实验 6 - 传输层与应用层协议分析

一. 实验目的

1. 学习传输层基本概念;
2. 学习应用层基本概念;
3. 进行 eNSP 仿真，分析传输层与应用层协议;

二. 实验环境

1. eNSP 网络环境仿真平台
2. wireShark 抓包工具

三. 实验基本原理

传输层基本概念

- 网络层为主机之间提供逻辑通信，传输层则为应用进程之间提供端到端的逻辑通信
- TCP/IP 的传输层主要有两个协议:
  1. UDP
  2. TCP
- TCP
  1. 建立连接: 3 次握手
  2. 释放连接: 4 次握手

应用层基本概念

1. HTTP
   - 客户/服务器模式，采用请求/应答方式工作
   - HTTP 基于 TCP 工作
   - 默认端口号: 80
2. FTP
   - 文件传送协议
   - 客户/服务器模式，以命令/响应方式进行交互
   - FTP 基于 TCP 工作
   - 服务器和客户端端口号: 21
3. DHCP
   - 动态主机配置协议
   - 主机加入新网络时自动获取正确的 IP 地址等配置信息

- 客户/服务器模式，采用请求/应答方式工作
- DHCP 基于 UDP 工作
- 服务器端口号：67
- 客户端端口号：68

4. DNS
    - 将域名转换为 IP 地址
    - 一个联机分布式数据库系统，采用客户服务器模式
    - DNS 基于 UDP 工作
    - DNS 服务器端口号： 53

四. 实验案例

6.1 主机网络参数自动配置

1. 交换机配置 DHCP 服务器

```
dhcp enable

ip pool global
network 192.168.10.0 mask 24
gateway-list 192.168.10.100
excluded-ip-address 192.168.10.1 192.168.10.20
dns-list 192.168.10.12
lease day 2 hour 2 minute 30

interface Vlanif1
ip address 192.168.10.100 255.255.255.0
dhcp select global
```

2. PC 分配到的网络参数信息

```
PC>ipconfig

Link local IPv6 address.....: fe80::5689:98ff:fed0:870
IPv6 address.....: :: / 128
IPv6 gateway.....: ::
IPv4 address.....: 192.168.10.254
Subnet mask.....: 255.255.255.0
Gateway.....: 192.168.10.100
Physical address.....: 54-89-98-D0-08-70
DNS server.....: 192.168.10.12
```

3. 查看全局地址池地址分配情况

```
<Huawei>dis ip pool
  ------------------------------------------------------------------------------
  Pool-name      : pool1
  Pool-No        : 0
  Position       : Local           Status           : Unlocked
  Gateway-0      : 192.168.10.100
  Mask           : 255.255.255.0
  VPN instance   : --


  IP address Statistic
    Total        :253
    Used         :1          Idle         :232
    Expired      :0          Conflict     :0          Disable    :20
<Huawei>
```

4. DHCP 数据包分析

```
    16 16.016000    0.0.0.0          255.255.255.255  DHCP     410 DHCP Discover - Transaction ID 0x200
    17 16.531000    HuaweiTechno_4d:3d:… Broadcast        ARP       60 Who has 192.168.10.254? Tell 192.168.10.100
    18 17.547000    192.168.10.100   192.168.10.254   DHCP     342 DHCP Offer    - Transaction ID 0x200
    19 17.906000    HuaweiTechno_4d:3d:… Spanning-tree-(for-… STP      119 MST. Root = 32768/0/4c:1f:cc:4d:3d:d4  Cost = 0  Port = 0x8001
    20 18.016000    0.0.0.0          255.255.255.255  DHCP     410 DHCP Request  - Transaction ID 0x200
    21 18.016000    192.168.10.100   192.168.10.254   DHCP     342 DHCP ACK      - Transaction ID 0x200
    22 19.031000    HuaweiTechno_d0:08:… Broadcast        ARP       60 Gratuitous ARP for 192.168.10.254 (Request)
```

1. DHCP Discover

PC 广播寻找 IP

```
Ethernet II, Src: HuaweiTechno_d0:08:70 (54:89:98:d0:08:70), Dst: Br
  Destination: Broadcast (ff:ff:ff:ff:ff:ff)
  Source: HuaweiTechno_d0:08:70 (54:89:98:d0:08:70)
  Type: IPv4 (0x0800)
```

```
Option: (53) DHCP Message Type (Discover)
    Length: 1
    DHCP: Discover (1)
```

2. DHCP 服务器发送 ARP 请求确定 IP 未被占用

```
Ethernet II, Src: HuaweiTechno_4d:3d:d4 (4c:1f:cc:4d:3d:d4), Dst: Broad
  Destination: Broadcast (ff:ff:ff:ff:ff:ff)
  Source: HuaweiTechno_4d:3d:d4 (4c:1f:cc:4d:3d:d4)
  Type: ARP (0x0806)
  Padding: 000000000000000000000000000000000000
Address Resolution Protocol (request)
  Hardware type: Ethernet (1)
  Protocol type: IPv4 (0x0800)
  Hardware size: 6
  Protocol size: 4
  Opcode: request (1)
  Sender MAC address: HuaweiTechno_4d:3d:d4 (4c:1f:cc:4d:3d:d4)
  Sender IP address: 192.168.10.100
  Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
  Target IP address: 192.168.10.254
```

