**实验报告**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **学　　号** |  | **姓　　名** |  | **专业、班** |  |

# 实验4 传输层协议分析

一、实验目的

1、学习3CDaemon FTP服务器的配置和使用，分析TCP报文格式，理解TCP的连接建立、和连接释放的过程。

2、学习3CDaemon TFTP服务器的配置和使用，分析UDP报文格式，理解TCP协议与UDP协议的区别。

二、实验工具软件3CDaemon软件简介

3CDaemon是3Com公司推出的功能强大的集FTP Server、TFTP Server、Syslog Server和TFTP Client于一体的集成工具，界面简单，使用方便。这里主要介绍实验中需要用到的FTP Server功能和TFTP Server功能。

1、FTP Server功能

（1）配置FTP Server功能：选中左窗格功能窗口，打开FTP Server按钮，单击窗格中的Configure FTP Server按钮，打开3CDaemon Configuration配置窗口，配置FTP Server功能。

这里需要设置的就是“Upload/Download”路径，作为FTP Server的文件夹，其它选项可以使用系统缺省设置。设置完成后，单击确认按钮，设置生效。

（2）在实验中，我们使用3CDaemon系统内置的匿名帐户“anonymous”登陆FTP服务器，客户端使用微软FTP客户端命令，关于Ftp命令的说明介绍如下。

(3) Ftp命令的说明

FTP的命令格式：ftp[-v][-d][-i][-n][-g][-w:windowsize][主机名/IP地址]

其中：

-v不显示远程服务器的所有响应信息；

-n限制ftp的自动登录；

-i在多个文件传输期间关闭交互提示

-d允许调试、显示客户机和服务器之间传递的全部ftp命令；

-g不允许使用文件名通配符；

-w：windowsize忽略默认的4096传输缓冲区。

使用FTP命令登录成功远程FTP服务器后进入FTP子环境，在这个子环境下，用户可以使用FTP的内部命令完成相应的文件传输操作。

FTP常用内部命令如下：

open host[port]：建立指定ftp服务器连接，可指定连接端口。

user user-name[password][account]：向远程主机表明身份，需要口令时必须输入。

append local-file[remote-file]：将本地文件追加到远程系统主机，若未指定远程系统文件名，则使用本地文件名。

cd remote-dir：进入远程主机目录。

cdup：进入远程主机目录的父目录。

cd[dir]：将本地工作目录切换至dir。

dir[remote-dir][local-file]：显示远程主机目录，并将结果存入本地文件。

get remote-file[local-file]：将远程主机的文件remote-file传至本地硬盘的local-file。

ls[remote-dir][local-file]：显示远程目录remote-dir，并存入本地文件local-file。

put local-file[remote-file]：将本地文件local-file传送至远程主机。

mput local-file：将多个文件传输至远程主机。

nlist[remote-dir][local-file]：显示远程主机目录的文件清单，存入本地硬盘local-file。

bye或quit：退出ftp会话过程。

2、TFTP Server功能

(1) TFTP Server功能配置基本同上（FTP erver功能）。

(2)实验中，为了与TFTP服务器连通，可以使用Windows命令行模式下的TFTP客户端命令，命令格式如下：

TFTP[-i]host[GET|PUT]source[destination]

参数说明如下：

-i以二进制方式传输；

host指定本地或远程主机；

GET下载文件；

PUT上传文件；

source指定要传输的文件名；

destination指定传输的目的路径。

三、实验内容和步骤

1、TCP协议分析实验

（1）按照上面3CDaemon软件的介绍方法在PC1上建立FTP服务器；

（2）在PC1和PC2中运行Ethereal，开始截获报文，为了只截获到与我们实验有关的内容，将截获条件设置为对方主机的IP地址，如PC1的截获条件为“host 192.168.1.xx”（注释：PC2的IP地址）；

（3）在PC2上打开命令行窗口，执行如下操作：

C:\Documents and Settings\Administrator>ftp

ftp>open

To 192.168.1.yy（注释：PC1的IP地址）

Connected to 192.168.1.yy.

220 3Com 3CDaemon FTP Server Version 2.0

User(192.168.1.yy:(none)):anonymous

331 User name ok,need password

Password:

230-The response'is not valid.

230-Next time,please use your email address as password.

