Departamento de
Automática y Computación
Automatika eta
Konputazio Saila

Campus de Arrosadía
Arrosadiko Campusa
31006 Pamplona - *Iruñea*
Tfno. 948 169113, Fax. 948 168924
Email: ayc@unavarra.es

Práctica 11 – Protocolos de nivel de aplicación

1- Objetivos

En esta práctica estudiaremos diversos protocolos de la capa de aplicación: Telnet, FTP, HTTP, DNS, SMTP/POP3/IMAP; los comandos existentes y problemas que se presentan. Capturaremos los paquetes transmitidos por la red con la herramienta Wireshark para luego extraer la información de la capa de aplicación y analizarla. Por último, nos familiarizaremos con la lectura de RFCs.

En esta primera sesión analizaremos los protocolos Telnet y FTP.

2- Avisos generales

Si quieren conservar cualquier fichero entre sesiones guárdenlo en una memoria USB, dado que no se asegura que los ficheros creados o modificados durante una sesión de prácticas se mantengan para la siguiente.

3- Introducción

Conviene recordar que aunque desde un punto de vista general, todos los servicios de Internet implican tráfico de algún tipo de ficheros, cuando estos son de tipos determinados, los servicios y programas que los ejecutan, reciben nombres especiales. Por ejemplo, un navegador es en cierta forma un programa FTP que recibe un tipo especial de documentos (HTML), y que además es capaz de mostrarlos en pantalla. En este caso el protocolo de transferencia utilizado es muy específico (HTTP). Un programa de correo electrónico es también un caso especial de transferencia de ficheros de una clase muy concreta (e-mail); el protocolo específico es SMTP, etc. Sin embargo, FTP se reserva para un uso genérico y es sinónimo de transferencia de cualquier tipo de ficheros: ejecutables; imagen; multimedia, etc, sin ninguna elaboración posterior. Es decir, el mero hecho de transferirlos entre máquinas (enviar por la Red una copia de un fichero contenido en el servidor, y guardarlo en el disco de la máquina cliente).

Dispone de información adicional en las RFCs correspondientes en: www.faqs.org/rfcs

Where do RFCs come from? http://www.ietf.org/newcomers.html#whither

Las conexiones TELNET y FTP se realizarán contra una máquina virtual cuya dirección IP se proporcionará al inicio de la sesión de prácticas.

4- Protocolo Telnet

El protocolo Telnet es un protocolo de Internet estándar que permite conectar terminales y aplicaciones en Internet. El protocolo proporciona reglas básicas que permiten vincular a un cliente (PC) con un intérprete de comandos (del lado del servidor).

El protocolo Telnet se aplica en una conexión TCP para enviar datos en formato ASCII codificados en 8 bits, entre los cuales se encuentran secuencias de verificación Telnet. Por lo tanto, brinda un sistema de comunicación orientado bidireccional (semidúplex) codificado en 8 bits y fácil de implementar.

El protocolo Telnet se basa en tres conceptos básicos:

Campus de Arrosadía
Arrosadiko Campusa
31006 Pamplona - *Iruñea*
Tfno. 948 169113, Fax. 948 168924
Email: ayc@unavarra.es

- El paradigma Terminal virtual de red (NVT);
- El principio de opciones negociadas;
- Las reglas de negociación.

Éste es un protocolo base, al que se le aplican otros protocolos del conjunto TCP/IP (FTP, SMTP, POP3, etc.). Las especificaciones Telnet no mencionan la autenticación porque Telnet se encuentra totalmente separado de las aplicaciones que lo utilizan (el protocolo FTP define una secuencia de autenticación sobre Telnet). Además, el protocolo Telnet no es un protocolo de transferencia de datos seguro, ya que los datos que transmite circulan en la red como texto sin codificar (de manera no cifrada). Cuando se utiliza el protocolo Telnet para conectar un host remoto a un equipo que funciona como servidor, a este protocolo se le asigna el puerto 23.

Excepto por las opciones asociadas y las reglas de negociación, las especificaciones del protocolo Telnet son básicas. La transmisión de datos a través de Telnet consiste sólo en transmitir bytes en el flujo TCP (el protocolo Telnet especifica que los datos deben agruparse de manera predeterminada —esto es, si ninguna opción especifica lo contrario— en un búfer antes de enviarse. Específicamente, esto significa que de manera predeterminada los datos se envían línea por línea). Cuando se transmite el byte 255, el byte siguiente debe interpretarse como un comando. Por lo tanto, el byte 255 se denomina IAC (Interpretar como comando). Los comandos se describen más adelante en este documento.

