性，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
S1						
R1						

Pref: 路由表项优先级; Cost: 路由表项代价。

常见路由种类及优先级：

路由种类	优先级
D-Direct	0
S-STATIC	1
E-OSPF	110
R-RIPv1、v2	120
B-BGP	200
.....	

步骤 5：在 S2 上配置各个 VLAN 以及接口地址，并启动 RIP 协议（命令参考 S1 的配置），并测试各个 PC 机之间的连通性。在 PC1 上用 **tracert -d 10.1.2.14**（PC4 的 IP 地址），查看 PC1-PC4 的路由连通路程。

步骤 6：拔掉 S1 与 S2 的直连线，测试 PC2 与 PC3 的连通性，在 PC2 上用 **tracert -d 10.1.2.13**，查看 PC2-PC3 的路由连通路程。（如果不能连通，请过一段时间重新测试。）

6.7 RIP 报文结构及路由的更新

6.7.1 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 协议有两个版本，即版本 1（RFC 1058）和版本 2（RFC 2453），实验是以版本 2 为例进行测试

试验。图 5-3 是 RIP 版本 2 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		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

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。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。

6.7.2 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。

6.8 RIP 报文捕获及结果分析

步骤 7：在前面配置的基础上，将交换机 S1 与 R1 相连接的端口镜像到 S1 与 PC1 相连接的端口。参考命令如下（配置端口以实际连接端口为准）：

```
S1(Config)#monitor session 1 source interface ethernet 0/0/1 both
S1(Config)#monitor session 1 destination interface ethernet 0/0/3
```

步骤 8：停止交换机 S1 上的 RIP 协议；

```
S1(config)# no router rip
```

步骤 9：在 PC1 上运行 WireShark 截获报文，然后在 S1 上启动 RIP 协议（配置命令参考步骤 4）。观察截获的请求报文和应答报文，选择一对 RIP 的请求/应答报文填写在表 5-2 和 5-3 中并理解其含义。

表 5-2 RIP 协议的请求报文

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		

表 5-3 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		

6.9 互动讨论主题

- 1) 解释名词术语：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 报文的启动与报文形成次序的关系。

6.10 进阶自设计

在上述实验结果的基础上，自主设计实验（例：把 S1-S2 之间的网线各插拔一次）获取 S1 和 R1 之间的 RIP 交互报文，结合报文分析 S1 和 R1 路由表项的生成、更新、失效和删除等过程。

7 实验七 OSPF 路由协议分析

7.1 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。

7.2 实验内容

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

7.3 实验原理

7.3.1 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(Interior Gateway Protocol,简称 IGP)，用于在单一自治系统(autonomous system,AS)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者一个自治系统 AS (Autonomous System) 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。

7.3.2 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 HelloInterval 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。

7.3.3 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。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。

7.3.4 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 2 字节的选项字段，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。

7.3.5 LSA 类型及报文结构

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

7.4 实验环境与分组

- 1) DCR-2626 路由器 2 台，DCRS-5650 交换机 1 台。
- 2) 每 4 位同学一组，共同配置路由器。

7.5 实验组网

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。

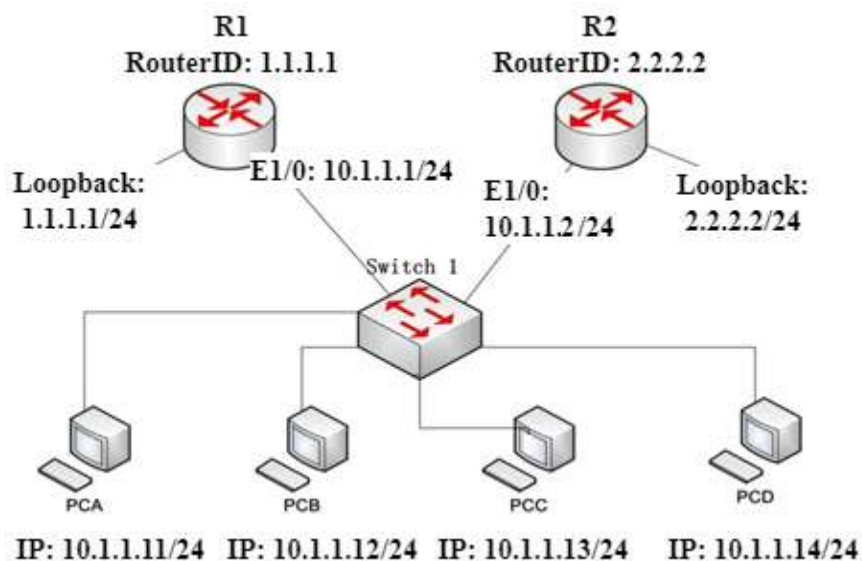


图 6-3 OSPF 邻居建立和报文交换过程组网图

7.6 实验步骤

步骤 1：按图连接好各实验设备，配置 IP 地址；交换机不用划分 VLAN，各端口都在一个 VLAN 中。

步骤 2：将交换机上连接两个路由器的端口镜像到其中一台 PC 连接的端口上。

例：若两个路由器连接到交换机的 25、26 口，PCA 连接在交换机的 1 口，将 25、26 口的流量镜像到 1 端口的命令如下：

```
switch(Config)#monitor session 1 source interface ethernet 0/0/25-26 both
switch(Config)#monitor session 1 destination interface ethernet 0/0/1
```

步骤 3：在每台 PC 上开始截获报文。

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，路由器 R1 配置的参考命令如下：

```
Router_config#interface loopback0                !配置环回接口
Router_config_l0#ip address 1.1.1.1 255.255.255.0
Router_config#interface e1/0                      !配置 ethernet0 接口
Router_config_e1/0#ip address 10.1.1.1 255.255.255.0
Router_config_e1/0#no shutdown
Router_config#router ospf 1                        !启动 ospf 进程，进程号为 1
Router_config_ospf_1#network 10.1.1.0 255.255.255.0 area 0  !指定 OSPF 区域
Router_config_ospf_1#network 1.1.1.0 255.255.255.0 area 0
```

同理配置 R2 路由器。

步骤 5：“show ip route”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。

7.7 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) 说明路由其中产生的 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。

7.8 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。

7.9 进阶自设计

在本实验的基础上，利用实验环境中的 2 台路由和 1 台三层交换构建一个支持 OSPF 协议的局域网络，并通过其中一台路由的 NAT 协议连接到校园网。分析该协议使用的路径算法。

8 实验八 防火墙与 SSLVPN 实验

8.1 实验方案及目的

SSL VPN 是以 SSL/TLS 协议为安全基础的 VPN 远程接入技术，移动办公人员（在 SSL VPN 中被称为远程用户）使用 SSL VPN 可以安全、方便的接入企业内网，访问企业内网资源，提高工作效率。在 SSLVPN 解决方案中，远程用户通过 SSLVPN 客户端程序，在不可靠的公网建立一条加密的 SSL 数据通道，直接连接到了企业内网中，这对远程/全球办公室的建立非常必要。本实验的目的是利用 CISCO ASA5505 防火墙设备的 SSL VPN 技术构建一个虚拟专用网 VPN 解决企业内部资源的安全访问问题。

8.2 SSL VPN 基础

8.2.1 功能特点

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。

8.2.2 技术特点

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。

Cisco ASA 防火墙提供了两种 SSL VPN 模式：无客户端 WebVPN 和 AnyConnect VPN。无客户端 WEBVPN 模式中，用户的计算机不需要安装 VPN 客户端，只需打开 Web 浏览器，输入 ASA 防火墙的 IP 地址，通过了身份认证，即可通过防火墙进行内部网络的 Web 访问。但没有完整的网络访问。

使用客户端 Anyconnect 的 VPN 可以提供完全的网络访问。远程用户将使用 anyconnect 客户端连接到 ASA 防火墙，并将从 VPN 池接收 IP 地址，从而允许完全访问网络。

在本实验中，我们将使用无客户端 WebVPN 来安装 anyconnect VPN 客户端。远程用户将打开 Web 浏览器，输入 ASA 的 IP 地址，然后它将自动下载 anyconnect VPN 客户端并建立连接。

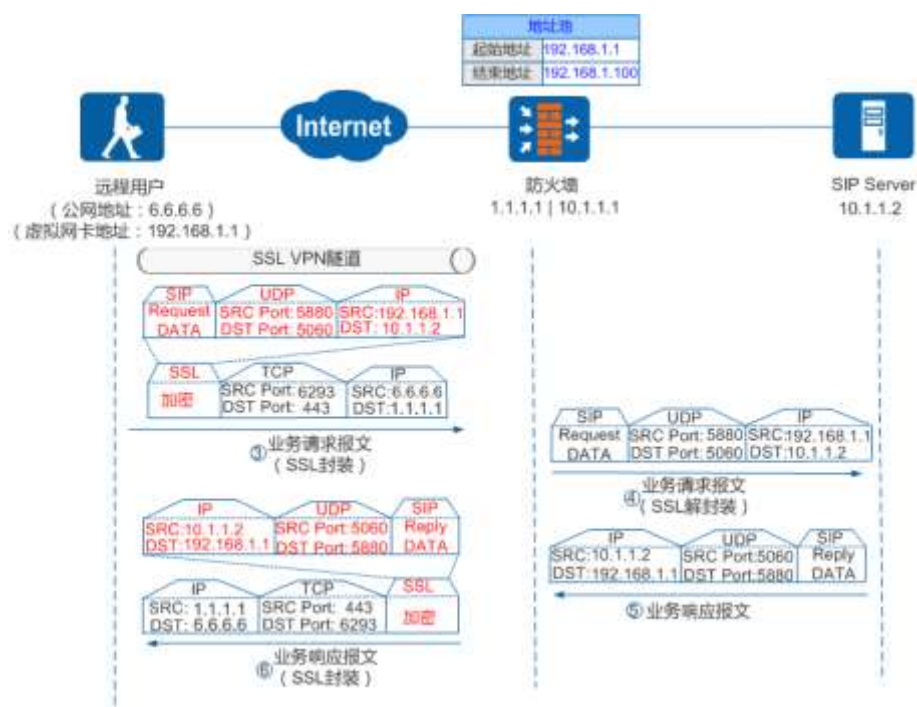


图 8-1 SSL VPN 的工作原理图

图 8-1 给出了一个典型的 SSLVPN 的工作原理图，远程用户与内部网络的 SIP 服务器的通信，完全被封装在一个 SSL 隧道中传输，内容是加密的，所以在公网中也是安全的。

