第 5 章

传输层实验

实验 19　运输层协议分析

19.1　实 验 目 的

(1) 理解端到端通信和端口的概念、分类。

(2) 了解 UDP 报文的格式。

(3) 掌握 TCP 建立连接的过程,理解 TCP 的工作原理。

19.2　实 验 环 境

(1) 设备要求：计算机若干台(安装有 Windows 操作系统,安装有网卡),局域网环境,主机装有 Wireshark 工具。

(2) 每组 1 人,独立完成。

19.3　实验预备知识

1. 运输层的通信实现

运输层实现两个主机端到端的通信,即应用进程之间的通信。实现进程之间的通信需要使用端口号,简称为端口(Port)。端口号是一个 16b 的标识符,取值范围是 0～65 535。端口号只具有本地意义,每个主机上的 TCP 和 UDP 各有一套。进程之间的通信需要使用 IP 地址＋端口号(套接字)来实现。

IANA(互联网数字分配机构)将端口分为以下三种类别。

(1) 熟知端口,其数值为 0～1023。这类端口是因特网赋号管理局(IANA)控制的,一些常用的应用程序固定使用。

(2) 登记端口,其数值为 1024～49 151。IANA 既不分配也不控制,可以在 IANA 登记,防止重复使用。

(3) 动态端口,其数值为 49 152～65 535。这类端口是留给客户进程选择作为临时端口使用的。

2. UDP 报文结构

每个 UDP 报文分为 UDP 报头和 UDP 数据两部分。报头由 4 个 16b 长(2B)的字段

组成，分别说明该报文的源端口、目的端口、报文长度和校验值。UDP 报文格式如图 5-1 所示。

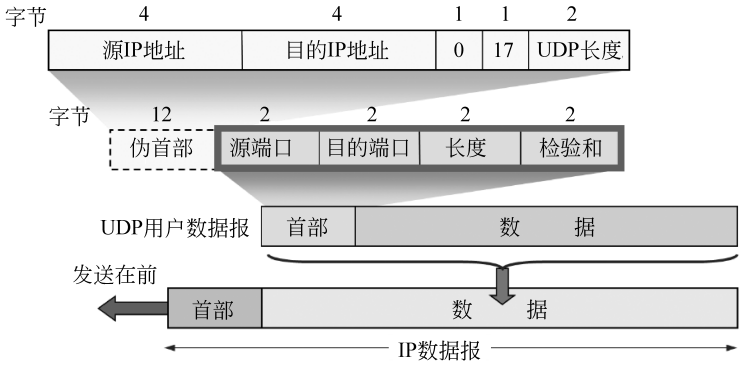

图 5-1　UDP 报文结构

UDP 报文中每个字段的含义如下。

- 源端口：这个字段占据 UDP 报文头部的前 16 位，通常包含发送数据报的应用程序所使用的 UDP 端口。接收端的应用程序利用这个字段的值作为发送响应的目的地址。这个字段是可选的，所以发送端的应用程序不一定会把自己的端口号写入该字段中。如果不写入端口号，则把这个字段设置为 0。这样，接收端的应用程序就不能发送响应了。
- 目的端口：接收端计算机上 UDP 软件使用的端口，占据 16 位。
- 长度：该字段占据 16 位，表示 UDP 数据报长度，包含 UDP 报文头部和 UDP 数据长度。因为 UDP 报文头部长度是 8B，所以这个值最小为 8。
- 校验值：该字段占据 16 位，可以检验数据在传输过程中是否被损坏。

3. TCP 报文段的结构

TCP 是 TCP/IP 体系中运输层的重要协议。它为应用层提供面向连接的、可靠的数据传递服务。在提供数据可靠性的同时，TCP 还为应用层提供了全双工的数据传输服务。