Las especificaciones básicas del protocolo Telnet se encuentran disponibles en la RFC (petición de comentarios) 854, mientras que las distintas opciones están descriptas en la RFC 855 hasta la RFC 861.

RFC (peticiones de comentarios) relacionadas con Telnet	
RFC 854	Especificaciones del protocolo Telnet
RFC 855	Especificaciones de opciones de Telnet
RFC 856	Transmisión binaria en Telnet
RFC 857	Opción Eco de Telnet
RFC 858	Opción de suprimir continuación en Telnet
RFC 859	Opción Estado de Telnet
RFC 860	Opción Marca de tiempo de Telnet
RFC 861	Opción Lista extendida de opciones de Telnet

La noción de terminal virtual

Cuando surgió Internet, la red (ARPANET) estaba compuesta de equipos cuyas configuraciones eran muy poco homogéneas (teclados, juegos de caracteres, resoluciones, longitud de las líneas visualizadas). Además, las sesiones de los terminales también tenían su propia manera de controlar el flujo de datos entrante/saliente.

Campus de Arrosadía
Arrosadiko Campusa
31006 Pamplona - *Iruñea*
Tfno. 948 169113, Fax. 948 168924
Email: ayc@unavarra.es

Por lo tanto, en lugar de crear adaptadores para cada tipo de terminal, para que pudiera haber interoperabilidad entre estos sistemas, se decidió desarrollar una interfaz estándar denominada NVT (Terminal virtual de red). Así, se proporcionó una base de comunicación estándar, compuesta de:

- Caracteres ASCII de 7 bits, a los cuales se les agrega el código ASCII extendido;
- Tres caracteres de control;
- Cinco caracteres de control opcionales;
- Un juego de señales de control básicas.

Por lo tanto, el protocolo Telnet consiste en crear una abstracción del terminal que permita a cualquier host (cliente o servidor) comunicarse con otro host sin conocer sus características.

El principio de opciones negociadas

Las especificaciones del protocolo Telnet permiten tener en cuenta el hecho de que ciertos terminales ofrecen servicios adicionales, no definidos en las especificaciones básicas (pero de acuerdo con las especificaciones), para poder utilizar funciones avanzadas. Estas funcionalidades se reflejan como opciones. Por lo tanto, el protocolo Telnet ofrece un sistema de negociaciones de opciones que permite el uso de funciones avanzadas en forma de opciones, en ambos lados, al iniciar solicitudes para su autorización desde el sistema remoto.

Las opciones de Telnet afectan por separado cada dirección del canal de datos. Entonces, cada parte puede negociar las opciones, es decir, definir las opciones que:

- Desea usar (DO);
- Se niega a usar (DON'T);
- Desea que la otra parte utilice (WILL);
- Se niega a que la otra parte utilice (WON'T).

De esta manera, cada parte puede enviar una solicitud para utilizar una opción. La otra parte debe responder si acepta o no el uso de la opción. Cuando la solicitud se refiere a la desactivación de una opción, el destinatario de la solicitud no debe rechazarla para ser completamente compatible con el modelo NVT.

Opciones negociadas de Telnet		
Solicitud	Respuesta	Interpretación
DO	WILL	El remitente comienza utilizando la opción.
	WON'T	El remitente no debe utilizar la opción.
WILL	DO	El remitente comienza utilizando la opción, después de enviar *DO*
	DON'T	El remitente no debe utilizar la opción

DON'T	WON'T	El remitente indica que ha desactivado la opción
WON'T	DON'T	El remitente indica que el remitente debe desactivar la opción

Existen 255 códigos de opción. De todas maneras, el protocolo Telnet proporciona un espacio de dirección que permite describir nuevas opciones. La RFC (petición de comentarios) 855 explica cómo documentar una nueva opción.