8.3 实验规划及拓扑结构

8.3.1 需要的设备及环境

CISCO ASA5505 防火墙设备 1 台；4 台计算机 PC1 到 PC4 分别承担不同角色和作用。

图 8-2 给出了在 CISCO ASA5505 防火墙上进行 SSLVPN 配置的组网图。图中的参数只作为参考，鼓励各小组灵活自定义 IP 等参数。

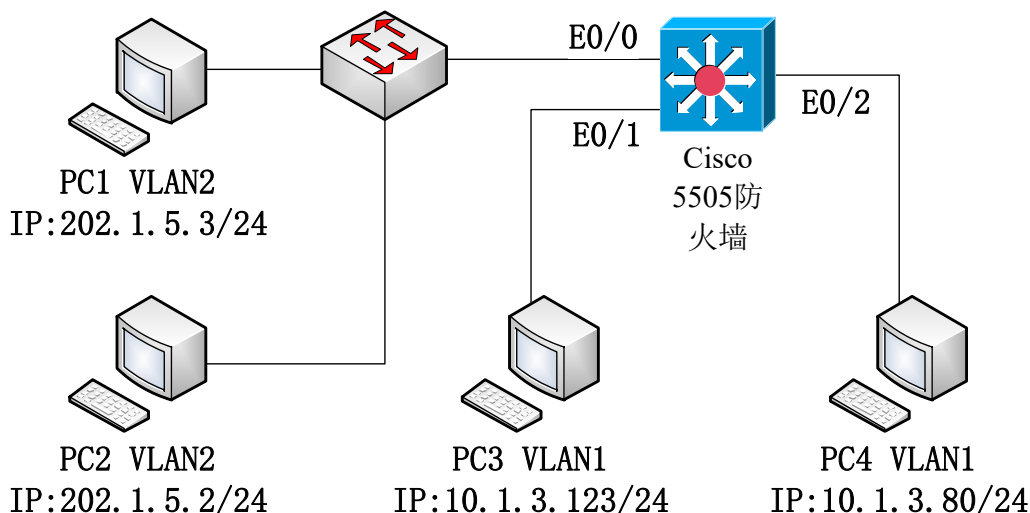


图 8-2 SSL VPN 组网图

8.3.2 实验的主要工作

- 1) 检查 CISCO ASA5505 防火墙设备状态，查看该设备上有关的软件系统。SSL VPN 的支持软件为 anyconnect-win-2.2 开头的文件；
- 2) 按照实验设计图连接有关设备；为 CISCO ASA5505 划分 vlan 和接口，vlan1 是其缺省值，包含了所有的 8 个以太网接口；激活有设备连接的接口；
- 3) 为 CISCO ASA5505 配置 dhcp 服务，该服务可以为内部网络和外部网络分配 IP 地址；
- 4) 配置 SSL VPN 参数；
- 5) 配置 WEB VPN 隧道组与组策略；
- 6) 在组策略中启用 SSL VPN；
- 7) 创建 SSL VPN 用户，并将策略赋予用户；
- 8) 在外部客户端启动 SSL VPN，浏览内部 PC 上的 Web 资源，同时捕获有关报文；
- 9) 在内部客户端浏览另一个内部 PC 上的 Web 资源，同时捕获有关报文；
- 10) 对捕获有关报文进行对比分析。

8.4 实验主要步骤

实验前需将防火墙和交换机恢复出厂设置，参考命令如下：

交换机：

```
Switch> enable    !进入特权用户模式
Switch# set default !启动初始化
Are you sure? [Y/N] = y    ! 确认初始化，显示初始化信息
Switch# write    ! 写入初始化信息到启动文件
Switch# reload    ! 重新启动交换机
```

先查看防火墙版本号，参考命令：

```
ciscoasa> enable
Password:          !直接敲回车
ciscoasa#show version
```

```
ciscoasa> enable
Password:
ciscoasa# show version

Cisco Adaptive Security Appliance Software Version 7.2(4)
Device Manager Version 5.2(4)

Compiled on Sun 06-Apr-08 13:39 by builders
System image file is "disk0:/asa724-k8.bin"
Config file at boot was "startup-config"
```

如果为 Version 8.0，可以直接进行“恢复出厂设置”操作；如果为 Version 7.2，则需要先升级，参考命令：

```
ciscoasa> enable
ciscoasa#config t
ciscoasa(config)#no boot system disk0:/asa702-k8.bin
ciscoasa(config)#boot system disk0:/asa802-k8.bin
ciscoasa(config)#exit
ciscoasa#reload
```

升级重启完毕后，提示“**Pre-configure Firewall now through interactive prompts [yes]?**”时输入“**N**”，登录设备，查看版本号，版本号为 Version 8.0 表示升级成功。

```
Cryptochecksum (changed): d41d8cd9 8f00b204 e9800998 ecf8427e
Pre-configure Firewall now through interactive prompts [yes]? n

Type help or '?' for a list of available commands.
ciscoasa> enable
Password:
ciscoasa# show version

Cisco Adaptive Security Appliance Software Version 8.0(2)
Device Manager Version 5.2(4)
```

防火墙恢复出厂设置：

```
ciscoasa> enable          !进入特权模式，回应 Password: 时按回车。
ciscoasa#write erase       !清除当前设备全部配置，恢复到出厂状态。
Erase configuration in flash memory? [confirm] Y
ciscoasa#reload           !重新启动设备。
Proceed with reload? [confirm] Y
Pre-configure Firewall now through interactive prompts [yes]? N !注意不要选错
```

按照拓扑图连接有关设备，设置各 PC 的 IP 地址和**网关**。

步骤 1：为 CISCO ASA5505 划分 vlan 和接口

```
ciscoasa# config t      ! 进入配置模式
```

```

ciscoasa(config)# show switch vlan      ! 查看系统目前配置
ciscoasa(config)# interface vlan 2      ! 创建 vlan 2, 进入接口配置模式
ciscoasa(config-if)#
ciscoasa(config-if)# nameif outside     ! 命名 vlan 2 为 outside, 安全级别缺省为 0
ciscoasa(config-if)# ip address 202.1.5.1 255.255.255.0    ! 为 vlan 2 设置 ip
ciscoasa(config-if)# q
ciscoasa(config)# interface vlan 1      ! 进入 vlan 1
ciscoasa(config-if)# nameif inside      ! 命名 vlan 1 为 inside, 安全级别缺省为 100
ciscoasa(config-if)# ip address 10.1.3.1 255.255.255.0
ciscoasa(config-if)# show ip

```

步骤 2: 为 Vlan 分配接口并开启

```

ciscoasa(config)# interface e0/0        ! 进入设备 0 号端口
ciscoasa(config-if)# switchport access vlan 2    ! 0 端口分到 vlan 2, 其余在 vlan 1
ciscoasa(config-if)# no shutdown        ! 开启 0 号端口
ciscoasa(config-if)# show interface vlan 2      ! 查看 vlan 2 的全部配置参数

```

同理开启 vlan 1 的 e0/1 和 e0/2 端口, 观察其配置参数和状态

```

ciscoasa(config)# show switch vlan      ! 查看 vlan 的端口分配情况

```

步骤 3: 启用 HTTP 服务及内网 DHCP 服务器

```

ciscoasa(config)# http server enable    ! 开启 http server
ciscoasa(config)# http 10.1.3.0 255.255.255.0 inside    ! 配置 DHCP Server
ciscoasa(config)# dhcpd address 10.1.3.2-10.1.3.33 inside !内部用户地址池
ciscoasa(config)# dhcpd enable inside    ! 启动内部 DHCP
ciscoasa(config)# show dhcpd state      ! 查看 dhcpd 状态

```

步骤 4: 在外网口上启动 WEBVPN, 并同时启动 SSL VPN 功能

接下来启动 SSL VPN, 并指定 SSL VPN Client 的软件包文件名, **注: 如果发生错误, 可能名字不对, 请从防火墙上用 dir 查看具体软件包名字。**

```

ciscoasa(config)# webvpn                ! 配置 WebVPN 服务
ciscoasa(config-webvpn)# enable outside    ! 在外网口上启动 WEBVPN
ciscoasa(config-webvpn)# svc image disk0:/anyconnect-win-2.0.0343-k9.pkg
ciscoasa(config-webvpn)# svc enable
ciscoasa(config)# show webvpn svc        ! 查看 webvpn 服务状态

```

步骤 5: 创建 SSL VPN 用户 IP 地址池 ssluser

```

ciscoasa(config)# ip local pool ssluser 10.10.10.1-10.10.10.10
ciscoasa(config)# access-list go-vpn permit ip 10.1.3.0 255.255.255.0 10.10.10.0 255.255.255.0 !定义存取控制列表 go-vpn
ciscoasa(config)# show access-list
ciscoasa(config)# nat (inside) 0 access-list go-vpn    !对 inside 访问不做 NAT 翻译
ciscoasa(config)# show nat

```

步骤 6: WEB VPN 隧道组与策略组的配置

创建名为 *mypolicy* 的组策略，并为其配置内部组策略特性：设置隧道协议类型 *webvpn*，并在组策略中启用 *SSL VPN*

```
ciscoasa(config)# group-policy mypolicy internal
ciscoasa(config)# group-policy mypolicy attributes
ciscoasa(config-group-policy)# vpn-tunnel-protocol webvpn
ciscoasa(config-group-policy)# webvpn
ciscoasa(config-group-webvpn)# svc enable
ciscoasa(config-group-webvpn)# exit
ciscoasa(config-group-policy)# exit
ciscoasa(config)#
```