TCP 接收应用层的数据，添加 TCP 首部后形成 TCP 报文段。TCP 报文段需要被下层的 IP 协议封装，发送到目的地，如图 5-2 所示。

- 源端口和目的端口：16b，分别对应发送数据的应用进程和接收数据的应用进程。TCP 用这两个字段来实现多路复用和多路分解。
- 序号和确认号：32b，TCP 将连接上发送的每一个字节都进行编号，序号和确认号用来实现可靠的数据传输。其中，序号是 TCP 报文段数据部分的第一个字节的编号；确认号是告诉对方期望收到对方的下一个字节的编号。
- 数据偏移：4b，表示 TCP 报文段中的数据部分距离 TCP 首部的起始位置有多少字节。它实际上就是 TCP 首部的长度。
- 保留字段：6b，保留作为以后扩展。
- 标志字段：6b，当其值为 1 时称为置位。这里有 6 个位，分别是 URG 表示紧急指针，ACK 表示确认，PSH 表示请求推送，RST 表示连接复位，SYN 表示同步序

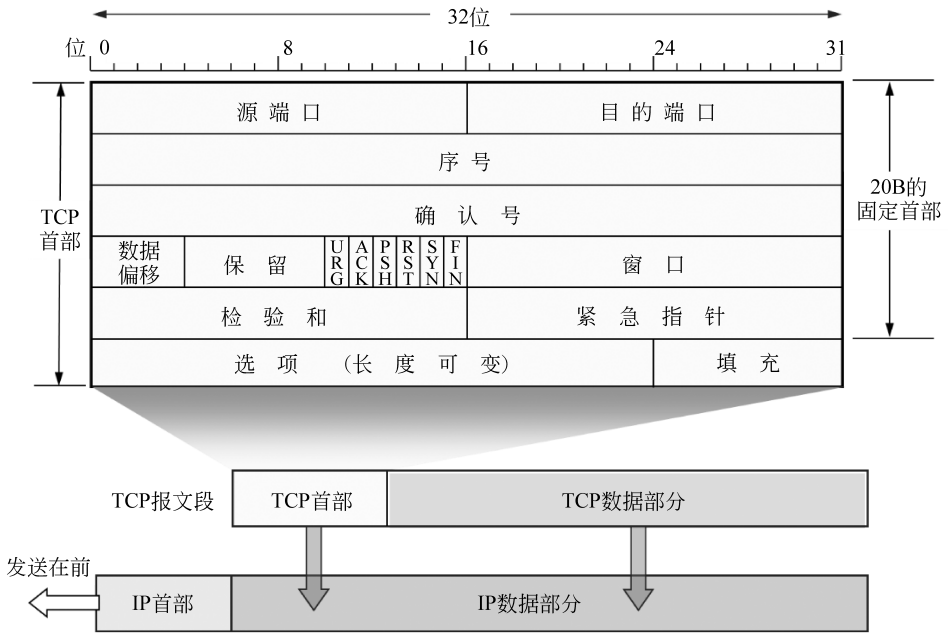

图 5-2　TCP 报文段的组成和封装

号，FIN 表示终止连接。

- 窗口大小：16b，主要用于流量控制，用来告诉对方的 TCP 自己接收缓存的大小。
- 检验和：用来确保数据的可靠性。
- 紧急指针：给出紧急数据距离当前序号的偏移量。
- 可选项：可选的，TCP 规定一种可选项，最大报文段长度（MSS），规定 TCP 报文段数据的最大字节数。
- 填充项：当可选项字段的长度不是 4B 的整倍数时，填充项字段需要将其补足，填充项字段全部都是 0。

4. TCP 连接的建立与断开

TCP 提供面向连接的传输服务。利用 TCP 通信的两个应用进程要首先建立连接，这个连接是虚拟的连接，并不是一条实际的物理线路。TCP 连接的三次握手如图 5-3 所

