Elementos de Configuración de Enrutadores Cisco

=====

Notas:

- * Los comandos precedidos por el signo de pesos "\$", deben ser ejecutados como un usuario general - y no como superusuario (root).
- * Los comandos precedidos por el signo de número "#", deben ser ejecutados por el superusuario (root).
- * Los comandos precedidos por líneas de comando más específicas (e.g. "rtrX>" or "mysql>") deben ser ejecutados en equipos remotos, dentro de otras aplicaciones.
- * Si la línea de comandos termina con una barra invertida "\", quiere decir que el comando continua en la próxima línea y todas líneas deben ser tratadas como un comando de sola línea.
- * Referencias a "N", representan su número de grupo.

Ejercicios - Parte I

=====

0. Trabajando en grupos

Para este ejercicio estarán trabajando en grupos de trabajo. Cada grupo debe asignar a una persona para que ejecute los comandos. Puede haber hasta cuatro (4) personas por grupo. Por ejemplo, los miembros del Grupo Uno (1) serán los participantes utilizando las máquinas pc1-pc4, Grupo Dos (2) tiene a los participantes que utilizan pc4-pc8, Grupo Tres (3) será formado por los participantes que utilizarán pc9-pc12, etc.

Si no está seguro de a que grupo usted pertenece, por favor referirse a la sección "Diagrama de Topología" que está en la página wiki del taller (<http://noc.ws.nsrc.org/>) y seleccionando cualquiera de los dos diagramas en esa sección.

1. Conectandose al enrutador

Conectese a una de sus PCs e instale "Telnet":

```
$ sudo apt-get install telnet
```

Obviamente, este paso no es necesario si su PC ya tiene instalada la aplicación de Telnet.

Desde la PC, deberá conectarse al enrutador para su grupo. Si no está seguro de cual es el enrutador para su grupo, recuerde que puede consultar el diagrama de la red. Seleccione el enlace "Diagrama de Topología" en la página del NOC:

```
http://noc.ws.nsrc.org/
```

Ahora conectese a su enrutador:

```
$ telnet 10.10.N.254
```

```
username: cisco  
password: cisco
```

Para visualizar información sobre su enrutador:

```

routerN>enable
  Password:                (password por defecto es "cisco")
RouterN#show run           (utilize la barra espaciadora para continuar)
RouterN#show int FastEthernet0/0 (para ver el estado de la interfaz FastEthernet0/0)
RouterN#show ?            (presenta todas las opciones para el comando)
RouterN#exit              (desconectarse del enrutador)

```

2. Configure su enrutador para solo utilizar SSH

Los pasos en este ejercicio servirán para:

- * Crear una clave de SSH para su enrutador
- * Crear una contraseña de acceso encriptada para el usuario "cisco"
- * Crear y encriptar la contraseña del nivel privilegiado (cisco)
- * Deshabilitar el acceso via telnet (sin encryption) para su enrutador
- * Habilitar el acceso via SSH (version 2) para el enrutador

Deberá trabajar en grupos de hasta cuatro (4) personas. Comuníquese con los miembros de su grupo y asigne a una persona para entrar los comandos en el enrutador. Para comenzar, deberá conectarse a una de las PCs virtuales que son utilizados por su grupo. Desde esa PC, deberá conectarse a su enrutador utilizando el comando "telnet":

```
$ telnet rtrN.ws.nsrc.org (or "telnet 10.10.N.254")
```

```
username: cisco
password: cisco
```

```

rtrN> enable                (en)
password: cisco
rtrN# configure terminal    (conf t)
rtrN(config)# aaa new-model
rtrN(config)# ip domain-name ws.nsrc.org
rtrN(config)# crypto key generate rsa

```

```
How many bits in the modulus [512]: 2048
```

Deberá esperar mientras la clave es generada. Después de terminar, usted podrá definir nuevas contraseñas y éstas serán encriptadas. Para comenzar, vamos a remover temporalmente el usuario "cisco" y recrearlo de nuevo:

```

rtrN(config)# no username cisco
rtrN(config)# username cisco secret 0 <CONTRASEÑA>

```

Ahora la nueva contraseña para el usuario "cisco" está encriptada. El próximo paso es el encriptar la contraseña del nivel privilegiado:

```
rtrN(config)# enable secret 0 <CONTRASEÑA>
```

Ahora vamos a configurar el enrutador para que solo acepte conexiones de SSH para las cinco (5) terminales que hemos definido (vty0-vty4):

```

rtrN(config)# line vty 0 4
rtrN(config-line)# transport input ssh
rtrN(config-line)# exit