步骤 7: 创建 SSL VPN 用户 *vpnuser1* 和 *vpnuser2*，赋予访问策略

大概步骤是：先创建用户及密码，再把组策略赋予用户，然后定义 *webvpn* 类型的隧道组 *mytg*，并使用地址池 *ssluser*。最后进入隧道组 *mytg* 的 *webvpn-attributes* 命令模式，为隧道组起别名 *vpntest*，简化 SSLVPN 用户访问。

```
ciscoasa(config)# username vpnuser1 password vpnuser1
ciscoasa(config)# username vpnuser1 attributes
ciscoasa(config-username)# vpn-group-policy mypolicy
ciscoasa(config-username)# exit
ciscoasa(config)# tunnel-group mytg type webvpn
ciscoasa(config)# tunnel-group mytg general-attributes
ciscoasa(config-tunnel-general)# address-pool ssluser
ciscoasa(config-tunnel-general)# exit
ciscoasa(config)#
ciscoasa(config)# tunnel-group mytg webvpn-attributes
ciscoasa(config-tunnel-webvpn)# group-alias vpntest enable
ciscoasa(config-tunnel-webvpn)# exit
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# tunnel-group-list enable
ciscoasa(config-webvpn)# exit
ciscoasa(config)# write
```

步骤 8: 在内部 PC4 ([10.1.3.80](#)) 上创建测试用 Web 资源服务

启动 HFS (*http file server*)，添加共享文件资源，设置内部 IP (*exp* 接口的地址) 和端口 (*80*)，构建一个可以供外部 VPN 用户访问的 Web 服务。在本机和另外一台内部 PC 上用浏览器测试。

步骤 9: 在外网 PC1 和 PC2 用 SSLVPN 接入并下载内部 Web 资源。

1) 在浏览器中输入 <https://202.1.5.1> 访问 WEB VPN，在随后弹出的对话框中输入用户名和密码单击登陆。两个 PC 的用户名不能取同一个。

2) 系统会弹出要求安装 SSL VPN CLIENT 程序, 单击“YES”, 系统自动安装并连接 SSLVPN, 在 SSLVPN 连通之后在任务栏的右下角会出现一个小锁, 你可以双击打开查看其状态。**如果没有弹出, 可以在 Web 页面手动下载安装。**

3) 在 VPN 软件环境下, 分别以客户端模式和 web 模式访问内部 Web 资源服务器, 并运行 ping 测试网络连通性 (比如在 PC1 ping PC4)。

4) 查看**本地网卡配置, 参考路由表信息 (在 cmd 命令行执行 route print 命令)**, 分析外部 PC 如何通过 VPN 安全访问服务器上的资源。

注: 如果 VPN 用户重新登陆时提示登陆失败, 需要在防火墙中注销已登陆的 VPN 用户, 参考命令:

```
ciscoasa(config)# vpn-sessiondb logoff all
```

步骤 10: 捕获报文并分析

分别在内网和外网(web 模式和客户端模式)请求 Web 资源服务器(PC4, 10.1.3.80)上的同一个资源并捕获报文, 分析几种模式的差别, 解释外部 PC 通过 VPN 访问内网的安全性。

备注: 抓包分析时, 需在 PC 机 (exp 网卡、虚拟网卡) 和服务器端同时抓包, 分析访问的整体过程。

8.5 进阶自设计

分别在校内网和外网 (通过校园 VPN 服务 <http://vpn.xjtu.edu.cn/>) 访问校内资源, 通过抓包分析对比三种模式 (内网访问、外网 WebVPN 访问和外网 SSLVPN 访问) 的访问过程及相关参数 (**物理网卡/虚拟网卡参数、路由表、通信协议、数据包源/目的地址等**)。

8.6 CISCO ASA5505 防火墙其它参考命令

序号	命令	含义
1	Ciscoasa>enable	进入特权模式#, 提示 Password 时按回车键
2	ciscoasa#dir	查看文件系统
3	ciscoasa#config t	进入配置模式 ciscoasa(config)#
4	ciscoasa#?	查看当前模式下的可用命令或参数
5	ciscoasa#show IP	查看当前配置的 IP
6	ciscoasa#show switch vlan	查看 VLAN 配置
7	ciscoasa#show webvpn svc	查看 SSLVPN 提供给客户端的可用文件
8	ciscoasa(config)#q	退出当前命令模式
9	ciscoasa# show run	查看系统目前配置

8 实验八 防火墙与 SSLVPN 实验

10	ciscoasa# show route	查看路由表
11	ciscoasa# no 命令	取消命令的原有结果
12	ciscoasa#write erase	清除当前设备全部配置，恢复到出厂状态。Erase configuration in flash memory? [confirm] Y
13	ciscoasa#reload	重新启动设备。Proceed with reload? [confirm] Y Pre-configure Firewall now through interactive prompts [yes]? N

9 选做实验

说明：选做实验使用 eNSP 来实现，实验题目中选做 1 个以上。
涉及到使用 3 个三层端口，模拟设备选用 AR2220。



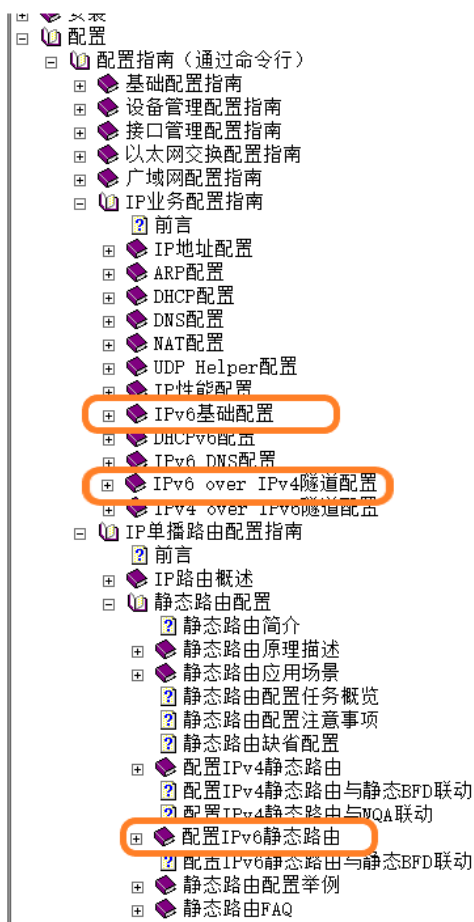
1 选做实验一：IPv6 与路由

1.1 实验介绍

1.1.1 关于本实验

本实验重点帮助同学理解 IPv6 地址以及转发，以及 IPv4/IPv6 过渡技术；IPv6 路由协议与 IPv4 模型很相似，本实验不再重点配置，有兴趣的同学可以参考相关配置手册自行验证。

实验参考相应的产品文档，本实验可参考章节如下：



1.1.2 实验目的

- 掌握 IPv6 地址
- 掌握 IPv6 基础路由转发
- 掌握 IPv4/IPv6 过渡隧道技术

1.2 IPv6 地址配置

1.2.1 说明

以 1 号 PC 为例：

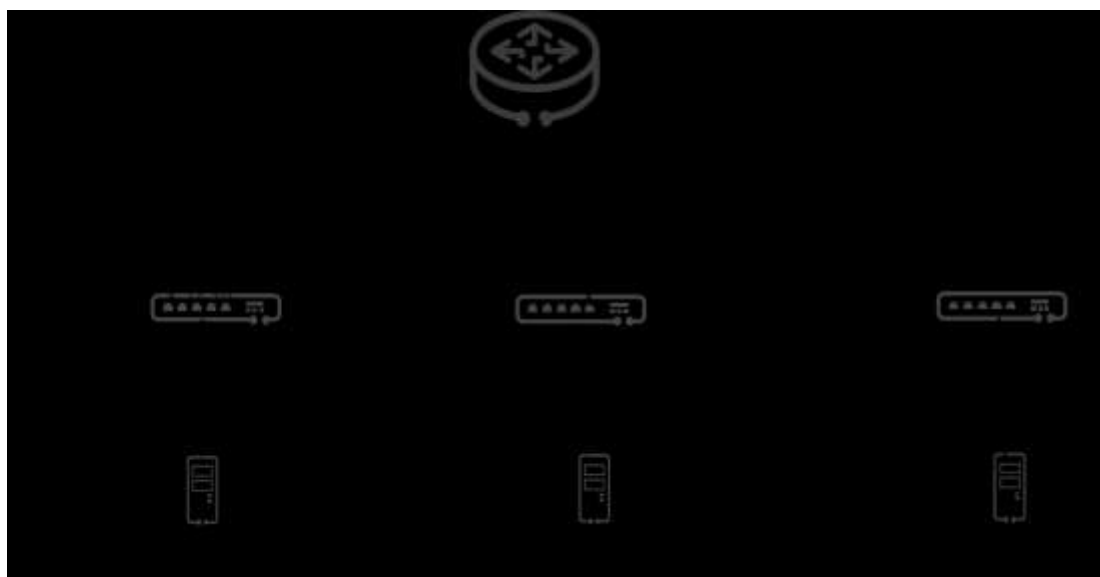
- 1) PC 机地址配置为 `fc00:1::2/64`，对应的接入交换机 VLANIF 接口地址配置为 `fc00:1::1/64`；
- 2) 交换机至 AR 间接口地址配置为 `fc00:101::1/64`，AR 接口地址配置为 `fc00:101::2/64`

1.2.1.1 实验任务

- 1) 配置交换机与 PC 机间的接口 IPv6 地址
- 2) 配置交换机与 AR 间的接口 IPv6 地址

1.2.2 实验组网

交换机、路由器 都支持 IPv4/IPv6 双栈部署，本实验组网可以继续沿用 IPv4 组网。



1.2.3 操作步骤

```
# 配置 Switch 1。  
[Switch_1] ipv6                //整机使能 ipv6  
  
[Switch_1] interface vlanif 10  
[Switch_1-Vlanif10] ipv6 enable //接口使能 ipv6
```

```
[Switch_1-Vlanif10] ipv6 address fc00:1::1/64
[Switch_1-Vlanif10] quit

[Switch_1] interface vlanif 100
[Switch_1-Vlanif10] ipv6 enable    //接口使能 ipv6
[Switch_1-Vlanif10] ipv6 address fc00:101::1/64
[Switch_1-Vlanif10] quit
```