Las reglas de negociación

Las reglas de negociación para las opciones permiten evitar situaciones en las que una de las partes envía solicitudes de negociación de opciones a cada confirmación de la otra parte:

1. Las solicitudes sólo deben enviarse en el momento de un cambio de modo.
2. Cuando una de las partes recibe la solicitud de cambio de modo, sólo debe confirmar su recepción si todavía no se encuentra en el modo apropiado.
3. Sólo debe insertarse una solicitud en el flujo de datos en el lugar en el que surte efecto.

Caracteres de control de salida

Los siguientes caracteres son comandos que permiten controlar la visualización del terminal virtual de red:

Comandos de control para la visualización:			
Número;	Código	Nombre	Significado
0	NULL	Nulo	Este comando permite enviar datos al host remoto sin que se interpreten (en particular para indicar que el host local todavía esta en línea).
1	LF	Avance de línea	Este comando permite ubicar el cursor en la línea siguiente, en la misma posición horizontal.
2	CR	Retorno de carro	Este comando permite ubicar el cursor en el extremo izquierdo de la línea actual.

Así, se define el comando CRLF, compuesto de dos comandos CR y LF uno después del otro (en cualquier orden). Esto permite ubicar el cursor en el extremo izquierdo de la línea siguiente.

Caracteres de control opcionales

Los caracteres anteriores son los únicos (entre los 128 caracteres del código ASCII básico y los 128 caracteres del código ASCII extendido) que tienen un significado particular para el terminal virtual de red. Los siguientes caracteres pueden tener un significado en un terminal virtual de red, pero no se utilizan necesariamente.

Comandos de control para la visualización			
Número	Código	Nombre	Significado

7	BEL	Campana	Este comando permite enviar una señal visual o sonora sin cambiar la posición del cursor.
8	BS	Retroceso	Este comando permite cambiar la posición del cursor a su posición anterior.
9	HT	Tabulación horizontal	Este comando permite que la posición del cursor pase a la siguiente tabulación a la derecha.
11	VT	Tabulación vertical	Este comando permite que la posición del cursor pase a la siguiente tabulación de la línea siguiente.
12	FF	Avance de página	Este comando permite que la posición del cursor pase al final de la siguiente página mientras conserva su posición horizontal.

Caracteres de control de sesión

Los siguientes caracteres son comandos que permiten controlar la sesión Telnet. Para que puedan interpretarse como tal, estos comandos deben estar precedidos por el carácter de escape IAC (Interpretar como comando). Si estos bytes se transmiten sin estar precedidos por el carácter IAC, se procesarán como caracteres simples. Para transmitir el carácter IAC, este mismo debe estar precedido por un carácter de escape. En otras palabras, debe estar duplicado.

Los comandos relacionados con una negociación de opciones deben estar seguidos de un byte que especifique la opción. Estos comandos permiten interrumpir señales, eliminar información en el caché del terminal, etc.

Caracteres de control de sesión			
Número	Código	Nombre	Significado
240	SE		Fin de negociación de opciones
241	NOP	Sin operación	Este comando permite enviar datos al host remoto sin que se interpreten (en particular para indicar que el host local todavía esta en línea).
242	DM	Marca de datos	Permite vaciar todos los búferes entre el terminal virtual de red y el host remoto. Se relaciona con la pulsación del botón de sincronización (Synch) NVT y debe vincularse con una indicación de notificación urgente TCP.
243	BRK	Interrupción	Pausa de caracteres del terminal virtual.
244	IP	Interrumpir proceso	Este comando permite suspender, interrumpir o abandonar el proceso remoto.
245	AO	Abortar salida	Este comando permite suspender, interrumpir o abandonar la visualización del proceso remoto.
246	AYT	¿Estás ahí?	Este comando permite controlar que el sistema remoto todavía esté "vivo".
247	EC	Borrar carácter	Este comando permite borrar el carácter anterior.
248	EL	Borrar línea	Este comando permite borrar la línea anterior.
249	GA	Adelante	Este comando permite revertir el control, para conexiones semidúplex

250	SB	SB	Este comando indica que los datos que siguen son una negociación de la opción anterior.
251	WILL	Código de opción	
252	WON'T	Código de opción	
253	DO	Código de opción	
254	DON'T	Código de opción	
255	IAC	Interpretar como comando	Este comando permite interpretar el byte siguiente como un comando. El comando IAC permite ir más allá de los comandos básicos.

