

# PRÁCTICA

## Captura y análisis de una conexión FTP

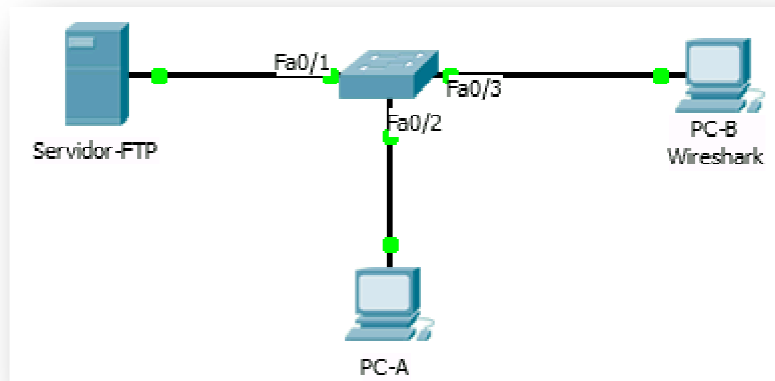


Figura 1: topología

**Objetivo:** analizar el tráfico generado por la conexión FTP entre PC-A y Servidor-FTP.

### **Desarrollo:**

**Parte 1:** Cablear y configurar la red de la figura 1.

**Parte 2:** Instalar FileZilla Server (FileZilla Server: <https://filezilla-project.org/download.php?type=server>) en el PC que hará de servidor (ver manual de instalación/configuración). Introducir en el directorio del servidor FTP un fichero llamado hola.txt. Este fichero será el que descargue el PC-A en la parte 4 de la práctica.

**Parte 3:** Configurar el puerto del switch fa0/3 como port mirroring (SPAN).

#### **Documentación:** Port mirroring

Cuando en una red conmutada se quiere monitorizar todo el tráfico, es necesario configurar el puerto del switch en el que va a estar el equipo monitor (equipo con Wireshark) para que pueda recibir todo el tráfico aunque no vaya dirigido a él. Esta característica se conoce como port mirroring . Otras denominaciones: port monitoring, Switched Port Analyzer (SPAN).

```
Switch#configure terminal
Switch(config)#monitor session 1 source interface fa0/1 both
Switch(config)#monitor session 1 destination interface fa0/3
```

NOTA: con *source interface* indicamos qué puerto va a ser monitoreado (el parámetro both se utiliza para capturar tanto el tráfico entrante como el tráfico saliente de esa

interfaz), con *destination interface* indicamos el puerto que va a actuar como mirroring port.

**Parte 4:** Arrancar Wireshark en el PC-B e iniciar la captura de tráfico. Desde el PC-A establecer una conexión FTP con el servidor FTP para descargar el fichero hola.txt. Para realizar la conexión con el servidor utiliza la línea de comandos del PC-A. Una vez cerrada la conexión FTP, parar la captura de tráfico en PC-B.

**Parte 5:** Analizar el tráfico capturado. Limpiar la captura con el siguiente filtro:

```
(ftp and ip.addr==ip_del_servidor_FTP) || (tcp and ip.addr== ip_del_servidor_FTP)
```