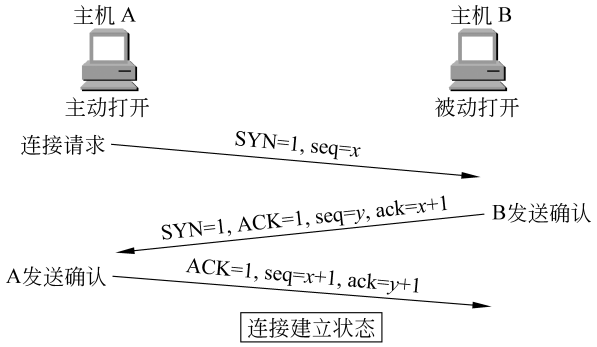

图 5-3　TCP 连接的建立

示。建立连接的目的是使通信双方在开始传输数据前建立联系，使双方都确定对方愿意与之通信；同时在建立连接的过程中传递和协商一些必要的参数（如发送字节的起始编号和最大报文段长度），为后面的数据传递打下基础。连接建立后，两边的应用进程就可以开始全双工地通信，在此期间，连接两端的 TCP 会记录数据发送和接收的情况，利用控制信息始终保持这个连接，直到数据传输完毕。最后 TCP 还要负责关闭这个连接，释放与这个连接相关的资源，连接的断开如图 5-4 所示。

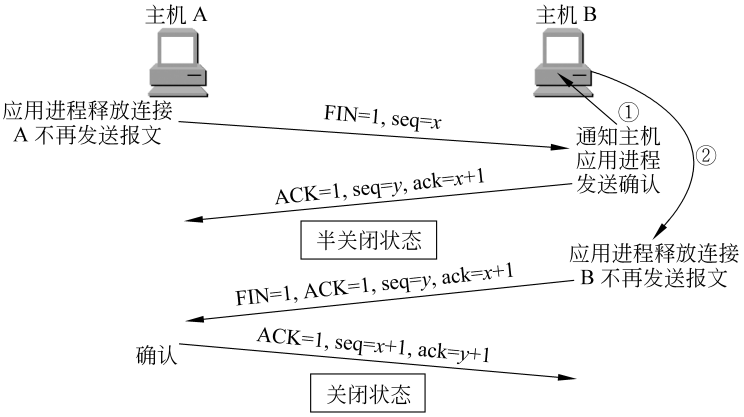

图 5-4　TCP 连接的断开

19.4　实验内容与步骤

本实验利用 Wireshark 捕捉数据包，分析 UDP 和 TCP 的报文结构，并分析 TCP 建立连接的过程。

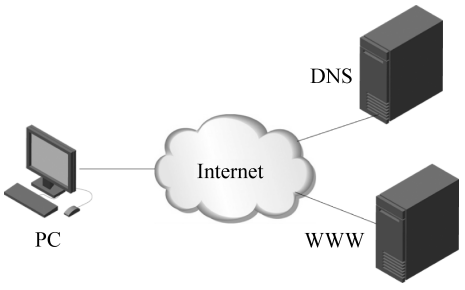

图 5-5　实验网络拓扑图

使用实验室网络或者家庭网络完成次实验。一般情况下，网络拓扑结构如图 5-5 所示。

Wireshark 软件安装在 PC 主机上，实验主要通过连入 Internet 的 PC 主机访问 WWW 服务器上的网站而抓取相应的数据报。PC 主机通过域名访问网站时，需要对域名进行解析，因此，PC 主机首先访问自己的 DNS 缓存，如果缓存中找不到域名对应的 IP 地址时，则向 DNS 服务器进行请求（发送一个数据包），DNS 查询后响应（回复给 PC 一个数据包），PC 主机然后根据 DNS 查询到的 WWW 服务器的 IP 地址向 WWW 服务器进行请求，WWW 服务器给予响应，则其流向如图 5-6 所示。我们则利用 Wireshark 抓取向 DNS 请求以及响应的数据报，抓取向 WWW 请求以及响应的数据报。