Más información

RFC 854 original: http://www.ietf.org/rfc/rfc854.txt

Analizando TELNET

Nota: *no haga nada hasta terminar de leer el apartado completo (hasta el checkpoint 10.1)*

Lance en su PC-SC el analizador de protocolos Wireshark y póngalo a capturar tramas Ethernet habilitando las opciones de mostrar la captura en tiempo real y scroll automático. Para un mejor análisis de la información capturada, aplique el siguiente filtro:

```
ip.src==10.1.1.XY o ip.dst==10.1.1.XY
```

Siga estas dos secuencias de pasos para el análisis de TELNET:

A. 1.Wireshark capturando.

2. Abra un terminal e inicie una sesión de Telnet con su máquina virtual asociada: `telnet <ip>`

3. Sin hacer login, espere hasta el cierre de la conexión.

4. Pare Wireshark y analice las tramas capturadas.

B. 1.Wireshark capturando.

2. Abra un terminal e inicie una sesión de Telnet con su máquina virtual asociada: `telnet <ip>`

3. Haga login.

Campus de Arrosadía
Arrosadiko Campusa
31006 Pamplona - *Iruñea*
Tfno. 948 169113, Fax. 948 168924
Email: ayc@unavarra.es

4. Ejecute algunos comandos: cambie de ruta de directorio, liste archivos, muestre su contenido por pantalla.

5. Pare Wireshark y analice las tramas capturadas.

Deberá ser capaz de identificar las tramas correspondientes a:

- Establecimiento de la conexión
- Negociación del terminal virtual (NVT)
- Proceso de login
- Cierre de la conexión

Identifique también algunos de los comandos de control indicados anteriormente, así como las tramas en las que se envían datos de los que deberá averiguar su significado.

¿Qué inconveniente encuentra en un acceso remoto a otro equipo mediante este protocolo? ¿Es seguro? ¿Conoce alguna alternativa a Telnet que ofrezca un acceso remoto seguro? Identifíquela con la RFC correspondiente.

Realice una captura de Wireshark en la que se aprecie el acceso seguro a su máquina virtual o a cualquier otro equipo del laboratorio.

Checkpoint 11.1: Muestra al profesor de prácticas la diferencia entre un acceso remoto seguro frente al clásico Telnet. ¿Puede utilizar Telnet en los equipos reales del laboratorio?¿Y su equivalente seguro?

Vuelva a conectarse mediante Telnet a su máquina virtual y utilice el comando `netstat` para visualizar los servicios disponibles en dicha máquina y en qué estado se encuentran; LISTEN, ESTABLISHED,… Empleen para ello las opciones -a ó –l. Consulten su manual. Pueden pasar el resultado de `netstat` al comando `grep` mediante un pipe("|") para depurar aún más su salida.

```
netstat –a |grep ftp

netstat –a |grep telnet

netstat –a |grep ESTABLISHED

netstat –a |grep LISTEN
```

Obtendrán un listado completo de todos los posibles servicios(y puertos asociados) de su máquina virtual en `/etc/services`

También pueden hacer uso del comando `who` para ver quién está conectado al sistema.

5- Protocolo FTP

El protocolo FTP (Protocolo de transferencia de archivos) es, como su nombre indica, un protocolo para transferir archivos.

Campus de Arrosadía
Arrosadiko Campusa
31006 Pamplona - *Iruñea*
Tfno. 948 169113, Fax. 948 168924
Email: ayc@unavarra.es

La implementación del FTP se remonta a 1971 cuando se desarrolló un sistema de transferencia de archivos (descrito en RFC141) entre equipos del Instituto Tecnológico de Massachusetts (MIT, Massachusetts Institute of Technology). Desde entonces, diversos documentos de RFC (petición de comentarios) han mejorado el protocolo básico, pero las innovaciones más importantes se llevaron a cabo en julio de 1973.

El protocolo FTP está definido por la RFC 959 y diversas actualizaciones en materia de seguridad.

La función del protocolo FTP

El protocolo FTP define la manera en que los datos deben ser transferidos a través de una red TCP/IP.

