English • Deutsch • Español • Français • Italiano • ??? • Polski • Português • ??????? • Svenska • ???(????)? • ???(??)? •

Contents

Telnet

Telnet es una manera facil de acceder a la Linea de Comandos (Shell) de tu WRT54G y acceder a configuración no disponible via la interfaz web. Ya que las contraseñas de Telnet no estan encriptadas, es vulnerable a ataques de sniffing. Secure Shell es un reemplazo para Telnet que usa encripción dura, y es recomendado su uso sobre Telnet en cualquier red pública. (Ver Sección SSH abajo.) Telnet opera en el puerto 23 y usa un protocolo ASCII.

Configurando

Desde la Interface Web
-Click en el tab **Administration >> Services**
-Dejar **Enabled** en la sección **Telnet**
-Guardar Cambios

Uso

-Abrir tu cliente Telnet favorito
-connect to <Direccion_IP_LAN_del_Router>

-Cuando pregunte por nombre de usuario (*username*), ingresar *root*
--Debe ser root y no el nombre de usuario al que cambiaste de haberlo hecho -Cuando pregunte por la Contraseña, ingresar la contraseña del router

En Windows, Puedes usar Inicio: Ejecutar: telnet <Direccion_IP_LAN_del_Router>

SSH

Descripción

SSH, o Secure Shell, es un protocolo encriptado y programa asociado con la intención de reemplazar a Telnet. También puede ser usado para la creación de túneles seguros, de alguna forma similar a las Redes Privadas Virtuales (VPN). A menos que sea cambiado, todo ssh operará en el puerto 22.

SSH opera al igual que Telnet con una combinación de usuario/contraseña o con una infraestructura de llave Pública/Privada. Para posterior trabajo, una pequeña llave publica es entregada al servidor y el servidor entrega su llave pública al cliente. Tu cliente encripta la información para el servidor usando la llave pública de este y el servidor hace lo mismo usando la clave de tu cliente. Las llaves privadas nunca son intercambiadas, y son usadas para desencriptar la informacion encriptada con la llave pública asociada.

El firmware DD-WRT puede usar usuario/contraseña o solo permitir conexiones de clientes cuyas llaves publicas son ingresadas manualmente via la interfaz web. Multiples llaves pueden ser ingresadas separandolas por una linea en blanco entre ellas.
Si quieres usar usuario/contraseña para ingresar via SSH ingresa el usuario "root" con la contraseña que configuraste en la interfaz web

De hecho puedes configurar manualmente (via telnet o ssh) la variable sshd_authorized_keys de nvram. ej nvram set sshd_authorized_keys=key1 key2 key3 etc

También puedes editar manualmente /tmp/root/.ssh/authorized_keys y agregar las llaves (aunque estas desaparecerán cuando reinicies el router a menos que tengas un script de inicio alterando el archivo).

Vale la pena señalar que las llaves ssh son cadenas de texto bastante largas, asi que si piensas copiar y pegarlas debes tener cuidado que no se te pase ningun salto de linea (ej es una sola linea larga). o sino no funcionará.

Configurando

Método de Llave Pública
Primero debes generar un par de llaves Pública/Privada en tu maquina de escritorio. Esto puede ser hecho via "Puttygen" en windows si es que usar clientes como Putty o WinSCP, o ssh-keygen en Linux. Copia la **llave pública** al portapapeles y guardar la llave privada en algun lado de tu computador. No hay necesidad de guardar la llave pública. Si la olvidas, puedes instruir a Puttygen que abra tu llave privada en vez de generar un nuevo par de llaves, y te dirá cual es tu llave pública. Es recomendado que no asegures tu par de llaves con contraseña, ya que de hacerlo te pedirá esta contraseña cada vez que intentes conectarte, perdiendo el sentido de facilitar la conexion, pero ganando en seguridad.

Desde la [Interface Web] -Has Click en la pestaña **Administration**
-Marca **Enabled** en la sección **SSHD** para habilitar el demonio SSH
-Has click en el boton **Save Settings**
-Click en el boton **Continue**
-Pega tu **llave pública** en **authorized key** de la sección **SSHD** que ha aparecido. Necesitaras generar las llaves en tu computador de escritorio si no lo has hecho ya.

Método de ingreso por Contraseña
Si no quieres molestarte en generar las llaves ssh, querrás usar el metodo de ingreso via contraseña.