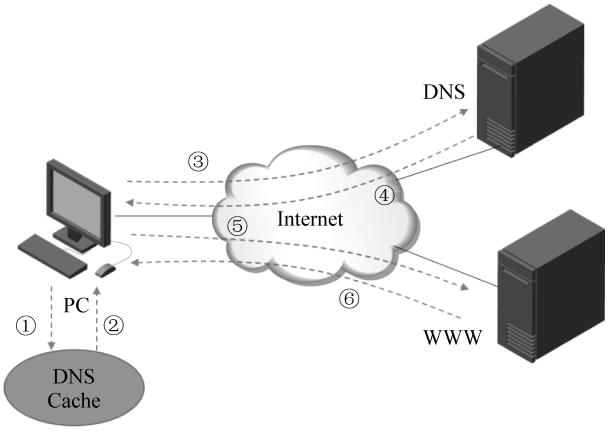

图 5-6　数据流向图

1. 清空 DNS Cache(迫使 PC 主机向 DNS 发起请求)

打开 CMD 命令行窗口,输入“ipconfig　/flushdns”命令清空 DNS Cache,如图 5-7 所示。注意,查看 DNS Cache 可以使用“ipconfig　/displaydns”命令。

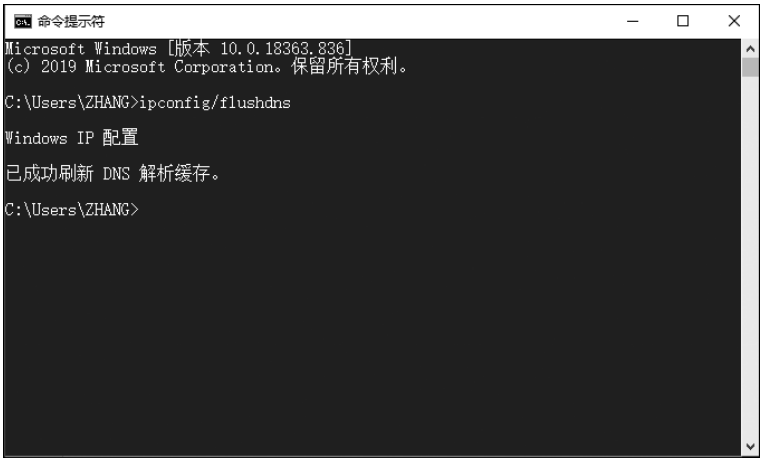

图 5-7　清空 DNS Cache

2. 抓取数据包(通过域名访问网站)

(1) 在 PC 主机上打开 Wireshark 软件并开始抓取数据包。

(2) 在 PC 主机上打开 IE 浏览器,地址栏输入“www.seig.edu.cn”,然后按 Enter 键访问该网站。

(3) 待网站打开后停止抓取数据包。

3. 分析 UDP 报文(通过 DNS 数据包进行分析)

(1)为了分析时更好地和本机信息进行比较,在分析之前先查阅本机(即 PC 主机)的 TCP/IP 属性等相关信息。在 CMD 命令行中使用“ipconfig　/all”命令查询,并按要求记录在表 5-1 中。

表 5-1　PC 主机的 TCP/IP 属性

属　性　名	属　性　值
IP 地址	
子网掩码	
默认网关	
首选 DNS(第一个 DNS)IP	
备用 DNS(第二个 DNS)IP	

(2) 过滤 DNS 数据包,即在过滤框中输入“dns”(注意小写),然后按 Enter 键,则只显示 DNS 的数据报,如图 5-8 所示。在 Wireshark 软件的数据报列表框中找到“Info”字段中包含刚才访问的域名信息(即有 www.seig.edu.cn)的数据包。应该是成对出现,一个请求报文,一个响应报文。