El objetivo del protocolo FTP es:

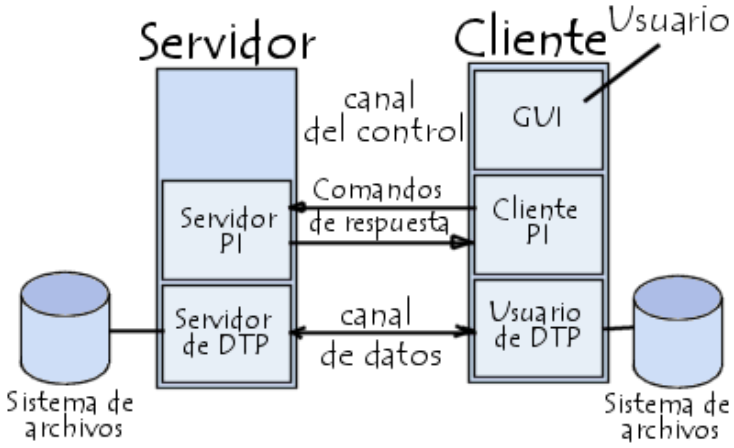
- Permitir que equipos remotos puedan compartir archivos
- Permitir la independencia entre los sistemas de archivo del equipo del cliente y del equipo del servidor
- Permitir una transferencia de datos eficaz

El modelo FTP

El protocolo FTP está incluido dentro del modelo cliente-servidor, es decir, un equipo envía órdenes (el cliente) y el otro espera solicitudes para llevar a cabo acciones (el servidor).

Durante una conexión FTP, se encuentran abiertos dos canales de transmisión:

- Un canal de comandos (canal de control)
- Un canal de datos



Por lo tanto, el cliente y el servidor cuentan con dos procesos que permiten la administración de estos dos tipos de información:

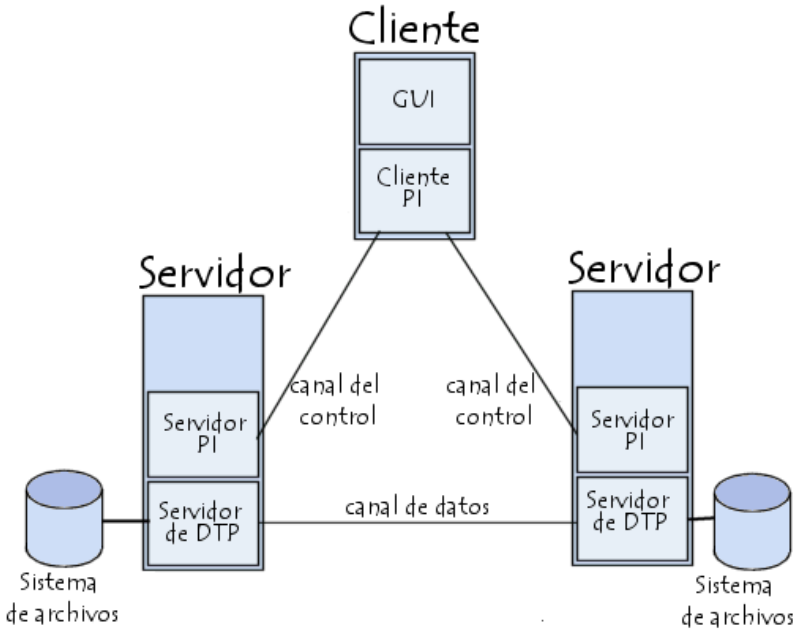
- DTP (Proceso de transferencia de datos) es el proceso encargado de establecer la conexión y de administrar el canal de datos. El DTP del lado del servidor se denomina SERVIDOR DE DTP y el DTP del lado del cliente se denomina USUARIO DE DTP.

- PI (Intérprete de protocolo) interpreta el protocolo y permite que el DTP pueda ser controlado mediante los comandos recibidos a través del canal de control. Esto es diferente en el cliente y el servidor:

- El SERVIDOR PI es responsable de escuchar los comandos que provienen de un USUARIO PI a través del canal de control en un puerto de datos, de establecer la conexión para el canal de control, de recibir los comandos FTP del USUARIO PI a través de éste, de responderles y de ejecutar el SERVIDOR DE DTP.

- El USUARIO PI es responsable de establecer la conexión con el servidor FTP, de enviar los comandos FTP, de recibir respuestas del SERVIDOR PI y de controlar al USUARIO DE DTP, si fuera necesario.