Desde la [Interface Web] -Click en la pestaña **Administration**
-Marca **Enable** en la sección **SSHD** para habilitar el demonio SSH
-Has click en el boton **Save Settings**
-Click en el boton **Continue**
-Marca **Enable** en **Password Login** para habilitar el ingreso via contraseña

Despues de esto podras entrar como usuario "root" con la contraseña configurada en la interfaz web

Cliente SSH

Provee un alternativa segura a Telnet.
Un buen cliente para Windows es Putty
Configura el cliente para usar la llave privada que guardaste con anterioridad.
La mayoría de las distribuciones de Linux ya vienen con cliente Telnet y SSH.

SCP

Secure Copy (SCP) permite copiar archivos desde o hacia el router, desde un computador remoto.
Un buen cliente para Windows es WinSCP
Configura el cliente para usar la llave privada que guardaste con anterioridad, o utiliza el usuario "root" y contraseña configurada via interfaz web
Recuerda: solo las particiones /tmp y /jffs pueden ser escritas!

Drop Bear

DropBear es un cliente/servidor SSH que se instala por defecto en los WRT54G. DropBear permite conectarse desde el WRT54G a un servidor SSH para usar scp, etc. No creo que el demonio SSHD deba estar habilitado via la Interface Web para poder usar el cliente DropBear.

Si tienes un servidor SSH en tu maquina de escritorio (como OpenSSH) puedes enviar archivos desde tu maquina de escritorio usando el comando scp. Esto puede ser utilizado para copiar archivos desde tu maquina de escritorio en un Script de Inicio

La Linea de Comandos de DD-WRT

Conocida tambien como la shell Linux de DD-WRT

Esta es una shell 'ash'. Ash es una version de sh, literalmente 'A SHell' (una shell) (Un interprete de comandos)

Sintaxis Basica

La Linea de Comandos de Linux (Ash) no es lo mismo que la linea de comandos de Windows/DOS.

/ (y no \) es usado para separar los directorios en rutas, tal como en internet.

Para ejecutar un comando, la ruta del comando debe ser provista. Esto puede ser la ruta completa o una ruta relativa.

Operadores de Ruta Relativa

Hay dos operadores de ruta relativa.

```
.        La ruta actual
..       Un directorio atras de la ruta actual
```

Ejemplos

1) si te encuentras en el directorio **/jffs/usr/bin** y quieres ejecutar el comando **/jffs/usr/bin/noip** usa:

```
/jffs/usr/bin # /jffs/usr/bin/noip
```

o

```
/jffs/usr/bin # ./noip
```

2) si te encuentras en el directorio **/jffs/usr/bin** y quieres ejecutar el comando **/jffs/usr/kismet** usa:

```
/jffs/usr/bin # /jffs/usr/kismet
```

o

```
/jffs/usr/bin # ../kismet
```

or

```
/jffs/usr/bin # cd ..
/jffs/usr # ./kismet
```

3) Las rutas relativas pueden ser usadas tambien como argumentos. Si instalaste el paquete noip , notarás que el comando es instalado en **/jffs/usr/bin/noip** pero la configuracion se encuentra en **/jffs/etc/no-ip.conf** Cuando ejecutas noip, es por esto que se debe dar la ruta al archivo de configuración mediante el argumento -c. Esto puede ser efectuado de la siguiente forma:

```
/jffs/usr/bin # ./noip -c /jffs/etc/no-ip.conf
```

o

```
/jffs/usr/bin # ./noip -c ../../etc/noip.conf
```

Nota que el primer *../* nos lleva a /jffs/usr/. El segundo *../* nos dirigue a /jffs/, y entonces el resto de la ruta puede ser agregado.

4) Mientras los otros ejemplos mostraban como ahorrar tipéo, puedes también puedes jugar con las rutar relativas. Para ejecutar el comando noip en el ejemplo 1, también puedes usar

```
/jffs/usr/bin # ../../../jffs/./usr/./bin/./././../bin/./././noip
```

Aqui nos dirigimos hasta la raiz del sistema de archivos **/**, despues subimos nuevamente hasta **/jffs/usr/bin**, nos devolvemos hasta **/jffs/usr** y subimos nuevamente hasta **/jffs/usr/bin**.
Referencias a **/./** son puestas solo para mezclar las cosas. Mira como **/./** siempre hace referencia al entonces actual directorio, no a la ruta de la shell cuando el comando fue ejecutado.

Redirecciones y Tuberias

La salida de un comando puede ser Entubado *piped* a travez de otros comandos o redirigido a dispositivos o archivos.

< y > son operadores de redirección.