230 User logged in

ftp>quit

221 Service closing control connection

C:\Documents and Settings\Administrator>

（4）停止截获报文，将截获的结果保存为FTP-学号，按下列要求分析截获的结果；

a）结合本节TCP协议介绍部分的内容，分析TCP连接建立的“三次握手”过程，找到对应的报文，填写表1（传输方向填写PC2－> PC1或PC2<-PC1）。

表1 TCP连接建立报文分析

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 报文号 | 传输方向 | 源端口 | 目的端口 | 序号 | 确认序号 | 同步位SYN | 确认位  ACK |
| 828 | PC1->  PC2 | 54900 | 21 | 0 | 0 | Set | Not set |
| 829 | PC2->  PC1 | 21 | 54900 | 0 | 1 | Set | Set |
| 830 | PC1->  PC2 | 54900 | 21 | 1 | 1 | Not set | Set |

b）从FTP-学号的报文中的第一个FIN=1的TCP报文开始分析TCP连接释放的“四次握手”过程，填写表2。

表2 TCP连接释放报文分析

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 报文号 | 传输方向 | 源端口 | 目的端口 | 序号 | 确认序号 | 终止位  FIN | 同步位  SYN | 确认位  ACK |
| 1383 | PC2->  PC1 | 21 | 54900 | 136 | 33 | Set | Not set | Set |
| 1384 | PC1->  PC2 | 54900 | 21 | 33 | 137 | Not set | Not set | Set |
| 1385 | PC1->  PC2 | 54900 | 21 | 33 | 137 | Set | Not set | Set |
| 1386 | PC2->  PC1 | 21 | 54900 | 137 | 34 | Not set | Not set | Set |

2、UDP协议分析实验

（1）按照上面3CDaemon TFTP Server软件的介绍方法在PC1上建立TFTP服务器；在根

目录下保存一个用于数据传输的文件（为便于观察，文件不要太大），例如f1.txt。

（2）在PC1和PC2中运行Ethereal，开始截获报文，为了只截获到与我们实验有关的内容，将截获条件设置为对方主机的IP地址，如PC1的截获条件为“host 192.168.1.xx”（注释：PC2的IP地址）；

（3）在PC2上打开命令行窗口，接收TFTP服务器的文件，执行如下操作：

TFTP –i 192.168.1.yy GET f1.txt（注释：“host 192.168.1.xx”为 PC2的IP地址）；

（4）停止截获报文，将截获的结果命名为UDP-学号并保存，分析UDP报文结构，

回答如下问题。

UDP报文头部有几个字段，绘制UDP报文的结构图。

选择第一个UDP报文，分析其结构，填写表3。

表3 UDP报文分析

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| IP报文 | 源IP地址 |  | | 协议 |  |
| 目的IP地址 |  | | 总长度 |  |
| UDP  报文 | 字段名 | 字段长度 | 字段值 | 字段表达信息 | |
|  |  |  |  | |
|  |  |  |  | |
|  |  |  |  | |
|  |  |  |  | |
|  |  |  |  | |

