UNIVERSIDAD DE COLIMA

FIME-ICI

ARQUITECTURA DE SERVIDORES

TIPO DE SERVIDOR

PROFESOR:

OSWALDO CARRILLO ZEPEDA

ALUMNA:

GUADALUPE MONSERRAT

PERALTA SÁNCHEZ

6.-D

FEBRERO 2024

REMOTO TELNET

REMOTO TELNET

Fue desarrollado en 1969,Telnet es un protocolo de ordenador que fue desarrollado para interactuar con los ordenadores remotos. Permite la comunicación de terminal a terminal y se puede utilizar para varios fines.

La utilidad de Telnet permite a un usuario remoto tener acceso para probar la conectividad con equipos remotos y emitir comandos a través de un teclado. Aunque la mayoría de

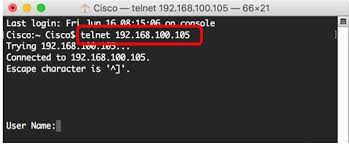
los usuarios optan por trabajar con interfaces gráficas, Telnet es una de las formas más simples de comprobar la conectividad en determinados puertos.

**MODOS DEL PROTOCOLO DE TELNET**

El protocolo Telnet generalmente tiene tres modos de operación. En todos ellos, su teclado produce datos salientes a través de la estructura de comando Telnet, viaja mediante una conexión Telnet TCP y llega a una terminal virtual o física para satisfacer una conexión entre terminal y ordenador.

**MODO PREDETERMINADO**

* En caso de no invocarse otros modos, Telnet asumirá este modo de manera predeterminada.
* En este modo el usuario realiza un eco.
* Aquí, el usuario puede escribir un carácter y el cliente replica dicho caracter en la pantalla. Sin embargo, no se enviará hasta completar la línea completa.

Este modo también es conocido como “modo operativo de dispositivo semidúplex” o “modo half-duplex”. Requiere que el comando Telnet GA (GO AHEAD) desde el servidor antes de aceptar cualquier dato introducido por el usuario.

La motivación para esto es el alto costo potencial de las interrupciones por entrada de la red de procesamiento junto con la especificación NVT que “hace eco” de no atravesar la red.

**MODO DE CARACTER**

* En el modo de caracter de Telnet, solo se transmite un carácter a la vez (dirección usuario a servidor).
* El intérprete de telnet en el servidor reconocerá la recepción del caracter replicándolo al cliente.
* Luego, el software de cliente Telnet enviará de regreso un paquete TCP ACK al servidor para informar la recepción del eco que proviene de este.
* Telnet genera un paquete de datagrama de IP para cada caracter, lo cual podría causar retrasos de conectividad debido al alto volumen del tráfico de red (en sistemas más antiguos)

**MODO DE LÍNEA**

* El modo de línea (más conocido como “modo de línea a la vez”) deriva del modo de caracter de Telnet.
* En este modo, se hace eco de los caracteres mediante una señal explícita definida localmente y se envían al servidor de Telnet una vez completados.
* En el modo de línea, se deshabilitan los comandos ECHO o el SUPPRESS GO AHEAD.

**Sección de comando de Telnet**

Los comandos de Telnet se distinguen por el uso de diversos caracteres con el conjunto de bit más relevantes. La porción de flujo de datos de Telnet garantiza la incorporación de los comandos invocados por los usuarios de red. Los comandos se introducen a través del decimal 255, también conocido como el caracter Interpretar como comando (IAC).

**Los comandos de Telnet definidos constan de:**

WILL - 251 - Ofrecer o aceptar habilitar

WON'T - 252 - Aceptar u ofrecer deshabilitar

DO - 253 - Solicitar o Aprobar la operación de habilitación

DON'T - 254 - Desaprobar habilitar o Solicitar deshabilitar

SE - 240 - Término de los parámetros de subnegociación

NOP - 241 - Ninguna operación

DM - 242- El comando “data mark” indica y localiza la secuencia Telnet Synch dentro del flujo de datos (fundamental como complemento de la notificación de urgencia de Protocolo de Control de Transmisión (TCP)).