Cuando un cliente FTP se conecta con un servidor FTP, el USUARIO PI inicia la conexión con el servidor de acuerdo con el protocolo Telnet. El cliente envía comandos FTP al servidor, el servidor los interpreta, ejecuta su DTP y después envía una respuesta estándar. Una vez que se establece la conexión, el servidor PI proporciona el puerto por el cual se enviarán los datos al Cliente DTP. El cliente DTP escucha el puerto especificado para los datos provenientes del servidor. Es importante tener en cuenta que, debido a que los puertos de control y de datos son canales separados, es posible enviar comandos desde un equipo y recibir datos en otro. Entonces, por ejemplo, es posible transferir datos entre dos servidores FTP mediante el paso indirecto por un cliente para enviar instrucciones de control y la transferencia de información entre dos procesos del servidor conectados en el puerto correcto.



Campus de Arrosadía
Arrosadiko Campusa
31006 Pamplona - *Iruñea*
Tfno. 948 169113, Fax. 948 168924
Email: ayc@unavarra.es

En esta configuración, el protocolo indica que los canales de control deben permanecer abiertos durante la transferencia de datos. De este modo, un servidor puede detener una transmisión si el canal de control es interrumpido durante la transmisión.

Los comandos FTP

Toda comunicación que se realice en el canal de control sigue las recomendaciones del protocolo Telnet. Por lo tanto, los comandos FTP son cadenas de caracteres Telnet (en código NVT-ASCII) que finalizan con el código de final de línea Telnet (es decir, la secuencia <CR>+<LF>, Retorno de carro seguido del carácter Avance de línea indicado como <CRLF>). Si el comando FTP tiene un parámetro, éste se separa del comando con un espacio (<SP>).

Los comandos FTP hacen posible especificar:

- El puerto utilizado
- El método de transferencia de datos
- La estructura de datos
- La naturaleza de la acción que se va a realizar (Recuperar, Enumerar, Almacenar, etc.)

Existen tres tipos de comandos FTP diferentes:

1. Comandos de control de acceso
2. Comandos de parámetros de transferencia
3. Comandos de servicio FTP

Comandos de control de acceso	
Comando	**Descripción**
USER	Cadena de caracteres que permite identificar al usuario. La identificación del usuario es necesaria para establecer la comunicación a través del canal de datos.
PASS	Cadena de caracteres que especifica la contraseña del usuario. Este comando debe ser inmediatamente precedida por el comando *USER*. El cliente debe decidir si esconder la visualización de este comando por razones de seguridad.
ACCT	Cadena de caracteres que especifica la cuenta del usuario. El comando generalmente no es necesario. Durante la respuesta que acepta la contraseña, si la respuesta es 230, esta etapa no es necesaria; Si la respuesta es 332, sí lo es.
CWD	*Change Working Directory (Cambiar el directorio de trabajo)*: este comando permite cambiar el directorio actual. Este comando requiere la ruta de acceso al directorio para que se complete como un argumento.
CDUP	*Change to Parent Directory (Cambiar al directorio principal)*: este comando permite regresar al directorio principal. Se introdujo para resolver los problemas de denominación del directorio principal según el sistema (generalmente "..").
SMNT	*Structure Mount (Montar estructura)*:

REIN	*Reinitialize (Reinicializar)*:
QUIT	Comando que permite abandonar la sesión actual. Si es necesario, el servidor espera a que finalice la transferencia en progreso y después proporciona una respuesta antes de cerrar la conexión.

Comandos de parámetros de transferencia	
Comando	**Descripción**
PORT	Cadena de caracteres que permite especificar el número de puerto utilizado.
PASV	Comando que permite indicar al servidor de DTP que permanezca a la espera de una conexión en un puerto específico elegido aleatoriamente entre los puertos disponibles. La respuesta a este comando es la dirección IP del equipo y el puerto.
TYPE	Este comando permite especificar el tipo de formato en el cual se enviarán los datos.
STRU	Carácter Telnet que especifica la estructura de archivos (F de *File [Archivo]*, R de *Record [Registro]*, P de *Page [Página]*).
MODE	Carácter Telnet que especifica el método de transferencia de datos (S de *Stream [Flujo]*, B de *Block [Bloque]*, C de *Compressed [Comprimido]*).