其它的交换机配置类似，这里不做具体描述

```
# 配置 AR1
[AR_1] ipv6    //整机使能 ipv6
[AR_1] interface gigabitethernet 0/0/0
[AR_1-GigabitEthernet0/0/0] undo portswitch
[AR_1-GigabitEthernet0/0/0] ipv6 enable
[AR_1-GigabitEthernet0/0/0] ipv6 address fc00:101::2/64
```

AR 其它接口配置类似，这里不做具体描述

1.2.4 实验验证

- 1) PC 机能够 ping 通 fc00:101::1
- 2) 交换机上 能够 ping ipv6 通 fc00:101::2

1.3 IPv6 静态路由

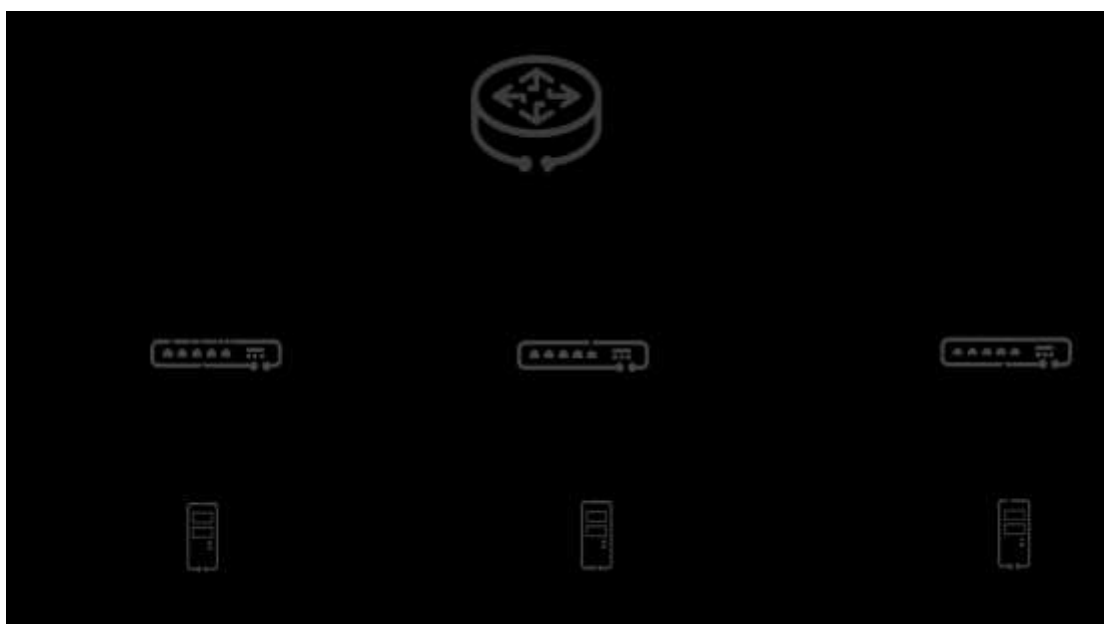
1.3.1 说明

IPv6 静态路由与 IPv4 静态路由模型很类似，参考配置即可。

1.3.2 实验任务

在 AR 路由器上配置 fc00:200::1/64 这个地址，这个地址不通过路由协议发布。通过配置静态路由方式，PC 机能够 ping 通此地址。

1.3.3 实验组网



1.3.4 操作步骤

交换机上相关 IP 配置沿用 5.2 配置.

- 1) AR 路由器增加一个 IP 地址 fc00:200::1/64

```
[AR_1]interface loopback 0
[AR_1_Loopbak0] ipv6 enable
```

```
[AR_1_Loopbak0] ipv6 address fc00:200::1/64
```

- 2) 交换机上配置 fc00:200::1 的静态路由

```
[Switch_1] ipv6 route-static fc00:200::1 64 vlanif100
fc00:101::2
```

- 3) AR 路由器上配置至 fc00:1::1/64 网段的静态路由

```
[AR_1] ipv6 route-static fc00:1::1 64 gigabitethernet 0/0/0
fc00:101::1
```

1.3.5 实验验证

- 1) PC 机能够 ping 通 fc00:200::1

1.4 IPv4/IPv6 过渡(高阶)

1.4.1 说明

由于 IPv4 地址的枯竭和 IPv6 的先进性，IPv4 过渡为 IPv6 势在必行。因为 IPv6 与 IPv4 的不兼容性，所以需要对原有的 IPv4 设备进行替换。但是如果贸然将 IPv4 设备大量替换所需成本会非常巨大，且现网运行的业务也会中断，显然并不可行。所以，IPv4 向 IPv6 过渡是一个渐进的过程。

在过渡初期，IPv4 网络已经大量部署，而 IPv6 网络只是散落在各地的“孤岛”，IPv6 over IPv4 隧道就是通过隧道技术，使 IPv6 报文在 IPv4 网络中传输，实现 IPv6 网络之间的孤岛互连。

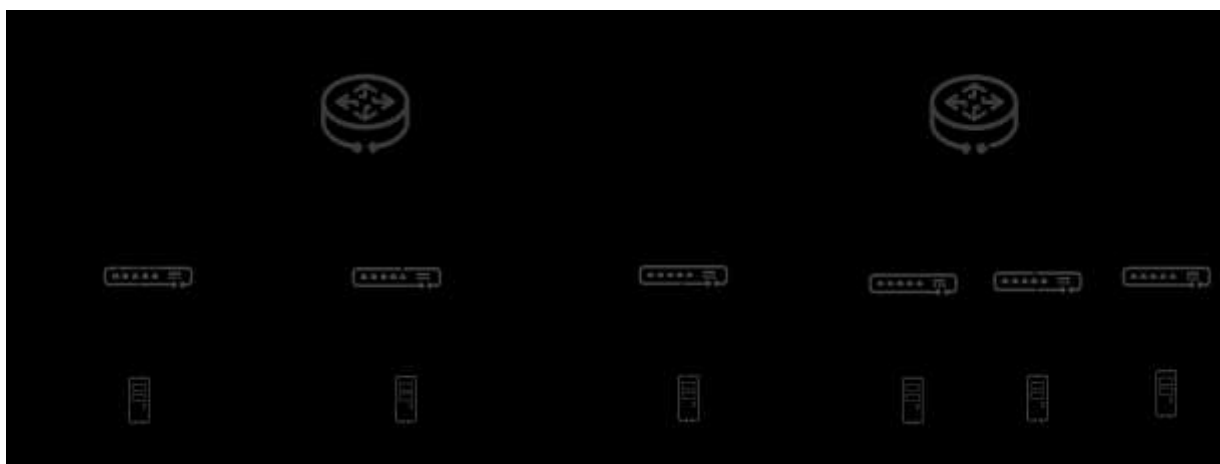
IPv6 过渡技术有多种，本实验验证 IPv6 over IPv4 隧道技术中的手工隧道技术

1.4.2 实验任务

完成两组 IPv6 组网间的 IPv6 over IPv4 隧道。

1.4.3 实验组网

两组 AR 间启用 IPv6 over IPv4 隧道。



1.4.4 操作步骤

交换机上相关 IP 配置沿用 5.3 配置. AR 间接口地址参见 4.6

1) AR1 路由器增加 Ipv6 隧道

```
# 配置协议类型为 IPv6-IPv4。
[AR_1] interface tunnel 0/0/1
[AR_1-Tunnel0/0/1] tunnel-protocol ipv6-ipv4
# 配置隧道接口的 IPv6 地址、源接口、目的地址。
[AR_1-Tunnel0/0/1] ipv6 enable
[AR_1-Tunnel0/0/1] ipv6 address fc00:220::1/64
[AR_1-Tunnel0/0/1] source gigabitethernet 0/0/3
[AR_1-Tunnel0/0/1] destination 150.10.70.2
[AR_1-Tunnel0/0/1] quit
```

2) AR1 路由器配置 路由入 IPv6 隧道

```
[AR_1] ipv6 route-static fc00:4::64 tunnel0/0/1
[AR_1] ipv6 route-static fc00:5::64 tunnel0/0/1
[AR_1] ipv6 route-static fc00:6::64 tunnel0/0/1
```

3) AR2 路由器增加 Ipv6 隧道，入隧道路由

类似配置，这里不做描述

4) 交换机 1 上配置 fc00:200::1 的静态路由

```
[Switch_1] ipv6 route-static fc00:200::1 64 vlanif100
fc00:101::2
[Switch_1] ipv6 route-static fc00:4::1 64 vlanif100
fc00:101::2
[Switch_1] ipv6 route-static fc00:5::1 64 vlanif100
fc00:101::2
[Switch_1] ipv6 route-static fc00:6::1 64 vlanif100
fc00:101::2
```

1.4.5 实验验证

- 1) Switch1 上能 ping 通 4 交换机 fc00:4::1 地址，命令为 ping ipv6 fc00:4::1
- 2) PC 机 1 能够 ping 通 fc00:4::2 地址

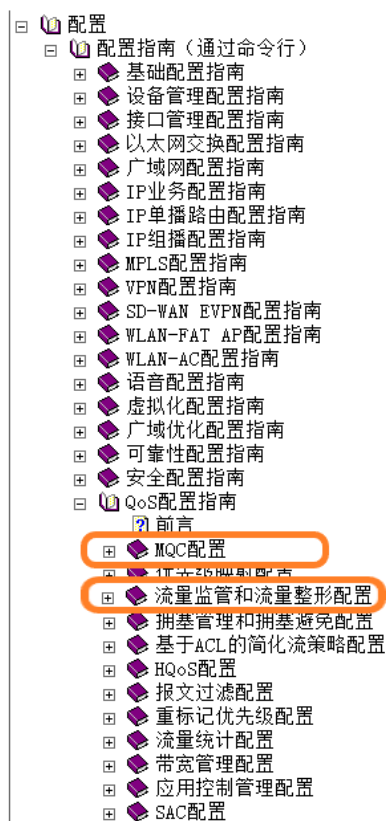
2 选做实验二：QoS

2.1 实验介绍

2.1.1 关于本实验

服务质量 QoS（Quality of Service）用于评估服务方满足客户服务需求的能力。通过配置 QoS，对企业的网络流量进行调控，避免并管理网络拥塞，减少报文的丢失率，同时也可以为企业用户提供专用带宽或者为不同的业务（语音、视频、数据等）提供差分服务。