3. DHCP Offer

DHCP 服务器提供 IP 给 PC

```
Ethernet II, Src: HuaweiTechno_4d:3d:d4 (4c:1f:cc:4d:3d:d4), Dst: Hua
  Destination: HuaweiTechno_d0:08:70 (54:89:98:d0:08:70)
  Source: HuaweiTechno_4d:3d:d4 (4c:1f:cc:4d:3d:d4)
  Type: IPv4 (0x0800)
```

```
Option: (53) DHCP Message Type (Offer)
    Length: 1
    DHCP: Offer (2)
Option: (1) Subnet Mask (255.255.255.0)
    Length: 4
    Subnet Mask: 255.255.255.0
Option: (3) Router
    Length: 4
    Router: 192.168.10.100
Option: (51) IP Address Lease Time
    Length: 4
    IP Address Lease Time: 2 days, 2 hours, 30 minutes (181800)
Option: (59) Rebinding Time Value
Option: (58) Renewal Time Value
Option: (54) DHCP Server Identifier (192.168.10.100)
    Length: 4
    DHCP Server Identifier: 192.168.10.100
```

4. DHCP Request

PC 请求使用服务器提供的 IP

```
Option: (53) DHCP Message Type (Request)
    Length: 1
    DHCP: Request (3)
Option: (54) DHCP Server Identifier (192.168.10.100)
    Length: 4
    DHCP Server Identifier: 192.168.10.100
Option: (50) Requested IP Address (192.168.10.254)
    Length: 4
    Requested IP Address: 192.168.10.254
Option: (61) Client identifier
    Length: 7
    Hardware type: Ethernet (0x01)
    Client MAC address: HuaweiTechno_d0:08:70 (54:89:98:d0:08:70)
Option: (55) Parameter Request List
    Length: 4
    Parameter Request List Item: (1) Subnet Mask
    Parameter Request List Item: (3) Router
    Parameter Request List Item: (6) Domain Name Server
    Parameter Request List Item: (15) Domain Name
```

5. DHCP ACK

DHCP 服务器允许 PC 使用请求 IP

```
Your (client) IP address: 192.168.10.254
Next server IP address: 0.0.0.0
Relay agent IP address: 0.0.0.0
Client MAC address: HuaweiTechno_d0:08:70 (54:89:98:d0:08:70)
Client hardware address padding: 00000000000000000000
Server host name not given
Boot file name not given
Magic cookie: DHCP
Option: (53) DHCP Message Type (ACK)
    Length: 1
    DHCP: ACK (5)
Option: (1) Subnet Mask (255.255.255.0)
    Length: 4
    Subnet Mask: 255.255.255.0
Option: (3) Router
    Length: 4
    Router: 192.168.10.100
Option: (51) IP Address Lease Time
    Length: 4
    IP Address Lease Time: 2 days, 2 hours, 30 minutes (181800)
```

6. Gratuitous ARP

免费 ARP 请求，请求自己的 IP 对应的 MAC 地址，能够避免 IP 冲突

```
Address Resolution Protocol (request/gratuitous ARP)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (1)
    [Is gratuitous: True]
    Sender MAC address: HuaweiTechno_d0:08:70 (54:89:98:d0:08:70)
    Sender IP address: 192.168.10.254
    Target MAC address: Broadcast (ff:ff:ff:ff:ff:ff)
    Target IP address: 192.168.10.254
```

6.2 DNS 服务简单配置与分析

1. DNS 服务器表项配置

2. 连通性测试

```
PC>ping ftp.xidian.edu.cn

Ping ftp.xidian.edu.cn [192.168.10.12]: 32 data bytes, Press Ctrl_C to break
From 192.168.10.12: bytes=32 seq=1 ttl=255 time=31 ms
From 192.168.10.12: bytes=32 seq=2 ttl=255 time<1 ms
From 192.168.10.12: bytes=32 seq=3 ttl=255 time=15 ms
From 192.168.10.12: bytes=32 seq=4 ttl=255 time<1 ms
From 192.168.10.12: bytes=32 seq=5 ttl=255 time<1 ms

--- 192.168.10.12 ping statistics ---
  5 packet(s) transmitted
  5 packet(s) received
  0.00% packet loss
  round-trip min/avg/max = 0/9/31 ms

PC>ping www.xidian.edu.cn

Ping www.xidian.edu.cn [192.168.10.12]: 32 data bytes, Press Ctrl_C to break
From 192.168.10.12: bytes=32 seq=1 ttl=255 time<1 ms
From 192.168.10.12: bytes=32 seq=2 ttl=255 time<1 ms
From 192.168.10.12: bytes=32 seq=3 ttl=255 time=31 ms
From 192.168.10.12: bytes=32 seq=4 ttl=255 time=16 ms
```

