



Instituto Politécnico Nacional
Escuela Superior de Cómputo



ALUMNO:MERCADO ROGEL MARTÍN ISAURO

BOLETA:2014090449

UNIDAD DE APRENDIZAJE: APLICACIONES PARA LA COMUNICACIÓN
EN RED

GRUPO:
CURSO DE RECUPERACIÓN ACADÉMICA

Práctica 2:

Respaldo de configuración con TFTP de forma automática

Introducción

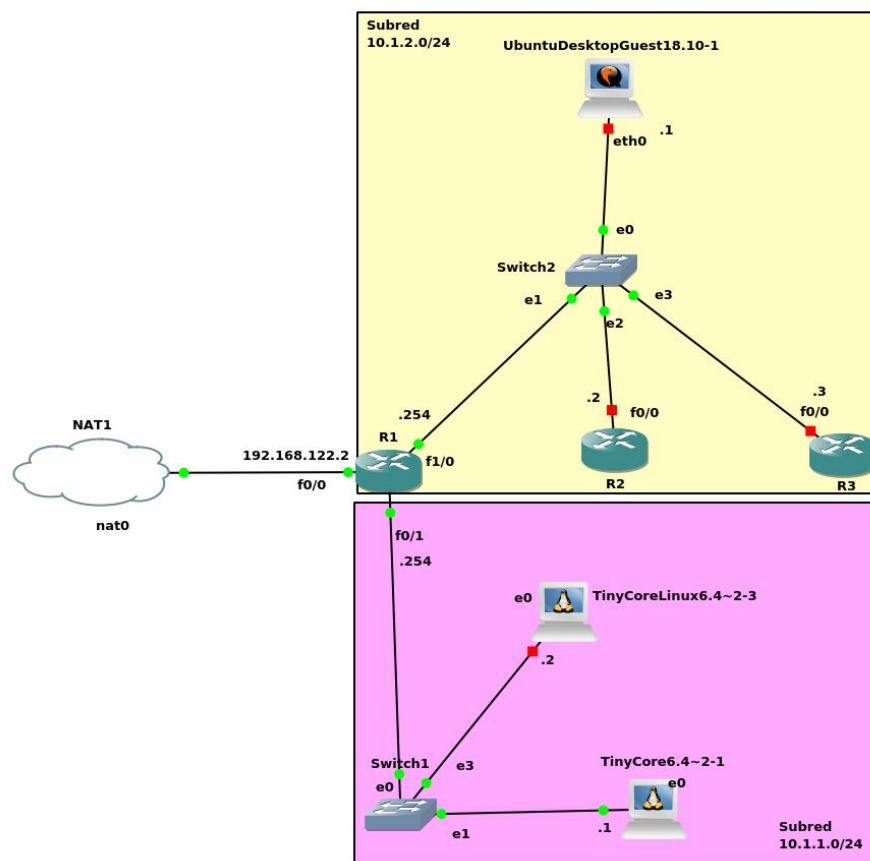
Como se revisó en la tarea 3 TFTP es un protocolo de transferencia muy simple semejante a una versión básica de FTP, utilizado a menudo para transferir pequeños archivos entre computadoras en una red.

Precisamente en esta práctica utilizaremos TFTP para montar un servidor que almacene los archivos de configuración de una red de routers. Para ello en el anfitrión se creará un script que se conectará a cada uno de los routers para solicitarle su archivo de configuración, el script creará una carpeta que le asignará la IP del router y dentro almacenará el archivo de configuración.

Ahora procederemos a mostrar el desarrollo de la práctica y lo que utilizaremos para lograrla.

Topología y configuración

Para esta práctica cree la siguiente topología:



Tengo tres routers que deseo respaldar en mi host que tiene como dirección ip 10.1.2.1, y todos los routers pertenecen a esa red. A su vez tengo una NAT que me conecta a internet con mi router y otra subred 10.1.1.0 dónde anteriormente había hecho unas pruebas de conectividad, en realidad esta se podría omitir.

