计算机网络实验

杭州电子科技大学
HANGZHOU DIANZI UNIVERSITY

徐建 编

二〇一六年

目录

实验一 网线制作

【实验目的】

掌握非屏蔽双绞线的RJ-45接头的制作方法、非屏蔽双绞线直通电缆的制作方法及剥线钳、压线钳和网线测试仪的使用方法。

【实验环境及器材】

非屏蔽5类双绞线若干米，RJ-45水晶头若干，用于剥接水晶头的专用剥线/压线钳，用于测试线缆是否通畅的网线测试仪。

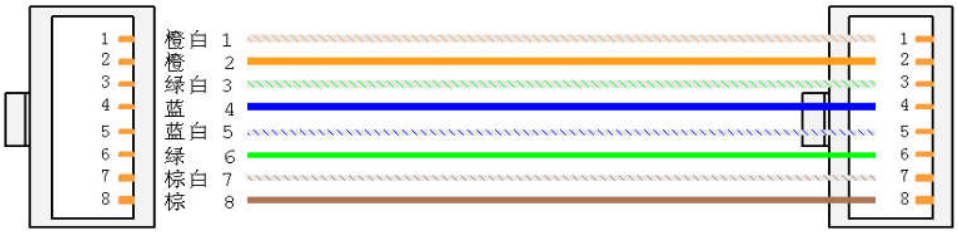
【实验内容 】

1、取一根双绞线用剥线/压线钳将其两端的最外层线皮剥去；

2、将剥好的双绞线根据T568B标准

（即白橙，橙，白绿，蓝，白蓝，绿，白棕，棕）的排

线顺序进行排线（如下图）；



3、将排好的双绞线用手摆平捋直且不要松手，用剥线/压线钳将八根线的线头绞成一样长短；

4、取一只RJ-45水晶头，将带有铜芯的一侧朝上，将剪好的双绞线送入水晶头内并用剥线/压线钳将其压好；

5、用同样的方法将另一端也进行以上操作；

6、用网线测试仪测试线缆是否通畅。

实验二 基本报文分析

【实验目的】

1、理解 IP 层的作用以及 IP 地址的分类方法；

2、理解子网的划分和子网掩码的作用；

3、掌握 IP 数据包的组成和网络层的基本功能；

【实验环境】

图2-1实验拓扑图

【实验内容】

1、学会根据 IP 地址的分类方式区分各类 IP 地址；

2、掌握 IP 数据报的格式、长度以及各字段的功能；

3、学会利用子网掩码确定 IP 地址的网络号、子网号和主机号；

4、学会分析给定数据包的 IP 首部信息；

5、学会手工计算 IP 校验和的方法；

【实验流程】

1、安装wireshark；

2、熟悉软件使用；

3、分析IP数据包格式；

4、抓包分析http、ping等协议。

【实验原理】

网际协议 IP 是 TCP/IP 协议栈的心脏，也是网络层中最重要的协议。目前几乎所有的上层网络协议都是基于 IP 协议。在接收数据的时候，网络层接收由数据链路层发送的数据包进行解封装，并把该数据包发送到更高层——传输层，在发送数据的时候，网络层接受由传输层发送的数据包进行 IP 封装，然后把数据报交给下层——数据链路层。

IP 协议处于 TCP/IP 协议栈的网际层，用于管理数据通信中源端和目的端之间的报文传送，是互联网最重要的网际协议。IP 地址是也叫逻辑地址，用于在网络中标识主机。在 IP网络中，主机之间进行通信时使用 IP 地址来指定接收端的主机地址。

数据进行封装过程中，IP层负责将数据封装成 IP包，IPv4数据包报文格式如下图所示。

图2-3 IP 报文格式

如上图所示，在 IP 包中，各字段含义如下所述：

版本：长度为 4 比特，含义为版本号，对于 IPv4 来说，版本号为 4。

报头长度：报头长度字段为 4 比特，用于表示 IP 报头长度，在 IPv4 中，由于选项字段长度可变，因此，报头长度并不固定，报头字节长度为这一字段值的 4 倍。

业务类型：业务类型字段长度为 8 比特，主要用于标识 QOS 服务等级。

总长度：总长度字段共 16 比特，因此 IP 报的最大长度为 65535 字节。

标识符（Identifier）：长度 16 比特。该字段和标识及分段偏移字段联合使用，对大的上层数据包进行分段（fragment）操作。

标记（Flags）：长度 3 比特。该字段第一位不使用，第二位是 DF 位，DF 位设为1 时表明路由器不能对该上层数据包分段。如果一个上层数据包无法在不分段的情况下进行转发，则路由器会丢弃该上层数据包并返回一个错误信息。第三位是 MF位，当路由器对一个上层数据包分段，则路由器会在除了最后一个分段的 IP 包的包头中将 MF 位设为 1。

分段偏移（Fragment Offset）：长度 13 比特。用于指明分片 IP 包在原 IP 包中的偏移量。由于 IP 包在网络上传送的时候不一定能按顺序到达，这个字段保证了目标路由器在接受到 IP 包之后能够还原分段的上层数据包。当某个包含分段的上层数据包的 IP 包在传送时丢失，则整个一系列包含分段的上层数据包的 IP 包都会被要求重传。

生存时间（TTL）：长度 8 比特。当 IP 包进行传送时，先会对该字段赋予某个特定的值。当 IP 包经过每一个路由器的时候，路由器会将 IP 包的 TTL 值减少 1。如果TTL 减少为 0，则该 IP 包会被丢弃。这个字段可以防止由于路由故障而导致 IP 包在网络中不停被转发。

协议号（Protocol）：长度 8 比特。标识了上层所使用的协议。

报头校验和（Header Checksum）：长度 16 位，由于 IP 包头是变长的，所以提供

一个头部校验来保证 IP 包头中信息的正确性。

源和目标地址（Source and Destination Addresses）：这两个地段都是 32 比特。标识了这个 IP 包的起源和目标地址。

可选项（Options）：这是一个可变长的字段。该字段由起源设备根据需要改写。

【实验步骤】

步骤一：设定实验环境

1、参照实验拓扑连接网络拓扑；

2、配置 PC 机及路由器 IP 地址；

步骤二：wireshark安装使用

wireshark是非常流行的网络封包分析软件，功能十分强大。可以截取各种网络封包，显示网络封包的详细信息。使用wireshark的人必须了解网络协议，否则就看不懂wireshark了。

为了安全考虑，wireshark只能查看封包，而不能修改封包的内容，或者发送封包。

wireshark能获取HTTP，也能获取HTTPS，但是不能解密HTTPS，所以wireshark看不懂HTTPS中的内容，总结，如果是处理HTTP,HTTPS 还是用Fiddler, 其他协议比如TCP,UDP 就用wireshark.

wireshark 开始抓包

开始界面

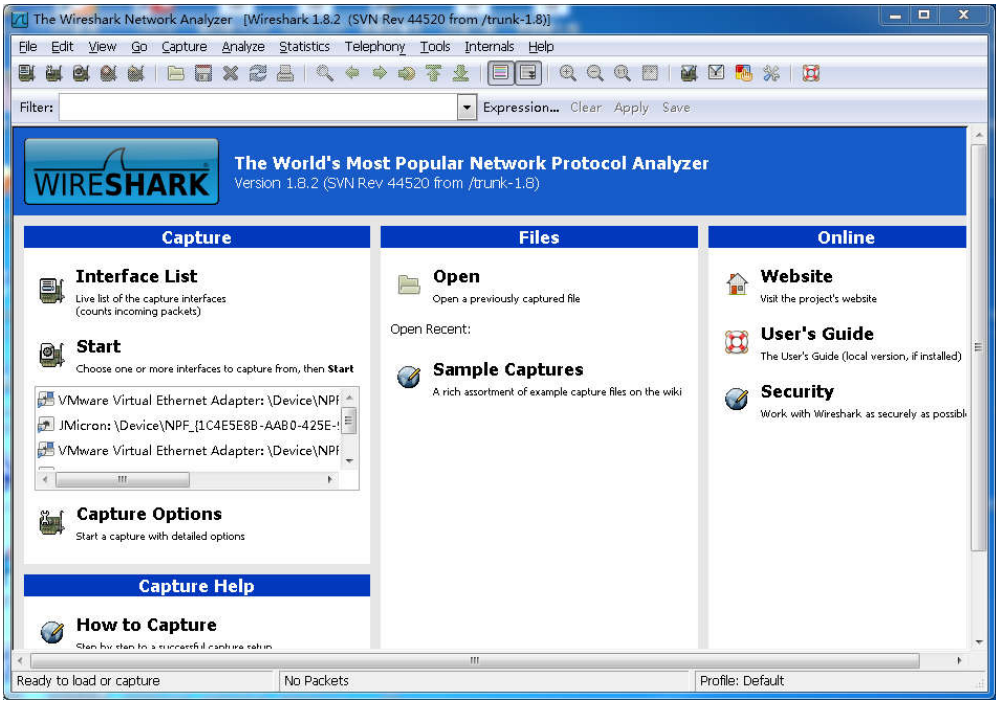


图 2-4

wireshark是捕获机器上的某一块网卡的网络包，当你的机器上有多块网卡的时候，你

需要选择一个网卡。

点击Caputre->Interfaces.. 出现下面对话框，选择正确的网卡。然后点击"Start"按钮，开始抓包

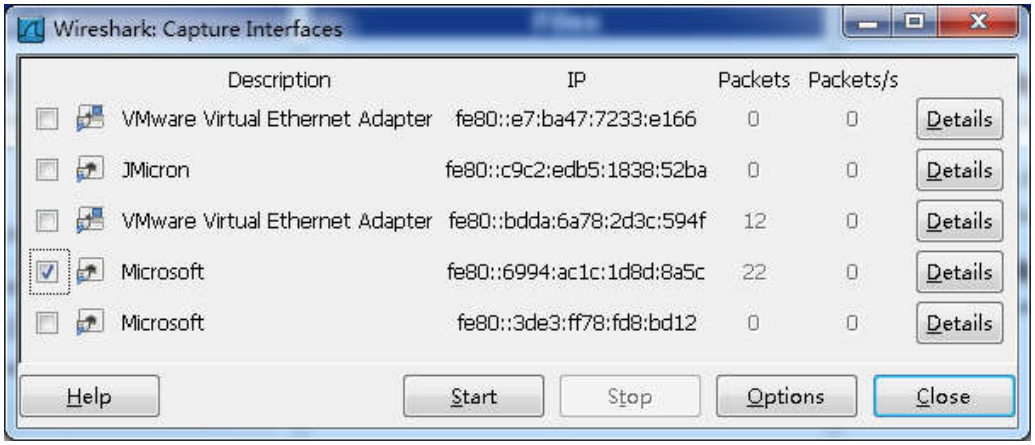


图 2-5

Wireshark 窗口介绍

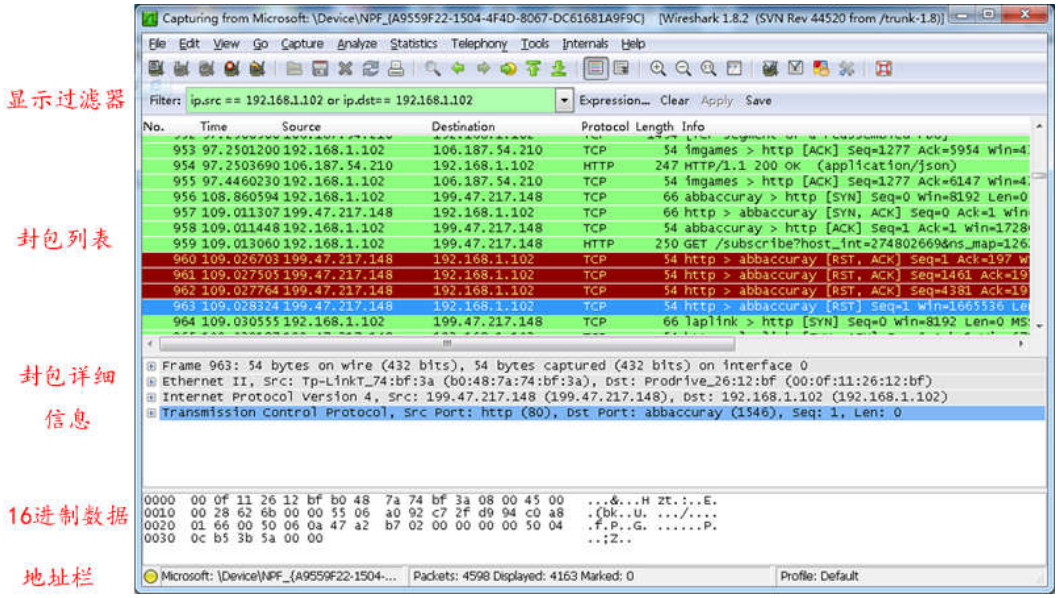


图 2-6

WireShark 主要分为这几个界面

1. Display Filter(显示过滤器)， 用于过滤

2. Packet List Pane(封包列表)， 显示捕获到的封包， 有源地址和目标地址，端口号。

3. Packet Details Pane(封包详细信息)， 显示封包中的字段

4. Dissector Pane(16进制数据)

5. Miscellanous(地址栏，杂项)

Wireshark 显示过滤

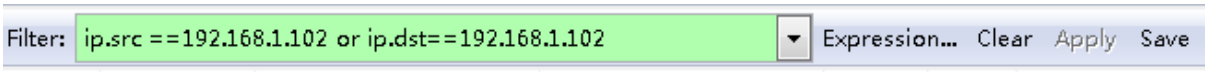


图 2-7

使用过滤是非常重要的， 初学者使用wireshark时，将会得到大量的冗余信息，在几千甚至几万条记录中，以至于很难找到自己需要的部分。搞得晕头转向。

过滤器会帮助我们在大量的数据中迅速找到我们需要的信息。

过滤器有两种，

一种是显示过滤器，就是主界面上那个，用来在捕获的记录中找到所需要的记录

一种是捕获过滤器,用来过滤捕获的封包,以免捕获太多的记录。在Capture -> Capture Filters 中设置

保存过滤

在Filter栏上，填好Filter的表达式后，点击Save按钮， 取个名字。比如"Filter 102",

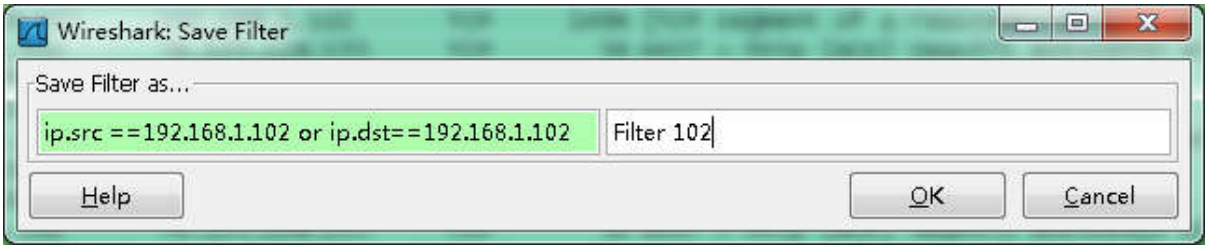
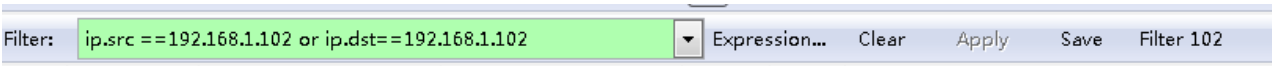


图 2-8

Filter栏上就多了个"Filter 102" 的按钮。



过滤表达式	用途
http	只查看 HTTP 协议的记录
ip.src ==192.168.1.102 or ip.dst==192.168.1.102	源地址或者目标地址是 192.168.1.102

图 2-9

封包列表(Packet List Pane)

封包列表的面板中显示，编号，时间戳，源地址，目标地址，协议，长度，以及封包信息。 你可以看到不同的协议用了不同的颜色显示。

你也可以修改这些显示颜色的规则， View ->Coloring Rules.

No.	Time	Source	Destination	Protocol	Length	Info
265	15.8906110	192.168.1.102	74.125.128.156	TCP	66	[TCP Dup ACK 257#4] 8577 > http [ACK] Seq=372
266	15.8921280	74.125.128.156	192.168.1.102	TCP	1484	[TCP Retransmission] [TCP segment of a reassem
267	15.8921780	192.168.1.102	74.125.128.156	TCP	66	[TCP Dup ACK 257#5] 8577 > http [ACK] Seq=372
268	15.8926100	74.125.128.156	192.168.1.102	TCP	630	[TCP Retransmission] [TCP segment of a reassem
269	15.8926540	192.168.1.102	74.125.128.156	TCP	66	[TCP Dup ACK 257#6] 8577 > http [ACK] Seq=372
270	16.5576320	114.80.142.90	192.168.1.102	HTTP	264	HTTP/1.0 304 Not Modified
271	16.5680360	192.168.1.102	180.168.255.118	DNS	76	Standard query 0x30ee A www.blogjava.net
272	16.5685810	192.168.1.102	180.168.255.118	DNS	75	Standard query 0xd4be A www.cppblog.com
273	16.5695380	192.168.1.102	180.168.255.118	DNS	75	Standard query 0xba0a A www.hujiang.com
274	16.7500800	192.168.1.102	114.80.142.90	TCP	54	8561 > http [ACK] Seq=2094 Ack=421 Win=16860 L
275	16.8642490	114.80.142.90	192.168.1.102	HTTP	264	[TCP Retransmission] HTTP/1.0 304 Not Modifie
276	16.8643460	192.168.1.102	114.80.142.90	TCP	66	[TCP Dup ACK 274#1] 8561 > http [ACK] Seq=2094
277	17.0615280	180.168.255.118	192.168.1.102	DNS	91	Standard query response 0xd4be A 61.155.169.1
278	17.0637590	192.168.1.102	180.168.255.118	DNS	77	Standard query 0x7272 A www.hjenglish.com
279	17.0661740	180.168.255.118	192.168.1.102	DNS	169	Standard query response 0xba0a CNAME www.huji
280	17.0683610	192.168.1.102	180.168.255.118	DNS	74	Standard query 0xa994 A www.chinaz.com
281	17.0690520	180.168.255.118	192.168.1.102	DNS	92	Standard query response 0x30ee A 61.155.169.1
282	17.0753540	192.168.1.102	180.168.255.118	DNS	71	Standard query 0x0a16 A blog.39.net
283	17.1430580	180.168.255.118	192.168.1.102	DNS	175	Standard query response 0x7272 CNAME www.hjer
284	17.1455140	192.168.1.102	180.168.255.118	DNS	75	Standard query 0x5493 A down.admin5.com