3. 抓包

555	1137.156000	HuaweiTechno_d0:08:…	Broadcast	ARP	60	Who has 192.168.10.12? Tell 192.168.10.254
556	1137.156000	HuaweiTechno_e8:2c:…	HuaweiTechno_d0:08:…	ARP	60	192.168.10.12 is at 54:89:98:e8:2c:60
557	1137.187000	192.168.10.254	192.168.10.12	DNS	77	Standard query 0xbe18 A www.xidian.edu.cn
558	1137.328000	192.168.10.12	192.168.10.254	DNS	93	Standard query response 0xbe18 A www.xidian.edu.cn A 192.168.10.12
559	1138.187000	192.168.10.254	192.168.10.12	ICMP	74	Echo (ping) request id=0x47b0, seq=1/256, ttl=128 (reply in 560)
560	1138.187000	192.168.10.12	192.168.10.254	ICMP	74	Echo (ping) reply id=0x47b0, seq=1/256, ttl=255 (request in 559)

- 查询报文

```
> User Datagram Protocol, Src Port: 46825, Dst Port: 53
v Domain Name System (query)
    Transaction ID: 0xbe18
  v Flags: 0x0100 Standard query
      0... .... .... .... = Response: Message is a query
      .000 0... .... .... = Opcode: Standard query (0)
      .... ..0. .... .... = Truncated: Message is not truncated
      .... ...1 .... .... = Recursion desired: Do query recursively
      .... .... .0.. .... = Z: reserved (0)
      .... .... ...0 .... = Non-authenticated data: Unacceptable
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  v Queries
    v www.xidian.edu.cn: type A, class IN
        Name: www.xidian.edu.cn
        [Name Length: 17]
        [Label Count: 4]
        Type: A (1) (Host Address)
```

- 响应报文

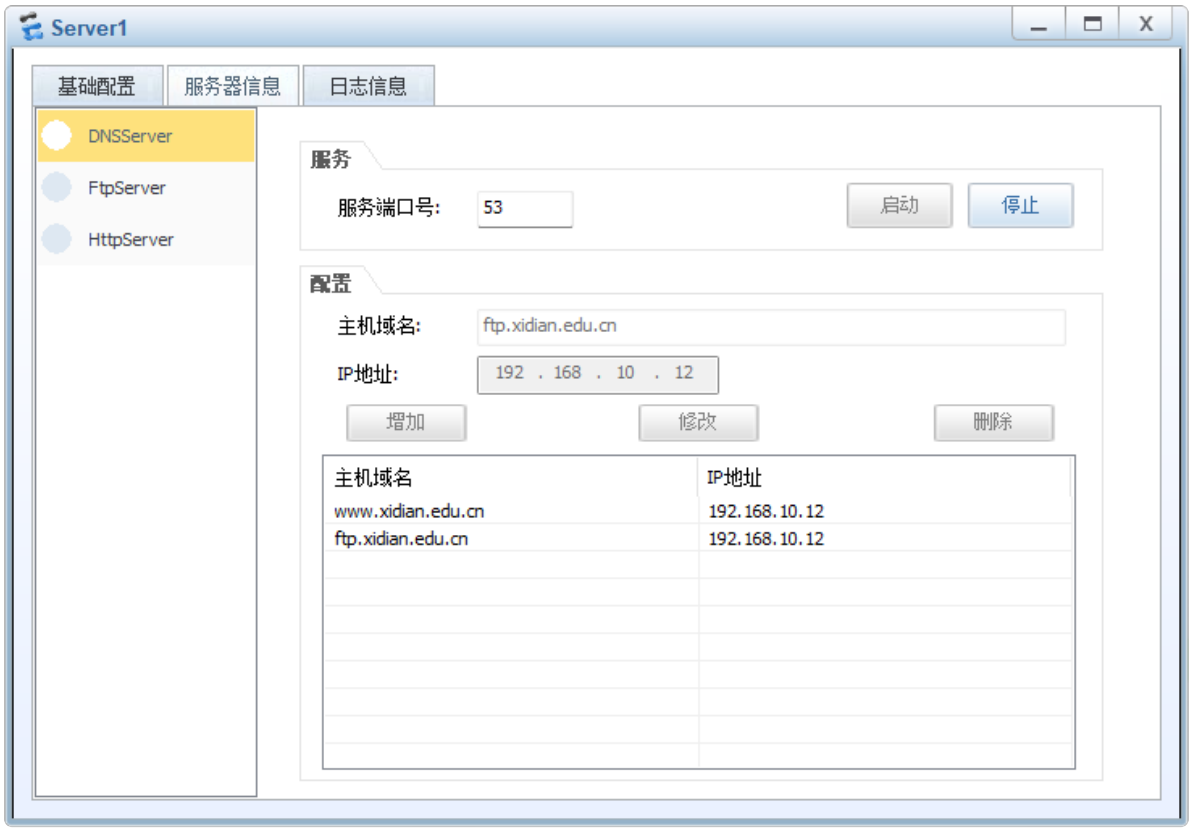
```
Domain Name System (response)
    Transaction ID: 0xbe18
  Flags: 0x8100 Standard query response, No error
      1... .... .... .... = Response: Message is a response
      .000 0... .... .... = Opcode: Standard query (0)
      .... .0.. .... .... = Authoritative: Server is not an authority for
      .... ..0. .... .... = Truncated: Message is not truncated
      .... ...1 .... .... = Recursion desired: Do query recursively
      .... .... 0... .... = Recursion available: Server can't do recursiv
      .... .... .0.. .... = Z: reserved (0)
      .... .... ..0. .... = Answer authenticated: Answer/authority portic
      .... .... ...0 .... = Non-authenticated data: Unacceptable
      .... .... .... 0000 = Reply code: No error (0)
    Questions: 1
    Answer RRs: 1
    Authority RRs: 0
    Additional RRs: 0
  Queries
    www.xidian.edu.cn: type A, class IN
        Name: www.xidian.edu.cn
        [Name Length: 17]
        [Label Count: 4]
        Type: A (1) (Host Address)
        Class: IN (0x0001)
  Answers
    www.xidian.edu.cn: type A, class IN, addr 192.168.10.12
```