实验参考相应的产品文档，本实验可参考章节如下：



2.1.2 实验目的

- 掌握 MQC 原理和配置方法
- 掌握流量监管原理和配置方法。

2.2 MQC 原理和配置方法

2.2.1 说明

模块化 QoS 命令行 MQC（Modular QoS Command-Line Interface）是指通过将具有某类共同特征的报文划分为一类，并为同一类报文提供相同的服务，也可以对不同类的报文提供不同的服务。

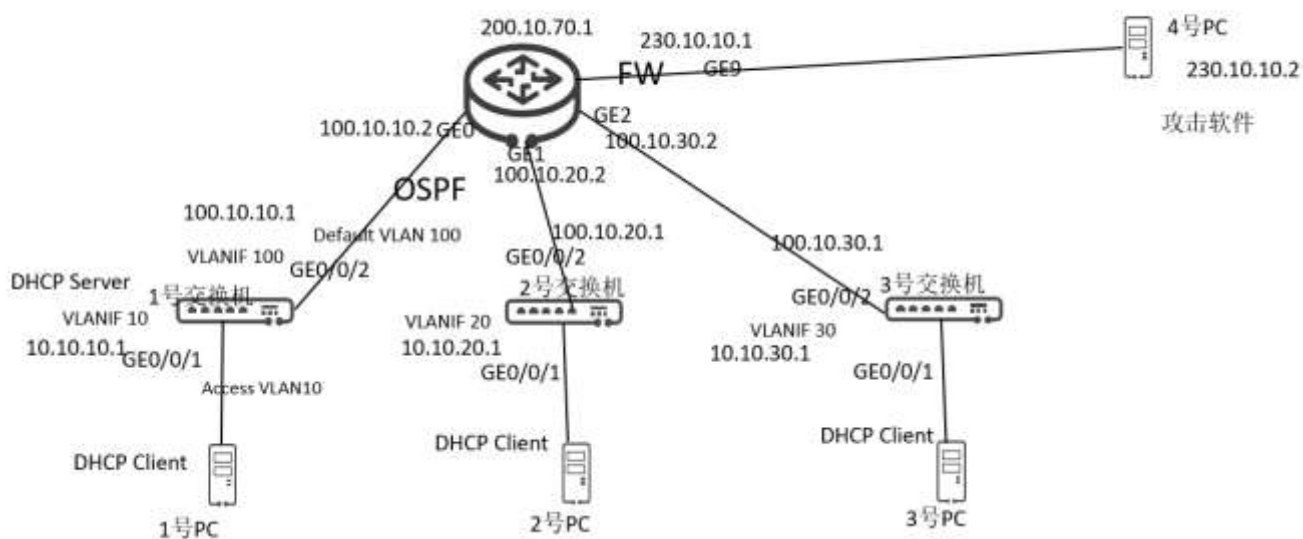
随着网络中 QoS 业务的不断丰富，在网络规划时若要对不同流量（如不同业务或不同用户）的差分服务，会使部署比较复杂。MQC 的出现，使用户能对网络中的流量进行精细化处理，用户可以更加便捷的针对自己的需求对网络中的流量提供不同的服务，完善了网络的服务能力。

MQC 包含三个要素：流分类（traffic classifier）、流行为（traffic behavior）和流策略（traffic policy）。

2.2.2 实验任务

使用 MQC，统计各位 PC 的报文发送个数。

2.2.3 实验组网



2.2.4 操作步骤

物理实验室环境在交换机、路由器上都可以完成此功能。

eNSP 仿真只能在路由器上完成该功能，并且**路由器需要选择 AR2240**。

本实验配置以物理环境上 1 号交换机配置举例。其它环境配置类似：

1) 创建流分类

a) 配置匹配 PC1 的 ACL，假设 PC1 地址为 10.10.10.253

```
[Switch_1] acl 3001
```

```
[Switch_1-acl-adv-3001] rule permit ip source 10.10.10.253 0
```

b) 创建流分类

创建流分类 c_pc1，匹配 acl 3001，目的地址是 pc2 的报文。

```
[Switch_1] traffic classifier c_pc1
```

```
[Switch_1-classifier-c_pc1] if-match acl 3001
```

```
[Switch_1-classifier-c_pc1] quit
```

2) 配置流行为：

创建流行为 b_pc2，动作为 statistic，即统计匹配指定规则的报文。

```
[Switch_1] traffic behavior b_statis
```

```
[Switch_1-behavior-b_statis] statistic enable
```

```
[Switch_1-behavior-b_statis] quit
```

3) 配置流策略

创建流策略 p_pc1_statis，绑定流分类 c_pc1 和流行为 b_statis。

```
[Switch_1] traffic policy p_pc1_statis
```

```
[Switch_1-trafficpolicy-p_pc1_statis] classifier c_pc1 behavior b_statis
```

```
[Switch_1-trafficpolicy-p_pc1_statis] quit
```

4) 应用流策略

在接口 GE0/0/1 的入方向应用流策略 p1。

```
[Switch_1] interface gigabitethernet 0/0/1
```

```
[Switch_1-GigabitEthernet0/0/1] traffic-policy p_pc1_statis inbound
[Switch_1-GigabitEthernet0/0/1] quit
```

2.2.5 实验验证

1) PC 间 ping 报文时，查看统计计数

```
disp traffic policy statistics interface GigabitEthernet 0/0/1 inbound
```

```
Interface: GigabitEthernet0/0/1
Traffic policy inbound: pc1-statis
Rule number: 1
Current status: OK!
```

Item	Sum(Packets/Bytes)
Rate(pps/bps)	

Matched	10/
1/	
	980
184	
+--Passed	10/
1/	
	980
184	
+--Dropped	0/
0/	
	0
0	
+--Filter	0/
0/	
	0
0	
+--CAR	0/
0/	
	0
0	
+--Queue Matched	0/
0/	
	0

0		
0/	+-Enqueued	0/
0		0
0/	+-Discarded	0/
0		0
0/	+-Car	0/

2.3 流量监管和流量整形

2.3.1 说明

流量监管和流量整形通过监督进入网络的流量速率，用来限制流量及其资源的使用，保证更好的为用户提供服务。

如果报文的发送速率大于接收速率，或者下游设备的接口速率小于上游设备的接口速率，就会引起网络拥塞。如果不限制用户发送的业务流量，大量用户不断突发的业务数据会使网络更加拥挤。为了使有限的网络资源能够更好地发挥效用，更好地为更多的用户服务，必须对用户的业务流量加以限制。

流量监管和流量整形就是一种通过对流量规格的监督，来限制流量及其资源使用的流控策略。

1) 流量监管

流量监管 TP (Traffic Policing) 就是对流量进行控制，通过监督进入网络的流量速率，对超出部分的流量进行“惩罚”，使进入的流量被限制在一个合理的范围之内，从而保护网络资源和用户的利益。

2) 流量整形

流量整形 TS (Traffic Shaping) 是一种主动调整流量输出速

率的措施。当下游设备的入接口速率小于上游设备的出接口速率或发生突发流量时，下游设备入接口处可能出现流量拥塞的情况，此时用户可以通过在上游设备的接口出方向配置流量整形，将上游不规整的流量进行削峰填谷，输出一条比较平整的流量，从而解决下游设备的拥塞问题。

流量整形与流量监管的主要区别在于，流量整形对原本要被丢弃的报文进行缓存，当令牌桶有足够的令牌时，再均匀的向外发送这些被缓存的报文。流量整形与流量监管的另一区别是，整形可能会增加延迟，而监管几乎不引入额外的延迟。

本实验只实现流量监管

2.3.2 实验任务

调整每台 PC 允许的最大带宽，观察流量限制情况

2.3.3 实验组网

AR WAN 侧 GE8 端口与 4 号 PC 机相连，4 号 PC 机模拟外网的网络攻击。

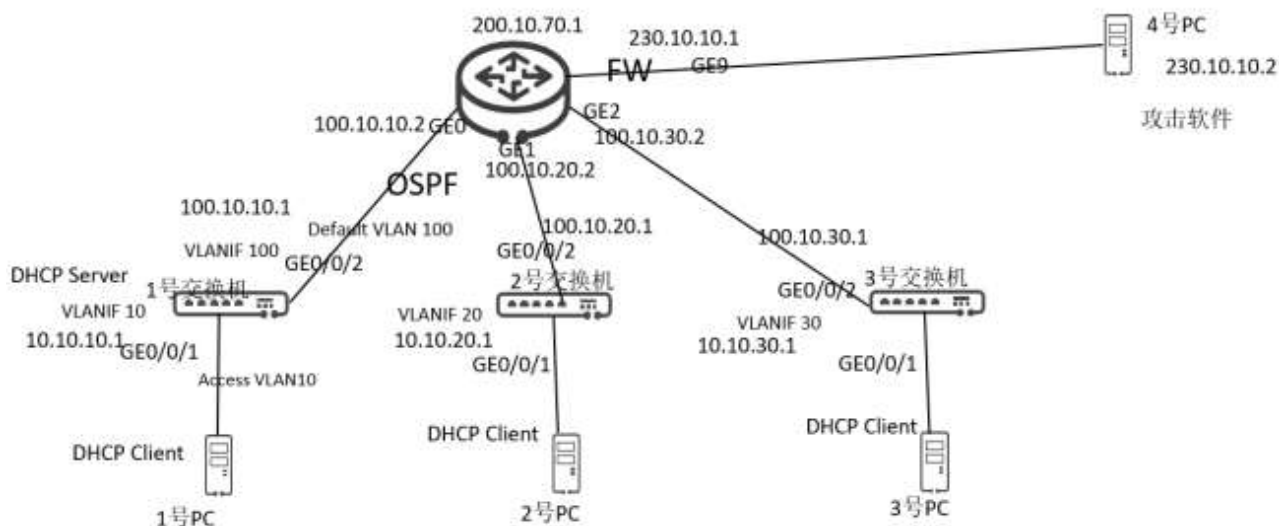


图2-1 物理环境组网

2.3.4 操作步骤

物理实验室环境在交换机、路由器上都可以完成此功能。

eNSP 仿真交换机不支持，只能在路由器上完成该功能，并且**路由器需要选择 AR2240**。

本实验配置以物理环境上 1 号交换机配置举例。其它环境配置类似：

1) 创建流分类，匹配 PC 机发送的流量

a) 配置匹配 PC1 的 ACL，假设 PC1 地址为 10.10.10.253

```
[Switch_1] acl 3001
[Switch_1-acl-adv-3001] rule permit ip source 10.10.10.253 0
```

b) 创建流分类

创建流分类 c_pc1，匹配 acl 3001，目的地址是 pc2 的报文。

```
[Switch_1] traffic classifier c_pc1
[Switch_1-classifier-c_pc1] if-match acl 3001
[Switch_1-classifier-c_pc1] quit
```