BRK - 243 - Comando de interrupción. Indica que se presionó la tecla de “atención” o “interrupción”

IP - 244 - Suspende, interrumpe o aborta la conexión del Terminal de Red Virtual correspondiente al proceso específico

AO - 245 - Aborta salida - permite que se complete el proceso, pero no que envíe datos

AYT - 246 - Este significa "Are you there?" (¿Estás ahí?) - solicita enviar de regreso evidencia visible de que AYT fue recibido del Terminal Virtual de Red (NVT)

EC - 247 - Borrar comando de caracter - el receptor del comando debe borrar el último comando sin borrar precedente

EL - 248 - Borrar comando de línea - borra caracteres del flujo de regreso a, aunque sin incluir, el retorno de carro/salto de línea (CRLF)

GA - 249 - El comando Telnet Go Ahead - utilizado principalmente para informar al otro extremo de que puede comenzar a transmitir datos

SB - 250 - Indica la subnegociación de las opciones incluidas a seguir

IAC - 255 - El caracter “Interpretar como comando”

**Opciones de comando de protocolo de Telnet**

Varias especificaciones de opción en Telnet están disponibles para negociar entre el cliente y el servidor de Telnet. Esto puede realizarse utilizando comandos en cualquier etapa siempre que la conexión persista. A continuación, dejamos una lista de las opciones de comandos más importantes.

Asignaciones de código real

1 echo

3 suppress go ahead

5 status

6 timing mark

24 terminal type

31 window size

32 terminal speed

33 remote flow control

34 linemode

36 environment variables

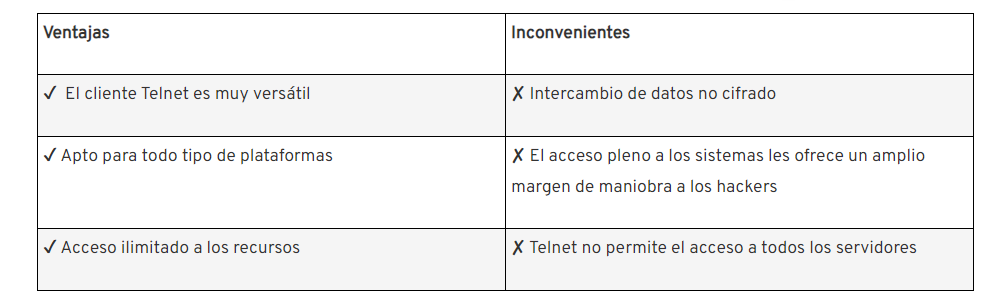
Las opciones atraviesan un proceso de negociación para presentar al cliente y al servidor una vista común de las posibles capacidades adicionales que inciden en el intercambio y el funcionamiento de las aplicaciones.

Ambos extremos en un diálogo por Telnet pueden habilitar o deshabilitar las opciones de manera local o remota.

## VENTAJAS E INCONVENIENTES DEL PROTOCOLO TELNET

Las conexiones Telnet son conexiones compatibles con los estándares de TCP, por lo que se puede emplear el cliente para **utilizar o examinar otros servicios**que recurren a TCP como protocolo de transporte. De esta manera y con una solicitud simple se puede comprobar, por ejemplo, la funcionalidad de un servidor HTTP o el estado de un servidor de correo electrónico.

El protocolo de conexión se puede utilizar **independientemente de la plataforma**, puesto que solo son algunos los dispositivos que no soportan el estándar oficial de IETF. El hecho de que un ordenador de cliente o de servidor se base en el mismo sistema operativo no tiene ninguna relevancia. Otra de las ventajas de Telnet es que este permite el acceso ilimitado a los recursos del sistema controlado siempre y cuando se cuente con los permisos necesarios para ello.

Este último punto plantea, en combinación con otros inconvenientes, un riesgo elevado, y es que ni el establecimiento de la conexión ni la transmisión de los datos **se cifran** durante la utilización del protocolo Telnet. De este modo, la información que se envía puede ser accesible por parte de terceros en forma de texto sin cifrar, al igual que los **datos de registro** para el acceso remoto. Como consecuencia, los criminales lo tienen fácil a la hora de acceder a los sistemas. Una alternativa segura a Telnet es [el protocolo de cifrado SSH](https://www.ionos.mx/digitalguide/servidores/herramientas/protocolo-ssh/).