- 传输层采取 UDP 协议

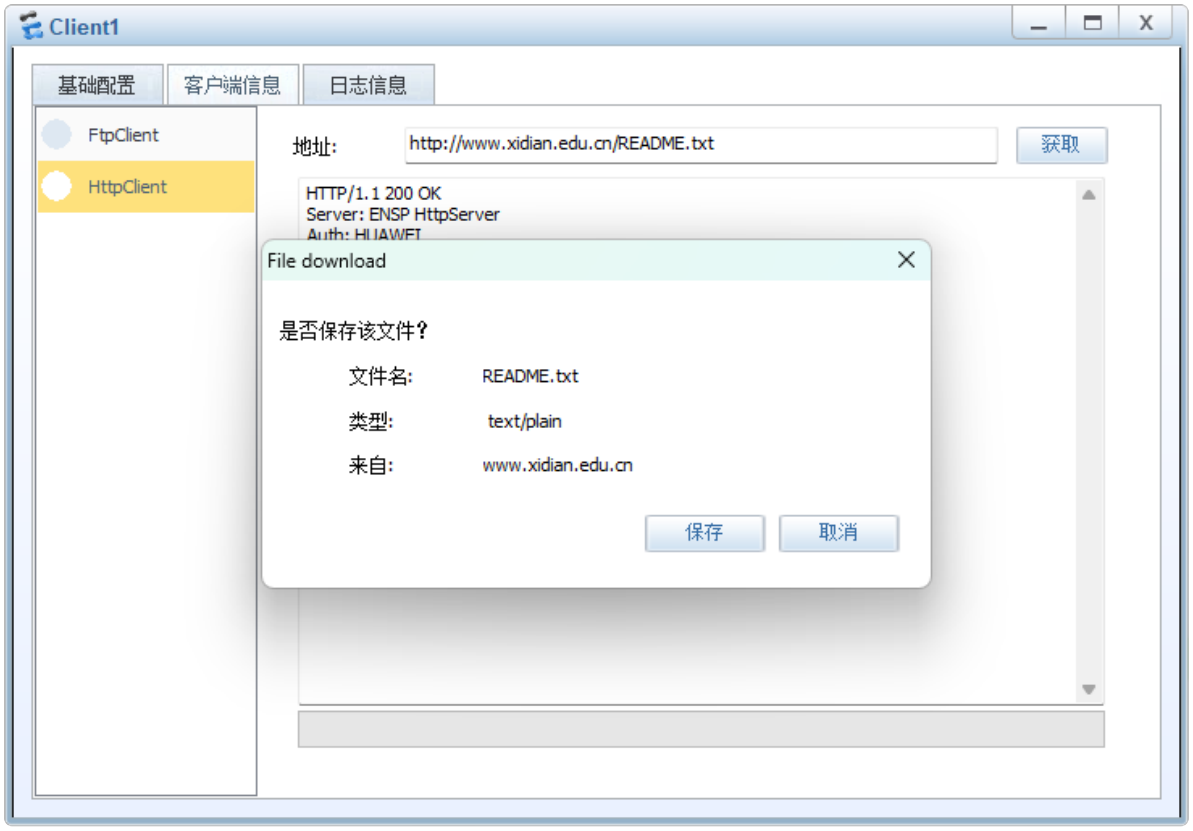
```
Internet Protocol Version 4, Src: 192.168.10.12, Dst: 192.168.10.254
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 79
    Identification: 0x0009 (9)
  000. .... = Flags: 0x0
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 255
    Protocol: UDP (17)
    Header Checksum: 0x253a [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.10.12
    Destination Address: 192.168.10.254
User Datagram Protocol, Src Port: 53, Dst Port: 46825
    Source Port: 53
    Destination Port: 46825
    Length: 59
    Checksum: 0x2802 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 0]
  [Timestamps]
    UDP payload (51 bytes)
```