Comandos de servicio FTP	
Comando	**Descripción**
RETR	Este comando (*RETRIEVE [RECUPERAR]*) le pide al servidor de DTP una copia del archivo cuya ruta de acceso se da en los parámetros.
STOR	Este comando (*store [almacenar]*) le pide al servidor de DTP que acepte los datos enviados por el canal de datos y que los almacene en un archivo que lleve el nombre que se da en los parámetros. Si el archivo no existe, el servidor lo crea; de lo contrario, lo sobrescribe.
STOU	Este comando es idéntico al anterior, sólo le pide al servidor que cree un archivo cuyo nombre sea único. El nombre del archivo se envía en la respuesta.
APPE	Gracias a este comando (*append [adjuntar]*) los datos enviados se concatenan en el archivo que lleva el nombre dado en el parámetro si ya existe; si no es así, se crea.
ALLO	Este comando (*allocate [reservar]*) le pide al servidor que reserve un espacio de almacenamiento lo suficientemente grande como para recibir el archivo cuyo nombre se da en el argumento.
REST	Este comando (*restart [reiniciar]*) permite que se reinicie una transferencia desde donde se detuvo. Para hacer esto, el comando envía en el parámetro el marcador que representa la posición en el archivo donde la transferencia se había interrumpido. Después de este comando se debe enviar inmediatamente un comando de transferencia.
RNFR	Este comando (*rename from [renombrar desde]*) permite volver a nombrar un archivo. En los parámetros indica el nombre del archivo que se va a renombrar y debe estar inmediatamente seguido por el comando *RNTO*.
RNTO	Este comando (*rename from [renombrar a]*) permite volver a nombrar un archivo. En los parámetros indica el nombre del archivo que se va a renombrar y debe estar inmediatamente seguido por el comando *RNFR*.

Campus de Arrosadía
Arrosadiko Campusa
31006 Pamplona - *Iruñea*
Tfno. 948 169113, Fax. 948 168924
Email: ayc@unavarra.es

ABOR	Este comando (*abort [cancelar]*) le indica al servidor de DTP que abandone todas las transferencias asociadas con el comando previo. Si no hay conexión de datos abierta, el servidor de DTP no realiza ninguna acción; de lo contrario, cierra la conexión. Sin embargo, el canal de control permanece abierto.
DELE	Este comando (*delete [borrar]*) permite que se borre un archivo, cuyo nombre se da en los parámetros. Este comando es irreversible y la confirmación sólo puede darse a nivel cliente.
RMD	Este comando (*remove directory [eliminar directorio]*) permite borrar un directorio. El nombre del directorio que se va a borrar se indica en los parámetros.
MKD	Este comando (*make directory [crear directorio]*) permite crear un directorio. El nombre del directorio que se va a crear se indica en los parámetros.
PWD	Este comando (*print working directory [mostrar el directorio actual]*) hace posible volver a enviar la ruta del directorio actual completa.
LIST	Este comando permite que se vuelva a enviar la lista de archivos y directorios presentes en el directorio actual. Esto se envía a través del DTP pasivo. Es posible indicar un nombre de directorio en el parámetro de este comando. El servidor de DTP enviará la lista de archivos del directorio ubicado en el parámetro.
NLST	Este comando (*name list [lista de nombres]*) permite enviar la lista de archivos y directorios presentes en el directorio actual.
SITE	Este comando (*site parameters [parámetros del sistema]*) hace que el servidor proporcione servicios específicos no definidos en el protocolo FTP.
SYST	Este comando (*system [sistema]*) permite el envío de información acerca del servidor remoto.
STAT	Este comando (*Estado: [estado]*) permite transmitir el estado del servidor; por ejemplo, permite conocer el progreso de una transferencia actual. Este comando acepta una ruta de acceso en el argumento y después devuelve la misma información que LISTA pero a través del canal de control.
HELP	Este comando permite conocer todos los comandos que el servidor comprende. La información se devuelve por el canal de control.
NOOP	Este comando (*no operations [no operación]*) sólo se utiliza para recibir un comando OK del servidor. Sólo se puede utilizar para no desconectarse después de un período de inactividad prolongado.

Las respuestas FTP

Las respuestas FTP garantizan la sincronización entre el cliente y el servidor FTP. Por lo tanto, por cada comando enviado por el cliente, el servidor eventualmente llevará a cabo una acción y sistemáticamente enviará una respuesta.