PRINCIPALES SISTEMAS OPERATIVOS DE SERVIDOR

Telnet es considerado como un protocolo práctico para los administradores de las redes y los servidores. La posibilidad de la **gestión remota de dispositivos en la red** está especialmente indicada para las tareas de administración, debido a que el protocolo es apto para casi todo tipo de dispositivos. Asimismo, también puede utilizarse para comprobar la disponibilidad de determinados puertos o para diagnosticar errores en servidores de correo electrónico ([SMTP](https://www.ionos.mx/digitalguide/correo-electronico/cuestiones-tecnicas/smtp/), Port 25), para enviar correos electrónicos directamente desde el servidor. Telnet es también un medio eficaz para configurar servidores, por ejemplo, **servidores web.**En este sentido,los cambios en la estructura de los directorios, en los derechos de los archivos o en las contraseñas se llevan a cabo de un modo rápido y sencillo.

La palabra “Telnet” también se refiere a la utilidad de comando de línea “telnet”, disponible en sistemas que operen con Windows y Unix, incluidos Mac, Linux y otros. Utilizaremos el término “Telnet” principalmente en el contexto del software para clientes de telnet.

La utilidad de Telnet permite a un usuario remoto tener acceso para probar la conectividad con equipos remotos y emitir comandos a través de un teclado.  una de las formas más eficientes es usar el protocolo de red Telnet. Telnet le permite a los usuarios probar los puertos individuales y comprobar si están abiertos. El estado de los puertos en Windows 10, Windows Server 2022, 2016, 2012 y 2008. Aunque la mayoría de los usuarios optan por trabajar con interfaces gráficas, Telnet es una de las formas más simples de comprobar la conectividad en determinados puertos.

## ¿DÓNDE Y CÓMO SE PUEDE UTILIZAR TELNET?

El protocolo Telnet es necesario para establecer una **conexión a otro ordenador o a un componente de la red**. Todo tiene lugar a través de la línea de comandos basada en texto. En el pasado resultaba especialmente interesante para compartir los servicios de los mainframes. Sin embargo, Telnet se sigue utilizando para abrir aplicaciones, gestionar redes y compartir bases de datos, aunque cada vez con menos frecuencia.

### **ACCESO A BASES DE DATOS**

Durante años, Telnet desempeñó un papel decisivo para las instituciones que trabajan con grandes bases de datos: en las bibliotecas, el protocolo fue un elemento fundamental en los catálogos online públicos de los años 80, más conocidos por la abreviatura OPAC (Online Public Access Catalogue). Al principio, se podía acceder a estas **bases de datos de publicaciones digitales** a través de terminales en las **redes locales de las bibliotecas**. A medida que Internet fue ganando éxito, nació la posibilidad de acceso a través de interfaces web locales, cuya comunicación se basa, en muchos casos, en el protocolo Telnet.

### **INTERACCIÓN CON PROGRAMAS EN SERVIDORES DE APLICACIONES**

Otro ámbito de aplicación típico de los clientes Telnet era el **acceso a programas basados en texto** en un servidor de aplicaciones. De este modo, aún hoy en día se puede acceder al [Free Internet Chess Server](https://www.freechess.org/) a través de conexiones Telnet. Mediante la incorporación de texto se pueden seleccionar los oponentes disponibles y realizar los movimientos deseados. A pesar de todo, las interfaces gráficas como Jin Applet o Javaboard, que permiten llevar a cabo las jugadas por medio del ratón, han eliminado las entradas de información basadas en texto.

### ¿QUÉ ES SSH? ¿CUÁL ES SU PUERTO?

SSH significa “**Secure Shell**” o “**Secure Socket Shell**”. Corresponde a un protocolo seguro que permite la comunicación encriptada entre dos ordenadores.

Secure Shell utiliza el protocolo de transferencia de hipertexto (HTTP) para transferir hipertexto (páginas web) y datos compartidos.

Ya que SSH permite la comunicación encriptada entre dos equipos, es ideal para redes no protegidas.

SSH se utiliza principalmente para establecer una conexión de terminal virtual e iniciar sesión en un equipo remoto para ejecutar operaciones o transferir datos.**El puerto predeterminado para la conexión de cliente SSH es 22.** Usted puede cambiar la configuración predeterminada ingresando un número de puerto entre 1024 y 32.767.

Tenga en cuenta que en un sistema virtual (VSYS), la raíz y VSYS comparten el mismo número de puerto SSH. Esto significa que si usted cambia la configuración predeterminada del puerto SSH (22), el puerto también cambiará para todos los terminales virtuales.

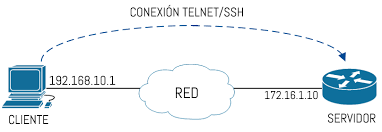
### ¿CÓMO FUNCIONA SSH?