6.3 HTTP 服务

1. 配置 HTTP 服务



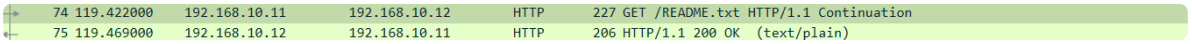
2. Client 使用 HTTP 服务



3. 数据包分析

```
    69 119.140000    192.168.10.11    192.168.10.12    DNS       77 Standard query 0x0002 A www.xidian.edu.cn
    70 119.390000    192.168.10.12    192.168.10.11    DNS       93 Standard query response 0x0002 A www.xidian.edu.cn A 192.168.10.12
    71 119.390000    192.168.10.11    192.168.10.12    TCP       58 2050 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460
    72 119.422000    192.168.10.12    192.168.10.11    TCP       58 80 → 2050 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460
    73 119.422000    192.168.10.11    192.168.10.12    TCP       54 2050 → 80 [ACK] Seq=1 Ack=1 Win=8192 Len=0
    74 119.422000    192.168.10.11    192.168.10.12    HTTP     227 GET /README.txt HTTP/1.1 Continuation
    75 119.469000    192.168.10.12    192.168.10.11    HTTP     206 HTTP/1.1 200 OK  (text/plain)
    76 119.672000    192.168.10.11    192.168.10.12    TCP       54 2050 → 80 [ACK] Seq=174 Ack=153 Win=8040 Len=0
    77 120.484000    192.168.10.11    192.168.10.12    TCP       54 2050 → 80 [FIN, ACK] Seq=174 Ack=153 Win=8040 Len=0
    78 120.484000    192.168.10.12    192.168.10.11    TCP       54 80 → 2050 [ACK] Seq=153 Ack=175 Win=8018 Len=0
    79 120.484000    192.168.10.12    192.168.10.11    TCP       54 80 → 2050 [FIN, ACK] Seq=153 Ack=175 Win=8018 Len=0
    80 120.484000    192.168.10.11    192.168.10.12    TCP       54 2050 → 80 [ACK] Seq=175 Ack=154 Win=8039 Len=0
```

HTTP 协议数据包



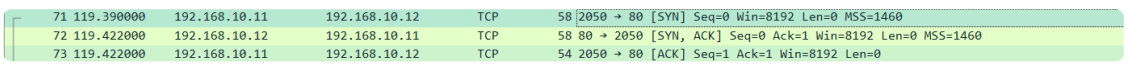
- 请求

```
Hypertext Transfer Protocol
  GET /README.txt HTTP/1.1\r\n
  Accept: */*\r\n
  Accept-Language: zh-cn\r\n
  User-Agent: Mozilla/4.0\r\n
  Accept-Encoding: gzip, deflate\r\n
  Host: www.xidian.edu.cn\r\n
  Connection: Keep-Alive\r\n
  \r\n
  [Full request URI: http://www.xidian.edu.cn/README.txt]
  [HTTP request 1/1]
  [Response in frame: 75]
Hypertext Transfer Protocol
```

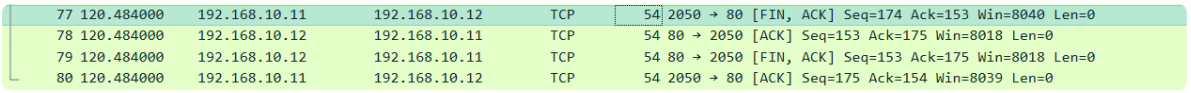
- 响应

```
Hypertext Transfer Protocol
  HTTP/1.1 200 OK\r\n
  Server: ENSP HttpServer\r\n
  Auth: HUAWEI\r\n
  Cache-Control: private\r\n
  Content-Type: text/plain\r\n
  Content-Length: 24\r\n
  \r\n
  [HTTP response 1/1]
  [Time since request: 0.047000000 seconds]
  [Request in frame: 74]
  [Request URI: http://www.xidian.edu.cn/README.txt]
  File Data: 24 bytes
Line-based text data: text/plain (3 lines)
  # TEST\r\n
  \r\n
  > Hello, eNSP!
```