2) 配置流行为：

创建流行为 b_car，动作为限速，即超过一定带宽报文会被丢弃。

```
[Switch_1] traffic behavior b_car
[Switch_1-behavior-b_statis] car cir 8           // 配置 cir 速率为 8k
```

[Switch_1-behavior-b_statis] statistic enable //可选，配置后可以查看统计信息

```
[Switch_1-behavior-b_statis] quit
```

3) 配置流策略

创建流策略 p_pc1_car，绑定流分类 c_pc1 和流行为 b_car。

```
[Switch_1] traffic policy p_pc1_car
```



```
[Switch_1-trafficpolicy-p_pc1_statis] classifier c_pc1 behavior
b_car
[Switch_1-trafficpolicy-p_pc1_statis] quit
```

4) 应用流策略

在接口 GE0/0/1 的入方向应用流策略 p1。

```
[Switch_1] interface gigabitethernet 0/0/1
[Switch_1-GigabitEthernet0/0/1] traffic-policy p_pc1_car
inbound
[Switch_1-GigabitEthernet0/0/1] quit
```

2.3.5 实验验证

- 1) PC1 ping PC2, icmp 报文长度设置为 1400。调整流行为 car 的值，观察是否会出现限速情况
- 2) 若 behavior 下使能过 statistic，则可以查看流策略的命中信息
 <Switch_1>disp traffic policy statistics interface g 0/0/1 inbound

```
Interface: GigabitEthernet0/0/1
Traffic policy inbound: p_pc1_car
Rule number: 2
Current status: OK!
```

Item	Sum(Packets/Bytes)
Rate(pps/bps)	

Matched	2,203/
1/	
	3,223,190
7,912	
+--Passed	1,056/
1/	
	1,517,496
4,216	
+--Dropped	1,147/
1/	
	1,705,694
3,688	
+--Filter	0/

0/		0
0		1,147/
	+--CAR	
1/		1,705,694
3,688		
	+--Queue Matched	0/
0/		0
0		0/
	+--Enqueued	
0/		0
0		0/
	+--Discarded	
0/		0
0		2,203/
	+--Car	
1/		3,223,190
7,912		
	+--Green packets	1,056/
1/		1,517,496
4,216		
	+--Yellow packets	0/
0/		0
0		1,147/
	+--Red packets	
1/		1,705,694
3,688		

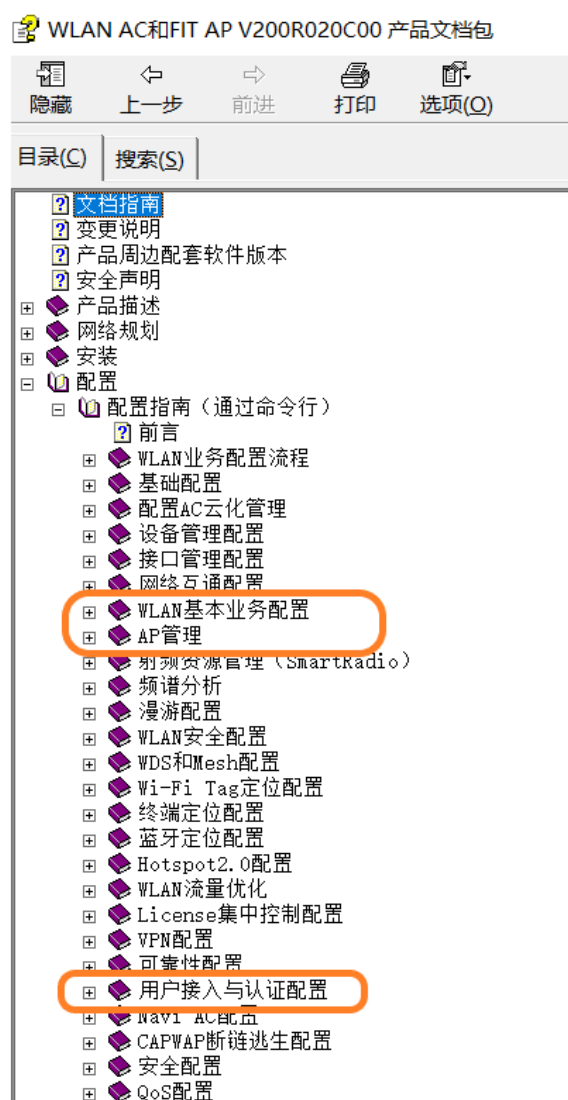
3 选做实验三：WLAN 配置

3.1 实验介绍

3.1.1 关于本实验

本实验完成 AP 接入 AC，终端接入至 WLAN 网络。

实验参考相应的产品文档，本实验参考无线接入控制器 (AC 和 FIT AP) V200R021C00 产品文档，可参考章节如下：



3.1.2 实验目的

- 掌握 WLAN 组网模型和配置方法
- 掌握 AP 接入 AC 配置方法

- 掌握终端安全接入配置方案

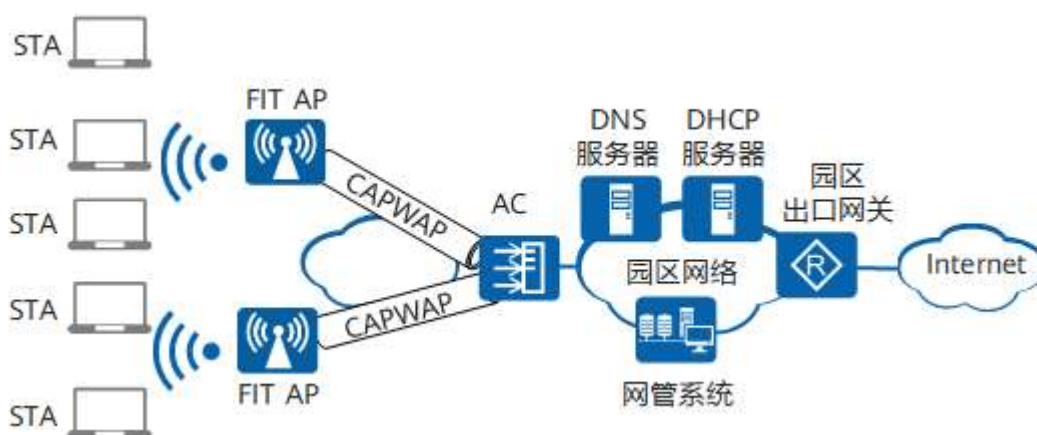
3.2 WLAN 网络架构&AP 接入网络

3.2.1 WLAN 网络架构

3.2.1.1 说明

WLAN 网络架构分有线侧和无线侧两部分，有线侧是指 AP 上行到 Internet 的网络使用以太网协议。无线侧是指 STA 到 AP 之间的网络使用 802.11 协议。无线侧接入的 WLAN 网络架构为集中式架构。

集中式架构又分为瘦接入点（FIT AP）架构和敏捷分布 Wi-Fi 方案架构。本实验只介绍 FIT AP 接入方式。



所有无线接入功能由 AP 和 AC 共同完成：

- AC 集中处理所有的安全、控制和管理功能，例如移动管理、身份验证、VLAN 划分、射频资源管理和数据包转发等。

- FIT AP 完成无线射频接入功能，例如无线信号发射与探测响应、数据加密解密、数据传输确认等。

- AP 和 AC 之间采用 CAPWAP 协议进行通讯，AP 与 AC 间可以跨越二层网络或三层网络。

用户接入无线网络的过程分两步：

1. FIT AP 与 AC 建立 CAPWAP 隧道，详细内容请参见 AP 接入网络过程。

2. STA 与 FITAP 的关联过程，详细内容请参见 STA 接入过程。

3.2.2 AP 接入网络

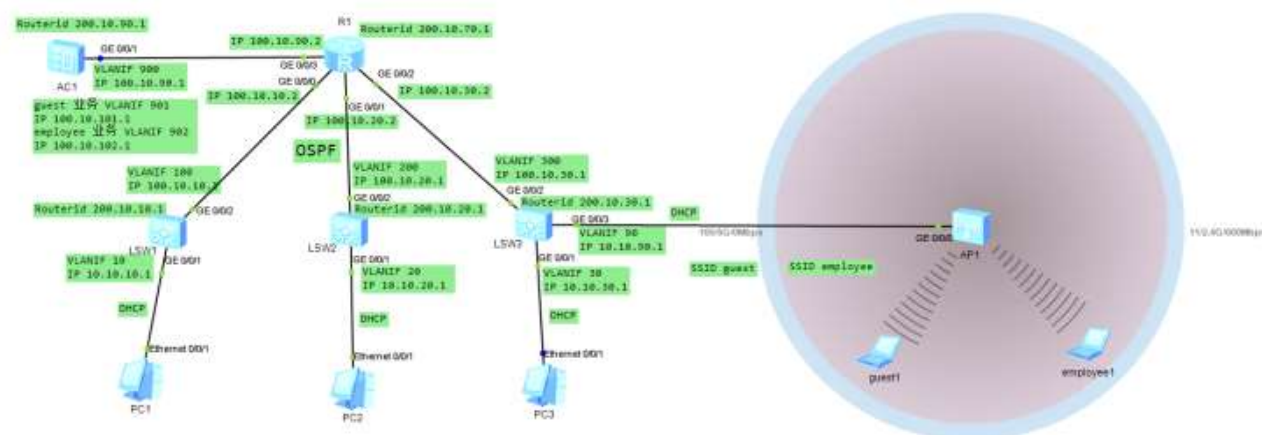
3.2.2.1 说明

本实验完成 FIT AP 接入网络过程

3.2.2.2 实验任务

AP 通过 CAPWAP 隧道接入 AC:

3.2.2.3 实验组网



3.2.2.4 操作步骤

以 1 号交换机配置举例，假设查询 2 号 PC 地址为 10.10.20.1:

1) 配置 AC 接入至网络中

#配置 AC 与 AR1 间接口地址。

AC 与交换机类似，需要采用 VLANIF 配置三层接口

#配置 AC 与 AR1 间启用 OSPF

AC 与交换机类似

2) 配置 AP 接入至网络中

以 AP 接在 LSW3, LSW3 作为 L3 交换机为例:

LSW3 配置 AP 接入的 VLANIF 接口

LSW3 配置 DHCP 服务, 为 AP 分配 IP 地址, 并告知 AP 接入 AC 的地址

#

interface Vlanif90

ip address 10.10.90.1 255.255.255.0

dhcp select interface

dhcp server option 43 sub-option 2 ip-address **100.10.90.1** //通过 DHCP option 告知 AP 接入 AC 的地址

#

3) 配置 AP 上线

#配置 capwap 隧道,允许 AP 与其建立 capwap 隧道
[AC]capwap source interface vlanif 200

#配置 AP 接入控制策略

[AC] wlan //系统试图下进入 WLAN 视图

[AC-wlan-view] ap auth-mode mac-auth // AC 上对 AP

接入认证, 缺省使用 AP mac 进行认证

#找到 AP mac 地址, 配置允许接入的 AP 白名单

查看 ap 上线失败, 会发现接入失败的 AP 信息

[AC6605-wlan-view]dis ap online-fail-record all

Info: This operation may take a few seconds. Please wait for a moment.done.

```
-----
--
MAC                               Last fail time           Reason
-----
--
00e0-fcb1-1a80    2022-04-29/08:43:15      Not in MAC
whitelist
-----
```

--
配置允许该 AP 接入到网络中

```
[AC6605-wlan-view]ap-mac 00e0-fcb1-1a80
```

3.2.2.5 实验验证

1) AP 能够接入至 AC 中

```
<AC6605>disp ap all
```

```
Info: This operation may take a few seconds. Please wait for a moment.done.
```

```
Total AP information:
```

```
nor : normal [1]
```

```
-----
ID      MAC              Name              Group      IP
Type              State ST
A Uptime
-----
0        00e0-fcb1-1a80  00e0-fcb1-1a80  default  10.10.90.254
AP4030TN          nor    0
11M:32S
-----
-----
```

```
Total: 1
```

3.3 终端接入网络

3.3.1 终端接入网络

3.3.1.1 说明

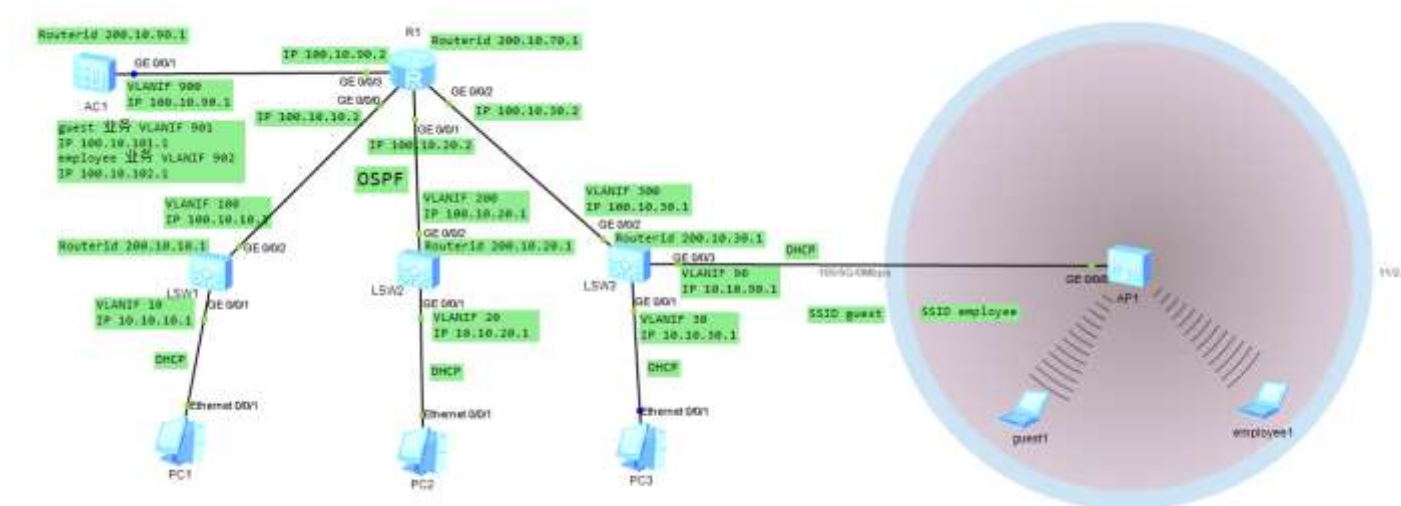
网络中会部署多个 **SSID**，提供不同服务。同时为了保证接入安全，需要配置不同的安全策略。

3.3.1.2 实验任务

部署 2 个 **SSID**，分别为访客、员工提供业务。举例中以配置 WPA2+PSK+AES 的安全策略为例，密码分别为“a1234567”和

“b1234567”，实际配置中请根据实际情况，配置符合实际要求的安全策略。

3.3.1.3 实验组网



3.3.1.4 操作步骤

1) 创建 SSID 模板

创建名为“guest”和“employee”的 SSID 模板，并分别配置 SSID 名称为“guest”和“employee”。

```
[AC-wlan-view] ssid-profile name guest
[AC-wlan-ssid-prof-guest] ssid guest
[AC-wlan-ssid-prof-guest] quit
[AC-wlan-view] ssid-profile name employee
[AC-wlan-ssid-prof-employee] ssid employee
[AC-wlan-ssid-prof-employee] quit
```

2) 创建安全策略

#配置 WPA2+PSK+AES 的安全策略

```
[AC-wlan-view] security-profile name guest
```



```

[AC-wlan-sec-prof-guest] security wpa2 psk pass-phrase
a1234567 aes
[AC-wlan-sec-prof-guest] quit
[AC-wlan-view] security-profile name employee
[AC-wlan-sec-prof-employee] security wpa2 psk pass-phrase
b1234567 aes
[AC-wlan-sec-prof-employee] quit

```

3) 创建 VAP 模板

创建名为“guest”和“employee”的 VAP 模板，配置业务数据转发模式、业务 VLAN，并且引用安全模板和 SSID 模板

```

[AC-wlan-view] vap-profile name guest
[AC-wlan-vap-prof-guest] forward-mode tunnel
[AC-wlan-vap-prof-guest] service-vlan vlan-id 901 //guest 业务 VLAN 901,从 guest SSID 上线的用户，数据报文会加上这个 VLAN,通过 capwap 隧道到达 AC.AC 侧需要能够处理此 VLAN
[AC-wlan-vap-prof-guest] security-profile guest
[AC-wlan-vap-prof-guest] ssid-profile guest
[AC-wlan-vap-prof-guest] quit

[AC-wlan-view] vap-profile name employee
[AC-wlan-vap-prof-employee] forward-mode tunnel
[AC-wlan-vap-prof-employee] service-vlan vlan-id 902 // employee 业务 VLAN 902
[AC-wlan-vap-prof-employee] security-profile employee
[AC-wlan-vap-prof-employee] ssid-profile employee
[AC-wlan-vap-prof-employee] quit

```

#AC 上配置业务 VLAN

```
[AC6605]vlan batch 901 902
```

#创建 vlanif 901/902 接口。需要注意，GE0/0/1 接口同时绑定多个 VLAN，需要变更 link-type 为 Trunk

```

interface GigabitEthernet0/0/1
port link-type trunk

```

```

port trunk pvid vlan 900
port trunk allow-pass vlan 900 to 902
#

#guest ssid 接入用户的 vlan
interface Vlanif901
ip address 100.10.101.1 255.255.255.0
dhcp select interface
# employee ssid 接入用户的 vlan
interface Vlanif902
ip address 100.10.102.1 255.255.255.0
dhcp select interface
#

```

4) AP 引用 VAP 模板

配置 AP 组引用 VAP 模板，AP 上所有射频使用 VAP 模板的配置。

```

[AC-wlan-view] ap-group name default
[AC-wlan-ap-group-default] vap-profile guest wlan 1 radio all
[AC-wlan-ap-group-default] vap-profile employee wlan 2 radio
all
[AC-wlan-ap-group-default] quit

```

3.3.1.5 实验验证

- 1) Guset1 PC 、 employee1 PC 都能上线

```

<AC6605>display station all
Rf/WLAN: Radio ID/WLAN ID
Rx/Tx: link receive rate/link transmit rate(Mbps)

```

```

-----
-----
STA MAC          AP ID Ap name      Rf/WLAN
Band  Type  Rx/Tx    RSSI  VLAN
      IP address  SSID
-----
-----

```

```

-----
5489-989f-20b4 0 00e0-fcb1-1a80 0/2 2.4G -
-/- - 902
100.10.102.214 employee
5489-98e0-6ff9 0 00e0-fcb1-1a80 0/1 2.4G -
-/- - 901
100.10.101.178 guest
-----