```

El comando "exit" anterior nos saca del nivel de configuración de línea

y nos pone en el modo de configuración general. Ahora vamos a decirle al enrutador que registre eventos relacionados con SSH y que solo acepte conexiones vía SSH versión 2:

```
rtrN(config)# ip ssh logging events
rtrN(config)# ip ssh version 2
```

Ahora que hemos terminado, podemos salir del modo de configuración:

```
rtrN(config)# exit
```

Como siempre, queremos guardar la configuración en la memoria permanente del enrutador:

```
rtrN# write memory          (wr mem)
```

Y eso es todo.

Si todo está funcionando correctamente, ya no podrán conectarse a los enrutadores utilizando el comando "telnet". De ahora en adelante, deberán utilizar conexiones vía SSH con el usuario "cisco" y la contraseña <CONTRASEÑA>. La contraseña del nivel privilegiado también será "cisco". Naturalmente, en una configuración real ustedes deberán utilizar contraseñas mucho más seguras.

Siempre es recomendable que cuando estamos haciendo cambios a la configuración de acceso de un enrutador, mantengamos la sesión original abierta hasta que hayamos confirmado que la nueva configuración funciona como debe ser. Ahora debemos verificar que nuestra configuración funciona como debe ser.

Primero, vamos a tratar de conectarnos usando "telnet":

```
$ telnet rtrN.ws.nsrc.org
```

Que pasó? ... Debieron haber visto algo parecido a:

```
Trying 10.10.N.254...
telnet: Unable to connect to remote host: Connection refused
```

Ahora vamos a tratar de conectarnos utilizando una sesión con SSH:

```
$ ssh cisco@rtrN.ws.nsrc.org
```

Debemos ver algo parecido a:

```
The authenticity of host 'rtr2.ws.nsrc.org (10.10.2.254)' can't be
established. RSA key fingerprint is 93:4c:eb:ad:5c:4a:a6:3e:8b:9e:
4f:e4:e2:eb:e4:7f. Are you sure you want to continue connecting
(yes/no)?
```

Escriba "yes" y presione <ENTER> para continuar ...

Ahora deberá ver en mensaje de entrar la contraseña. Escriba la contraseña "cisco" y presione <ENTER>:

```
Password: <CONTRASEÑA>
```

Si todo funciona como debe ser, usted entrará a la línea de comandos del enrutador:

```
rtrN>
```

Si todo funcionó, podemos desconectar la sesión inicial que teníamos vía "telnet" (debemos mantener abierta la sesión que usa SSH):

```
rtrN# exit
```

Para ejecutar comandos privilegiados en la sesión que tenemos vía SSH, debemos habilitar el nivel de acceso privilegiado:

```
rtrN> enable
Password: <CONTRASEÑA>
rtrN#
```

Ahora vamos a revisar la configuración actual del enrutador:

```
rtrN# show running (sh run)
```

Presione la barra espaciadora para continuar. Observe que algunas de las entradas que usted había configurado antes estén en la configuración:

```
enable secret 5 $1$p4/E$PnPk6VaF8QoZMhJx56oXs.
.
.
.
username cisco secret 5 $1$uNg1$MlyscHhYs..upaPP4p8gX1
.
.
.
line vty 0 4
  exec-timeout 0 0
  transport input ssh
```

Podrá observar que las contraseñas para el nivel privilegiado y para el usuario "cisco" han sido encriptadas. Eso es lo que queremos.

Para terminar este ejercicio, solo necesitamos desconectarnos del enrutador:

```
rtrN# exit
```

Mas Notas:

- * Si luego de hacer los cambios de contraseñas y de limitar el acceso a solo vía SSH usted no puede conectarse a su enrutador, comuníquelo a uno de los instructores para que puedan restaurar a su estado inicial la configuración del enrutador.
- * Por favor, asegúrese de que solo una persona por grupo esté ejecutando los comandos para este ejercicio, y que lo esté haciendo en el enrutador adecuado para su grupo. Si varias personas intentan modificar la configuración al mismo tiempo o si usted no está conectado al enrutador que debe, es muy posible que terminemos con problemas de configuración.
- * Durante el resto de la semana estaremos configurando varios servicios en el enrutador de su grupo, tales como, SNMP, Netflow y otros. De ahora en adelante usted puede utilizar SSH directamente desde su laptop o estación de trabajo.