TCP 连接（三次握手）

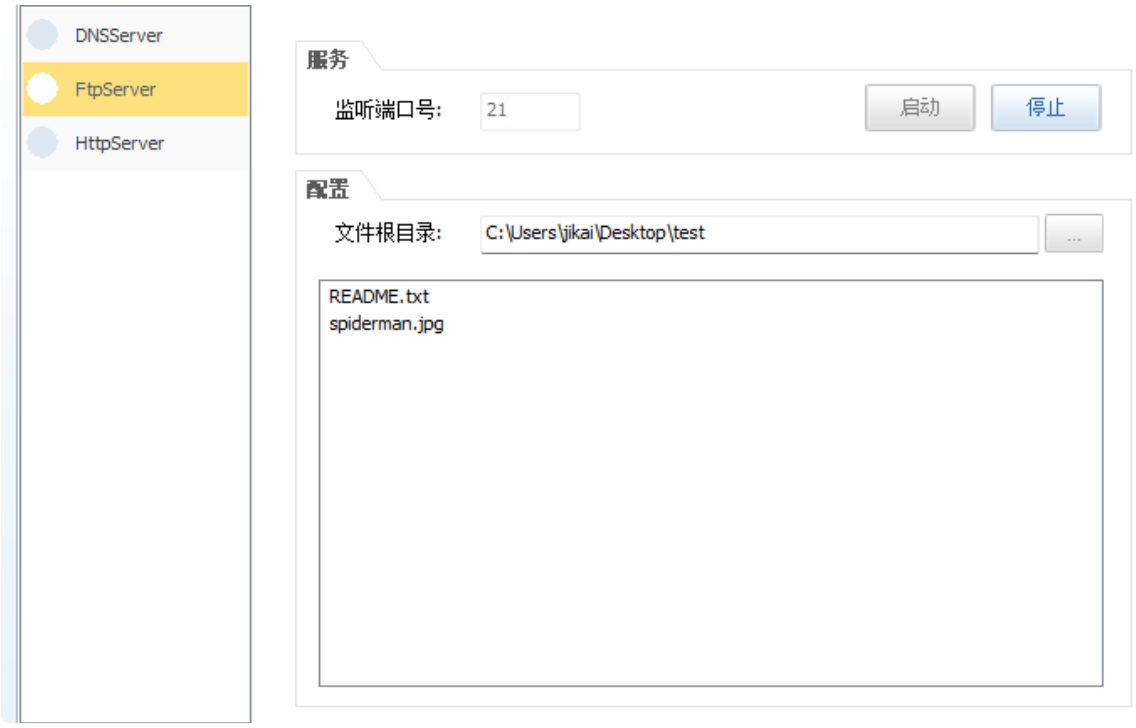


TCP 断开连接（四次握手）



6.4 FTP 服务

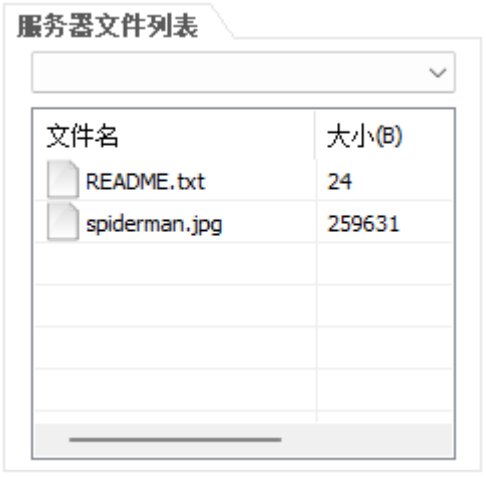
1. 服务端配置 FTP 服务



2. 登录时抓取数据包

1279	2709.672000	192.168.10.11	192.168.10.12	TCP	58 2052 → 21 [SYN] Seq=0 Win=8192 Len=0 MSS=1460
1280	2709.687000	192.168.10.12	192.168.10.11	TCP	58 21 → 2052 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460
1281	2709.687000	192.168.10.11	192.168.10.12	TCP	54 2052 → 21 [ACK] Seq=1 Ack=1 Win=8192 Len=0
1282	2709.734000	192.168.10.12	192.168.10.11	FTP	87 Response: 220 FtpServerTry FtpD for free
1283	2709.734000	192.168.10.11	192.168.10.12	FTP	62 Request: USER 1
1284	2709.765000	192.168.10.12	192.168.10.11	FTP	85 Response: 331 Password required for 1 .
1285	2709.765000	192.168.10.11	192.168.10.12	FTP	62 Request: PASS 1
1286	2709.797000	192.168.10.12	192.168.10.11	FTP	86 Response: 230 User 1 logged in , proceed
1287	2709.797000	192.168.10.11	192.168.10.12	FTP	59 Request: PWD
1288	2709.828000	192.168.10.12	192.168.10.11	FTP	84 Response: 257 "/" is current directory
1289	2709.828000	192.168.10.11	192.168.10.12	FTP	62 Request: TYPE A
1290	2709.890000	192.168.10.12	192.168.10.11	FTP	78 Response: 200 Type set to ASCII.
1291	2709.890000	192.168.10.11	192.168.10.12	FTP	60 Request: PASV
1292	2709.922000	192.168.10.12	192.168.10.11	FTP	101 Response: 227 Entering Passive Mode (192,168,10,12,8,1)
1293	2709.922000	192.168.10.11	192.168.10.12	FTP	61 Request: LIST
1294	2709.922000	192.168.10.12	192.168.10.11	TCP	58 2053 → 2049 [SYN] Seq=0 Win=8192 Len=0 MSS=1460
1295	2709.953000	192.168.10.12	192.168.10.11	TCP	58 2049 → 2053 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460
1296	2709.953000	192.168.10.11	192.168.10.12	TCP	54 2053 → 2049 [ACK] Seq=1 Ack=1 Win=8192 Len=0
1297	2709.984000	192.168.10.12	192.168.10.11	FTP	114 Response: 150 Opening ASCII NO-PRINT mode data connection for ls -l.
1298	2709.984000	192.168.10.12	192.168.10.11	FTP-DA…	123 FTP Data: 69 bytes (PASV) (LIST)
1299	2709.984000	192.168.10.12	192.168.10.11	FTP-DA…	127 FTP Data: 73 bytes (PASV) (LIST)
1300	2709.984000	192.168.10.11	192.168.10.12	TCP	54 2053 → 2049 [ACK] Seq=1 Ack=144 Win=8049 Len=0
1301	2709.984000	192.168.10.12	192.168.10.11	TCP	54 2053 → 2049 [FIN, ACK] Seq=1 Ack=144 Win=8049 Len=0
1302	2710.015000	192.168.10.12	192.168.10.11	TCP	54 2049 → 2053 [ACK] Seq=144 Ack=2 Win=8191 Len=0
1303	2710.203000	192.168.10.11	192.168.10.12	TCP	54 2052 → 21 [ACK] Seq=43 Ack=258 Win=7935 Len=0
1304	2710.203000	192.168.10.12	192.168.10.11	FTP	115 Response: 226 Transfer finished successfully. Data connection closed.
1305	2710.469000	192.168.10.12	192.168.10.11	TCP	54 2052 → 21 [ACK] Seq=43 Ack=319 Win=7874 Len=0