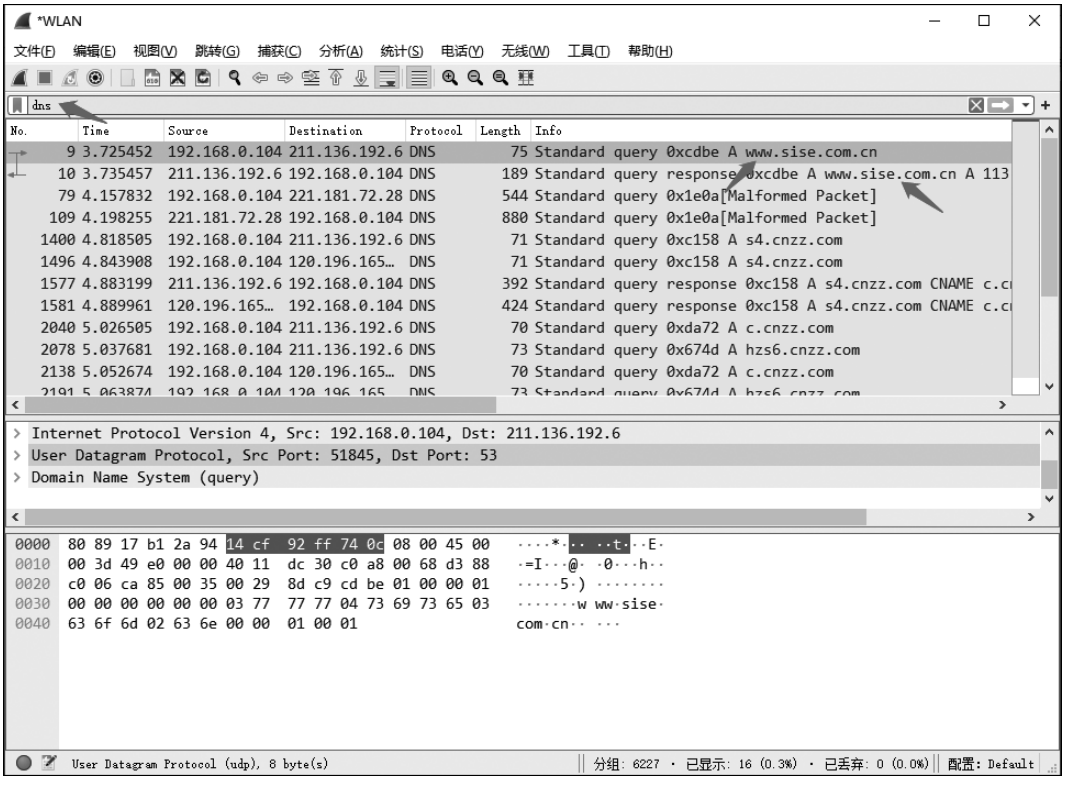

图 5-8　过滤 DNS 数据包

(3) 分别单击 PC 主机请求 DNS 的数据包(即源地址为 PC 主机的数据包)和 DNS 服务器的响应报文(即源地址为 DNS 服务器的数据包),在协议分析框进行分析。请根据要求进行分析填写表 5-2 和表 5-3。

表 5-2　DNS 报文分析结果

分 析 问 题	结　　果
DNS 服务器的 IP 地址	
DNS 的下一层(运输层)协议是	
www.seig.edu.cn 网站的 IP 地址	

表 5-3　UDP 报文分析结果

DNS 报文的下层协议分析	请 求 报 文	响 应 报 文
源端口号(Source Port)		
目的端口号(Destination Port)		
长度(Length)		
校验和(Checksum)		

4. 分析 TCP 报文

(1) 过滤 TCP 报文,只需要保留访问 www.seig.edu.cn 的 TCP 数据,则在过滤框中通过 www.seig.edu.cn 的 IP(即 WWW 服务器的 IP 地址)进行过滤。其 IP 在上述分析中已经填写在表 5-3 中。这里假设 IP 为 a.b.c.d(请实验时换作 WWW 服务器的真实 IP),则在过滤框中输入过滤规则为“ip.addr==a.b.c.d && tcp”,然后按 Enter 键。过滤结果如图 5-9 所示。

