

Modos de conexión FTP: activo vs pasivo

OBJETIVOS

- ✓ Describir los modos de conexión FTP entre el cliente y el servidor.

Una **conexión FTP** puede funcionar de dos modos: **activo** (el modo por defecto) y **pasivo** (conocido como *passive mode*).

Para entender cómo funcionan estos modos, debemos profundizar un poco más en el esquema cliente/servidor y explicar cómo se realiza paso a paso una conexión entre la máquina cliente y servidora.

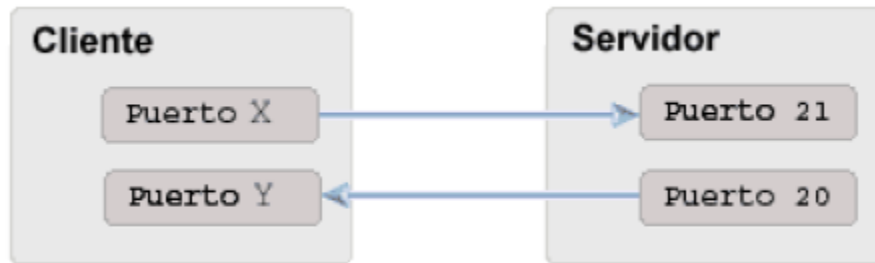
Para entender los siguientes pasos, debemos comprender un concepto muy importante del protocolo TCP/IP: el concepto de **puerto**.

Un puerto es un identificador de conexión remota. No es más que un número, e identifica la conexión de tal modo que para conectarnos a una máquina remota, debemos utilizar un puerto que esté libre. Normalmente, se admiten números de puerto desde 1 hasta 65535, y los 1024 primeros están reservados para el sistema (esto depende del sistema operativo). Cuando nos conectamos a una máquina remota, debemos indicar la dirección o nombre de la máquina (dirección IP y nombre de dominio) y el número de puerto del servidor (el identificador de nuestra conexión). De este modo, cuando llega un dato a la máquina remota, sabe perfectamente a qué conexión pertenece dicho dato. Pensad que si no existiera el puerto, una máquina sólo podría atender una conexión remota simultáneamente, porque no sería capaz de diferenciar los datos de las distintas conexiones. Tanto el cliente como el servidor deben tener un puerto activo durante la conexión. Normalmente, el que inicia la conexión (cliente) decide el puerto del servidor al que quiere conectarse y es el sistema el que asigna un número de puerto libre para el cliente.

Ahora vamos allá con los pasos de una conexión típica en FTP:

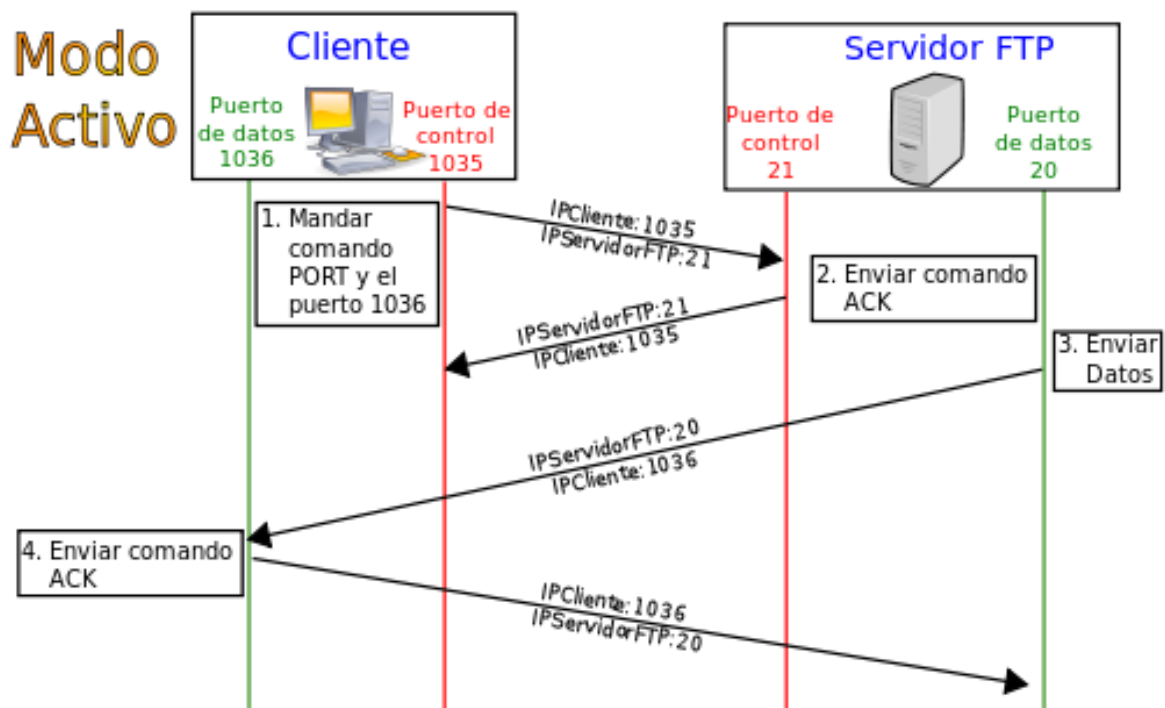
1. El cliente arranca e intenta conectarse contra el servidor. Para ello crea un canal de control estableciendo una conexión física a la dirección IP (o nombre de dominio) del servidor, y desde cualquier puerto del cliente (puerto X > 1024) hacia el puerto 21 del servidor.
2. Una vez que está establecida la conexión, se envía el comando PORT al servidor, para especificar el número de puerto que debe utilizar el servidor para crear la conexión de datos (puerto Y).
3. Para ciertas operaciones, es necesario realizar el envío de un fichero, por lo que se crea el canal de datos. Para ello **el servidor** crea una conexión física desde su puerto 20 hasta un número de puerto del cliente. Este número de puerto fue el que indicó el cliente a través del comando PORT (puerto Y > 1024). De este modo, el servidor establece el canal de datos por el que se transmite la información.

Este esquema que hemos visto es el denominado **modo activo**, porque es el servidor el que activamente crea el canal de datos. En la siguiente figura podéis ver un esquema de cómo y quién realiza las conexiones.



Modo activo

- El servidor es el que crea la conexión.
- El cliente debe tener un puerto abierto, y se lo indica con PORT



A continuación vamos a ver el modo pasivo y os daréis cuenta de la principal diferencia:

1. El cliente arranca e intenta conectarse contra el servidor. Para ello crea un canal de control estableciendo una conexión física a la dirección IP (o nombre de dominio) del servidor, y desde cualquier puerto del cliente (puerto X) hacia el puerto 21 del servidor. (Este punto es igual que en el modo activo).
2. El cliente envía el comando PASV para activar el modo pasivo. Como respuesta a este comando, el servidor retorna un número de puerto que tenga disponible (puerto Z > 1024).