图 2-10

封包详细信息（Packet Details Pane）

这个面板是我们最重要的，用来查看协议中的每一个字段。

各行信息分别为

Frame: 物理层的数据帧概况

Ethernet II: 数据链路层以太网帧头部信息

Internet Protocol Version 4: 互联网层IP包头部信息

Transmission Control Protocol: 传输层T的数据段头部信息，此处是TCP

Hypertext Transfer Protocol: 应用层的信息，此处是HTTP协议

wireshark 与对应的 OSI 七层模型

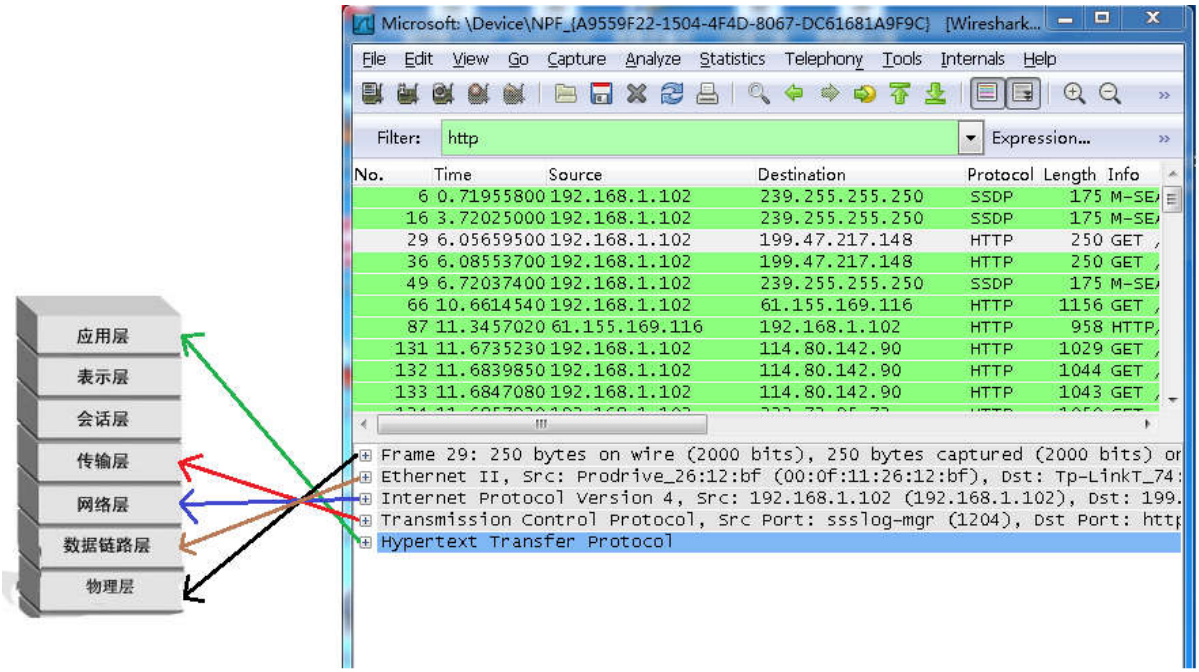


图 2-11

从下图可以看到wireshark捕获到的TCP包中的每个字段。

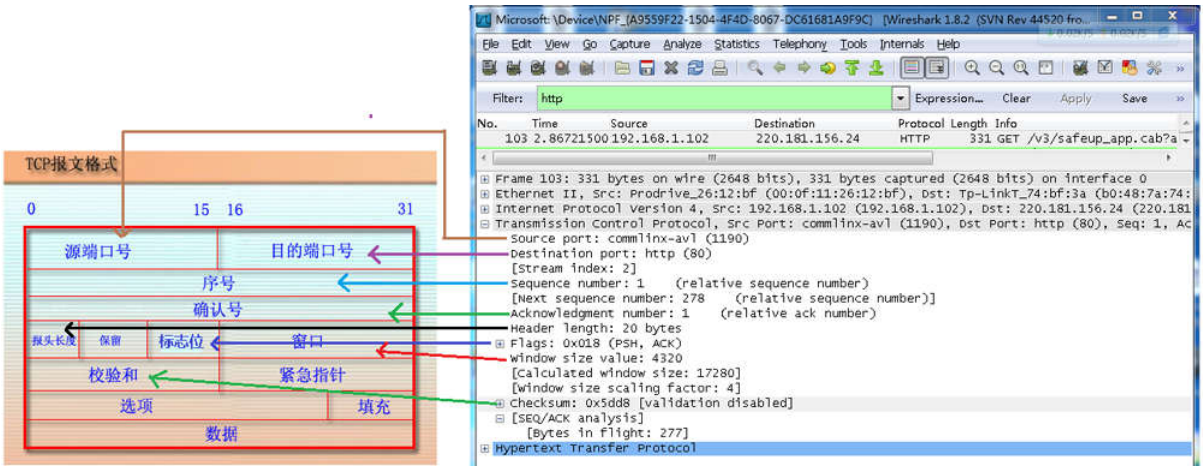


图 2-12

实例分析 TCP 三次握手过程

看到这， 基本上对wireshak有了初步了解， 现在我们看一个TCP三次握手的实例

三次握手过程为

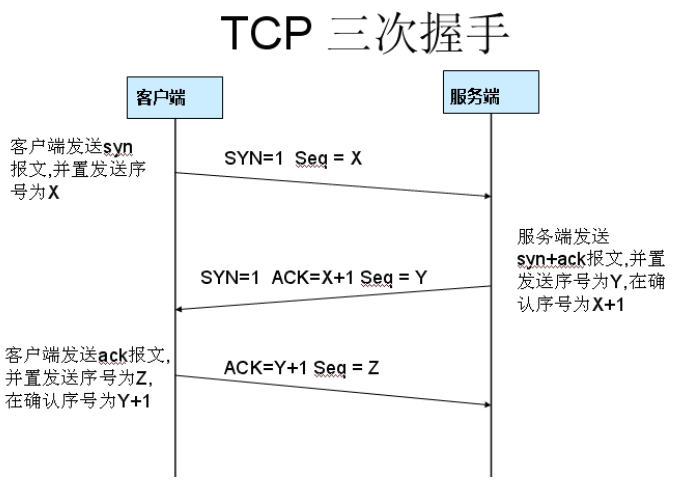


图 2-13

用wireshark实际分析下三次握手的过程。

打开wireshark, 打开浏览器输入某个网站，例如www.hdu.edu.cn

在wireshark中输入http过滤， 然后选中GET / HTTP/1.1的那条记录，右键然后点击"Follow TCP Stream",

这样做的目的是为了得到与浏览器打开网站相关的数据包，将得到如下图

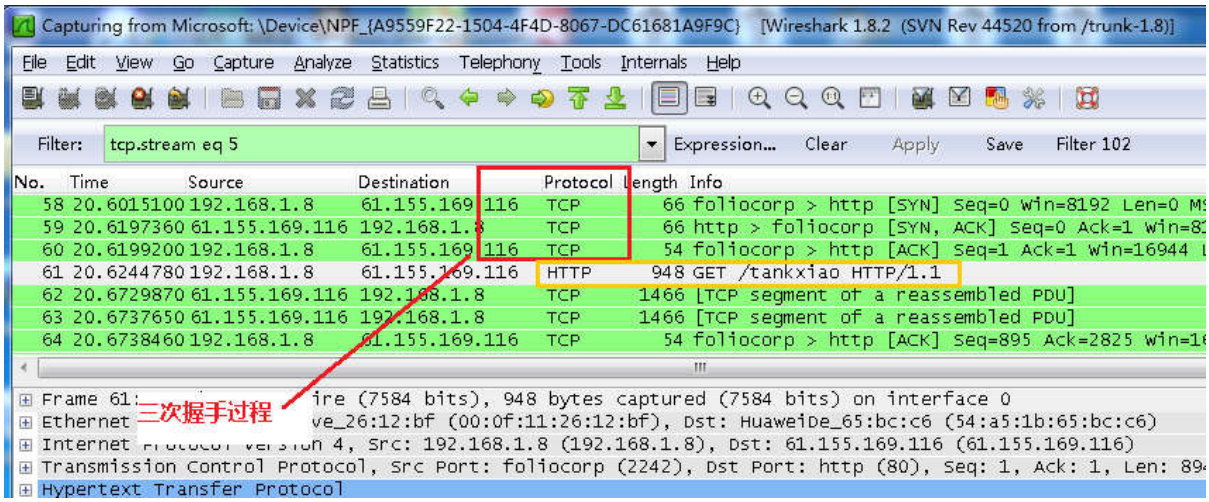


图 2-14

图中可以看到wireshark截获到了三次握手的三个数据包。第四个包才是HTTP的， 这说明HTTP的确是使用TCP建立连接的。

第一次握手数据包

客户端发送一个TCP，标志位为SYN，序列号为0， 代表客户端请求建立连接。 如下图

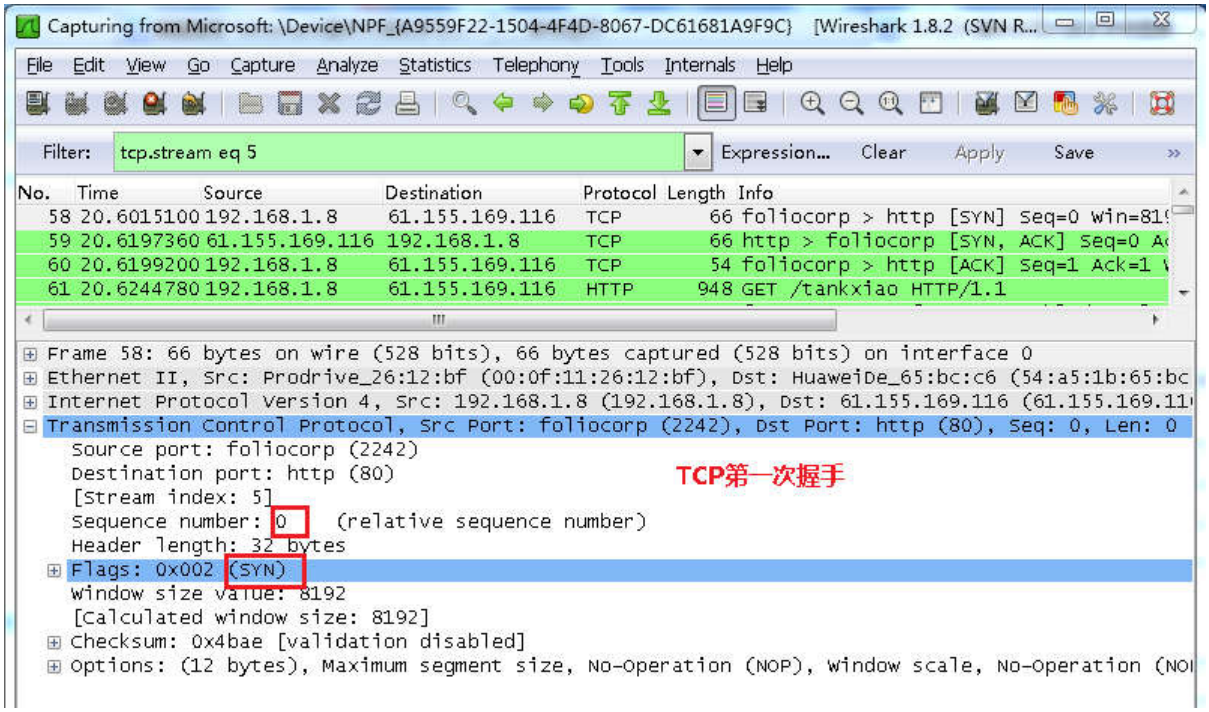


图 2-15

第二次握手的数据包

服务器发回确认包， 标志位为 SYN,ACK. 将确认序号(Acknowledgement Number)设置为客户的I S N加1以.即0+1=1， 如下图

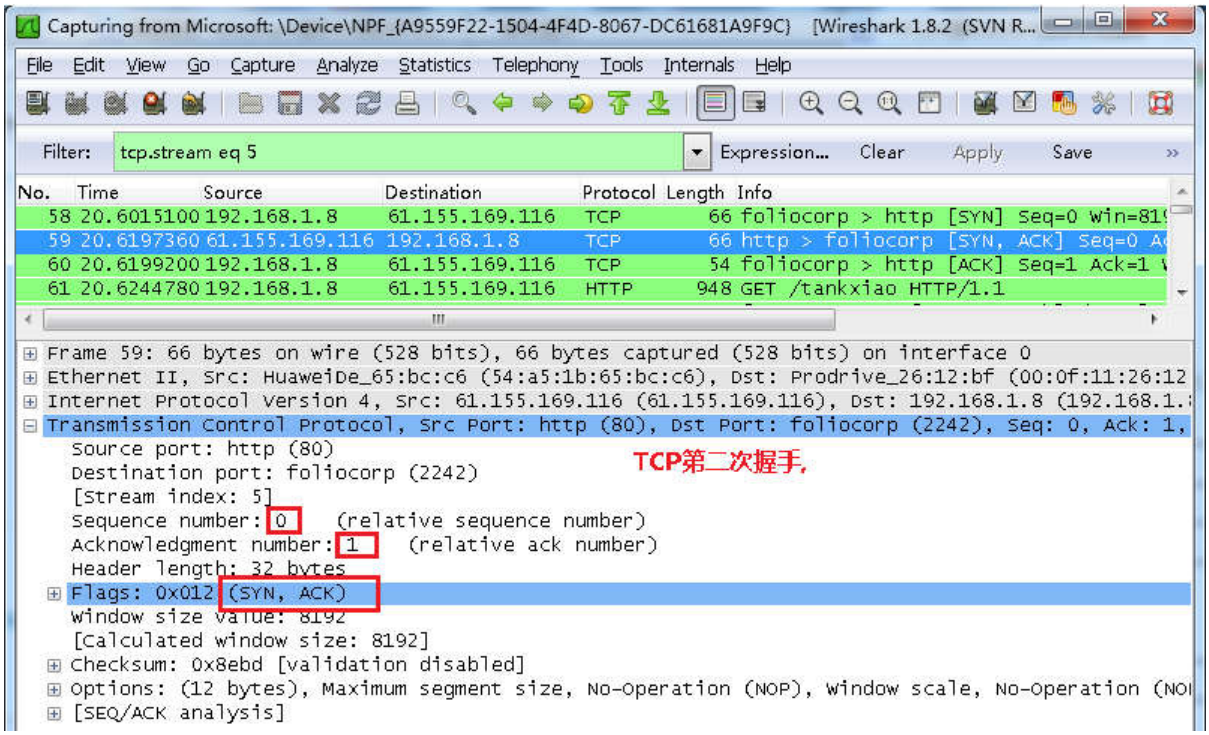


图 2-16

第三次握手的数据包

客户端再次发送确认包(ACK) SYN标志位为0,ACK标志位为1. 并且把服务器发来ACK的序号字段+1,放在确定字段中发送给对方. 并且在数据段放写ISN的+1, 如下图:

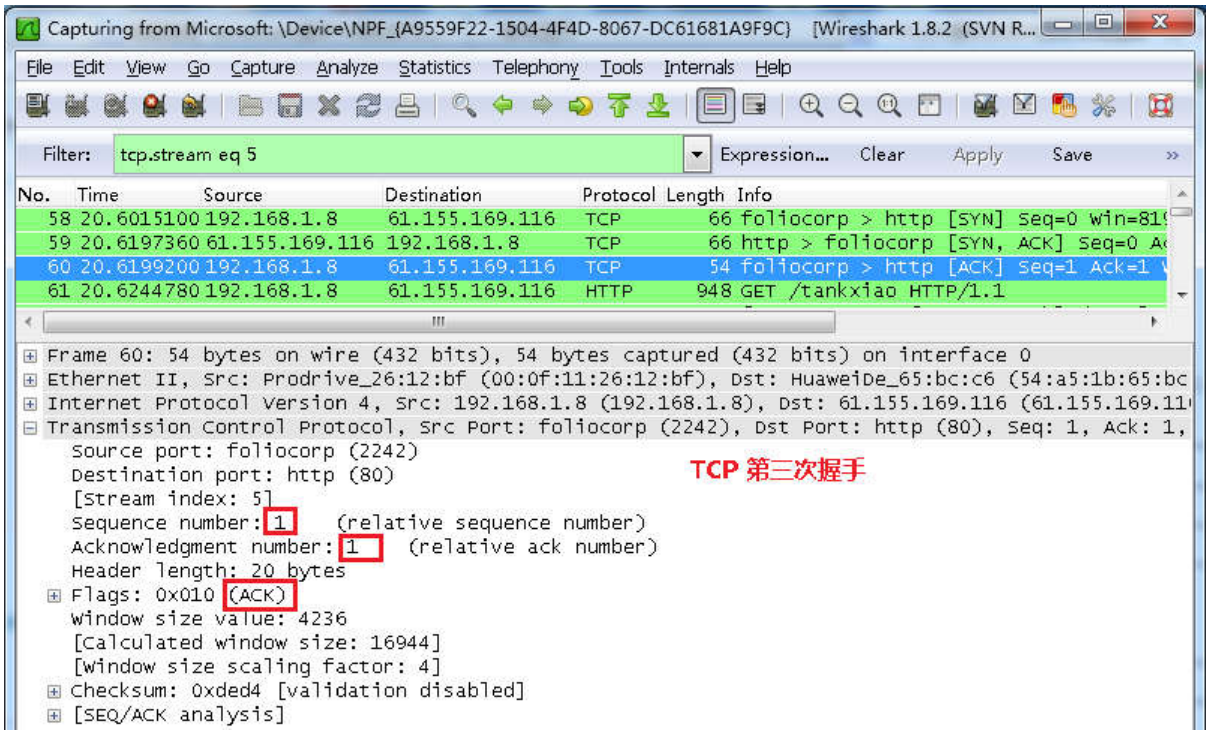


图 2-17

就这样通过了TCP三次握手，建立了连接

步骤三：wireshark捕获IP数据包格式分析

步骤四：wireshark捕获完整HTTP、ping数据流

【思考问题】

结合实验过程中的实验结果，问答下列问题：

1、实验所用主机的 IP 地址、子网掩码、网络号、子网号分别是多少？该主机的 IP 地址属于哪类？

2、IP 数据包在从源主机出发到达目的主机的过程中，IP 首部中的 IP 源地址和目的地址字段是否发生变化？

实验三 DNS 域名服务协议

【实验目的】

1、理解 DNS 实现的原理；

2、了解 DNS 解析的过程；

3、掌握 DNS 报文格式。

【实验环境】

本实验要求实验室主机能够连接到 Internet，并可浏览网页。

实验拓扑如图 3- 1 所示：

图 3-1 实验拓扑图

【实验内容】

1、学习 DNS 协议的原理和实现方法；

2、了解 DNS 的工作过程；

3、通过编辑 DNS 请求数据包，了解 DNS 的报文格式；

4、掌握 nslookup 命令和 ipconfig 命令的使用方法。

【实验流程】

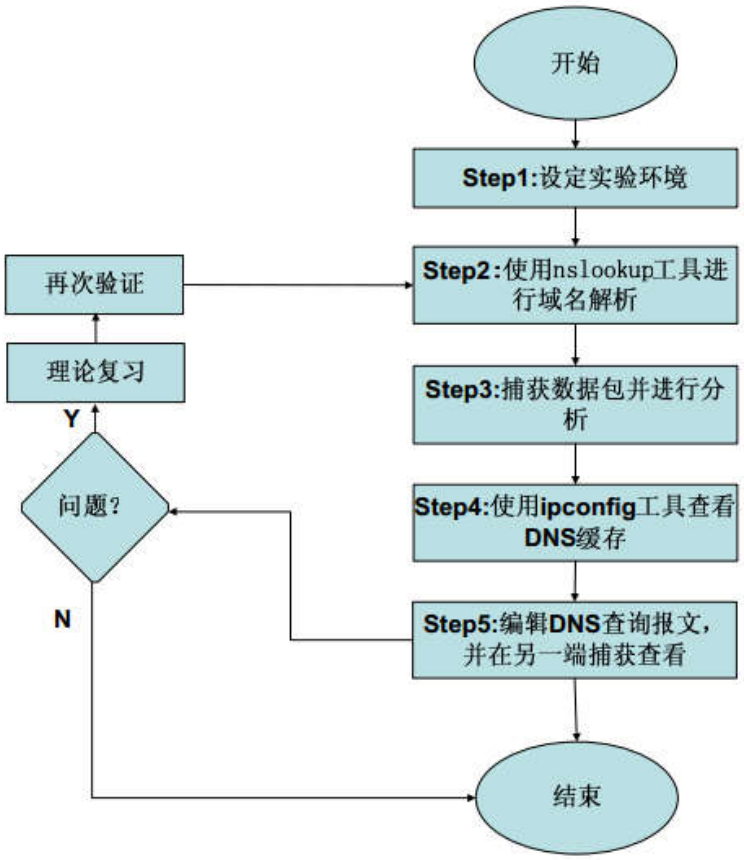


图 3- 2 实验流程图

【实验原理】

DNS 域名系统是服务器和客户程序相互通信的一种协议。它提供了主机域名和 IP 地址之间的转换。域名服务器使用固定的端口号 53，支持 UDP 和 TCP 访问。

DNS 协议

DNS 是域名系统（Domain Name System）的缩写，它是一种用于 TCP/IP 应用程序的分布式数据库，它提供主机名字和 I P 地址之间的转换及有关电子邮件的选路信息。所谓“分布式”是指在 Internet 上的单个站点不能拥有所有的信息。每个站点（如大学中的系、校园、公司或公司中的部门）保留它自己的信息数据库，并运行一个服务器程序供 Internet 上的其他系统（客户程序）查询。

在 Internet 中，域名可用来对某个组织或实体进行寻址。例如“www.sina.com”这个域名可用来对 IP 地址为 71.5.7.191 的 Internet 网点“sina.com”进行寻址，而特定的主机服务器名称为“www”。域名中的“com”部分表明该组织或实体的性质，“sina”定义了该组织或实体。

而 DNS 就像是一个自动的电话号码簿，我们可以直接拨打某人的名字来代替他的电话

号码（IP 地址）。DNS 在我们直接呼叫网站的名字以后，就会将像 www.sina.com 一样便于人类使用的名字转化成像 71.5.7.191 一样便于机器识别的 IP 地址。

这个转换工作称为域名解析，域名解析需要由专门的域名解析服务器来完成，DNS 就是进行域名解析的服务器。它是一种分布式网络目录服务，主要用于域名与 IP 地址的相互转换，以及控制因特网的电子邮件的发送。大多数因特网服务依赖于 DNS 而工作，一旦DNS 出错，就无法连接 Web 站点，电子邮件的发送也会中止。

在 DNS 命名方式中，采用了分散和分层的机制来实现域名空间的委派授权，以及域名与地址相转换的授权。通过使用 DNS 的命名方式来为遍布全球的网络设备分配域名，而这则是由分散在世界各地的服务器实现的。

命名系统是分层次的，域名树是倒置的，它的根级显示在最上方，分为若干顶级域（.com、.net、.edu、.gov、.org 等，以及 200 多个国家级的顶级域），这些域又被分成二级域，依此类推。它们由各自相应的政府或私有实体管理。

DNS 的分布式机制支持有效且可靠的名字到 IP 地址的映射。多数名字可以在本地映射，不同站点的服务器相互合作能够解决大网络的名字与 IP 地址的映射问题。单个服务器的故障不会影响 DNS 的正确操作。

DNS 工作流程

域名服务分为客户端和服务器端，客户端提出请求，询问一个 Domain Name 的 IP 地址，服务器端必须回答客户端的请求。本地 DNS 首先查询自己的数据库，如果自己的数据库中没有对应的 IP 地址，则向本地 DNS 上所设的上一级 DNS 询问，得到结果之后，将收到的结果保存在高速缓冲区，并回答给客户端。其简单过程如图3- 3 所示：