Para establecer un acceso por terminal remoto a través de Secure Shell, usted necesita de un cliente SSH en su ordenador para conectarse al servidor SSH.

El cliente SSH, una vez habilitado, este invoca el proceso de configuración de la conexión para procesar la comunicación protegida por una encriptación simétrica sólida.

El cliente depende de la criptografía de clave pública para verificar la identidad del servidor, seguido de los algoritmos hashing para garantizar la privacidad e integridad de los datos intercambiados entre el cliente y el servidor.

## ¿CUÁL ES LA DIFERENCIA ENTRE TELNET Y SSH?

Tanto Telnet como SSH son protocolos utilizados para gestionar un sistema informático remoto.

* Diferencia en la definición

Telnet es un protocolo de red de aplicación que permite la comunicación de usuario con un computador

remoto a través de una interfaz basada en texto. Telnet crea una conexión de terminal virtual, permitiendo a los usuarios acceder a las aplicaciones en un equipo remoto.

SSH cumple las mismas funciones principales que Telnet, pero añade seguridad al proceso. Permite el acceso seguro incluso cuando la red conectada no es segura, incorporando un mayor nivel de seguridad que el protocolo de Telnet. Además, los administradores de red pueden iniciar sesión en un equipo remoto a través de SSH, ejecutar comandos, transferir archivos y más.

* Diferencia en operación

Telnet requiere de una aplicación de servidor instalada en el ordenador remoto (aquella que usted desee gestionar) y de una aplicación de cliente instalada en el equipo local.

Telnet utiliza el protocolo de puerto TCP y el puerto 23 para establecer una conexión con ordenadores remotos. El sistema creado actúa como un servidor Telnet y está disponible para recibir comandos. Dichos comandos se envían a través del formato de Terminal Virtual de Red (NVT). Luego, son recibidos e interpretados por el servidor Telnet, para enviarse posteriormente a la aplicación correspondiente.

SSH garantiza una conexión segura al servidor a través del puerto 22. Genera una sesión después de que el cliente verifique el servidor a través de autenticación con clave. La sesión generada se envía al cliente y al servidor y todo el tráfico se encripta para la sesión actual.

En última instancia, el servidor verifica el cliente a través de un par clave SSH generado. Después de la autenticación exitosa del cliente, esta establece una conexión encriptada y los dos sistemas pueden intercambiar datos de forma segura.

* Diferencia en seguridad

Telnet no ofrece ninguna característica o protocolo de seguridad durante la transmisión de datos. El protocolo de red es altamente vulnerable a ciberamenazas, a menos que se utilice en redes privadas de confianza, de preferencia sin conexión.

Gracias a los pares de teclas utilizados para autenticación, es extremadamente difícil penetrar y leer los datos transferidos en SSH. Esto lo convierte en un protocolo mucho más seguro que Telnet, incluso para redes no seguras.

* Diferencia en formatos de datos

Telnet envía datos como texto plano mediante un formato NVT.

SSH envía los datos a través de un formato encriptado por medio de un canal seguro.

* Diferencia en autenticación

Telnet emplea un mecanismo sin autenticación.

SSH depende de una encriptación de clave pública.

* Diferencia en sistemas operativos admitidos

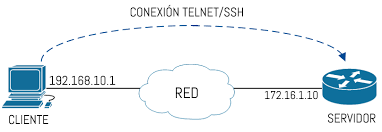
Tanto Telnet como SSH están disponibles en Windows, Mac OS y Linux (con algunas excepciones para Telnet en las versiones más recientes de Mac OS).

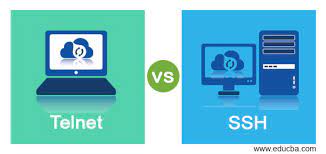
* Diferencia en utilización de ancho de banda

El uso de ancho de banda para conexión de Telnet es bajo.

El uso de ancho de banda para conexión de SSH es alto.

### ¿CUÁNDO USAR TELNET O SSH?



 Existen dos casos principales en los cuales se recomienda el uso de una conexión Telnet por sobre SSH.

* Al operar en redes de confianza (por ej., LAN) que no tengan conexión a internet.
* Al operar con un host remoto que no admita SSH.

En todos los demás casos, lo mejor es usar SSH dado que ofrece una alta seguridad para los dispositivos conectados a internet.

Además, SSH permite más opciones de funcionalidad que Telnet (por ej., transferencia de archivos más segura, asignación de puertos)