```

```

-----

```

```

-----
Total: 2 2.4G: 2 5G: 0

```

- 2) Guest1 PC 能够访问 1 号 PC
- 3) Guset1 PC 能够访问 employee1 PC

4 选做实验四：校园园区网搭建

4.1 实验介绍

4.1.1 关于本实验

使用已经学习到的网络技术，组合构建一张校园园区网络。

4.1.2 实验目的

综合运用网络技术，实践网络工程能力

4.1.3 实验内容

4.1.3.1 说明

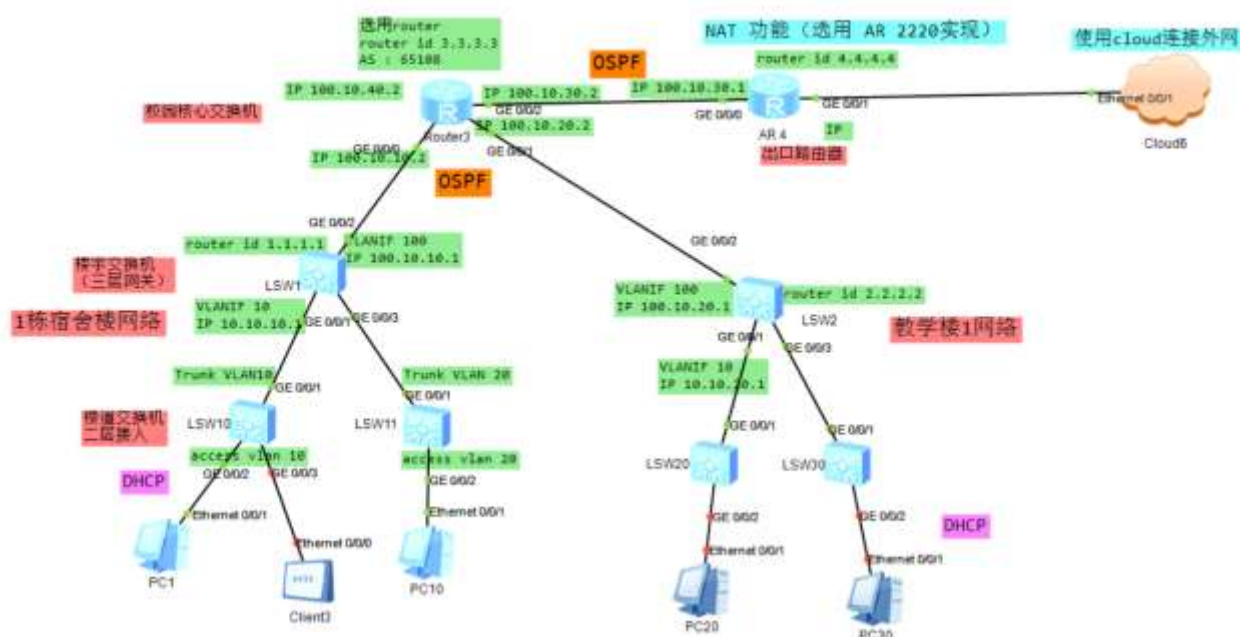
模拟部署校园网，校区内园区网络包括宿舍区、教学区，出口区域包括 **Internet** 区域

4.1.3.2 实验任务

需要同学们规划一张网络，要求：

- 1) 宿舍区、教学区 PC 都可以接入网络，含 IPv4；部署一台 **Http client**，模拟访问 **baidu** 页面
- 2) 宿舍区、教学区需要规划 **VLAN**，避免广播域过大。实验中可以每台接入交换机 1VLAN。
- 3) IP 网关部署在大楼的汇聚交换机上
- 4) 汇聚/核心/**Internet** 间 采用 **OSPF** 发布路由
- 5) 路由器至 **Internet** 静态路由
- 6) **Internet** 需要部署 **NAT**
- 7) 需要通过 **Cloud** 绑定 PC 机有线网口接入 **Internet**
- 8) 扩展实验：两位同学的网络通过 **Cloud**，构建更大的网络

4.1.3.3 实验组网



4.1.3.4 部署思路

- 1) 规划 VLAN，隔离接入交换机，接入交换机不能在汇聚交换机二层互通
- 2) 规划私网 IP 地址，校园网内唯一。IP 地址不能与实验手册相同，需独立规划；部署 DHCP 方式获取 IP 地址，DNS 地址 114.114.114.114
- 3) 路由协议设计：围绕核心交换机 OSPF，Internet 出口部署静态路由，并在 OSPF 中引入缺省路由(配置 default-route-advertise)。
- 4) Internet 出口部署 NAT，安全(暂不实现)

4.1.3.5 Cloud 部署说明

Cloud 的主要作用是将 eNSP 所模拟的虚拟设备（例如路由器、交换机、防火墙等）与运行该 eNSP 的真实 PC 进行连接，从而实现

虚拟设备与真实 PC 的连接。

使用 Cloud 用于模拟连接 PC 机上有线网卡，将 eNSP 内部网络与外部连通。

4.1.3.5.1 部署与 Internet 互联 Cloud

部署思路：无线网卡可以接入 Internet；PC 机上创建一个环回网卡，无线网卡共享网络给环回网卡。

eNSP 通过 Cloud 绑定环回网卡，从而接入校园网。

需要注意的是这种方式数据在 PC 机内部是走三层路由以及 NAT 转发。

1) PC 机创建环回网卡/环回适配器

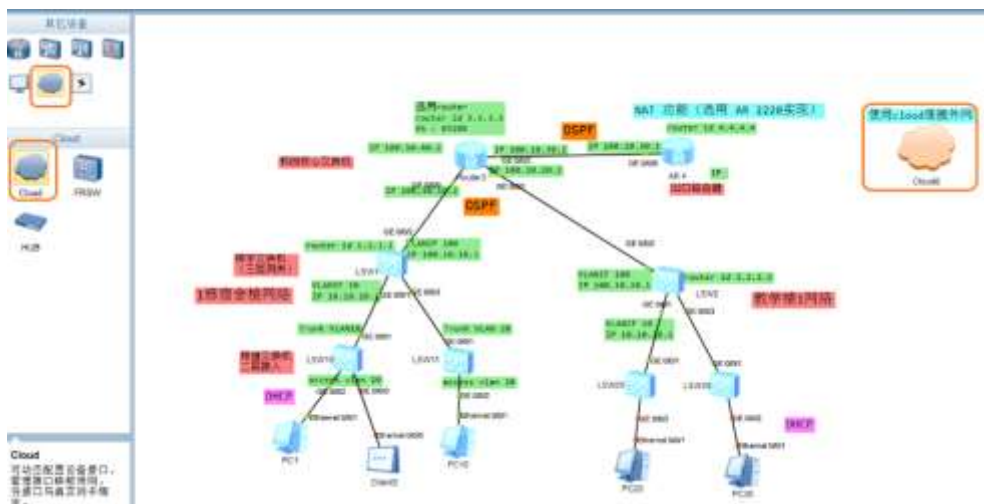
参考 https://blog.csdn.net/m0_59331971/article/details/125015332

2) 将无线网卡共享给环回网卡

参考 <https://cloud.tencent.com/developer/article/1678119>

需要注意 windows 网络共享后环网卡地址会变成 192.168.137.1

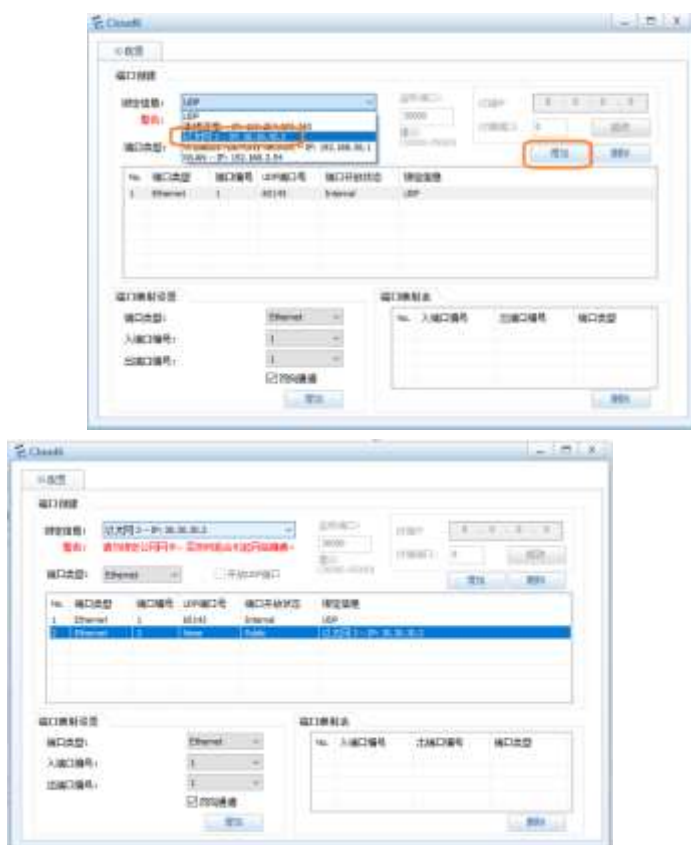
3) 部署 Cloud



4) 增加 eNSP 内部端口



5) 选择网卡



选择环回网卡，这个 IP 地址为 192.168.137.1，图片中未刷新
若选择时未找到环回网卡，可以参考如下解决方案。

<https://blog.csdn.net/csdnxiaohua/article/details/125617590>。若未找到 winpcap，找一下 npcap，卸载后重新安装 winpcap。

2 台 PC 机通过有线以太网卡接在一起。2 个 eNSP 网络通过 Cloud 绑定有线以太网卡，此时相当于是通过以太网连在一起。

这种方式数据在 PC 机内部是走二层转发，因此如 OSPF 等协议报文都可以互通。

4.1.3.6 实验验证

- 1) 各区域 PC 能够互 ping 通
- 2) 可访问 Internet，通过 client 模拟访问百度网页，能看到有回复消息
- 3) 扩展实验：两位同学的两个 eNSP 网络，通过 Cloud 连接，OSPF 发布路由