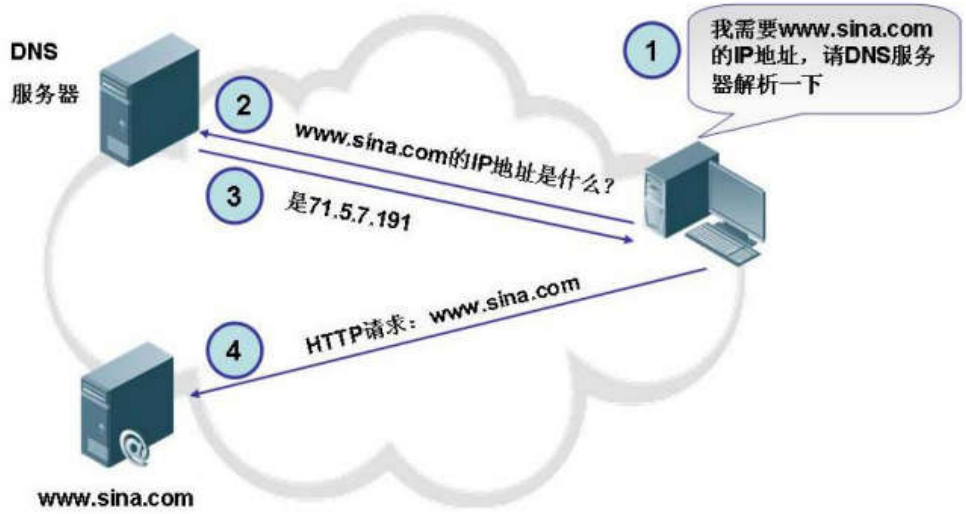


图 3- 3 DNS 的工作过程

在这个过程中，待查询的域名放在查询问题中，查询结果放在回答的资源记录中。

DNS 的报文格式

DNS定义了用于查询和响应的报文格式，图3-4 是查询和响应报文的总体格式：

图 3-4DNS 总体报文格式

这个报文由 1 2 字节长的首部和 4 个长度可变的字段组成。

标识字段由客户程序设置并由服务器返回结果。客户程序通过它来确定响应与查询是否匹配。16 bit 的标志字段被划分为若干子字段，如图3- 5 所示：

图 3-5 DNS 报文首部中的标志字段

标志中每一位的含义如下：

QR：是 1 bit 字段，0 表示查询报文，1 表示响应报文。

Opcode：报文类型，是一个 4 bit 字段，通常值为 0（标准查询），其他值为 1（反向查询）和 2（服务器状态请求）。

AA：是 1 bit 字段，表示“授权回答（authoritative answer）”，如果此位为 1，表示服务器对问题部分的回答是权威性的。

TC：是 1 bit 字段，表示“可截断的（truncated）”。使用 UDP 时，它表示当应答的总长度超过 512 字节时，只返回前 512 个字节。

RD：是 1 bit 字段，表示“期望递归（recursion desired）”。该比特能在一个查询中设置，并在响应中返回。这个标志告诉名字服务器必须处理这个查询，也称为一个递归查询。如果该位为 0，且被请求的名字服务器没有一个授权回答，它就返回一个能解答该查询的其他名字服务器列表，这称为迭代查询。

RA：是 1 bit 字段，表示“可用递归”。如果名字服务器支持递归查询，则在响应中将该比特设置为 1。

Zero：随后的 3 bit 字段必须为 0。

Rcode：是一个 4 bit 的返回码字段。通常的值为 0（没有差错）和 3（名字差错）。名字差错只有从一个授权 DNS 服务器上返回，它表示在查询中制定的域名不存在。

随后的 4 个 16 bit 字段说明最后 4 个变长字段中包含的条目数。对于查询报文，问题（question）数通常是 1，而其他 3 项则均为 0。类似地，对于应答报文，回答数至少是 1，剩下的两项可以是 0 或非 0。

图3- 6是DNS查询报文中的查询问题记录部分的格式，通常只有一个问题：

图 3- 6 DNS 查询问题记录格式

查询名是要查找的名字，它是一个或多个标识符的序列。每个标识符以首字节的计数值来说明随后标识符的字节长度，每个名字以最后字节为 0 结束，长度为 0 的标识符是根标识符。计数字节的值必须是 0 ~ 6 3 的数，因为标识符的最大长度仅为 6 3。

每个问题有一个查询类型，而每个响应（也称一个答案或资源记录）也有一个类型。大约有 20 个不同的类型值，其中的一些目前已经过时，常见的值如下表：

表3-1 类型值列表

名 字	数 值	描 述
A	1	IP 地址
NS	2	名字服务器
CNAME	5	规范名称
PTR	12	指针记录
HINFO	13	主机信息
MX	15	邮件交换记录

最常用的查询类型是 A 类型，表示期望获得查询名的 IP 地址。一个 PTR 查询则请求获得一个 IP 地址对应的域名。

查询类通常是 1，指互联网地址（某些站点也支持其他非 I P 地址）。

DNS 报文中最后的三个字段，答案字段、权威答案字段和附加答案字段，均采用一种称为资源记录 RR（Resource Record）的相同格式，图3- 43 是 DNS 响应报文中资源记录的格式：

图 3-7 DNS 资源记录的格式

域名：是记录中资源数据对应的名字。它的格式和前面介绍的查询名字段格式相同。

类型：说明 RR 的类型码。它的值和前面介绍的查询类型值是一样的。

类：通常为 1，指 Internet 数据。

生存时间：该字段是客户程序保留该资源记录的秒数。资源记录通常的生存时间值为 2 天。

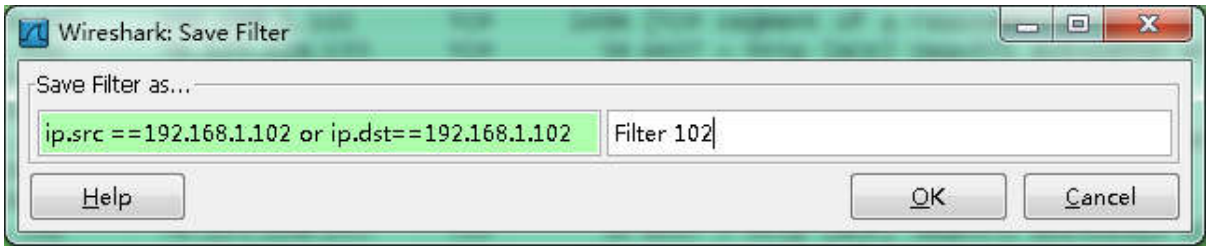
资源数据长度：说明资源数据的数量。该数据的格式依赖于类型字段的值。对于类型 1（A 记录）资源数据是 4 字节的 I P 地址。

【实验步骤】

步骤一：使用 nslookup 工具解析域名，捕获数据包并进行分析

1、在实验主机上启动网络协议分析仪进行数据捕获并设置过滤条件，在工具栏点击“过滤器”按钮，会弹出“设置&过滤器”对话框，在“过滤器类型”中选择“类型过滤器”，类型值中选

择“DNS 协议”，点击“设置参数”按钮后“确定”，开始进行数据包的捕获：



过滤表达式	用途
DNS	只查看 DNS 协议的记录
ip.src ==192.168.1.102 or ip.dst==192.168.1.102	源地址或者目标地址是 192.168.1.102

图 3- 8 设置 DNS 协议过滤器

2、使用 nslookup 工具进行域名的解析。

nslookup 命令是查询域名对应 IP 的工具，其用法可以直接在 Windows 系统的命令提示符下运行命令：nslookup 域名 来进行域名解析，例如：

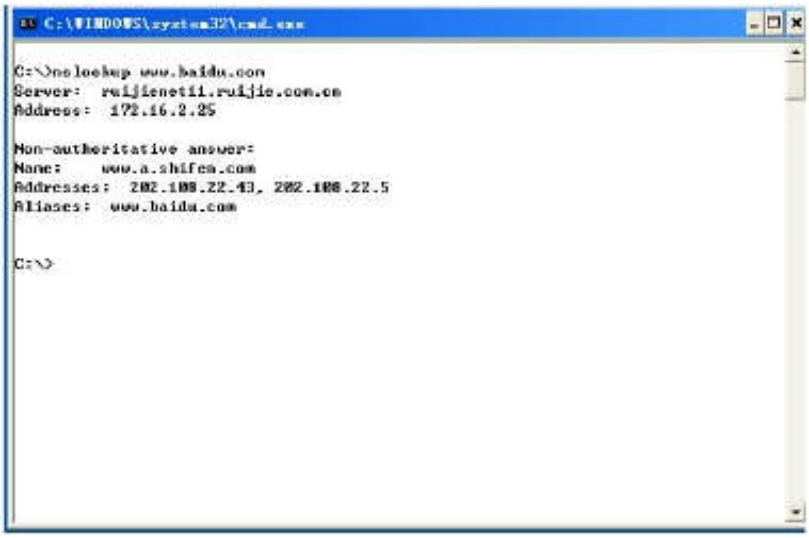


图 3-9 使用 nslookup 工具（一）

也可以仅仅运行 nslookup 命令(不需任何参数)，进入 nslookup 的交互界面，在“>”提示符后可以多次输入不同的域名，以实现多次的查询，例如可以在一次 nslookup 的交互过程中，进行 www.baidu.com、 www.yahoo.com、 www.google.com 的查询：

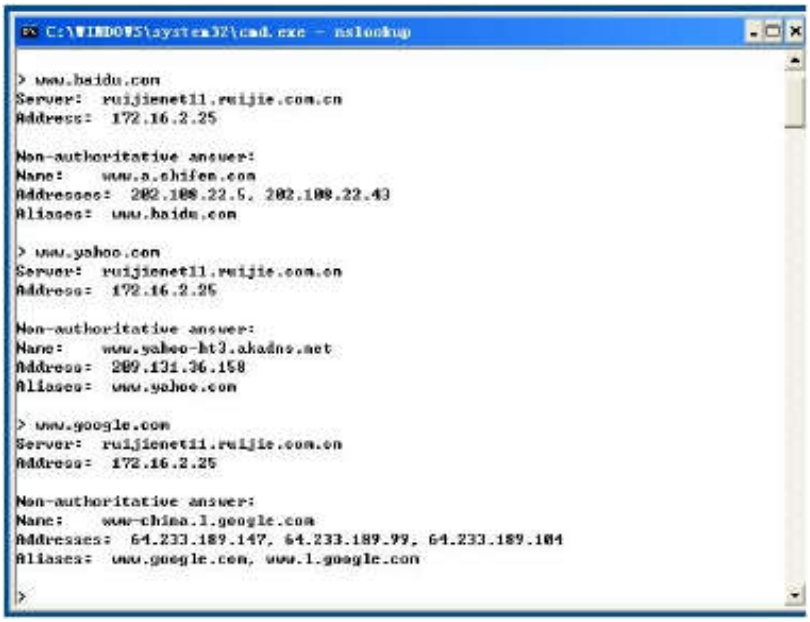


图 3-10 使用 nslookup 工具（二）

最后，可用“exit”命令退出 nslookup 的交互状态。

3、分析捕获到的数据报文。

分析一个 DNS 的查询报文，从中可以看到，报文的标识为 10，问题数是 1，答案数、权威答案数、附加答案数都是 0，而要查询的域名是 www.yahoo.com ：

分析一个响应报文，报文标识同样为 10，指明这个响应是针对哪一个查询报文的

步骤二：使用 ipconfig 命令查看 DNS 缓存

1、继续使用协议分析仪进行数据的捕获，同时打开 IE 浏览器，访问 www.baidu.com、www.yahoo.com、 www.google.com，观察此时是否还有 DNS 请求？

2、关闭 IE 浏览器后再重新打开，访问一个尚未访问过的网站，例如 www.sohu.com，观察此时是否有 DNS 请求？为什么？

3、在 Windows 系统的命令提示符下运行：ipconfig /displaydns 显示本机缓冲区中的DNS 解析内容，如图3-11 所示：

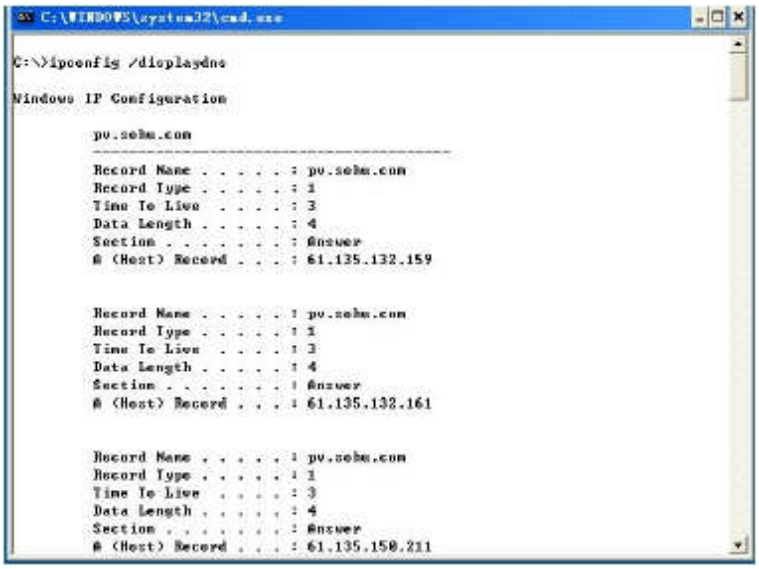


图 3-11 显示本机的 DNS 缓存

4、在 Windows 系统的命令提示符下运行：ipconfig /flushdns，则可以清除本机的 DNS 缓存记录，如图 3-12 所示：

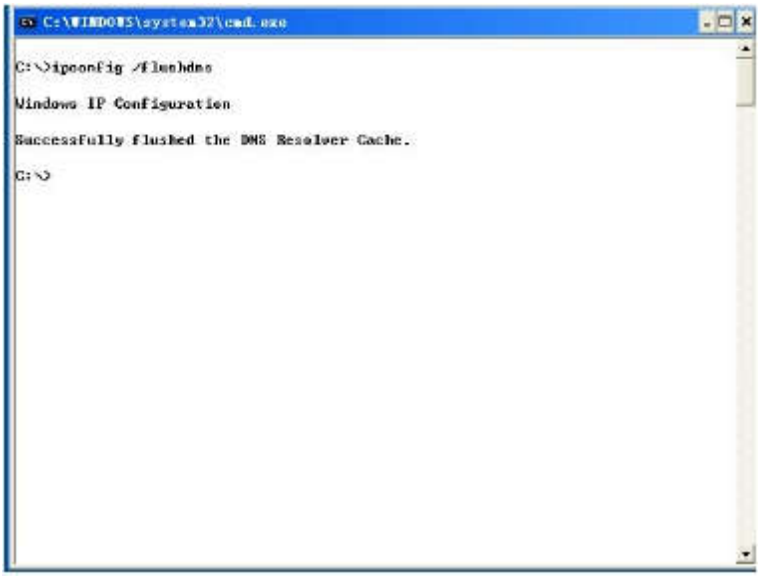


图 3-12 清除本机的 DNS 缓存

5、此时关闭 IE 浏览器再打开，访问刚才打开过的网站，观察是否有 DNS 请求？为什么？

【思考问题】

结合实验过程中的实验结果，回答下列问题：

1、根据步骤 1 中的捕获结果，分析 DNS 协议的工作流程。

2、域名与 IP 地址之间是否有一一对应的关系？

实验四 SOCKET 网络程序设计

【实验目的】

1、理解进程通信的原理及通信过程；

2、掌握基本的网络编程方法。

【实验内容】

1、进一步学习 UDP 及 TCP 协议的工作原理；

2、学习 SOCKET 编程的基本方法；

3、学习应用 C 语言与 WinSock2 进行简单的无连接的网络程序设计，实现网络数据传输；

4、学习应用 C 语言与 WinSock2 进行简单的面向连接的网络程序设计，实现网络数据传输。

【实验原理】

1、关于使用套接字编程的一些基本概念

半相关

网络中用一个三元组可以在全局唯一标示一个进程：（协议，本地地址，本地端口号）。这样一个三元组，叫做一个半相关（half-association），它指定连接的每半部分。

全相关

一个完整的网间进程通信需要由两个进程组成，并且只能使用同一种高层协议。也就是说，不可能通信的一端用 TCP 协议，而另一端用 UDP 协议。因此一个完整的网间通信需要一个五元组来标识：协议，本地地址，本地端口号，远地地址，远地端口号。这样一个五元组，叫做一个全相关（association），即两个协议相同的半相关才能组合成一个全相关。

TCP/IP 协议的地址结构为：

```
struct sockaddr_in
{
 short sin_family;/*协议的地址族，IP 协议是 AF_INET*/
 u_short sin_port;/*16 位端口号，网络字节顺序*/
 struct in addr sin addr; /*32 位 IP 地址，网络字节顺序*/
 char sin_zero[8]; /*填充*/
 }
```

套接字类型

TCP/IP 的 socket 提供下列三种类型套接字：

①、流式套接字（SOCK_STREAM）

提供了一个面向连接、可靠的数据传输服务，数据无差错、无重复地发送，且按发送顺序接收。内设流量控制，避免数据流超限；数据被看作是字节流，无长度限制。文件传送协议（FTP ）即使用流式套接字。

②、数据报套接字（SOCK_DGRAM）

提供了一个无连接服务。数据包以独立包形式被发送，不提供无错保证，数据可能丢失或重复，并且接收顺序混乱。网络文件系统（NFS）使用数据报式套接字。

③原始套接字（SOCK_RAW）

该接口允许对较低层协议，如 IP、ICMP 直接访问。常用于检验新的协议实现或访问现有服务中配置的新设备。

基本套接字系统调用为了更好地说明套接字编程原理，下面给出几个基本套接字系统调用说明：

①、创建套接字——Socket()

应用程序在使用套接字前，首先必须拥有一个套接字，系统调用 socket()向应用程序提供创建套接字的手段，其调用格式如下：

SOCKET socket(int af,int type,int protoCol);

该调用要接收三个参数：af、type、protocol 参数 af 指定通信发生的区域，UNIX 系统支持的地址族有：AF UNIX、AF INET、AF NS 等，而 DOS、WINDOWS 中仅支持 AF_INET，因此，地址族与协议族相同。参数 type 描述要建立的套接字的类型。参数 protocol 说明该套接字使用的特定协议，如果调用者不希望特别指定使用的协议，则置为 0，使用默认的连接模式。根据这几个参数建立一个套接字，并将相应的资源分配给它，同时返回一个整型套接字号。因此，socket()系统调用实际上指定了相关五元组中的“协议”这一元。

②、指定本地地址——bind()

当一个套接字用 socket()创建后，存在一个名字空间（地址族），但它没有被命名。bind()将套接字地址（包括本地主机地址与本地端口地址）与所创建的套接字号联系起来，即将名字赋予套接字，以指定本地半相关。其调用格式如下：

int bind(SOCKET s,const struct sockaddr FAR*name,int namelen);

参数 s 是由 socket()调用返回的并且未作连接的套接字描述符(套接字号)。参数 name是赋给套接字 s 的本地地址(名字)，其长度可变，结构随通信域的不同而不同。namelen表明了 name 的长度。如果没有错误发生，bind()返回 0。否则返回值 SOCKET ERROR。

地址在建立套接字通信过程中起着重要作用，作为一个网络应用程序设计者对套接字地址结构必须有明确认识。

③、建立套接字连接——connect()与 accept()

这两个系统调用用于完成一个完整相关的建立，其 connect()用于建立连接。无连接的

套接字进程也可以调用 connect()，但这时在进程之间没有实际的报文交换，调用将从本地操作系统直接返回。这样做的优点是程序员不必为每一数据指定目的地址，而且如果收到的一个数据报，其目的端口未与任何套接字建立“连接”，便能判断该端口不可操作。而 accept()用于使服务器等待来自某客户进程的实际连接。

connect()的调用格式如下：

int connect(SOCKET s,const struct sockaddr FAR*name,int namelen);

参数 s 是欲建立连接的本地套接字描述符。参数 name 指出说明对方套接字地址结构的指针。对方套按字地址长度由 namelen 说明。

如果没有错误发生，connect()返回 0。否则返回值 SOCKET_ERROR。在面向连接的协议中，该调用导致本地系统与外部系统之间连接实际建立。

由于地址族总被包含在套接字地址结构的前两个字节中，并通过 Socket()调用与某个协议族相关。因此 bind()和 connect()无须协议作为参数。

accept()的调用格式如下：

SOCKET accept(SOCKET s,struct sockaddr FAR*addr,int FAR*addrlen);

参数 s 为本地套接字描述符，在用做 accept()调用的参数前应该先调用过 listen()。addr指向客户方套接字地址结构的指针，用来接收连接实体的地址。 addr 的确切格式由套接字创建时建立的地址族决定。addrlen 为客户方套接字地址的长度(字节数)。如果没有错误发生，accept()返回一个 SOCKET 类型的值，表示接收到的套接字的描述符。否则返回值 INVALID_SOCKET。

accept()用于面向迎接服务器。参数 addr 和 addrlen 存放客户方的地址信息。调用前，参数 addr 指向一个初始值为主的地址结构，而 addrlen 的初始值为 0;调用 accept()后，服务器等待从编号为 s 的套接字上接受客户连接请求，而连接请求是由客户方的 connect()调用发出的。当有连接请求到达时，accept()调用将请求连接队列上的第一个客户方套接字地址及长度放入 addr 和 addrlen，并创建一个与 s 有相同特性的新套接字号。新的套接字可用于处理服务器开发请求。