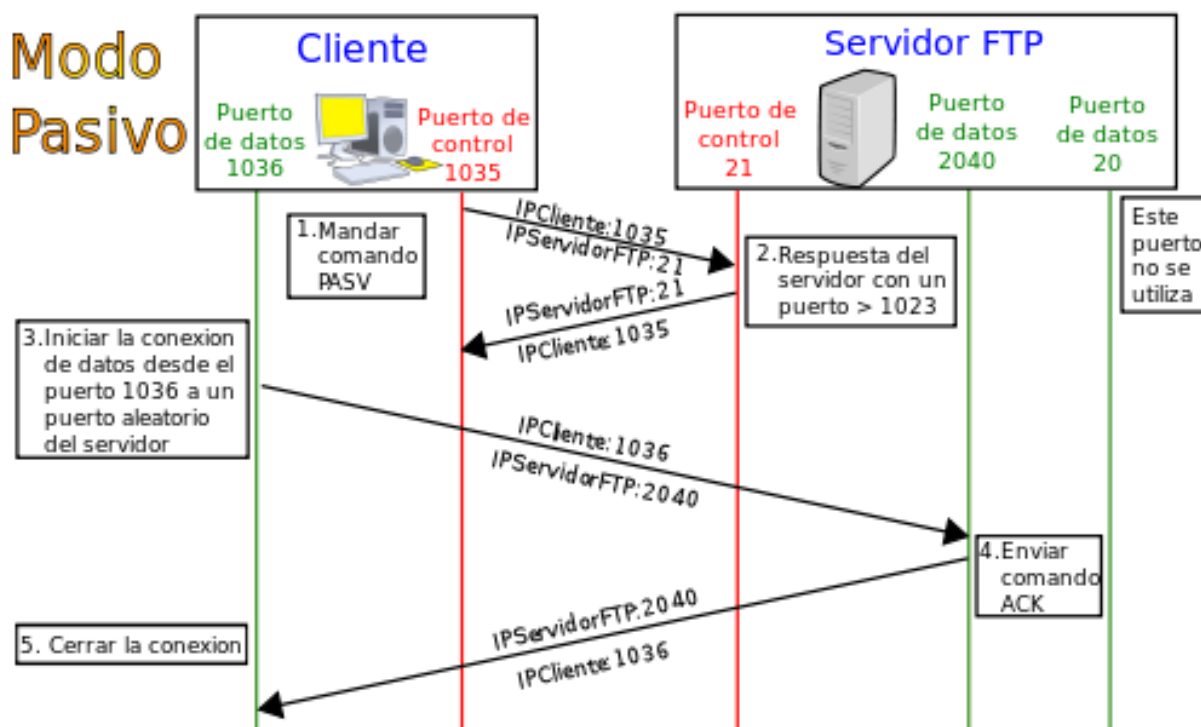
3. Para ciertas operaciones, es necesario realizar el envío de un fichero, por lo que se crea el canal de datos. Para ello **el cliente** crea una conexión física desde uno de sus puertos (puerto Y) hasta un número de puerto del servidor. Este número de puerto fue el que indicó el servidor como respuesta del comando PASV (puerto Z > 1024). De este modo, el cliente establece el canal de datos por el que se transmite la información.

Como habréis visto, la principal diferencia es que en el modo pasivo *es el cliente el que inicia las conexiones y nunca el servidor*. En la siguiente figura podéis ver un esquema de este modo de conexión:



Modo pasivo (El más habitual)

- El servidor tiene el puerto Z abierto, y nos lo indica por el canal de control mediante el comando PASV
- El servidor debe tener el puerto Z abierto



Esto, aunque parezca un detalle sin importancia, puede ser vital en algunas situaciones. Supongamos que nuestra conexión a internet utiliza un cortafuego (hoy en día algo muy recomendable).

El principal cometido del cortafuegos es cerrar los puertos para conexiones entrantes, es decir: que sobre ciertos puertos sea imposible realizar una conexión remota. Si el cliente FTP utiliza un cortafuegos, y se utiliza el modo activo de conexión, tendremos muchas posibilidades de que no funcione correctamente, ya que cuando el servidor necesite abrir el canal de datos, se podría utilizar uno de los puertos que el cortafuegos mantiene cerrado. Sin embargo, en el modo pasivo, un cortafuegos en el cliente no supone ningún problema, y además los servidores suelen tener un puerto abierto.

Así que, sabiendo esto, es muy recomendable (por no decir imprescindible) utilizar el modo pasivo si tenemos alguna sospecha de que puede haber sus cortafuegos en nuestra conexión, o si vemos que hay algún tipo de error en la conexión FTP.

Bibliografía

- Libro del módulo “Administración de servicios de transferencia de archivos y contenidos multimedia”.