UDP报文与TCP报文有何不同？体会UDP协议和TCP协议的区别。

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**附录：TCP和UDP基本原理**

TCP协议

TCP是传输控制协议（Transmission Control Protocal）的缩写，提供面向连接的可靠的传

输服务。在TCP/IP体系中，HTTP、FTP、SMTP等协议都是使用TCP传输方式的。

（1）TCP报文格式

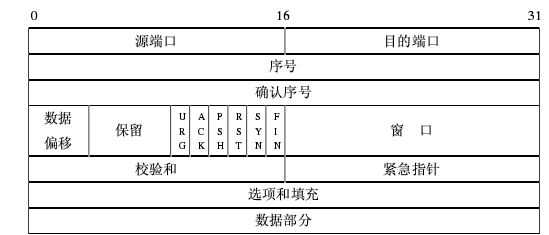


图1 TCP报文段格式

TCP报文分为首部和数据两个部分。如图1所示，TCP报文段首部的前20字节是固定的，后面有4×n字节是可选项。其中：

源端口和目的端口：各2字节，用于区分源端和目的端的多个应用程序；

序号：4字节，指本报文段所发送的数据的第一字节的序号；

确认序号：4字节，是期望下次接收的数据的第一字节的编号，表示该编号以前的数据已安全接收。

数据偏移：4位，指数据开始部分距报文段开始的距离，即报文段首部的长度，以32bit为单位。

标志字段：共有六个标志位：

①紧急位URG=1时，表明该报文要尽快传送，紧急指针启用；

②确认位ACK=1时，表头的确认号才有效；ACK=0，是连接请求报文；

③急迫位PSH=1时，表示请求接收端的TCP将本报文段立即传送到其应用层，而不

是等到整个缓存都填满后才向上传递；

④复位位RST=1时，表明出现了严重差错，必须释放连接，然后再重建连接；

⑤同步位SYN=1时，表明该报文段是一个连接请求或连接响应报文，

⑥终止位FIN=1时，表明要发送的字符串已经发送完毕，并要求释放连接。

窗口：2字节，指该报文段发送者的接收窗口的大小，单位为字节；

校验和：2字节，对报文的首部和数据部分进行校验；

紧急指针：2字节，指明本报文段中紧急数据的最后一个字节的序号，和紧急位URG配合使用；

选项：长度可变，若该字段长度不够四字节，有填充补齐。

（2）TCP连接的建立

TCP连接的建立采用“三次握手”的方法。

一般情况下，双方连接的建立由其中一方发起。如图2(a)所示：

主机A首先向主机B发出连接请求报文段，其首部的SYN同步位为1，同时选择一个序号x；

主机B收到此连接请求报文后，若同意建立连接，则向主机A发连接响应报文段。在响应报文段中，SYN同步位为1，确认序号为x+1，同时也为自己选择一个序列号y；

主机A收到此确认报文后，也向主机B确认，这时，序号为x+1，确认序号为y+1。

当连接建立后，A、B主机就可以利用TCP进行数据传输了。

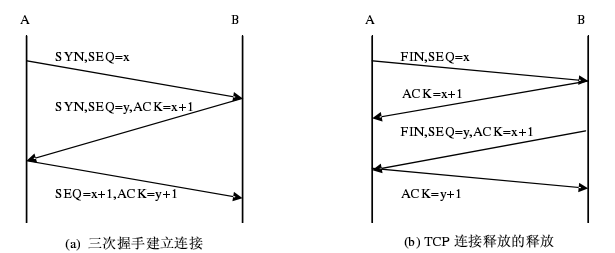


图2 TCP的连接和释放

（3）TCP连接的释放

在数据传输结束后，任何一方都可以发出释放连接的请求，释放连接采用所谓的“四次”方法。如图2(b)所示，假如主机A首先向主机B提出释放连接的请求，其过程如下：

主机A向主机B发送释放连接的报文段，其中，FIN终止位为1，序号x等于前面已

经发送数据的最后一个字节的序号加1；

主机B对释放连接请求进行确认，其序号等于x+1。这时从A到B的连接已经释放，

连接处于半关闭状态，以后主机B不再接收主机A的数据。但主机B还可以向主机A

发送数据，主机A在收到主机B的数据时仍然向主机B发送确认信息。

当主机B不再向主机A发送数据时，主机B也向主机A发释放连接的请求；

同样主机A收到该报文段后也向主机B发送确认。

（4）TCP数据传输

TCP可以通过检验序号和确认号来判断丢失、重复的报文段，从而保证传输的可靠性。

TCP将要传送的报文看成是由一个个字节组成的数据流，对每个字节编一个序号。在连接建立时，双方商定初始序号（即连接请求报文段中的SEQ值）。TCP将每次所传送的第一个字节的序号放在TCP首部的序号字段中，接收方的TCP对收到每个报文段进行确认，在其确认报文中的确认号字段的值表示其希望接收的下一个报文段的第一个数据字节的序号。

由于TCP能提供全双工通信，因此，通信中的每一方不必专门发送确认报文段，而可以在发送数据时，捎带传送确认信息，以此来提高传输效率。

UDP协议

UDP是用户数据报协议（User Datagram Protocol）的缩写，提供无连接的数据报文传输，不能保证数据完整到达目的地。

UDP数据传输不需要预先建立连接，传输过程中没有报文确认信息。因此，UDP报文格式比TCP的报文格式简单的多。UDP数据报也是由首部和数据两部分组成，其首部只有源端口、目的端口、消息长度和校验和四部分，各部分的意义和TCP首部对应字段的意义相同，这里不复赘言。

在TCP/IP体系中，使用UDP协议的应用有DNS和TFTP（Trivial File Transfer Protocol）。

TFTP是一个传输文件的简单协议，它基于UDP协议的，它只能从文件服务器上获得或写入文件，不能列出目录，不进行认证。