四个套接字系统调用，socket()、bind()、connect()、accept()，可以完成一个完全五元相关的建立。socket()指定五元组中的协议元，它的用法与是否为客户或服务器、是否面向连接无关。bind()指定五元组中的本地二元，即本地主机地址和端口号，其用法与是否面向连接有关：在服务器方，无论是否面向连接，均要调用 bind()；在客户方，若采用面向连接，则可以不调用 bind()，而通过 connect()自动完成。若采用无连接，客户方必须使用 bind()以获得一个唯一的地址。

以上讨论仅对客户/服务器模式而言，实际上套接字的使用是非常灵活的，唯一需遵循的原则是进程通信之前，必须建立完整的相关。

④、监听连接——listen()

此调用用于面向连接服务器，表明它愿意接收连接。listen()需在 accept()之前调用，其调用格式如一下：

int listen(SOCKET s,int backlog):参数 s 标识一个本地已建立、尚未连接的套接字号，服务器愿意从它上面接收请求。

backlog 表示请求连接队列的最大长度，用于限制排队请求的个数，目前允许的最大值为 5。

如果没有错误发生，listen()返回 0。否则它返回 SOCKET_ERROR。

listen()在执行调用过程中可为没有调用过 bind()的套接字 s 完成所必须的连接，并建立长度为 backlog 的请求迎接队列。

调用 listen()是服务器接收一个连接请求的四个步骤中的第二步。它在调用 socket()分配一个流套接字，且调用 bind()给 s 赋于一个名字之后调用，而且一定要在 accept()之前调用。

⑤、数据传输——send()与 recv()

当一个连接建立以后，就可以传输数据了。常用的系统调用有 send()和 recv()。send()调用用于在参数 s 指定的已连接的数据报或流套接字上发送输出数据，格式如下：

int send(SOCKET s,const char FAR*buf,int len,int flags):

参数 s 为已连接的本地套接字描述符。buf 指向存有发送数据的缓冲区的指针，其长度由 len 指定 oflags 指定传输控制方式，如是否发送带外数据等。如果没有错误发生，send()返回总共发送的字节数。否则它返回 SOCKET_ERROR。

recv()调用用于在参数 s 指定的已连接的数据报或流套接字上接收输入数据，格式如下：

int recv(SOCKET s,char FAR*buf,iht len,int flags):参数 s 为已连接的套接字描述符。buf指向接收输入数据缓冲区的指针，其长度由 len 指定。flags 指定传输控制方式，如是否接收带外数据等。如果没有错误发生，recv，()返回总共接收的字节数。如果连接被关闭，返回 0。否则它返回 SOCKET ERROR。

⑥、输入/输出多路复用——select()

select()调用用来检测一个或多个套接字的状态。对每一个套接字来说，这个调用可以请求读、写或错误状态方面的信息。请求给定状态的套接字集合由一个 fd_set 结构指示。

在返回时，此结构被更新，以反映那些满足特定条件的套接字的子集，同时，select()调用返回满足条件的套接字的数目，其调用格式如下

int select(int nfds,fd set FAR*readfds,fd set FAR*writefds,fd_set FAR:kexceptfds,const struct timeval FAR*timeout):参数 nfds 指明被检查的套接字描述符的

值域，此变量一般被忽略。参数 readfds 指向要做读检测的套接字描述符集合的指针，

调用者希望从中读取数据。参数 writefds 指向要做写检测的套接字描述符集合的指针。exceptfds指向要检测是否出错的套接字描述符集合的指针。timeout 指向 select()函数等待的最大时间，如果设为 NULL 则为阻塞操作。select()返回包含在 fd set 结构中已准备好的套接字描述符的总数目，或者是发生错误则返回 SOCKET_ERROR。

⑦、关闭套接字——closesocket()

closesocket()关闭套按字 s，并释放分配给该套接字的资源：如果 s 涉及一个打开的TCP连接，则该连接被释放。closesocket()的调用格式如下：

BOOL closesocket(SOCKET S)；参数 s 待关闭的套接字描述符。如果没有错误发生，closesocket()返回 0。否则返回值 SOCKET ERROR。

2、用于面向连接协议（如 TCP）的 SOCKET 系统调用流程框图

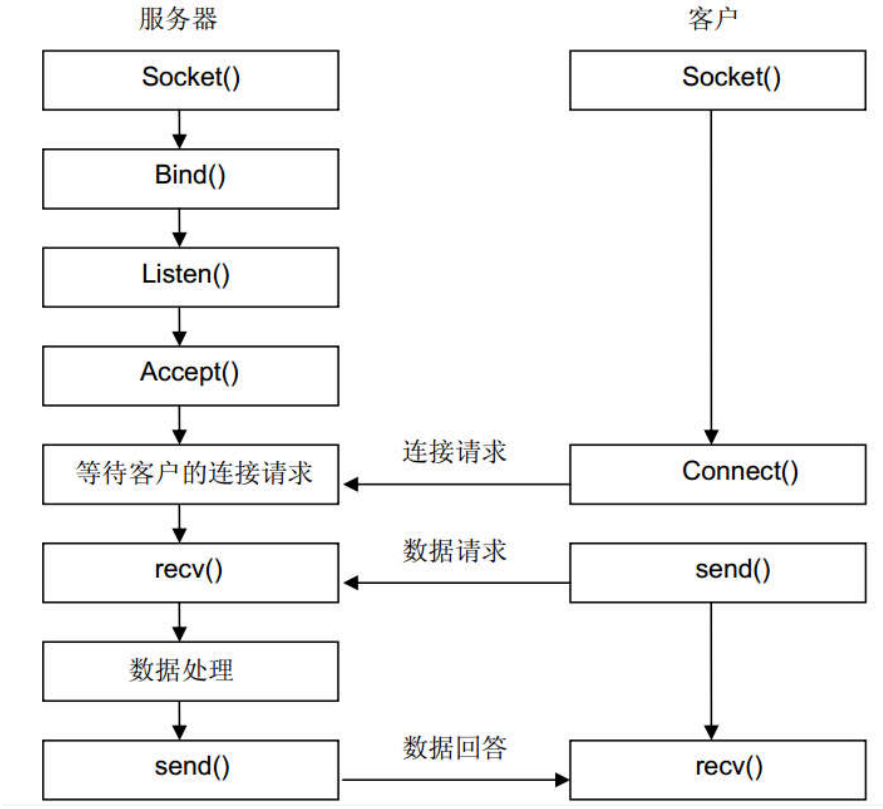


图 4-2 用于面向连接的 Socket 系统调用流程图

3、用于无连接协议（如 UDP）的 SOCKET 系统调用流程框图

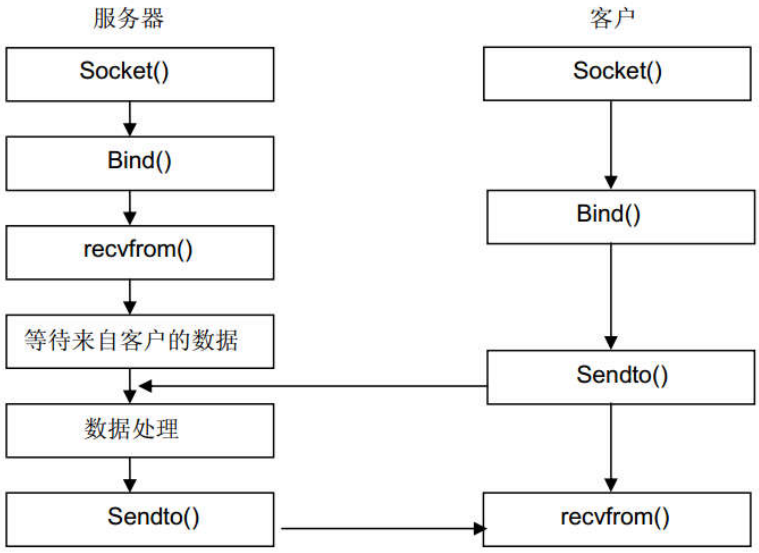


图 4-1 用于无连接的 Socket 系统调用流程图

【实验步骤】

步骤一：使用 TCP 协议的面向连接的客户-服务器程序设计

根据实验原理中介绍的内容，设计一个面向连接的客户-服务器系统，实现二者之间的数据传递。下面是一个简单的 TCP 客户-服务器程序：

面向连接的服务器程序：

```
// server.cpp : 定义控制台应用程序的入口点。
#include "stdafx.h"
#include <Winsock2.h>
#include <stdio.h>
#include <stdlib.h>
#define DEFAULT_PORT 5050 //服务端默认端口
int _tmain(int argc, char* argv[])
{
    int         iPort = DEFAULT_PORT;
    WSADATA     wsaData;
    SOCKET      sListen,sAccept;
    int         iLen; //客户地址长度
    int         iSend;//发送数据长度
    char        buf[] = "I am a server";//要发送给客户的信息
    struct sockaddr_in ser,cli;//服务器和客户的地址
    if(WSAStartup(MAKEWORD(2,2),&wsaData)!=0)
    {
        printf("Failed to load Winsock.\n");
        return -1;
    }
```

```
sListen = socket(AF_INET,SOCK_STREAM,0);//创建服务器端套接口
    if(sListen == INVALID_SOCKET)
    {
        printf("socket() Failed: %d\n",WSAGetLastError());
        return -1;
    }
    //以下建立服务器端地址
    //使用 IP 地址族
    ser.sin_family = AF_INET;
    //使用 htons()把双字节主机序端口号转换为网络字节序端口号
    ser.sin_port = htons(iPort);
    //htonl()把一个四字节主机序 IP 地址转换为网络字节序主机地址
    //使用系统指定的 IP 地址 INADDR_ANY
    ser.sin_addr.s_addr = htonl(INADDR_ANY);
    //bind()函数进行套接定与地址的绑定
    if(bind(sListen,(LPSOCKADDR)&ser,sizeof(ser)) == SOCKET_ERROR)
    {
        printf("bind() Failed: %d\n",WSAGetLastError());
        return -1;
    }
//进入监听状态
    if(listen(sListen,5) == SOCKET_ERROR)
    {
        printf("lisiten() Failed: %d\n",WSAGetLastError());
        return -1;
    }
    //初始化客户地址长度参数
    iLen = sizeof(cli);
    //进入一个无限循环，等待客户的连接请求
    while(1)
    {
        sAccept = accept(sListen,(struct sockaddr *)&cli,&iLen);
        if(sAccept == INVALID_SOCKET)
        {
            printf("accept() Failed: %d\n",WSAGetLastError());
            return -1;
        }
        //输出客户 IP 地址和端口号
        printf("Accepted client IP:[%s],port:[%d]\n",inet_ntoa(cli.sin_addr),ntohs(cli.sin_port));
    //给连接的客户发送信息
        iSend = send(sAccept,buf,sizeof(buf),0);
        if(iSend == SOCKET_ERROR)
        {
            printf("send() Failed: %d\n",WSAGetLastError());
```

```
                break;
            }
            else if(iSend == 0)
            {
                break;
            }
            else
            {
                printf("send() byte: %d\n",iSend);
            }
            closesocket(sAccept);
        }
        closesocket(sListen);
        WSACleanup();
        return 0;
}
```

面向连接的客户机程序：

```
// client.cpp : 定义控制台应用程序的入口点。
#include "stdafx.h"
#include <Winsock2.h>
#include <stdio.h>
#include <stdlib.h>
#define DATA_BUFFER 1024 //默认缓冲区大小
int _tmain(int argc, char * argv[])
{
        WSADATA wsaData;
        SOCKET sClient;
        int iPort = 5050;
        int iLen;//从服务器端接收的数据长度
        char buf[DATA_BUFFER];//接收数据的缓冲区
        struct sockaddr_in ser;//服务器端地址
        //判断参数输入是否正确：client [Server IP]
        if(argc<2)
        {
            //提示在命令行中输入服务器 IP 地址
            printf("Usage: client [server IP address]\n");
            return -1;
        }
memset(buf,0,sizeof(buf));//接收缓冲区初始化
        if(WSAStartup(MAKEWORD(2,2),&wsaData)!=0)
        {
            printf("Failed to load Winsock.\n");
            return -1;
```

```
    }
    //填写要连接的服务器地址信息
    ser.sin_family = AF_INET;
    ser.sin_port = htons(iPort);
    //inet_addr()将命令行中输入的点分 IP 地址转换为二进制表示的网络字节序 IP 地址
    ser.sin_addr.s_addr = inet_addr(argv[1]);
    //建立客户端流式套接口
    sClient = socket(AF_INET,SOCK_STREAM,0);
    if(sClient == INVALID_SOCKET)
    {
        printf("socket() Failed: %d\n",WSAGetLastError());
        return -1;
    }
//请求与服务器端建立 TCP 连接
    if(connect(sClient,(struct sockaddr *)&ser,sizeof(ser)) == INVALID_SOCKET)
    {
        printf("connect() Failed: %d\n",WSAGetLastError());
        return -1;
    }
    else
    {
        //从服务器端接收数据
        iLen = recv(sClient,buf,sizeof(buf),0);
        if(iLen == 0)
            return -1;
        else if(iLen == SOCKET_ERROR)
        {
            printf("recv() Failed: %d\n",WSAGetLastError());
            return -1;
        }
        else
            printf("recv() data from server: %s\n",buf);
    }
    closesocket(sClient);
    WSACleanup();
    return 0;
}
```

请学生认真阅读，然后根据实验原理二中介绍的内容，调试程序，实现客户与服务器间的数据传输。在协议数据发生器一端运行客户端进程，在网络协议分析仪端捕获数据并分析。

步骤二：使用 TCP 协议进行复杂的客户-服务器程序设计

上述的例子程序比较简单，有一些进程中往往同时存在几条连接，这样的进程在有报文

到来时，可以往它处理的任何 socket 上执行 recv 调用，但它不知道哪个 socket 上已有报文，哪个上没有，可以使用 select()系统调用来解决这样的问题。有兴趣的同学可自行编写这样较复杂的客户-服务器程序。

【思考问题】

结合实验过程中的实验结果，问答下列问题：

I、根据编程练习实验中记录的客户和服务器程序的端口号并结合程序，说明：在客户/服务器模型当中，客户进程的端口号和服务器进程的端口号都是由程序给出说明的吗？为什么？

2、在 TCP/IP 网络中，当客户与服务器进程建立了一条 TCP 连接以后，是否属于该连接的所有包都是经过同一路径（即一条虚电路）传递的？为什么？

实验五 交换机的基本配置

【实验目的】

掌握交换机命令行各种操作模式的区别，能够使用各种帮助信息，以及用命令进行基本的配置。

【背景描述】

你是某公司新进的网管，公司要求你熟悉网络产品，公司采用全系列锐捷网络产品，首先要求你登录交换机，了解、掌握交换机的命令行操作技巧，以及如何使用一些基本命令进行配置。

【需求分析】

需要在交换机上熟悉各种不同的配置模式以及如何在配置模式间切换，使用命令进行基本的配置，并熟悉命令行界面的操作技巧。

【实验拓扑】

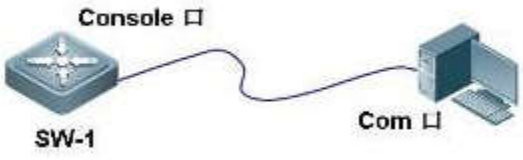


图 2-1 实验拓扑图

【实验设备】

三层交换机 1 台

【预备知识】

交换机的命令行界面和基本操作

【实验原理】

交换机的管理方式基本分为两种：带内管理和带外管理。通过交换机的 Console 口管理交换机属于带外管理，不占用交换机的网络接口，其特点是需要使用配置线缆，近距离配置。

第一次配置交换机时必须利用 Console 端口进行配置。

交换机的命令行操作模式，主要包括：用户模式、特权模式、全局配置模式、端口模式等几种。

用户模式

进入交换机后得到的第一个操作模式，该模式下可以简单查看交换机的软、硬件版本信息，并进行简单的测试。用户模式提示符为 switch>

特权模式

由用户模式进入的下一级模式，该模式下可以对交换机的配置文件进行管理，查看交换机的配置信息，进行网络的测试和调试等。特权模式提示符为switch#

全局配置模式

属于特权模式的下一级模式，该模式下可以配置交换机的全局性参数（如主机名、登录信息等）。在该模式下可以进入下一级的配置模式，对交换机具体的功能进行配置。全局模式提示符为 switch(config)#

端口模式

属于全局模式的下一级模式，该模式下可以对交换机的端口进行参数配置。端口模式提示符为 switch(config-if)#

交换机的基本操作命令包括：

Exit 命令是退回到上一级操作模式。

End 命令是指用户从特权模式以下级别直接返回到特权模式。

交换机命令行支持获取帮助信息、命令的简写、命令的自动补齐、快捷键功能。

配置交换机的设备名称和配置交换机的描述信息必须在全局配置模式下执行。

Hostname 配置交换机的设备名称。

当用户登录交换机时，你可能需要告诉用户一些必要的信息。你可以通过设置标题来达到这个目的。你可以创建两种类型的标题：每日通知和登录标题。

Banner motd 配置交换机每日提示信息 motdmessage of the day。

Banner login 配置交换机登录提示信息，位于每日提示信息之后。

查看交换机的系统和配置信息命令要在特权模式下执行。

a)Show version 查看交换机的版本信息，可以查看到交换机的硬件版本信息和软件版本信息，用于进行交换机操作系统升级时的依据。

b)Show mac-address-table 查看交换机当前的 MAC 地址表信息。

c)Show running-config 查看交换机当前生效的配置信息。

【实验步骤】

第一步：交换机各个操作模式直接的切换

Swtich>enable

！使用 enable 命令从用户模式进入特权模式

Swtich#configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

！使用 configure terminal 命令从特权模式进入全局配置模式

Swtich(config)#interface fastEthernet 0/1

！使用 interface 命令进入接口配置模式

Swtich(config-if)#

Swtich(config-if)#exit

！使用 exit 命令退回上一级操作模式

Swtich(config)#interface fastEthernet 0/2

Swtich(config-if)#end

Swtich#

！使用 end 命令直接退回特权模式

第二步：交换机命令行界面基本功能

Switch> ?

！显示当前模式下所有可执行的命令

disable Turn off privileged commands

enable Turn on privileged commands

exit Exit from the EXEC

help Description of the interactive help system

pingSend echo messages

rcommand Run command on remote switch

show Show running system information

telnet Open a telnet connection

tracerouteTrace route to destination

Swtich>en <tab>

Swtich>enable

！使用 tab 键补齐命令

Swtich#con?

configure connect

！使用？显示当前模式下所有以“con”开头的命令

Swtich#conf t

Enter configuration commands, one per line. End with CNTL/Z.

Swtich(config)#

！使用命令的简写

Swtich(config)#interface ？

！显示 interface 命令后可执行的参数

Aggregateport Aggregate port interface

Dialer Dialer interface

FastEthernet Fast IEEE 802.3

GigabitEthernet Gbyte Ethernet interface

Loopback Loopback interface

Multilink Multilink-group interface

Null Null interface

Tunnel Tunnel interface

Virtual-ppp Virtual PPP interface

Virtual-template Virtual Template interface

Vlan Vlan interface

range Interface range command

Switch(config)#interface

Swtich(config)#interface fastEthernet 0/1

Switch(config-if)# ^Z

Switch#

！使用快捷键“Ctrl+Z”可以直接退回到特权模式

Switch#ping 1.1.1.1

sending 5, 100-byte ICMP Echos to 1.1.1.1,

timeout is 2000 milliseconds.

. ^C

Switch#

！在交换机特权模式下执行 ping 1.1.1.1 命令，发现不能 ping 通目标地址，交换机默认情况下需要发送 5 个数据包，如不想等到 5 个数据包均不能 ping 通目标地址的反馈出现，可在数据包未发出 5 个之前通过执行快捷键“Ctrl+C”终止当前操作。

第三步：配置交换机的名称和每日提示信息

Switch(config)#hostname SW-1

！使用 hostname 命令更改交换机的名称

SW-1(config)#banner motd $

！使用 banner 命令设置交换机的每日提示信息，参数 motd 指定以哪个字符为信息的结束符

Enter TEXT message. End with the character '$'.

Welcome to SW-1, if you are admin, you can config it.

If you are not admin, please EXIT!

$

SW-1(config)#

SW-1(config)#exit

SW-1#Nov 25 22:04:01 %SYS-5-CONFIG_I: Configured from console by console

SW-1#exit

SW-1 CON0 is now available

Press RETURN to get started

Welcome to SW-1, if you are admin, you can config it.

If you are not admin, please EXIT!