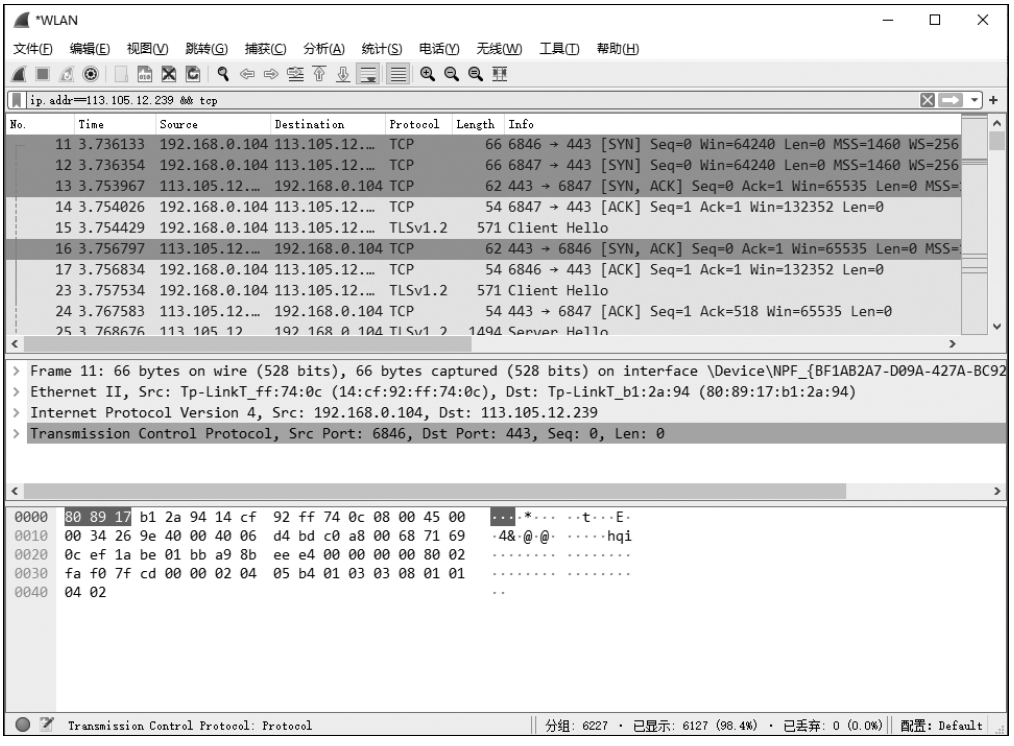

图 5-9　过滤 TCP 报文段

(2) 根据 TCP 建立连接的三次握手的原理(某些字段的特征,如 SYN 字段),请找出三次握手的三个 TCP 报文段,并进行分析,将分析结果填入表 5-4 中。

表 5-4 TCP 三次握手报文段分析

三次握手报文段	源端口	目的端口	序号	确认号	头部长度	6 个标志位中,值为 1 的	窗口大小	MSS 选项
第 1 次								
第 2 次								
第 3 次								

(3) 请设计实验抓取 TCP 关闭连接的 4 个报文段并进行分析(**选做**)。

19.5 练习与思考

1. 选择题

(1) 如果要列出本机当前建立的连接,可以使用的命令是(　　)。

A. netstat -s　　B. netstat -o　　C. netstat -a　　D. netstat -r

(2) TCP 的主要功能是(　　)。

A. 进行数据分组　　B. 保证可靠传输

C. 确定数据传输路径　　D. 提高传输速度

(3) TCP 报文段中序号字段指的是(　　)的序号。

A. 数据部分第一个字节　　B. 数据部分最后一个字节

C. 报文首部第一个字节　　D. 报文最后一个字节

(4) TCP 报文中确认序号指的是(　　)。

A. 已经收到的最后一个数据序号　　B. 期望收到的第一个字节序号

C. 出现错误的数据序号　　D. 请求重传的数据序号

(5) TCP 的确认是对接收到的数据中的(　　)表示确认。

A. 最高序号　　B. 第一个序号

C. 第二个序号　　D. 倒数第二个序号

(6) TCP 发送一段数据报,其序号是 35～150,如果正确到达,接收方对其确认的序号为(　　)。

A. 36　　B. 150　　C. 35　　D. 151

2. 填空题

(1) TCP 报文的首部最小长度是(　　)。

(2) TCP 报文段中给源端口分配了(　　)字节的长度。

(3) TCP 报文段中序号字段为(　　)字节。

(4) TCP 报文段中的数据偏移实际指明的是(　　)。