



Práctica 5 FTP

FTP Consta de 2 conexiones independientes

- Una para control
- otra para datos

Tipicamente

- Control por el puerto 21 del servidor
- datos por el puerto 20 del servidor

Para establecer la conexión, existen 2 modos:

Modo activo

El cliente se conecta al servidor por el puerto de control (puerto 21) mediante un puerto no privilegiado

Puertos privilegiados (puertos en el rango 0-1023)

El puerto se escoge aleatoriamente

Por tanto, los puertos de conexión serán (N, 21)

En cuanto a la conexión de datos, se suele utilizar la N+1 y el servidor el 20, (N+1, 20)

El servidor es el que inicia la conexión de datos.



Si el cliente quiere utilizar un puerto distinto al N+1, debe notificarlo al servidor mediante la conexión de control

Mediante los comando **PORT** o **EPRT**

- PORT

sintaxis: PORT a1,a2,a3,a4,p1,p2

- a1,a2,a3,a4 indica la dirección IP
- p1,p2 permiten determinar el puerto
 - $\text{puerto} = p1 \cdot 256 + p2$

- EPRT

sintaxis: EPRT |1| a1,a2,a3,a4|puerto|

- el 1 indica si se utiliza IPV4, (a1,a2,a3,a4) dirección IP
- puerto, el puerto el que quieres que se conecte el servidor

Modo Pasivo

Si el cliente tiene un firewall, el modo activo puede no ser optimo ya que el cliente es el que inicia la conexión de datos

El modo pasivo soluciona este inconveniente

El cliente inicia la conexión de control y de datos

A través de (N, 21) y antes de transferir datos

El cliente debe enviar EPSV o PASV

Gracias a esto el servidor sabe que la conexión va a ser en modo pasivo

Debe seleccionar un $S > 1024$ y notificarlo al cliente por la conexión de control

($N+1$, S) para datos



- Primero miramos cual es la IP de www.cc.uah.es

23	2.746959	172.29.16.32	192.168.153.140	DNS	73 Standard query 0xe31c A www.cc.uah.es
24	2.747414	192.168.153.140	172.29.16.32	DNS	89 Standard query response 0xe31c A www.cc.uah.es A 193.146.58.130

```
▼ Queries
  ▼ www.cc.uah.es: type A, class IN
    Name: www.cc.uah.es
    [Name Length: 13]
    [Label Count: 4]
    Type: A (Host Address) (1)
    Class: IN (0x0001)
  ▼ Answers
    ▼ www.cc.uah.es: type A, class IN, addr 193.146.58.130
      Name: www.cc.uah.es
      Type: A (Host Address) (1)
      Class: IN (0x0001)
      Time to live: 172800 (2 days)
      Data length: 4
      Address: 193.146.58.130
```

- Establezco conexión TCP (ESTABLECIMIENTO EN 3 PASOS)

25	2.747605	172.29.16.32	193.146.58.130	TCP	74	42058 → 21 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM=1 TSval=9681095 TSecr=0 WS=128
26	2.748338	193.146.58.130	172.29.16.32	TCP	74	21 → 42058 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSval=970649166 TSecr=9681095 WS=64

```

Transmission Control Protocol, Src Port: 42058, Dst Port: 21, Seq: 0, Len: 0
- Source Port: 42058
- Destination Port: 21
- [Stream index: 0]
- [Conversation completeness: Complete, WITH_DATA (31)]
- [TCP Segment Len: 0]
- Sequence Number: 0      (relative sequence number)
- Sequence Number (raw): 1693998184
- [Next Sequence Number: 1      (relative sequence number)]
- Acknowledgment Number: 0
- Acknowledgment number (raw): 0
- 1010 .... = Header Length: 40 bytes (10)
▼ Flags: 0x002 (SYN)
- 000. .... = Reserved: Not set
- ...0 .... = Nonce: Not set
- .... 0... = Congestion Window Reduced (CWR): Not set
- .... .0.. = ECN-Echo: Not set
- .... ..0. = Urgent: Not set
- .... ...0 = Acknowledgment: Not set
- .... .... 0... = Push: Not set
- .... .... .0.. = Reset: Not set
▶ .... .... ..1. = Syn: Set
- .... .... 0 = Fin: Not set

```

El servidor contesta al establecimiento de conexión

```

Transmission Control Protocol, Src Port: 21, Dst Port: 42058, Seq: 0, Ack: 1, Len: 0
- Source Port: 21
- Destination Port: 42058
- [Stream index: 0]
- [Conversation completeness: Complete, WITH_DATA (31)]
- [TCP Segment Len: 0]
- Sequence Number: 0      (relative sequence number)
- Sequence Number (raw): 3968568933
- [Next Sequence Number: 1      (relative sequence number)]
- Acknowledgment Number: 1      (relative ack number)
- Acknowledgment number (raw): 1693998185
- 1010 .... = Header Length: 40 bytes (10)
▼ Flags: 0x012 (SYN, ACK)
  000. .... = Reserved: Not set
  ...0 .... = Nonce: Not set
  .... 0... = Congestion Window Reduced (CWR): Not set
  .... .0.. = ECN-Echo: Not set
  .... ..0. = Urgent: Not set
  .... ...1 .... = Acknowledgment: Set
  .... .... 0... = Push: Not set
  .... .... .0.. = Reset: Not set
  ► .... .... ..1. = Syn: Set

```

Cliente responde

```

Transmission Control Protocol, Src Port: 42058, Dst Port: 21, Seq: 1, Ack: 1, Len: 0
  Source Port: 42058
  Destination Port: 21
  [Stream index: 0]
  [Conversation completeness: Complete, WITH_DATA (31)]
  [TCP Segment Len: 0]
  Sequence Number: 1      (relative sequence number)
  Sequence Number (raw): 1693998185
  [Next Sequence Number: 1      (relative sequence number)]
  Acknowledgment Number: 1      (relative ack number)
  Acknowledgment number (raw): 3968568934
  1000 .... = Header Length: 32 bytes (8)
  ▼ Flags: 0x010 (ACK)
    000. .... = Reserved: Not set
    ...0 .... = Nonce: Not set
    .... 0... = Congestion Window Reduced (CWR): Not set
    .... .0.. = ECN-Echo: Not set
    .... ..0. = Urgent: Not set
    .... ...1 = Acknowledgment: Set
    .... .... 0... = Push: Not set
    .... .... .0.. = Reset: Not set
    .... .... ..0. = Syn: Not set

```

Ejemplo de conexion

A traves de netcat, entrar en modo pasivo y descargar el archivo /public/Docs/listado.txt

- nc server port_number (Iniciar como Cliente)
 - PASV
 - USER anonymous
 - PASS anonymous
 - CWD public/Docs
 - RETR listado.txt
- nc -l -p port_number (Iniciar como Servidor)

- nc ftp.servidor.com numero_puerto
- pasv
- user nombre_usuario
- pass contraseña_usuario
- cwd public/Docs
- retr listado.txt

Conexión de control

- nc servidor.com 21
- user usuario
- pass contraseña
- pasv
 - 227 Entering Passive Mode (193,166,3,1,145,46)
 - $145 * 256 + 46 = 37166$
-
- cwd /dire/asf
- retr README.TXT

Conexion de datos

- nc servidor.com 37166