SW-1>

第四步：配置接口状态

锐捷全系列交换机 Fastethernet 接口默认情况下是 10M/100Mbit/s 自适应端口，双工模式也为自适应（端口速率、双工模式可配置）。默认情况下，所有交换机端口均开启。

如果网络中存在一些型号比较旧的主机，还在使用 10Mbit/s 半双工的网卡，此时为了能够实现主机之间的正常访问，应当在交换机上进行相应的配置，把连接这些主机的交换机端口速率设为 10Mbit/s，传输模式设为半双工。

SW-1(config)#interface fastEthernet 0/1

！进入端口 F0/1 的配置模式

SW-1(config-if)#speed 10

！配置端口速率为 10M

SW-1(config-if)#duplex half

！配置端口的双工模式为半双工

SW-1(config-if)#no shutdown

！开启端口，使端口转发数据。交换机端口默认已经开启。

SW-1(config-if)#description "This is a Accessport."

！配置端口的描述信息，可作为提示。

SW-1(config-if)#end

SW-1#Nov 25 22:06:37 %SYS-5-CONFIG_I: Configured from console by console

SW-1#

SW-1#show interface fastEthernet 0/1

Index(dec):1 (hex):1

FastEthernet 0/1 is UP , line protocol is UP

Hardware is marvell FastEthernet

Description: "This is a Accessport."

Interface address is: no ip address

MTU 1500 bytes, BW 10000 Kbit

Encapsulation protocol is Bridge, loopback not set

Keepalive interval is 10 sec , set

Carrier delay is 2 sec

RXload is 1 ,Txload is 1

Queueing strategy: WFQ

Switchport attributes:

interface's description:""This is a Accessport.""

medium-type is copper

lastchange time:329 Day:22 Hour: 5 Minute: 2 Second

Priority is 0

admin duplex mode is Force Half Duplex, oper duplex is Half

admin speed is 10M, oper speed is 10M

flow control admin status is OFF,flow control oper status is OFF

broadcast Storm Control is OFF,multicast Storm Control is OFF,unicast Storm

Control is OFF

5 minutes input rate 0 bits/sec, 0 packets/sec

5 minutes output rate 0 bits/sec, 0 packets/sec

0 packets input, 0 bytes, 0 no buffer, 0 dropped

Received 0 broadcasts, 0 runts, 0 giants

0 input errors, 0 CRC, 0 frame, 0 overrun, 0 abort

0 packets output, 0 bytes, 0 underruns , 0 dropped

0 output errors, 0 collisions, 0 interface resets

SW-1#

如果需要将交换机端口的配置恢复默认值，可以使用 default 命令。

SW-1(config)#interface fastEthernet 0/1

SW-1(config-if)#default bandwidth

！恢复端口默认的带宽设置

SW-1(config-if)#default description

！取消端口的描述信息

SW-1(config-if)#default duplex

！恢复端口默认的双工设置

SW-1(config-if)#end

SW-1#Nov 25 22:11:13 %SYS-5-CONFIG_I: Configured from console by console

SW-1#

SW-1#show interface fastEthernet 0/1

Index(dec):1 (hex):1

FastEthernet 0/1 is UP , line protocol is UP

Hardware is marvell FastEthernet

Interface address is: no ip address

MTU 1500 bytes, BW 100000 Kbit

Encapsulation protocol is Bridge, loopback not set

Keepalive interval is 10 sec , set

Carrier delay is 2 sec

RXload is 1 ,Txload is 1

Queueing strategy: WFQ

Switchport attributes:

interface's description:""

medium-type is copper

lastchange time:329 Day:22 Hour:11 Minute:13 Second

Priority is 0

admin duplex mode is AUTO, oper duplex is Full

admin speed is AUTO, oper speed is 100M

flow control admin status is OFF,flow control oper status is ON

broadcast Storm Control is OFF,multicast Storm Control is OFF,unicast Storm

Control is OFF

5 minutes input rate 0 bits/sec, 0 packets/sec

5 minutes output rate 0 bits/sec, 0 packets/sec

0 packets input, 0 bytes, 0 no buffer, 0 dropped

Received 0 broadcasts, 0 runts, 0 giants

0 input errors, 0 CRC, 0 frame, 0 overrun, 0 abort

0 packets output, 0 bytes, 0 underruns , 0 dropped

0 output errors, 0 collisions, 0 interface resets

SW-1#

第五步：查看交换机的系统和配置信息

SW-1#show version

！查看交换机的系统信息

System description : Ruijie Dual Stack Multi-Layer Switch(S3760-24) By Ruijie Network

！交换机的描述信息（型号等）

System start time : 2008-11-25 21:58:44

System hardware version : 1.0

！设备的硬件版本信息

System software version : RGNOS 10.2.00(2), Release(27932)

！操作系统版本信息

System boot version : 10.2.27014

System CTRL version : 10.2.24136

System serial number : 0000000000000

SW-1#

SW-1#show running-config

！查看交换机的配置信息

Building configuration...

Current configuration : 1279 bytes

!

version RGNOS 10.2.00(2), Release(27932)(Thu Dec 13 10:31:41 CST 2007 -ngcf32)

hostname SW-1

!

vlan 1

!

no service password-encryption

!

interface FastEthernet 0/1

!

interface FastEthernet 0/2

!

interface FastEthernet 0/3

!

.

.

.

interface GigabitEthernet 0/28

!

!

line con 0

line vty 0 4

login

!

!

banner motd ^C

Welcome to SW-1, if you are admin, you can config it.

If you are not admin, please EXIT!

^C

!

end

第六步：保存配置

下面的 3 条命令都可以保存配置

SW-1#copy running-config startup-config

SW-1#write memory

SW-1#write

【注意事项】

1、命令行操作进行自动补齐或命令简写时，要求所简写的字母必须能够惟一区别该命令。

如 switch#conf 可以代表 configure，但 switch#co 无法代表 configure，因为 co 开头的命令

有两个 copy 和 configure，设备无法区别。

2、注意区别每个操作模式下可执行的命令种类。交换机不可以跨模式执行命令。

3、配置设备名称的有效字符是 22 个字节。

4、配置每日提示信息时，注意终止符不能在描述文本中出现。如果键入结束的终止符后仍然输入字符，则这些字符将被系统丢弃。

5、交换机端口在默认情况下是开启的，AdminStatus 是 UP 状态，如果该端口没有实际连接其他设备，OperStatus 是 down 状态。

6、show running-config 查看的是当前生效的配置信息，该信息存储在 RAM（随机存储器里），当交换机掉电，重新启动时会重新生成新的配置信息。

实验六 跨交换机实现 VLAN 间路由

【实验目的】

利用三层交换机跨交换机实现 VLAN 间路由。

【背景描述】

为减小广播包对网络的影响，网络管理员在公司内部网络中进行了 VLAN 的划分，为了实现不同 VLAN 间的互相访问，网络管理员利用三层交换机实现 VLAN 间路由。但是由于网络中主机数量较大，部分主机需要通过二层交换机接入到网络中，再利用三层交换机的路由功能实现和其他 VLAN 间路由。

【需求分析】

在二层交换机上划分 VLAN 配置 Trunk 实现不同 VLAN 的主机接入，在三层交换机上划分VLAN 配置 Trunk 并配置 SVI 接口实现不同 VLAN 间路由。

【实验拓扑】

实验的拓扑图，如图6-1 所示。

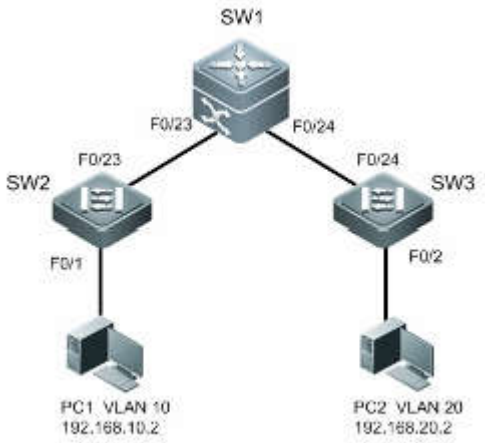


图 6-1

【实验设备】

三层交换机 1 台二层交换机 2 台 PC 机 2 台

【预备知识】

交换机转发原理、交换机基本配置、三层交换机路由功能。

【实验原理】

在二层交换机上划分 VLAN 可实现不同 VLAN 的主机接入，而 VLAN 间的主机通信为

不同网段间的通信，需要通过三层设备对数据进行路由转发才可以实现，通过在三层交换机上为各 VLAN 配置 SVI 接口，利用三层交换机的路由功能可以实现 VLAN 间的路由。

【实验步骤】

步骤 1在 SW1 中创建 VLAN。

```
SW1(config)#vlan 10
SW1(config-vlan)#vlan 20
SW1(config-vlan)#exit
```

步骤 2在 SW1 上给 VLAN 配置 IP 地址。

```
SW1(config)#interface vlan 10
SW1(config-if)#ip address 192.168.10.1 255.255.255.0
SW1(config-if)#no shutdown
SW1(config-if)#exit
SW1(config)#interface vlan 20
SW1(config-if)#ip address 192.168.20.1 255.255.255.0
SW1(config-if)#no shutdown
SW1(config-if)#exit
```

步骤 3W1 上配置 Trunk。

```
SW1(config)#interface fastEthernet 0/23
SW1(config-if)#switchport mode trunk
SW1(config-if)#exit
SW1(config)#interface fastEthernet 0/24
SW1(config-if)#switchport mode trunk
SW1(config-if)#exit
```

步骤 4在 SW2 和 SW3 上创建相应的 VLAN，并将端口划分到 VLAN。

```
SW2(config)#vlan 10
SW2(config-vlan)#exit
SW2(config)#interface fastEthernet 0/1
SW2(config-if)#switchport access vlan 10
SW2(config-if)#exit
SW3(config)#vlan 20
```

SW3(config-vlan)#exit

SW3(config)#interface fastEthernet 0/2

SW3(config-if)#switchport access vlan 20

SW3(config-if)#exit

步骤 5在 SW2 和 SW3 上配置 Trunk。

SW2(config)#interface fastEthernet 0/24

SW2(config-if)#switchport mode trunk

SW2(config-if)#exit

SW3(config)#interface fastEthernet 0/24

SW3(config-if)#switchport mode trunk

SW3(config-if)#exit

步骤 6验证测试。

按照拓扑配置 PC 并且连线，从 VLAN10 中的 PC1 ping VLAN20 中的 PC2，结果如下：

C:\Documents and Settings\shil>ping 192.168.20.2

Pinging 192.168.20.2 with 32 bytes of data:

Reply from 192.168.20.2: bytes=32 time<1ms TTL=64

Reply from 192.168.20.2: bytes=32 time<1ms TTL=64

Reply from 192.168.20.2: bytes=32 time<1ms TTL=64

Reply from 192.168.20.2: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.20.2:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

Approximate round trip times in milli-seconds:

Minimum = 0ms, Maximum = 0ms, Average = 0ms

从上述测试结果可以看到，通过接入层交换机上的 VLAN 划分和三层交换机的 SVI 配置，不同 VLAN 中的主机可以互相通信。

【注意事项】

交换机之间级联的端口需要配置为 Trunk。

【参考配置】

```
SW1#show running-config
Building configuration...
Current configuration : 1424 bytes
!
hostname SW1
!
vlan 1
!
vlan 10
!
vlan 20
!
!
enable secret 5 $1$khi7$zBty5tE6xwvCw3Dv
!
interface FastEthernet 0/1
!
interface FastEthernet 0/2
!
interface FastEthernet 0/3
.
.
.
interface FastEthernet 0/22
!
interface FastEthernet 0/23
switchport mode trunk
!
interface FastEthernet 0/24
switchport mode trunk
 !
interface GigabitEthernet 0/25
!
interface GigabitEthernet 0/26
```

```
!
interface GigabitEthernet 0/27
!
interface GigabitEthernet 0/28
!
interface VLAN 10
ip address 192.168.10.1 255.255.255.0
!
interface VLAN 20
ip address 192.168.20.1 255.255.255.0
!
!
line con 0
line vty 0 4
login
!
End
SW2#show running-config
System software version : 1.68 Build Apr 25 2007 Release
Building configuration...
Current configuration : 181 bytes
!
!
hostname SW2
vlan 1
!
vlan 10
!
interface fastEthernet 0/1
switchport access vlan 10
!
interface fastEthernet 0/24
switchport mode trunk
!
```

```
End
SW3#show running-config
System software version : 1.68 Build Apr 25 2007 Release
Building configuration...

Current configuration : 181 bytes
!
hostname SW3
vlan 1
!
vlan 20
!
interface fastEthernet 0/2
switchport access vlan 20
!
interface fastEthernet 0/24
switchport mode trunk
!
end
```

实验七 路由器的基本操作

【实验目的】

理解路由器的工作原理，掌握路由器的基本操作。

【背景描述】

你是某公司新进的网管，公司要求你熟悉网络产品，公司采用全系列锐捷网络产品，首先要求你登录路由器，了解、掌握路由器的命令行操作，进行路由器设备名的配置，配置路由器登录时的描述信息，对路由器的端口配置基本的参数。

【需求分析】

将计算机的 Com 口和路由器的 Console 口通过 Console 线缆连接起来，使用Windows提供的超级终端工具进行连接，登录路由器的命令行界面进行配置。

【实验拓扑】

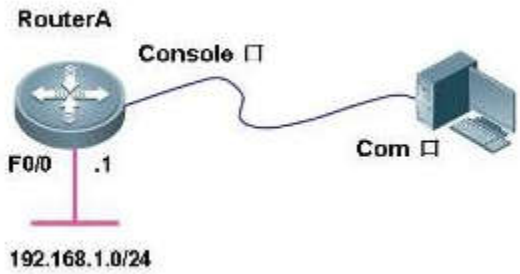


图 7-1 实验拓扑图

【实验设备】

路由器 1 台计算机 1 台

【预备知识】

路由器的工作原理和基本配置方法

【实验原理】

路由器的管理方式基本分为两种：带内管理和带外管理。通过路由器的 Console 口管

理路由器属于带外管理，不占用路由器的网络接口，但特点是线缆特殊，需要近距离配置。第一次配置路由器时必须利用 Console 进行配置，使其支持 telnet 远程管理。

路由器的命令行操作模式，主要包括：用户模式、特权模式、全局配置模式、端口模式等等几种。

用户模式

进入路由器后得到的第一个操作模式，该模式下可以简单查看路由器的软、硬件版本信息，并进行简单的测试。用户模式提示符为 Red-Giant>

特权模式

由用户模式进入的下一级模式，该模式下可以对路由器的配置文件进行管理，查看路由器的配置信息，进行网络的测试和调试等。特权模式提示符为 Red-Giant#

全局配置模式

属于特权模式的下一级模式，该模式下可以配置路由器的全局性参数（如主机名、登录信息等）。在该模式下可以进入下一级的配置模式，对路由器具体的功能进行配置。全局模式提示符为 Red-Giant (config)#

端口模式

属于全局模式的下一级模式，该模式下可以对路由器的端口进行参数配置。

Exit 命令是退回到上一级操作模式，

end 命令是直接退回到特权模式

路由器命令行支持获取帮助信息、命令的简写、命令的自动补齐、快捷键功能。

配置路由器的设备名称和路由器的描述信息必须在全局配置模式下执行。

Hostname 配置路由器的设备名称即命令提示符的前部分信息。

当用户登录路由器时，你可能需要告诉用户一些必要的信息。你可以通过设置标题来达到这个目的。你可以创建两种类型的标题：每日通知和登录标题。

Banner motd 配置路由器每日提示信息 motdmessage of the day。

Banner login 配置路由器远程登录提示信息，位于每日提示信息之后。

锐捷路由器接口 Fastethernet 接口默认情况下是 10M/100M 自适应端口，双工模式也为自适应。

在路由器的物理端口可以灵活配置带宽，但最大值为该端口的实际物理带宽。

查看路由器的系统和配置信息命令要在特权模式下执行。

Show version 查看路由器的版本信息，可以查看到路由器的硬件版本信息和软件版本信息，用于进行路由器操作系统升级时的依据。

Show ip route 查看路由表信息。

Show running-config 查看路由器当前生效的配置信息。

【实验步骤】

第一步：路由器命令行的基本功能

RSR20>?

！使用？显示当前模式下所有可执行的命令

Exec commands:

<1-99> Session number to resume

disable Turn off privileged commands

disconnectDisconnect an existing network connection

enable Turn on privileged commands

exit Exit from the EXEC

help Description of the interactive help system

lock Lock the terminal

ping Send echo messages

ping6 ping6

show

start-terminal-service

telnet

traceroute

Show running system information

Start terminal service

Open a telnet connection

Trace route to destination

RSR20>e?

enable exit

！显示当前模式下所有以 e 开头的命令

RSR20>en <tab>

！按键盘的 Tab 键自动补齐命令，路由器支持命令的自动补齐

RSR20>enable

！使用 enable 命令从用户模式进入特权模式

RSR20#copy ?

！显示 copy 命令后可执行的参数

flash: Copy from flash: file system

running-config Copy from current system configuration

startup-config Copy from startup configuration

tftp: Copy from tftp: file system

xmodem: Copy from xmodem: file system

RSR20#copy

% Incomplete command.

！提示命令未完，必须附带可执行的参数

RSR20#conf t

！路由器支持命令的简写，该命令代表 configure terminal

！进入路由器的全局配置模式

Enter configuration commands, one per line. End with CNTL/Z.

RSR20(config)#interface fastEthernet 0/0

！进入路由器端口 Fa0/0 的接口配置模式

RSR20(config-if)#

RSR20(config-if)#exit

！使用 exit 命令返回上一级的操作模式

RSR20(config)#interface fastEthernet 0/0

RSR20(config-if)#end

！使用 end 命令直接返回特权模式

RSR20#

RSR20(config)#interface fastEthernet 0/0

RSR20(config-if)#^Z

！使用快捷键 ctrl+Z 直接退回到特权模式

RSR20#

RSR20#ping 1.1.1.1

Sending 5, 100-byte ICMP Echoes to 1.1.1.1, timeout is 2 seconds:

<press Ctrl+C to break >

..^C

Success rate is 0 percent (0/3)

！在路由器特权模式下执行 ping 1.1.1.1 命令，发现不能 ping 通目标地址，路由器默认情况下需要发送 5 个数据包，若不想等到 5 个数据包均不能 ping 通目标地址时才认为目的地址不可到达，可在数据包未发出 5 个之前通过快捷键 Ctrl+C 终止当前操作。

第二步：配置路由器的名称和每日提示信息

RSR20>enable

RSR20#configure terminal

Enter configuration commands, one per line.

End with CNTL/Z.

RSR20(config)#hostname RouterA

！将路由器的名称设置为 RouterA

RouterA(config)#

RouterA(config)#banner motd &

！设置路由器的每日提示信息，motd 后面的参数为设置的终止符

Enter TEXT message. End with the character '&'.

Welcome to RouterA, if you are admin, you can config it.

If you are not admin, please EXIT.

&

RouterA(config)#

验证测试：

RouterA#exit

RouterA CON0 is now available

Press RETURN to get started

Welcome to RouterA, if you are admin, you can config it.

If you are not admin, please EXIT.

RouterA>

第三步：配置路由器的接口并查看接口配置

RouterA#configure terminal

Enter configuration commands, one per line.

End with CNTL/Z.