3. 客户端登陆 FTP 服务



> 与服务端文件列表一致

4. 服务端通过响应 PASV 命令将数据连接端口告诉客户端

1291	2709.890000	192.168.10.11	192.168.10.12	FTP	60 Request: PASV
1292	2709.922000	192.168.10.12	192.168.10.11	FTP	101 Response: 227 Entering Passive Mode (192,168,10,12,8,1)

```
File Transfer Protocol (FTP)
    227 Entering Passive Mode (192,168,10,12,8,1)\r\n
        Response code: Entering Passive Mode (227)
        Response arg: Entering Passive Mode (192,168,10,12,8,1)
        Passive IP address: 192.168.10.12
        Passive port: 2049
```

5. 客户端通过 LIST 命令获得服务器文件列表

```
1293 2709.922000  192.168.10.11  192.168.10.12  FTP      61 Request: LIST
1294 2709.922000  192.168.10.11  192.168.10.12  TCP      58 2053 → 2049 [SYN] Seq=0 Win=8192 Len=0 MSS=1460
1295 2709.953000  192.168.10.12  192.168.10.11  TCP      58 2049 → 2053 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460
1296 2709.953000  192.168.10.11  192.168.10.12  TCP      54 2053 → 2049 [ACK] Seq=1 Ack=1 Win=8192 Len=0
1297 2709.984000  192.168.10.12  192.168.10.11  FTP     114 Response: 150 Opening ASCII NO-PRINT mode data connection for ls -l.
1298 2709.984000  192.168.10.12  192.168.10.11  FTP-DA… 123 FTP Data: 69 bytes (PASV) (LIST )
1299 2709.984000  192.168.10.12  192.168.10.11  FTP-DA… 127 FTP Data: 73 bytes (PASV) (LIST )
```

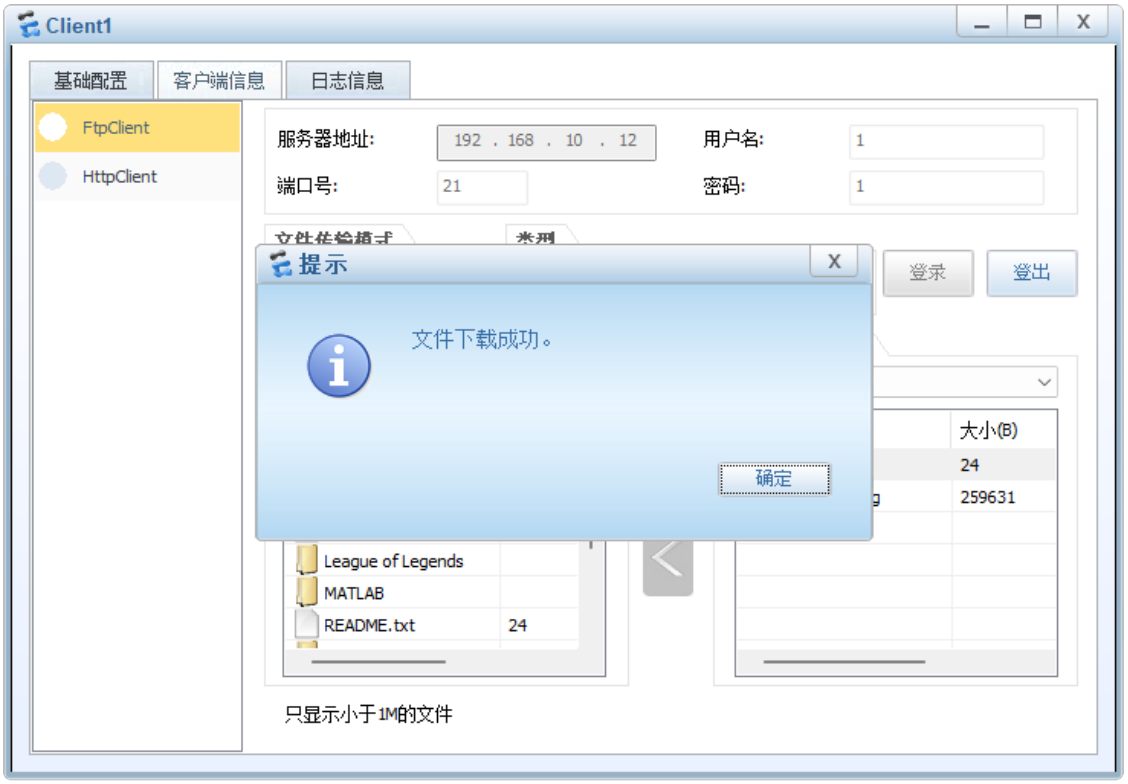
```
Line-based text data (1 lines)
    -rwxrwxrwx  1 1         nogroup           24 Jun 9  2024 README.txt\r\n
```

```
Line-based text data (1 lines)
    -rwxrwxrwx  1 1         nogroup       259631 Feb 23  2024 spiderman.jpg\r\n
```