Las respuestas están compuestas por un código de 3 dígitos que indica la manera en la que el comando enviado por el cliente ha sido procesado. Sin embargo, debido a que el código de 3 dígitos resulta difícil de leer para las personas, está acompañado de texto (cadena de caracteres Telnet separada del código numérico por un espacio).

Los códigos de respuesta están compuestos por 3 números, cuyos significados son los siguientes:

- El primer número indica el estado de la respuesta (exitosa o fallida)
- El segundo número indica a qué se refiere la respuesta.

- El tercer número brinda un significado más específico (relacionado con cada segundo dígito).

Primer número		
Dígito	**Significado**	**Descripción**
1yz	Respuesta positiva preliminar	La acción solicitada está en progreso. Se debe obtener una segunda respuesta antes de enviar un segundo comando.
2yz	Respuesta de finalización positiva	La acción solicitada se ha completado y puede enviarse un nuevo comando.
3yz	Respuesta intermedia positiva	La acción solicita está temporalmente suspendida. Se espera información adicional del cliente.
4yz	Respuesta de finalización negativa	La acción solicitada no se ha realizado debido a que el comando no se ha aceptado temporalmente. Se le solicita al cliente que intente más tarde.
5yz	Respuesta negativa permanente	La acción solicitada no se ha realizado debido a que el comando no ha sido aceptado. Se le solicita al cliente que formule una solicitud diferente.

Segundo número		
Dígito	**Significado**	**Descripción**
x**0**z	Sintaxis	La acción tiene un error de sintaxis o sino, es un comando que el servidor no comprende.
x**1**z	Información	Ésta es una respuesta que envía información (por ejemplo, una respuesta a un comando STAT).
x**2**z	Conexiones	La respuesta se refiere al canal de datos.
x**3**z	Autenticación y cuentas	La respuesta se refiere al inicio de sesión (USUARIO/CONTRASEÑA) o a la solicitud para cambiar la cuenta (CPT).
x**4**z	No utilizado por el protocolo FTP.	
x**5**z	Sistema de archivos	La respuesta se relaciona con el sistema de archivos remoto.

Analizando FTP

Siga el mismo procedimiento empleado para el análisis de Telnet.

Lance en su PC-SC el analizador de protocolos Wireshark y póngalo a capturar tramas Ethernet. Aplique el siguiente filtro: `ip.src==10.1.1.XY o ip.dst==10.1.1.XY`

Departamento de
Automática y Computación
Automatika eta
Konputazio Saila

Campus de Arrosadía
Arrosadiko Campusa
31006 Pamplona - *Iruñea*
Tfno. 948 169113, Fax. 948 168924
Email: ayc@unavarra.es

Inicie una sesión FTP en su máquina virtual. Consulte el manual del comando `ftp` (`man ftp`) y averigüe la utilidad de la opción `-d`. Utilícela.

Transfiera un archivo del equipo local PC-SC al equipo remoto(máquina virtual).

Renombre dicho archivo transferido a la máquina virtual y por último elimínelo.

¿Qué comandos FTP ha utilizado?

Pare la captura de Wireshark y analice cada uno de estos comandos, así como los protocolos involucrados en la sesión FTP. ¿Puede ver la contraseña en la captura obtenida?

Guarde la captura en su PC-SC.

Vuelva a lanzar Wireshark. Aplique los mismos filtros.

Conéctese mediante Telnet al servicio FTP de su máquina virtual.

Mediante los comandos apropiados, al menos, cree un directorio y bórrelo.

Detenga la captura de Wireshark y compárela con la guardada anteriormente. ¿Qué diferencias encuentra? ¿Cuál es el mayor inconveniente que observa en el protocolo FTP? ¿Conoce alguna RFC en la que se incremente la seguridad de dicho protocolo? ¿Qué protocolo usaría para una transferencia segura de archivos? Repita la operación anterior mediante dicho protocolo. ¿Cuál es ahora la diferencia respecto FTP?

Checkpoint 11.2: Muestra al profesor de prácticas los puertos que utiliza el servicio FTP tanto en el cliente como en el servidor. ¿Cuántos puertos se utilizan? ¿Por qué?

Encuentre la diferencia entre los modos activo y pasivo de un servidor FTP. ¿Qué utilidad tienen? ¿Cuál considera que es más indicado para garantizar la compatibilidad en la arquitectura cliente-servidor?