RouterA(config)#interface fastEthernet 0/0

！进入端口 Fa0/0 的接口配置模式

RouterA(config-if)#ip address 192.168.1.1 255.255.255.0

！配置接口的 IP 地址

RouterA(config-if)#no shutdown

！开启该端口

RouterA(config-if)#end

RouterA#show interfaces fastEthernet 0/0

！查看端口 Fa0/0 的状态是否为 UP，地址配置和流量统计等信息

Index(dec):1 (hex):1

FastEthernet 0/0 is UP , line protocol is UP

Hardware is MPC8248 FCC FAST ETHERNET CONTROLLER FastEthernet,

address is 00d0.f86b.3832 (bia 00d0.f86b.3832)

Interface address is: 192.168.1.1/24

ARP type: ARPA,ARP Timeout: 3600 seconds

MTU 1500 bytes, BW 100000 Kbit

Encapsulation protocol is Ethernet-II, loopback not set

Keepalive interval is 10 sec , set

Carrier delay is 2 sec

RXload is 1 ,Txload is 1

Queueing strategy: FIFO

Output queue 0/40, 0 drops;

Input queue 0/75, 0 drops

Link Mode: 100M/Full-Duplex

5 minutes input rate 1 bits/sec, 0 packets/sec

5 minutes output rate 1 bits/sec, 0 packets/sec

1 packets input, 60 bytes, 0 no buffer, 0 dropped

Received 1 broadcasts, 0 runts, 0 giants

0 input errors, 0 CRC, 0 frame, 0 overrun, 0 abort

1 packets output, 42 bytes, 0 underruns , 0 dropped

0 output errors, 0 collisions, 2 interface resets

第四步：查看路由器的配置

RouterA#show version

！查看路由器的版本信息

System description : Ruijie Router(RSR20-04) by Ruijie Network

System start time : 2009-8-16 5:37:38

System hardware version : 1.01

！硬件版本号

System software version : RGNOS 10.1.00(4), Release(18443)

！软件版本号

System boot version : 10.2.24515

System serial number : 1234942570135

```
RouterA#show ip route
！查看路由表信息
Codes: C - connected, S - static, R - RIP B - BGP
O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default
Gateway of last resort is no set
C      192.168.1.0/24 is directly connected, FastEthernet 0/0
C      192.168.1.1/32 is local host.
RouterA#show running-config
！查看路由器当前生效的配置信息
Building configuration...
Current configuration : 540 bytes
!
version RGNOS 10.1.00(4), Release(18443)(Tue Jul 17 20:50:30 CST 2007
-ubu1server)
hostname RouterA
!
!
interface FastEthernet 0/0
ip address 192.168.1.1 255.255.255.0
duplex auto
speed auto
!
interface FastEthernet 0/1
duplex auto
speed auto
!
line con 0
line aux 0
line vty 0 4
login
```

```
!
banner motd ^C
Welcome to RouterA, if you are admin, you can config it.
If you are not admin, please EXIT.
^C
!
end
```

【注意事项】

1、命令行操作进行自动补齐或命令简写时，要求所简写的字母必须能够唯一区别该命令。

如 Red-Giant# conf 可以代表 configure，但 Red-Giant#co 无法代表 configure，因为 co 开头的命令有两个 copy 和 configure，设备无法区别。

2、注意区别每个操作模式下可执行的命令种类。路由器不可以跨模式执行命令。

3、配置设备名称的有效字符是 22 个字节。

4、配置每日提示信息时，注意终止符不能在描述文本中出现。如果键入结束的终止符后仍然输入字符，则这些字符将被系统丢弃。

5、Serial 接口正常的端口速率最大是 2.048M（2000K）。

6、Show interface 和 show ip interface 之间的区别。

7、Show running-config 是查看当前生效的配置信息。Show startup-config 是查看保存在 NVRAM 里的配置文件信息。

8、路由器的配置信息全部加载在 RAM 里生效。路由器在启动过程中是将 NVRAM 里的配置文件加载到 RAM 里生效的。

实验八 配置静态 NAT

【实验目的】

配置网络地址变换，提供到公司共享服务器的可靠外部访问。

【背景描述】

某 IT 企业因业务扩展，需要升级网络，他们选择 172.16.1.0/24 作为私有地址，并用 NAT 来处理和外部网络的连接。

【需求分析】

公司需要将 172.16.1.5 和 172.16.1.6 两台主机作为共享服务器，需要外网能够访问，考虑到包括安全在内的诸多因素，公司希望对外部隐藏内部网络。

【实验拓扑】

实验的拓扑图，如图 8-1 所示。

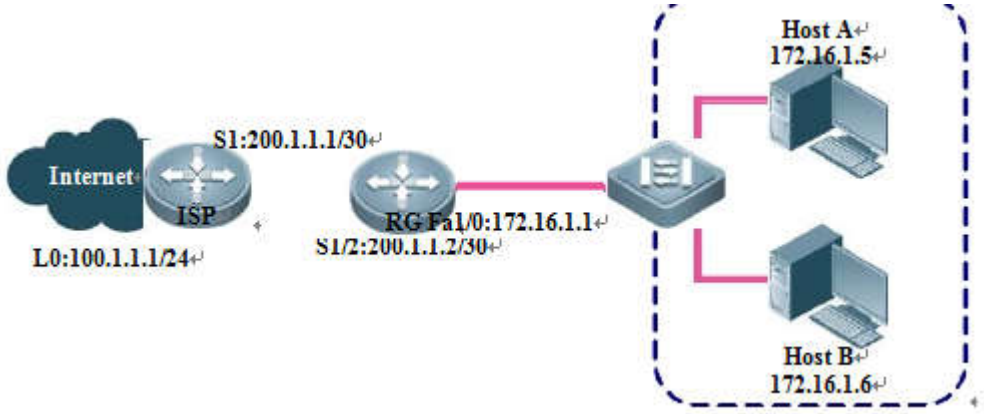


图 8-1

【实验设备】

路由器 2 台交换机 1 台 PC 机 2 台

【预备知识】

路由器基本配置知识、IP 路由知识、NAT 原理。

【实验原理】

在路由器上把 172.16.1.5、172.16.1.6 两台主机静态映射到外部，把内网隐藏起来。

【实验步骤】

步骤 1 在路由器上配置 IP 路由选择和 IP 地址。

RG#config t

RG(config)#interface serial 1/2

RG(config-if) #ip address 200.1.1.2 255.255.255.252

RG(config-if) #clock rate 64000

RG(config)#interface FastEthernet 1/0

RG(config-if) #ip address 172.16.1.1 255.255.255.0

RG(config)#ip route 0.0.0.0 0.0.0.0 serial 1/2

步骤 2 配置静态 NAT。

RG(config)#ip nat inside source static 172.16.1.5 200.1.1.80

RG(config)#ip nat inside source static 172.16.1.6 200.1.1.81

步骤 3 指定一个内部接口和一个外部接口。

RG(config)#interface serial 1/2

RG(config-if)#ip nat outside

RG(config)#interface FastEthernet 1/0

RG(config-if)#ip nat inside

步骤 4 验证测试。

用 telnet 登录远程主机 100.1.1.1 来测试 NAT 的转换。

C:\>telnet 100.1.1.1

User Access Verification

Password:

RG#sh ip nat translations

Pro Inside global	Inside local	Outside local	Outside global
tcp 200.1.1.80:1172	172.16.1.5:1172	100.1.1.1:23	100.1.1.1:23
tcp 200.1.1.81:1173	172.16.1.6:1173	100.1.1.1:23	100.1.1.1:23

RG#debug ip nat

RG#NAT: [A] pk 0x03f470e4 s 172.16.1.5->200.1.1.80:1172 [3980]

NAT: [B] pk 0x03f5b540 d 200.1.1.80->172.16.1.5:1172 [259]

NAT: [A] pk 0x03f4b3ac s 172.16.1.5->200.1.1.80:1172 [3981]

NAT: [B] pk 0x03f4a888 d 200.1.1.80->172.16.1.5:1172 [260]

NAT: [A] pk 0x03f478c8 s 172.16.1.5->200.1.1.80:1172 [3982]

NAT: [B] pk 0x03f4a6f4 d 200.1.1.80->172.16.1.5:1172 [261]

NAT: [A] pk 0x03f4bd24 s 172.16.1.5->200.1.1.80:1172 [3983]

NAT: [B] pk 0x03f498a8 d 200.1.1.80->172.16.1.5:1172 [262]。

【备注事项】

在做本实验前，一定要先配置好路由，要使用整个网络通信后再启用 NAT。

【参考配置】

```
RG#sh run
Building configuration...
Current configuration : 692 bytes
!
version 8.4 (building 15)
hostname RG
enable secret 5 $1$yLhr$s2r9y51xyE7yFA12
!
no service password-encryption
!
interface serial 1/2
ip nat outside
ip address 200.1.1.2 255.255.255.252
clock rate 64000
!
interface serial 1/3
clock rate 64000
!
interface FastEthernet 1/0
ip nat inside
ip address 172.16.1.1 255.255.255.0
duplex auto
speed auto
```

```
!
interface FastEthernet 1/1
duplex auto
speed auto
!
interface Null 0
!
ip nat inside source static 172.16.1.3 200.1.1.80
!
ip route 0.0.0.0 0.0.0.0 serial 1/2
!
line con 0
line aux 0
line vty 0
login
password 7 013244
line vty 1 4
login
```

实验九 配置动态 NAT

【实验目的】

配置网络地址变换，为私有地址的用户提供到外部网络的资源的访问。

【背景描述】

某 IT 企业因业务扩展，需要升级网络，他们选择 172.16.1.0/24 作为私有地址，并用 NAT 来处理和外部网络的连接。

【需求分析】

ISP 提供商给 IT 企业的一段公共 IP 地址的地址段为 200.1.1.200~100.1.1.210，需要内网使用这段址去访问 Internet，考虑到包括安全在内的诸多因素，公司希望对外部隐藏内部网络。

【实验拓扑】

实验的拓扑图，如图 9-1 所示。

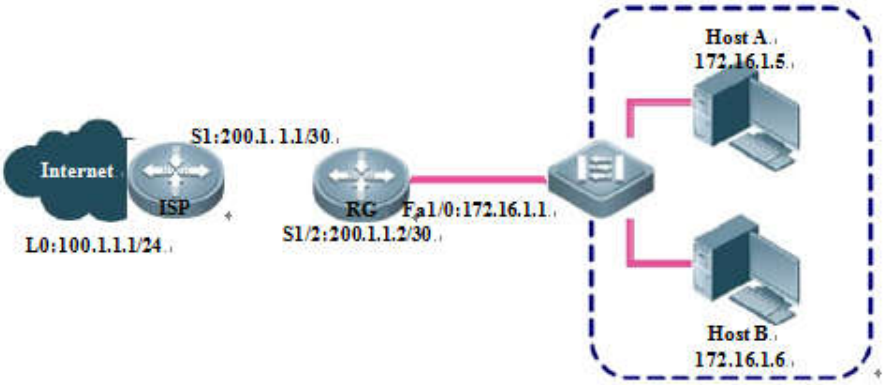


图 9-1

【实验设备】

路由器 2 台交换机 1 台 PC 机 2 台

【预备知识】

路由器基本配置知识、IP 路由知识、NAT 原理。

【实验原理】

在路由器上定义内网与外网接口，利用 NAT 地址池实现内网对外网的访问，并把内网隐藏起来。

【实验步骤】

步骤 1 在路由器上配置 IP 路由选择和 IP 地址。

RG#config t
RG(config)#interface serial 1/2
RG(config-if) #ip address 200.1.1.2 255.255.255.252
RG(config-if) #clock rate 64000
RG(config)#interface FastEthernet 1/0
RG(config-if) #ip address 172.16.1.1 255.255.255.0
RG(config)#ip route 0.0.0.0 0.0.0.0 serial 1/2

步骤 2 定义一个 IP 访问列表。
RG(config)#access-list 10 permit 172.16.1.0 0.0.0.255

步骤 3 配置动态 NAT。
RG(config)# ip nat pool ruijie 200.1.1.200 200.1.1.210 prefix-length 24
RG(config)#ip nat inside source list 10 pool ruijie

步骤 4 指定一个内部接口和一个外部接口。
RG(config)#interface serial 1/2
RG(config-if)#ip nat outside
RG(config)#interface FastEthernet 1/0
RG(config-if)#ip nat inside

步骤 5 验证测试。

用两台主机 telnet 登录远程主机 100.1.1.1 来测试 NAT 的转换。
C:\>telnet 100.1.1.1
User Access Verification
Password:
[root@lab ~]# telnet 100.1.1.1
Trying 100.1.1.1...
Connected to 100.1.1.1 (100.1.1.1).
Escape character is '^]'.
User Access Verification
Password:

RG#sh ip nat translations

Pro Inside global	Inside local	Outside local	Outside global
tcp 200.1.1.201:1174	172.16.1.6:1174	100.1.1.1:23	100.1.1.1:23
tcp 200.1.1.204:1026	172.16.1.5:1026	100.1.1.1:23	100.1.1.1:23

RG#debug ip nat
RG#NAT: [A] pk 0x03f553ec s 172.16.1.6->200.1.1.201:1176 [4082]

NAT: [B] pk 0x03f56d44 d 200.1.1.201->172.16.1.6:1174 [363]
NAT: [A] pk 0x03f560a4 s 172.16.1.6->200.1.1.201:1174 [4083]
NAT: [B] pk 0x03f4d044 d 200.1.1.201->172.16.1.6:1174 [364]
NAT: [A] pk 0x03f50620 s 172.16.1.6->200.1.1.201:1174 [4084]
NAT: [B] pk 0x03f4f968 d 200.1.1.201->172.16.1.6:1174 [365]
NAT: [A] pk 0x03f55580 s 172.16.1.6->200.1.1.201:1174 [4085]
……
NAT: [A] pk 0x03f54d84 s 172.16.1.5->200.1.1.204:1026 [52337]
NAT: [B] pk 0x03f56238 d 200.1.1.204->172.16.1.5:1026 [372]
NAT: [A] pk 0x03f56888 s 172.16.1.5->200.1.1.204:1026 [52339]
NAT: [A] pk 0x03f56560 s 172.16.1.5->200.1.1.204:1026 [52341]
NAT: [B] pk 0x03f566f4 d 200.1.1.204->172.16.1.5:1026 [373]
NAT: [A] pk 0x03f5b6d4 s 172.16.1.5->200.1.1.204:1026 [52343]
NAT: [B] pk 0x03f51c50 d 200.1.1.204->172.16.1.5:1026 [374]

【参考配置】

```
RG#sh run
Building configuration...
Current configuration : 789 bytes
version 8.4 (building 15)
hostname RG
enable secret 5 $1$yLhr$s2r9y51xyE7yFA12
access-list 10 permit 172.16.1.0 0.0.0.255
no service password-encryption
!
interface serial 1/2
ip nat outside
ip address 200.1.1.2 255.255.255.252
clock rate 64000
!
interface FastEthernet 1/0
ip nat inside
ip address 172.16.1.1 255.255.255.0
duplex auto
speed auto
!
interface FastEthernet 1/1
duplex auto
speed auto
!
interface Null 0
ip nat pool ruijie 200.1.1.200 200.1.1.210 prefix-length 24
```

```
ip nat inside source list 10 pool ruijie
ip route 0.0.0.0 0.0.0.0 serial 1/2
line con 0
line aux 0
line vty 0
login
password 7 093d12
line vty 1 4
login
!
```

实验十　RIP 路由协议基本配置

【实验目的】

掌握在路由器上如何配置 RIP 路由协议。

【背景描述】

假设在校园网在地理上分为 2 个区域，每个区域内分别有一台路由器连接了 2 个子网，需要将两台路由器通过以太网链路连接在一起并进行适当的配置，以实现这 4 个子网之间的互联互通。为了在未来每个校园区域扩充子网数量的时候，管理员不需要同时更改路由器的配置，计划使用 RIP 路由协议实现子网之间的互通。

【需求分析】

两台路由器通过快速以太网端口连接在一起，每个路由器上设置 2 个 Loopback 端口模拟子网，在所有端口运行 RIP 路由协议，实现所有子网间的互通。

【实验拓扑】

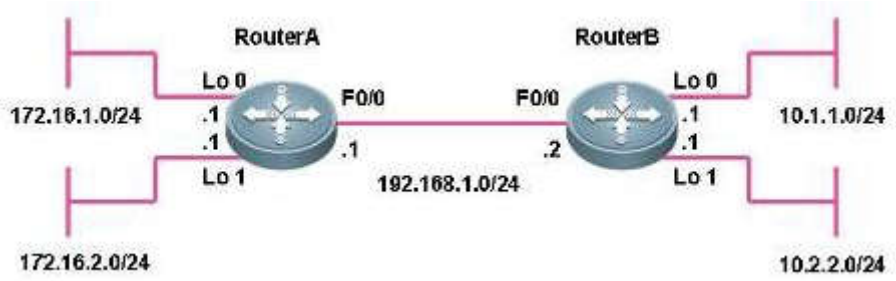


图 10 - 1　实验拓扑图

【实验设备】

路由器 2 台

【预备知识】

路由器的工作原理和基本配置方法，距离矢量路由协议，RIP 工作原理和配置方法

【实验原理】

RIP（Routing Information Protocols，路由信息协议）是应用较早、使用较普遍的 IGP（Interior Gateway Protocol，内部网关协议），适用于小型同类网络，是典型的距离矢量（distance-vector）协议。

RIP 协议以跳数做为衡量路径开销的，RIP 协议里规定最大跳数为 15。

RIP 在构造路由表时会使用到 3 种计时器：更新计时器、无效计时器、刷新计时器。它让每台路由器周期性地向每个相邻的邻居发送完整的路由表。路由表包括每个网络或子网的信息，以及与之相关的度量值。

【实验步骤】

第一步：配置两台路由器的主机名、接口 IP 地址

```
RSR20#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
RSR20(config)#hostname RouterA
RouterA(config)#
RouterA(config)#interface fastEthernet 0/0
RouterA(config-if)#ip address 192.168.1.1 255.255.255.0
RouterA(config-if)#no shutdown
RouterA(config-if)#exit
RouterA(config)#
RouterA(config)#interface loopback 0
RouterA(config-if)#Aug 15 23:46:32 RouterA %7:%LINE PROTOCOL CHANGE:
Interface Loopback 0, changed state to UP
RouterA(config-if)#ip address 172.16.1.1 255.255.255.0
RouterA(config-if)#exit
RouterA(config)#
RouterA(config)#interface loopback 1
RouterA(config-if)#Aug 15 23:47:00 RouterA %7:%LINE PROTOCOL CHANGE:
Interface Loopback 1, changed state to UP
RouterA(config-if)#ip address 172.16.2.1 255.255.255.0
RouterA(config-if)#exit

RSR20#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
RSR20(config)#hostname RouterB
RouterB(config)#
RouterB(config)#interface fastEthernet 0/0
RouterB(config-if)#ip address 192.168.1.2 255.255.255.0
RouterB(config-if)#no shutdown
RouterB(config-if)#exit
RouterB(config)#
RouterB(config)#interface loopback 0
RouterB(config-if)#Aug 8 21:00:00 RouterB %7:%LINE PROTOCOL CHANGE:
Interface Loopback 0, changed state to UP
RouterB(config-if)#ip address 10.1.1.1 255.255.255.0
RouterB(config-if)#exit
RouterB(config)#
```

RouterB(config)#interface loopback 1
RouterB(config-if)#Aug 8 21:00:28 RouterB %7:%LINE PROTOCOL CHANGE:
Interface Loopback 1, changed state to UP
RouterB(config-if)#ip address 10.2.2.1 255.255.255.0
RouterB(config-if)#exit

第二步：在两台路由器上配置 RIP 路由协议
RouterA(config)#router rip
RouterA(config-router)#network 192.168.1.0
RouterA(config-router)#network 172.16.1.0
RouterA(config-router)#exit
RouterB(config)#router rip
RouterB(config-router)#network 192.168.1.0
RouterB(config-router)#network 10.0.0.0
RouterB(config-router)#exit

第三步：查看 RIP 配置信息，路由表
RouterA#show ip route
Codes: C - connected, S - static, R - RIP B - BGP
O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default

Gateway of last resort is no set
R 10.0.0.0/8 [120/1] via 192.168.1.2, 00:00:17, FastEthernet 0/0
C 172.16.1.0/24 is directly connected, Loopback 0
C 172.16.1.1/32 is local host.
C 172.16.2.0/24 is directly connected, Loopback 1
C 172.16.2.1/32 is local host.
C 192.168.1.0/24 is directly connected, FastEthernet 0/0
C 192.168.1.1/32 is local host.
RouterA#
Routing Protocol is "rip"
Sending updates every 30 seconds, next due in 21 seconds
Invalid after 180 seconds, flushed after 120 seconds
Outgoing update filter list for all interface is: not set
Incoming update filter list for all interface is: not set
Default redistribution metric is 1
Redistributing:
Default version control: send version 1, receive any version
Interface Send Recv Key-chain
FastEthernet 0/0 1 12

```
Loopback 0          1               12
Loopback 1          1               12
Routing for Networks:
172.16.0.0
192.168.1.0
Distance: (default is 120)

RouterA#
RouterB#show ip route
Codes: C - connected, S - static, R - RIP B - BGP
O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default
Gateway of last resort is no set
C      10.1.1.0/24 is directly connected, Loopback 0
C      10.1.1.1/32 is local host.
C      10.2.2.0/24 is directly connected, Loopback 1
C      10.2.2.1/32 is local host.
R172.16.0.0/16 [120/1] via 192.168.1.1, 00:00:12, FastEthernet 0/0
C192.168.1.0/24 is directly connected, FastEthernet 0/0
C192.168.1.2/32 is local host.

RouterA#show ip rip database
10.0.0.0/8      auto-summary
10.0.0.0/8
[1] via 192.168.1.2 FastEthernet 0/0 00:09
172.16.0.0/16      auto-summary
172.16.1.0/24
[1] directly connected, Loopback 0
172.16.2.0/24
[1] directly connected, Loopback 1
192.168.1.0/24      auto-summary
192.168.1.0/24
[1] directly connected, FastEthernet 0/0

RouterA#show ip rip interface
FastEthernet 0/0 is up, line protocol is up
Routing Protocol: RIP
Receive RIPv1 and RIPv2 packets
Send RIPv1 packets only
Passive interface: Disabled
Split horizon: Enabled
```

V2 Broadcast: Disabled
Multicast registe: Registed
Interface Summary Rip:Not Configured
IP interface address:192.168.1.1/24
FastEthernet 0/1 is down, line protocol is down
RIP is not enabled on this interface
Null 0 is up, line protocol is up
RIP is not enabled on this interface
Loopback 0 is up, line protocol is up
Routing Protocol: RIP
Receive RIPv1 and RIPv2 packets
Send RIPv1 packets only
Passive interface: Disabled
Split horizon: Enabled
V2 Broadcast: Disabled
Multicast registe: Registed
Interface Summary Rip:Not Configured
IP interface address:172.16.1.1/24
Loopback 1 is up, line protocol is up
Routing Protocol: RIP
Receive RIPv1 and RIPv2 packets
Send RIPv1 packets only
Passive interface: Disabled
Split horizon: Enabled
V2 Broadcast: Disabled
Multicast registe: Registed
Interface Summary Rip:Not Configured
IP interface address:172.16.2.1/24

RouterB#show ip rip
Routing Protocol is "rip"
Sending updates every 30 seconds, next due in 21 seconds
Invalid after 180 seconds, flushed after 120 seconds
Outgoing update filter list for all interface is: not set
Incoming update filter list for all interface is: not set
Default redistribution metric is 1
Redistributing:
Default version control: send version 1, receive any version