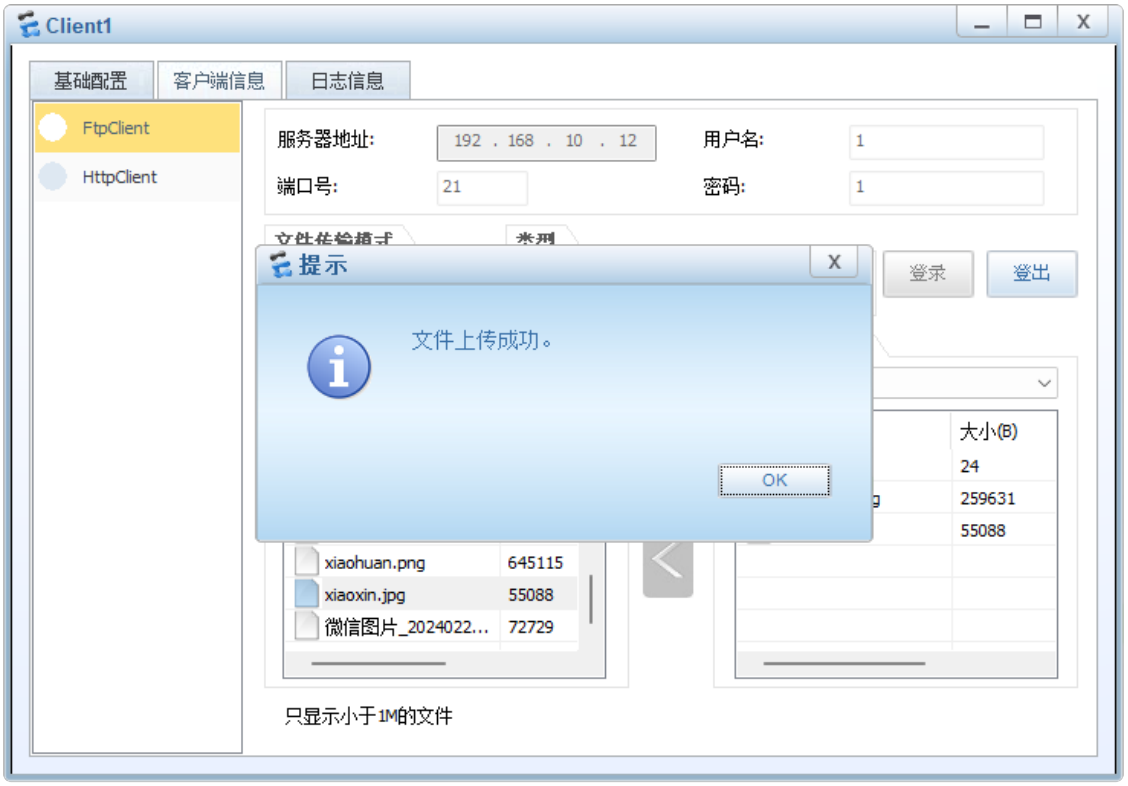
- 新建 TCP 连接
- 端口号
  - 服务器端口号：由服务器在响应`PASV`命令时指定的端口号
  - 客户端端口号：客户端从本地操作系统中获取的临时端口号
- 连接在传送完毕后释放

```
1304    2710.203000    192.168.10.12    192.168.10.11    FTP     115
Response: 226 Transfer finished successfully. Data connection closed.
```

6. 验证文件上传下载
   1. 下载



2. 上传



五。问题回答

1. 建立连接时 ACK 与 SEQ 值有何变化?
   - 客户端发送 SYN 包，SEQ 字段为`1000`（假设）。
   - 服务器发送 SYN-ACK 包，SEQ 字段为`2000`（假设），ACK 字段为`1001`。
   - 客户端发送的 ACK 包中，SEQ 字段为 `1001`（`1000` + 1），ACK 字段为`2001`（`2000` + 1）
2. 为什么释放连接比建立连接多一次?

   - 关闭连接时，客户端向服务端发送 `FIN` 时，仅仅表示客户端不再发送数据了但是还能接收数据。
   - 服务端收到客户端的 `FIN` 报文时，先回一个 `ACK` 应答报文，而服务端可能还有数据需要处理和发送，等服务端不再发送数据时，才发送 `FIN` 报文给客户端来表示同意现在关闭连接。

   从上面过程可知，服务端通常需要等待完成数据的发送和处理，所以服务端的 `ACK` 和 `FIN` 一般都会分开发送，因此是需要四次挥手。