InterfaceSend RecvKey-chain

FastEthernet 0/0 1 12
Loopback 0 1 12
Loopback 1 1 12

Routing for Networks:
10.0.0.0
192.168.1.0
Distance: (default is 120)

RouterB#show ip rip database
10.0.0.0/8 auto-summary
10.1.1.0/24
[1] directly connected, Loopback 0
10.2.2.0/24
[1] directly connected, Loopback 1
172.16.0.0/16 auto-summary
172.16.0.0/16
[1] via 192.168.1.1 FastEthernet 0/0 00:08
192.168.1.0/24 auto-summary
192.168.1.0/24
[1] directly connected, FastEthernet 0/0

RouterB#show ip rip interface
FastEthernet 0/0 is up, line protocol is up
Routing Protocol: RIP
Receive RIPv1 and RIPv2 packets
Send RIPv1 packets only
Passive interface: Disabled
Split horizon: Enabled
V2 Broadcast: Disabled
Multicast registe: Registed
Interface Summary Rip:Not Configured
IP interface address:192.168.1.2/24
FastEthernet 0/1 is down, line protocol is down
RIP is not enabled on this interface
Null 0 is up, line protocol is up
RIP is not enabled on this interface
Loopback 0 is up, line protocol is up
Routing Protocol: RIP
Receive RIPv1 and RIPv2 packets
Send RIPv1 packets only
Passive interface: Disabled
Split horizon: Enabled
V2 Broadcast: Disabled
Multicast registe: Registed
Interface Summary Rip:Not Configured
IP interface address:10.1.1.1/24

Loopback 1 is up, line protocol is up
Routing Protocol: RIP
Receive RIPv1 and RIPv2 packets
Send RIPv1 packets only
Passive interface: Disabled
Split horizon: Enabled
V2 Broadcast: Disabled
Multicast registe: Registed
Interface Summary Rip:Not Configured
IP interface address:10.2.2.1/24

第四步：测试网络连通性

```
RouterA#ping 10.1.1.1
Sending 5, 100-byte ICMP Echoes to 10.1.1.1, timeout is 2 seconds:
<press Ctrl+C to break >
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms

RouterA#ping 10.2.2.1
Sending 5, 100-byte ICMP Echoes to 10.2.2.1, timeout is 2 seconds:
<press Ctrl+C to break >
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10 ms

RouterB#ping 172.16.1.1
Sending 5, 100-byte ICMP Echoes to 172.16.1.1, timeout is 2 seconds:
<press Ctrl+C to break >
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms

RouterB#ping 172.16.2.1
Sending 5, 100-byte ICMP Echoes to 172.16.2.1, timeout is 2 seconds:
<press Ctrl+C to break >
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

第五步：用 debug 命令观察路由器接收和发生路由更新的情况

下面是一个完整的 RIP 路由器接收更新和发送更新的过程，从中可以看到 RouterB 接收到了 RouterA 发送的更新，其中包含一条路由信息 172.16.0.0（可以看到水平分割原则的作用），然后刷新了路由表。

RouterB 本身发送的更新报文则在 Fa0/0、Lo0 和 Lo1 三个端口发出，采用广播的方式，广播地址分别为 192.168.1.255，10.1.1.255，10.2.2.255，使用 UDP 的 520 端口。在水平

分割的原则下，每个端口发送的路由信息均不相同。

```
RouterB#debug ip rip
Aug      8 21:06:08 RouterB %7: [RIP] RIP recveived packet, sock=2125
src=192.168.1.1 len=24
Aug 8 21:06:08 RouterB %7: [RIP] Cancel peer remove timer
Aug 8 21:06:08 RouterB %7:[RIP] Peer remove timer shedule...
Aug 8 21:06:08 RouterB %7:          route-entry: family 2 ip 172.16.0.0 metric 1
Aug 8 21:06:08 RouterB %7: [RIP] Received version 1 response packet
Aug 8 21:06:08 RouterB %7: [RIP] Translate mask to 16
Aug8 21:06:08 RouterB %7: [RIP]routesrc=192.168.1.1 intf=1
Aug8 21:06:08 RouterB %7: [RIP]

Old path is: nhop=192.168.1.1
New path is: nhop=192.168.1.1

routesrc=192.168.1.1
Aug 8 21:06:08 RouterB %7: [RIP] [172.16.0.0/16] RIP route refresh!
Aug 8 21:06:08 RouterB %7: [RIP] [172.16.0.0/16] RIP distance apply from192.168.1.1!
Aug 8 21:06:08 RouterB %7: [RIP] [172.16.0.0/16] ready to refresh kernel...
Aug 8 21:06:08 RouterB %7: [RIP] NSM refresh: IPv4 RIP Route 172.16.0.0/16
distance=120 metric=1 nexthop_num=1 distance=120 nexhop=192.168.1.1ifindex=1
Aug 8 21:06:08 RouterB %7: [RIP] [172.16.0.0/16] cancel route timer
Aug 8 21:06:08 RouterB %7: [RIP] [172.16.0.0/16] route timer schedule...
Aug 8 21:06:23 RouterB %7: [RIP] Output timer expired to send reponse
Aug 8 21:06:23 RouterB %7: [RIP] Prepare to send BROADCAST response...
Aug 8 21:06:23 RouterB %7: [RIP] Building update entries on FastEthernet 0/0
Aug 8 21:06:23 RouterB %7:          network 10.0.0.0 metric 1
Aug 8 21:06:23 RouterB %7: [RIP] Send packet to 192.168.1.255 Port 520 onFastEthernet 0/0
Aug 8 21:06:23 RouterB %7: [RIP] Prepare to send BROADCAST response...
Aug 8 21:06:23 RouterB %7: [RIP] Building update entries on Loopback 0
Aug 8 21:06:23 RouterB %7:          network 10.2.2.0 metric 1
Aug 8 21:06:23 RouterB %7:          network 172.16.0.0 metric 2
Aug 8 21:06:23 RouterB %7:          network 192.168.1.0 metric 1
Aug 8 21:06:23 RouterB %7: [RIP] Send packet to 10.1.1.255 Port 520 onLoopback 0
Aug 8 21:06:23 RouterB %7: [RIP] Prepare to send BROADCAST response...
Aug 8 21:06:23 RouterB %7: [RIP] Building update entries on Loopback 1
Aug 8 21:06:23 RouterB %7:          network 10.1.1.0 metric 1
Aug 8 21:06:23 RouterB %7:          network 172.16.0.0 metric 2
Aug 8 21:06:23 RouterB %7:          network 192.168.1.0 metric 1
Aug 8 21:06:23 RouterB %7: [RIP] Send packet to 10.2.2.255 Port 520 onLoopback 1
Aug 8 21:06:23 RouterB %7: [RIP] Schedule response send timer
```

【注意事项】

1、配置 RIP 的 Network 命令时只支持 A、B、C 的主网络号，如果写入子网则自动转为主网络号。

2、No auto-summary 功能只有在 RIPv2 支持。

【参考配置】

```
RouterA#show running-config
Building configuration...
Current configuration : 612 bytes
!
version RGNOS 10.1.00(4), Release(18443)(Tue Jul 17 20:50:30 CST 2007 -ubu1server)
hostname RouterA
!
interface FastEthernet 0/0
ip address 192.168.1.1 255.255.255.0
duplex auto
speed auto
!
interface FastEthernet 0/1
duplex auto
speed auto
!
interface Loopback 0
ip address 172.16.1.1 255.255.255.0
!
interface Loopback 1
ip address 172.16.2.1 255.255.255.0
!
router rip
network 172.16.0.0
network 192.168.1.0
!
line con 0

line aux 0
line vty 0 4
login
!
end

RouterB#show running-config
Building configuration...
Current configuration : 606 bytes
!
```

```
version RGNOS 10.1.00(4), Release(18443)(Tue Jul 17 20:50:30 CST 2007 -ubu1server)
hostname RouterB
!
interface FastEthernet 0/0
ip address 192.168.1.2 255.255.255.0
duplex auto
speed auto
!
interface FastEthernet 0/1
duplex auto
speed auto
!
interface Loopback 0
ip address 10.1.1.1 255.255.255.0
!
interface Loopback 1
ip address 10.2.2.1 255.255.255.0
!
router rip
network 10.0.0.0
network 192.168.1.0
!
line con 0
line aux 0
line vty 0 4
login
!
End
```

实验十一 OSPF 基本配置

【实验目的】

掌握在路由器上配置 OSPF 单区域。

【背景描述】

假设校园网通过 1 台三层交换机连到校园网出口路由器，路由器再和校园外的另 1 台路由器连接，现做适当配置，实现校园网内部主机与校园网外部主机的相互通信。

本实验以两台路由器、1 台三层交换机为例。S3550 上划分有 VLAN10 和 VLAN50，其中 VLAN10 用于连接 RA，VLAN50 用于连接校园网主机。

【需求分析】

需要在路由器和交换机上配置 OSPF 路由协议，使全网互通，从而实现信息的共享和传递。

【实验拓扑】

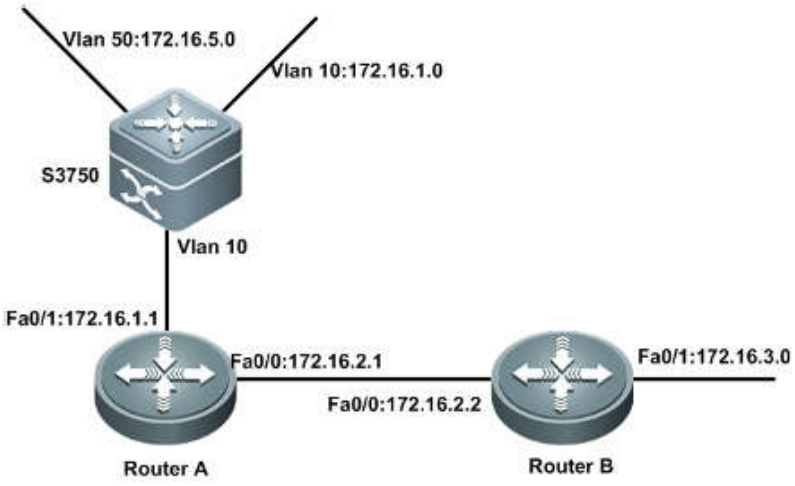


图 11-1 实验拓扑图

【实验设备】

三层交换机 1 台路由器 2 台交叉线或直连线 3 条

【预备知识】

路由器基本配置知识、OSPF

【实验原理】

OSPF（Open Shortest Path First，开放式最短路径优先）协议，是目前网络中应用最广泛的路由协议之一。属于内部网关路由协议，能够适应各种规模的网络环境，是典型的链路状态（link-state）协议。

OSPF 路由协议通过向全网扩散本设备的链路状态信息，使网络中每台设备最终同步一个具有全网链路状态的数据库（LSDB），然后路由器采用 SPF 算法，以自己为根，计算到达其他网络的最短路径，最终形成全网路由信息。

OSPF 属于无类路由协议，支持 VLSM（变长子网掩码）。OSPF 是以组播的形式进行链路状态的通告的。

在大规模的网络环境中，OSPF 支持区域的划分，将网络进行合理规划。划分区域时必须存在 area0（骨干区域）。其他区域和骨干区域直接相连，或通过虚链路的方式连接。

【实验步骤】

第一步：在路由器和三层交换机配置 IP 地址

```
switch#configure terminal
switch(config)#hostname S3750
S3750(config)#vlan 10
S3750(config-vlan)#exit
S3750(config)#vlan 50
S3750(config-vlan)#exit
S3750(config)#interface f0/1
S3750(config-if)#switchport access vlan 10
S3750(config-if)#exit
S3750(config)#interface f0/2
S3750(config-if)#switchport access vlan 50
S3750(config-if)#exit
S3750(config)#interface vlan 10
S3750(config-if)#ip address 172.16.1.2 255.255.255.0
S3750(config-if)#no shutdown
S3750(config-if)#exit
S3750(config)#interface vlan 50
S3750(config-if)#ip address 172.16.5.1 255.255.255.0
S3750(config-if)#no shutdown
S3750(config-if)#exit
```

```
RouterA(config)# interface fastethernet 0/1
RouterA(config-if)# ip address 172.16.1.1 255.255.255.0
RouterA(config-if)# no shutdown
RouterA(config-if)#exit
RouterA(config)# interface fastethernet 0/0
RouterA(config-if)# ip address 172.16.2.1 255.255.255.0
```

```
RouterB(config-if)# no shutdown
RouterB(config)# interface fastethernet 0/1
RouterB(config-if)# ip address 172.16.3.1 255.255.255.0
RouterB(config-if)# no shutdown
RouterB(config-if)#exit
RouterB(config)# interface fastethernet 0/0
RouterB(config-if)# ip address 172.16.2.2 255.255.255.0
RouterB(config-if)# no shutdown
```

第二步：配置 OSPF 路由协议

```
S3750(config)#router ospf
S3750(config-router)#network 172.16.5.0 0.0.0.255 area 0
S3750(config-router)#network 172.16.1.0 0.0.0.255 area 0
S3750(config-router)#end
RouterA(config)# router ospf
RouterA(config-router)#network 172.16.1.0 0.0.0.255 area 0
RouterA(config-router)#network 172.16.2.0 0.0.0.255 area 0
RouterA(config-router)#end
RouterB(config)#router ospf
RouterB(config-router)#network 172.16.2.0 0.0.0.255 area 0
RouterB(config-router)#network 172.16.3.0 0.0.0.255 area 0
RouterB(config-router)#end
```

第三步：验证测试

S3750#show vlan

VLAN	Name	Status	Ports
1	VLAN0001	STATIC	Fa0/3, Fa0/4, Fa0/5, Fa0/6, Fa0/7, Fa0/8, Fa0/9, Fa0/10, Fa0/11, Fa0/12, Fa0/13, Fa0/14, Fa0/15, Fa0/16, Fa0/17, Fa0/18, Fa0/22, Fa0/19, Fa0/20, Fa0/21, Fa0/23, Fa0/24, Gi0/25, Gi0/26, Gi0/27, Gi0/28
10	VLAN0010	STATIC	
50	VLAN0050	STATIC	Fa0/1, Fa0/2

S3750#show ip interface brief

Interface	IP-Address(Pri)	OK?	Status
VLAN 10	172.16.1.2/24	YES	UP
VLAN 50	172.16.5.1/24	YES	UP

RA#show ip interface brief

Interface	IP-Address(Pri)	OK?	Status
FastEthernet 0/0	172.16.2.1/24	YES	UP
FastEthernet 0/1	172.16.1.1/24	YES	UP

RB#show ip interface brief

Interface	IP-Address(Pri)	OK?	Status
FastEthernet 0/0	172.16.2.2/24	YES	UP
FastEthernet 0/1	172.16.1.3/24	YES	UP
Loopback 0	no address	YES	DOWN

S3750#show ip route

```
Codes: C - connected, S - static, R - RIP B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default

Gateway of last resort is no set
C    172.16.1.0/24 is directly connected, VLAN 10
C    172.16.1.2/32 is local host.
O    172.16.2.0/24 [110/2] via 172.16.1.1, 00:14:09, VLAN 10
O    172.16.3.0/24 [110/3] via 172.16.1.1, 00:04:39, VLAN 10
C    172.16.5.0/24 is directly connected, VLAN 50
C    172.16.5.1/32 is local host.
```

RA#show ip route

```
Codes: C - connected, S - static, R - RIP B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default

Gateway of last resort is no set
C    172.16.1.0/24 is directly connected, FastEthernet 0/1
```

```
C    172.16.1.1/32 is local host.
C    172.16.2.0/24 is directly connected, FastEthernet 0/0
C    172.16.2.1/32 is local host.
O    172.16.3.0/24 [110/2] via 172.16.2.2, 00:05:21, FastEthernet 0/0
O    172.16.5.0/24 [110/2] via 172.16.1.2, 00:14:51, FastEthernet 0/1
```

RB#show ip route

```
Codes: C - connected, S - static, R - RIP B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default

Gateway of last resort is no set
O    172.16.1.0/24 [110/2] via 172.16.2.1, 00:05:58, FastEthernet 0/0
C    172.16.2.0/24 is directly connected, FastEthernet 0/0
C    172.16.2.2/32 is local host.
C    172.16.3.0/24 is directly connected, FastEthernet 0/1
C    172.16.3.1/32 is local host.
O    172.16.5.0/24 [110/3] via 172.16.2.1, 00:15:22, FastEthernet 0/0
```

RA#show ip ospf neighbor

```
OSPF process 1:
Neighbor ID     Pri   State           Dead Time   Address         Interface
172.16.5.1        1   Full/DR         00:00:38    172.16.1.2      FastEthernet 0/1
172.16.2.2        1   Full/DR         00:00:36    172.16.2.2      FastEthernet 0/0
```

RA#show ip ospf interface fastEthernet 0/0

```
FastEthernet 0/0 is up, line protocol is up
Internet Address 172.16.2.1/24, Ifindex 1, Area 0.0.0.0, MTU 1500
Matching network config: 172.16.2.0/24
Process ID 1, Router ID 172.167.1.1, Network Type BROADCAST, Cost: 1
Transmit Delay is 1 sec, State BDR, Priority 1
Designated Router (ID) 172.16.2.2, Interface Address 172.16.2.2
Backup Designated Router (ID) 172.167.1.1, Interface Address 172.16.2.1
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
Hello due in 00:00:05
Neighbor Count is 1, Adjacent neighbor count is 1
Crypt Sequence Number is 82589
Hello received 114 sent 115, DD received 4 sent 5
LS-Req received 1 sent 1, LS-Upd received 5 sent 9
```

LS-Ack received 6 sent 4, Discarded 0

【注意事项】

1、在申明直连网段时，注意要写该网段的反掩码。

2、在申明直连网段时，必须指明所属的区域。

【参考配置】

```
S3750#show running-config

Building configuration...
Current configuration : 1399 bytes
!
version RGNOS 10.1.00(4), Release(18443)(Tue Jul 17 19:51:54 CST 2007
-ubu6server)
hostname S3750
!
vlan 1
!
vlan 10
!
vlan 50
!
interface FastEthernet 0/1
switchport access vlan 10
!
interface FastEthernet 0/2
switchport access vlan 50
!
interface FastEthernet 0/3
.
.
.
!
interface GigabitEthernet 0/27
!
interface GigabitEthernet 0/28
!
interface VLAN 10
ip address 172.16.1.2 255.255.255.0
!
interface VLAN 50
ip address 172.16.5.1 255.255.255.0
!
```

```
router ospf 1

network 172.16.1.0 0.0.0.255 area 0
network 172.16.5.0 0.0.0.255 area 0
!
line con 0
line vty 0 4
login
!
end

RB#show running-config

Building configuration...
Current configuration : 579 bytes
!
version RGNOS 10.1.00(4), Release(18443)(Tue Jul 17 20:50:30 CST 2007
-ubu1server)
hostname RB
!
interface FastEthernet 0/0
ip address 172.16.2.2 255.255.255.0
duplex auto
speed auto
!
interface FastEthernet 0/1
ip address 172.16.3.1 255.255.255.0
duplex auto
speed auto
!
interface Loopback 0
!
router ospf 1
network 172.16.2.0 0.0.0.255 area 0
network 172.16.3.0 0.0.0.255 area 0
!
line con 0
line aux 0
line vty 0 4
login
!
end

RA#show running-config
```

```
Building configuration...
Current configuration : 554 bytes
!
version RGNOS 10.1.00(4), Release(18443)(Tue Jul 17 20:50:30 CST 2007
-ubu1server)
hostname RA
!
interface FastEthernet 0/0
ip address 172.16.2.1 255.255.255.0
duplex auto
speed auto
!
interface FastEthernet 0/1
ip address 172.16.1.1 255.255.255.0
duplex auto
speed auto
!
router ospf 1
network 172.16.1.0 0.0.0.255 area 0
network 172.16.2.0 0.0.0.255 area 0
!
line con 0
line aux 0
line vty 0 4
login
!
end
```

实验十二 利用单臂路由实现 VLAN 间路由

【实验目的】

掌握如何路由器端口上划分子接口、封装 Dot1Q（IEEE 802.1Q）协议，实现 VLAN 间的路由。

【背景描述】

假设某企业有两个主要部门：销售部和技术部，员工都连接在 1 台二层交换机上，网络内有 1 台路由器用于连接 Internet。现在发现网络内的广播流量较多，需要对广播进行限制但不能影响 2 个部门进行相互通信，要在路由器上做适当配置来实现这一目标。

【需求分析】

需要在交换机上配置 VLAN，然后在路由器连接交换机的端口上划分子接口，给相应的 VLAN 设置 IP 地址，以实现 VLAN 间的路由。

【实验拓扑】

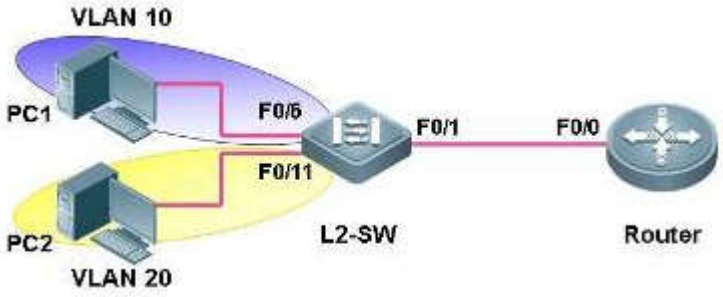


图 12-1 实验拓扑图

【实验设备】

路由器 1 台　　二层交换机 1 台

【预备知识】

交换机的基本配置方法，VLAN 的工作原理和配置方法，Trunk 的工作原理和配置方法，单臂路由的工作原理和配置方法

【实验原理】

在交换网络中，通过 VLAN 对一个物理网络进行了逻辑划分，不同的 VLAN 之间是无法直接访问的，必须通过三层的路由设备进行连接。一般利用路由器或三层交换机来实现不同 VLAN 之间的互相访问。

将路由器和交换机相连，使用 IEEE 802.1Q 来启动一个路由器上的子接口成为干道模式，

就可以利用路由器来实现 VLAN 之间的通信。

路由器可以从某一个 VLAN 接收数据包并且将这个数据包转发到另外的一个 VLAN，要实施 VLAN 间的路由，必须在一个路由器的物理接口上启用子接口，也就是将以太网物理接口划分为多个逻辑的、可编址的接口，并配置成干道模式，每个 VLAN 对应一个这种接口，这样路由器就能够知道如何到达这些互联的 VLAN。

【实验步骤】

第一步：配置交换机的主机名、划分 VLAN 和添加端口、设置 Trunk

```
Switch#configure terminal
Switch(config)#hostname L2-SW
L2-SW(config)#vlan 10
L2-SW(config-vlan)#name xiaoshou
L2-SW(config-vlan)#vlan 20
L2-SW(config-vlan)#name jishu
L2-SW(config-vlan)#exit
L2-SW(config)#interface range fastEthernet 0/6-10
L2-SW(config-if-range)#switchport mode access
L2-SW(config-if-range)#switchport access VLAN 10
L2-SW(config-if-range)#exit
L2-SW(config)#interface range fastEthernet 0/11-15
L2-SW(config-if-range)#switchport mode access
L2-SW(config-if-range)#switchport access vlan 20
L2-SW(config-if-range)#exit
L2-SW(config)#interface fastEthernet 0/1
L2-SW(config-if)#switchport mode trunk
L2-SW(config-if)#end
```

第二步：在路由器上设置名称、划分子接口、配置 IP 地址

```
RSR20#configure terminal
RSR20(config)#hostname Router
Router(config)#interface fastEthernet 0/0
Router(config-if)#no ip address
！去掉路由器主接口上的 IP 地址
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)#interface fastEthernet 0/0.10
！进入子接口 Fa0/0.10
Router(config-subif)#encapsulation dot1Q 10
！指定子接口 Fa0/0.10 对应 VLAN 10，并配置干道模式
Router(config-subif)#ip address 192.168.10.1 255.255.255.0
！配置子接口 Fa0/0.10 的 IP 地址
Router(config-subif)#exit
```

```
Router(config)#interface fastEthernet 0/0.20
！进入子接口 Fa0/0.20
Router(config-subif)#encapsulation dot1Q 20
！指定子接口 Fa0/0.20 对应 VLAN 20，并配置干道模式
Router(config-subif)#ip address 192.168.20.1 255.255.255.0
！配置子接口 Fa0/0.20 的 IP 地址
Router(config-subif)#end
```

第三步：查看交换机的 VLAN 和 Trunk 配置

```
L2-SW#show vlan
VLAN Name                                Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/1 ,Fa0/2 ,Fa0/3
                                                Fa0/4 ,Fa0/5 ,Fa0/16
                                                Fa0/17,Fa0/18,Fa0/19
                                                Fa0/20,Fa0/21,Fa0/22
                                                Fa0/23,Fa0/24
10   xiaoshou                         active    Fa0/1 ,Fa0/6 ,Fa0/7
                                                Fa0/8 ,Fa0/9 ,Fa0/10
20   jishu                            active    Fa0/1 ,Fa0/11,Fa0/12
                                                Fa0/13,Fa0/14,Fa0/15
L2-SW#
L2-SW#show interfaces fastEthernet 0/1 switchport

Interface Switchport Mode         Access Native      Protected VLAN lists
---------- ---------- --------- ------- -------- --------- --------------------
Fa0/1       Enabled    Trunk      1       1          Disabled     All
```

第四步：查看路由器的路由表

```
Router#show ip route

Codes:   C - connected, S - static, R - RIP B - BGP
         O - OSPF, IA - OSPF inter area
         N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
         E1 - OSPF external type 1, E2 - OSPF external type 2
         i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
         * - candidate default

Gateway of last resort is no set
C    192.168.10.0/24 is directly connected, FastEthernet 0/0.10
C    192.168.10.1/32 is local host.
C    192.168.20.0/24 is directly connected, FastEthernet 0/0.20
C    192.168.20.1/32 is local host.
```

第五步：测试网络连通性

给 PC1 和 PC2 分别配置 192.168.10.0/24 和 192.168.20.0/24 网段内的 IP 地址，并分别以 192.168.10.1 和 192.168.20.1 作为网关，例如 PC2 的 IP 地址配置为：

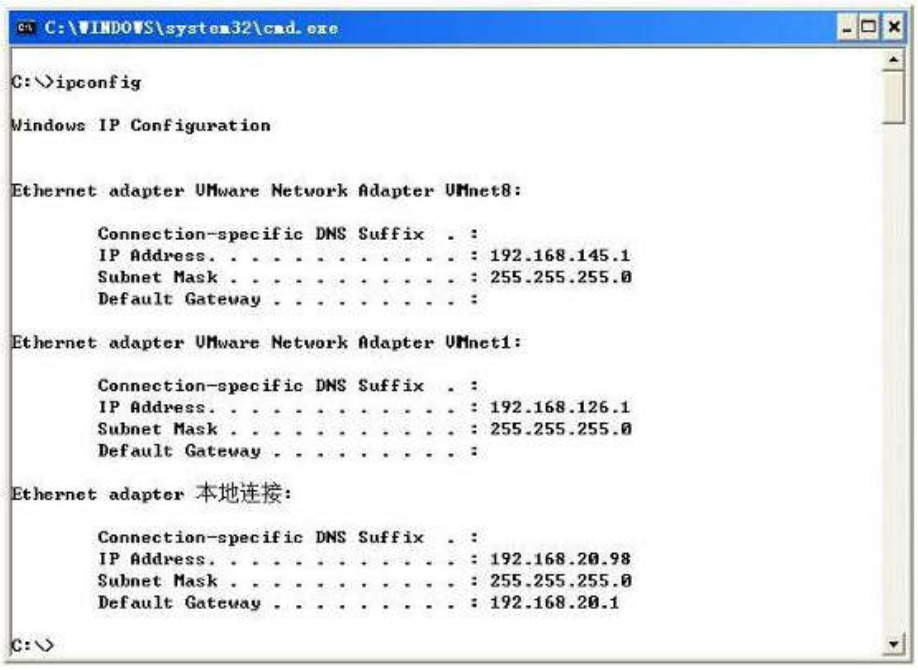


图 12-2 PC2 的 IP 地址配置

从 PC2 上 ping 所属 VLAN 的网关、VLAN 10 的网关和 PC1 的结果如下，说明配置单臂路由后，网络已经全部实现互联互通。

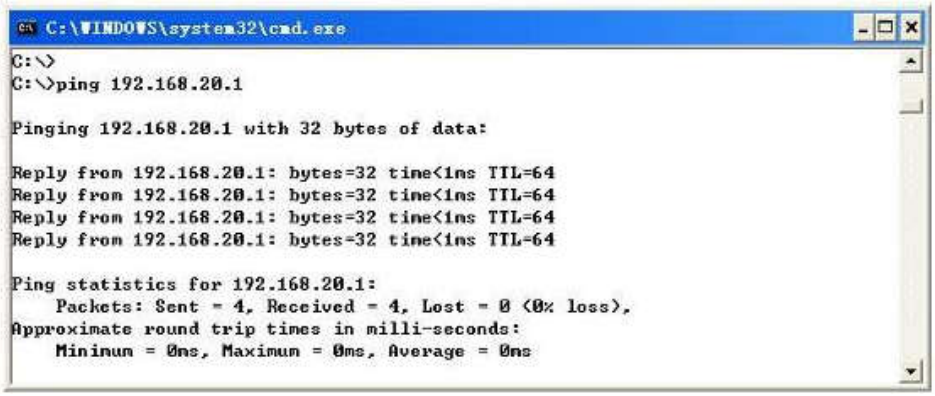


图 12-3 从 PC2 ping VLAN 20 的网关

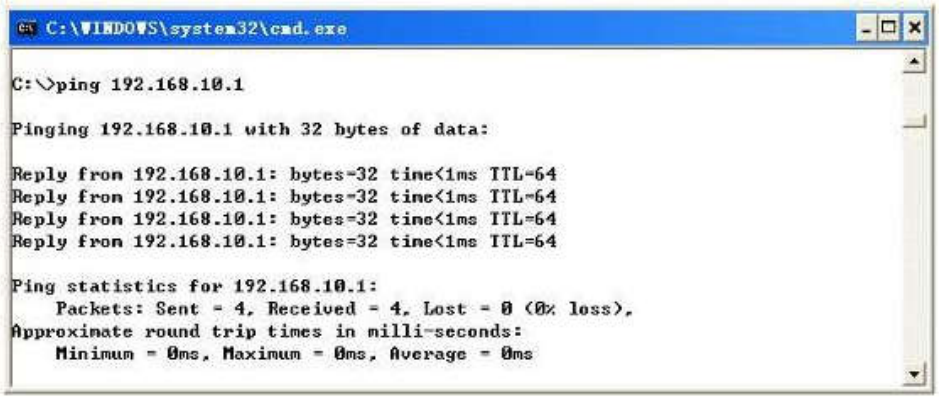


图 12-4 从 PC2 ping VLAN 10 的网关

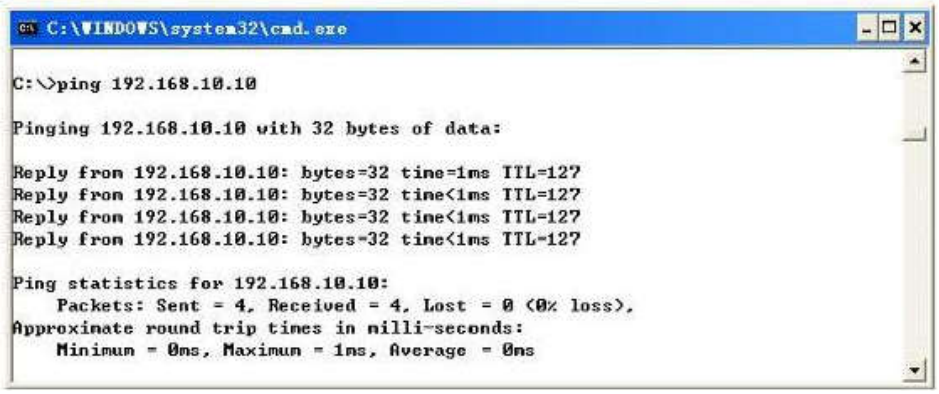


图 12-5 从 PC2 ping PC1

【注意事项】

1、 在给路由器的子接口配置 IP 地址之前，一定要先封装 dot1q 协议。

2、 各个 VLAN 内的主机，要以相应 VLAN 子接口的 IP 地址作为网关。

【参考配置】

```
Router#show running-config

Building configuration...
Current configuration : 586 bytes
!
version RGNOS 10.1.00(4), Release(18443)(Tue Jul 17 20:50:30 CST 2007 -ubu1server)
hostname Router
!
!
interface FastEthernet 0/0
duplex auto
speed auto
!
interface FastEthernet 0/0.10
encapsulation dot1Q 10
ip address 192.168.10.1 255.255.255.0
```

```
!
interface FastEthernet 0/0.20
encapsulation dot1Q 20
ip address 192.168.20.1 255.255.255.0
!
interface FastEthernet 0/1
duplex auto
speed auto
!
line con 0
line aux 0
line vty 0 4
login
!
end

L2-SW#show running-config

System software version : 1.68 Build Apr 25 2007 Release
Building configuration...
Current configuration : 757 bytes
!
version 1.0
!
hostname L2-SW
vlan 1
!
vlan 10
name xiaoshou
!
vlan 20
name jishu
!
interface fastEthernet 0/1
switchport mode trunk
!
interface fastEthernet 0/6
switchport access vlan 10
!
interface fastEthernet 0/7
switchport access vlan 10
!
interface fastEthernet 0/8
switchport access vlan 10
```

```
!
interface fastEthernet 0/9
switchport access vlan 10
!
interface fastEthernet 0/10
switchport access vlan 10
!
interface fastEthernet 0/11
switchport access vlan 20
!
interface fastEthernet 0/12
switchport access vlan 20
!
interface fastEthernet 0/13
switchport access vlan 20
!
interface fastEthernet 0/14
switchport access vlan 20
!
interface fastEthernet 0/15
switchport access vlan 20
!
End
```

实验十三 利用 IP 标准访问列表 ACL 进行网络流量的控制

【实验目的】

掌握路由器上编号的标准 IP 访问列表规则及配置

【背景描述】

你是一个公司的网络管理员，公司的经理部、财务部门和销售部门分属不同的 3 个网段，三部门之间用路由器进行信息传递，为了安全起见，公司领导要求销售部门不能对财务部门进行访问，但经理部可以对财务部门进行访问。

经理部的网段为 172.16.2.0，销售部门的网段为 172.16.1.0、财务部门的网段为 172.16.4.0。

【需求分析】

只允许网段 172.16.2.0 与 172.16.4.0 的主机进行通信，不允许 172.16.1.0 去访问 172.16.4.0 网段的主机。

【实验拓扑】

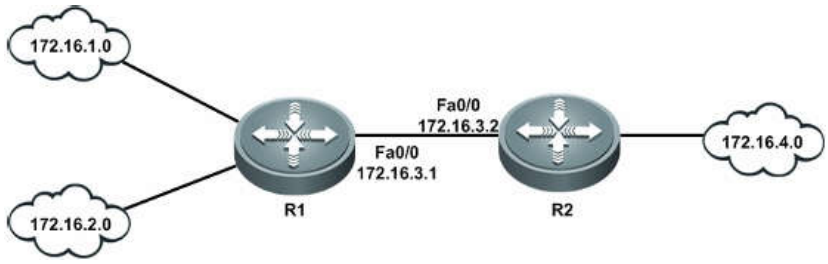


图 13-1 实验拓扑图

【预备知识】

路由器基本配置知识、访问控制列表知识

【实验设备】

路由器（两台）、V.35 线缆（1 条）、直连线或交叉线（3 条）

【实验原理】

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

IP ACL 分为两种：标准 IP 访问列表和扩展 IP 访问列表。

标准 IP 访问列表可以根据数据包的源 IP 地址定义规则，进行数据包的过滤。

扩展 IP 访问列表可以根据数据包的源 IP、目的 IP、源端口、目的端口、协议来定义规则，进行数据包的过滤。

IP ACL 基于接口进行规则的应用，分为：入栈应用和出栈应用。

入栈应用是指由外部经该接口进行路由器的数据包进行过滤。

出栈应用是指路由器从该接口向外转发数据时进行数据包的过滤。

IP ACL 的配置有两种方式：按照编号的访问列表，按照命名的访问列表。

标准 IP 访问列表编号范围是 1~99、1300~1999，扩展 IP 访问列表编号范围是 100~199、2000~2699。

【实验步骤】

第一步：路由器基本配置

```
R1(config)#
R1(config)# interface loopback 0
R1 (config-if)#ip add 172.16.1.1 255.255.255.0
R1 (config-if)#no shutdown
R1 (config-if)# interface loopback 1
R1 (config-if)#ip add 172.16.2.1 255.255.255.0
R1 (config-if)#no shutdown
R1 (config-if)#interface FastEthernet0/0
R1 (config-if)#ip add 172.16.3.1 255.255.255.0
R1 (config-if)#no shutdown
R1 (config-if)#end

R2(config)# interface FastEthernet 0/0
R2 (config-if)#ip add 172.16.3.1 255.255.255.0
R2 (config-if)#no shutdown
R2 (config-if)#exit
R2 (config-if)#interface FastEthernet 0/1
R2 (config-if)#ip add 172.16.4.1 255.255.255.0
R2 (config-if)#no shutdown
R2 (config-if)#end
```

第二步：配置路由

```
R1(config)#ip route 0.0.0.0 0.0.0.0 172.16.3.2
R2(config)#ip route 0.0.0.0 0.0.0.0 172.16.3.1
```

第三步：配置标准 IP 访问控制列表

```
R2(config)#access-list 10 deny 172.16.1.0 0.0.0.255
R2(config)#access-list 10 permit 172.16.2.0 0.0.0.255
R2(config)# interface FastEthernet 0/1
R2(config-if)#ip access-group 10 out
```

第三步：验证测试

在没有配置 ACL 时，可以使用原地址为 172.16.1.1，目标地址为 172.16.4.10（此为连接到 R2 接口 fa0/1 的一台主机），进行 ping 通信，如下所示。

```
R1#ping
  Protocol [ip]:
  Target IP address: 172.16.4.1
  Repeat count [5]:
  Datagram size [100]:
  Timeout in seconds [2]:
  Extended commands [n]: y
  Source address:172.16.1.1
  Time to Live [1, 64]:
  Type of service [0, 31]:
  Data Pattern [0xABCD]:0xabcd
  Sending 5, 100-byte ICMP Echoes to 172.16.4.1, timeout is 2 seconds:
  < press Ctrl+C to break >
  !!!!!
  Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

配置 ACL 后的测试，如下所示

```
R1#ping
  Protocol [ip]:
  Target IP address: 172.16.4.10
  Repeat count [5]:
  Datagram size [100]:
  Timeout in seconds [2]:
  Extended commands [n]: y
  Source address:172.16.1.1
  Time to Live [1, 64]:
  Type of service [0, 31]:
  Data Pattern [0xABCD]:0xabcd
  Sending 5, 100-byte ICMP Echoes to 172.16.4.10, timeout is 2 seconds:
  < press Ctrl+C to break >
  .....
  Success rate is 0 percent (0/5)

R1#ping
  Protocol [ip]:
  Target IP address: 172.16.4.10
  Repeat count [5]:
  Datagram size [100]:
  Timeout in seconds [2]:
```

```
Extended commands [n]: y
Source address:172.16.2.1
Time to Live [1, 64]:
Type of service [0, 31]:
Data Pattern [0xABCD]:0xabcd
Sending 5, 100-byte ICMP Echoes to 172.16.4.10, timeout is 2 seconds:
< press Ctrl+C to break >
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10 ms
```

ping（172.16.2.0 网段的主机不能 ping 通 172.16.4.0 网段的主机；172.16.1.0 网段的主机能 ping 通 172.16.4.0 网段的主机）。

```
R2#show access-lists

ip access-list standard 10
10 deny 172.16.1.0 0.0.0.255
20 permit 172.16.2.0 0.0.0.255
35 packets filtered

R2#sh ip access-group interface fa0/1
ip access-group 10 out
Applied On interface FastEthernet 0/1
```

【注意事项】

1、注意在访问控制列表的网络掩码是反掩码。

2、标准控制列表要应用在尽量靠近目的地址的接口。

【参考配置】

```
R1#show running-config

Building configuration...
Current configuration : 590 bytes
!
version RGNOS 10.1.00(4), Release(18443)(Tue Jul 17 20:50:30 CST 2007
-ubu1server)
hostname R1
!
interface FastEthernet 0/0
ip address 172.16.3.1 255.255.255.0
duplex auto
speed auto
!
interface FastEthernet 0/1
```

```
duplex auto
speed auto
!
interface Loopback 0
ip address 172.16.1.1 255.255.255.0
!
interface Loopback 1
ip address 172.16.2.1 255.255.255.0
!
ip route 0.0.0.0 0.0.0.0 172.16.3.2
!
line con 0
line aux 0
line vty 0 4
login
!
end

R2#show running-config

Building configuration...
Current configuration : 627 bytes
!
version RGNOS 10.1.00(4), Release(18443)(Tue Jul 17 20:50:30 CST 2007
-ubu1server)
hostname R2
!
ip access-list standard 10
10 deny 172.16.1.0 0.0.0.255
20 permit 172.16.2.0 0.0.0.255
!
interface FastEthernet 0/0
ip address 172.16.3.2 255.255.255.0
duplex auto
speed auto
!
interface FastEthernet 0/1
ip access-group 10 out
ip address 172.16.4.1 255.255.255.0
duplex auto
speed auto
!
ip route 0.0.0.0 0.0.0.0
!
```

```
line con 0
line aux 0
line vty 0 4
login
!
end
```

实验报告模板

实验报告

实验名称：	
实验台号：	实验时间：
实验小组：第　　组　　成员及本次实验分工：	
实验目的：	
实验环境说明：	
实验过程、步骤(可另附页、使用网络拓扑图等辅助说明)及结果：	
实验总结(遇到的问题及解决办法、体会)：	
器材、工具领用及归还负责人:	实验记录人：（签名）
实验执笔人：（签名）	报告协助人：（签名）
小组成员签名：（签名）	
验收人：	成绩评定：