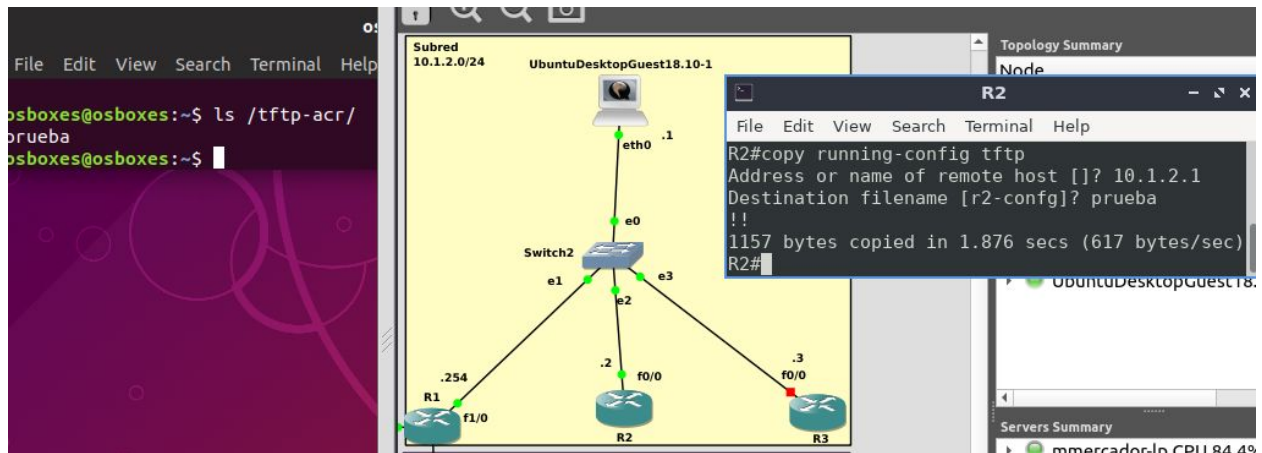
Ahora debo de instalar **tftpd-hpa** en mi máquina que respaldará los archivos:

```
osboxes@osboxes:~$ vi /etc/default/tftpd-hpa
osboxes@osboxes:~$ sudo vi /etc/default/tftpd-hpa
osboxes@osboxes:~$ sudo mkdir /tftp-acr
osboxes@osboxes:~$ sudo vi /etc/default/tftpd-hpa
osboxes@osboxes:~$ ls /
bin    dev    initrd.img    lib64    mnt    root    snap    tftp-acr    var
boot  etc    initrd.img.old  lost+found  opt    run    srv    tmp    vmlinuz
cdrom  home   lib           media     proc   sbin   sys    usr
osboxes@osboxes:~$ sudo systemctl status tftpd-hpa.service
● tftpd-hpa.service - LSB: HPA's tftp server
   Loaded: loaded (/etc/init.d/tftpd-hpa; generated)
   Active: active (running) since Tue 2020-09-15 10:36:24 EDT; 2min 42s ago
     Docs: man:systemd-sysv-generator(8)
    Tasks: 1 (limit: 1129)
   Memory: 708.0K
    CGroup: /system.slice/tftpd-hpa.service
            └─3398 /usr/sbin/in.tftpd --listen --user tftp --address :69 --secure

Sep 15 10:36:24 osboxes systemd[1]: Starting LSB: HPA's tftp server...
Sep 15 10:36:24 osboxes tftpd-hpa[3390]: * Starting HPA's tftp in.tftpd
Sep 15 10:36:24 osboxes tftpd-hpa[3390]:   ...done.
Sep 15 10:36:24 osboxes systemd[1]: Started LSB: HPA's tftp server.

osboxes@osboxes:~$ sudo chown tftp:tftp /tftp-acr
osboxes@osboxes:~$ sudo systemctl restart tftp-hpa
Failed to restart tftp-hpa.service: Unit tftp-hpa.service not found.
osboxes@osboxes:~$ sudo systemctl restart tftpd-hpa
```

Para probar el correcto funcionamiento de nuestro servidor tftp conectémonos a él desde un router y enviemos nuestro archivo de configuración:



Configuración de ssh

Para poder ejecutar nuestro script y que de manera automática enviemos los archivos de configuración desde el router a nuestro servidor tftp debemos poder controlar de manera remota nuestro router. Para ello utilizaremos una conexión con ssh.

Para la conexión hacia el router con ssh debemos seguir los siguientes pasos:

1. Configurar los hostname del dispositivo, en este caso los routers

El nombre que hemos asignado a nuestro dispositivo con **hostname** en la terminal de configuración.

2. Crear un nombre de dominio

Lo haremos con el comando **ip domain-name**. Este comando especifica el nombre del dominio al cual pertenece nuestro router. Se utiliza para generar certificados de seguridad para acceso IPSEC, SSH o HTTPS. Estos certificados se generarán utilizando las entradas de hostname y domain name.

```
P2-R2#config terminal
Enter configuration commands, one per line. End with CNTL/Z.
P2-R2(config)#hostname P2-R2
P2-R2(config)#ip domain-name mmercador.acr
```

3. Crear una llave ssh

Para generar la llave utilizaremos el comando **crypto key generate rsa modulus 512**.

Significa que utilizará 512 bits para cifrar nuestra llave, podemos asignar los que queramos

pero tardará más en su generación. Para ssh versión 2 tendremos que utilizar una llave de al menos 768 bits.

```
P2-R2(config)#crypto key generate rsa modulus 1024
% You already have RSA keys defined named P2-R2.mmercador.acr.
% They will be replaced.

% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

P2-R2(config)#
*Sep 15 15:38:18.315: %SSH-5-DISABLED: SSH 1.5 has been disabled
P2-R2(config)#
*Sep 15 15:38:19.767: %SSH-5-ENABLED: SSH 1.99 has been enabled
P2-R2(config)#show ip ssh
      ^
% Invalid input detected at '^' marker.

P2-R2(config)#exit
P2-R2#
*Sep 15 15:40:33.111: %SYS-5-CONFIG_I: Configured from console by console
P2-R2#show ip ssh
SSH Enabled - version 1.99
Authentication timeout: 120 secs; Authentication retries: 3
Minimum expected Diffie Hellman key size : 1024 bits
```

Version 1.99 significa que funcionará con v1 y v2.

4. Crear un usuario y contraseña

Primero debemos indicar al router cuántas conexiones simultáneas queremos realizar en el dispositivo con **line vty 0 4** indicamos 5 conexiones de 0 a 4. Después procedemos a permitir conexión vía ssh mediante **transport input ssh**.

Para poder utilizar nuestro dispositivo de manera remota necesitamos asignar un usuario y una contraseña. Este usuario y contraseña son para la sesión de ssh. Después activamos el ingreso al dispositivo mediante login con **login local**.


```

P2-R2(config)#line vty 0 4
P2-R2(config-line)#transport input ssh
P2-R2(config-line)#exit
P2-R2(config)#username martin password r2acr
^
% Invalid input detected at '^' marker.

P2-R2(config)#username martin password r2acr
P2-R2(config)#line vty 0 4
P2-R2(config-line)#login local
P2-R2(config-line)#exit
P2-R2(config)#

```

Terminando con esto probemos que nos podemos conectar a nuestro router desde ssh:

```

osboxes@osboxes:~$ ssh -c aes256-cbc martin@10.1.2.2
The authenticity of host '10.1.2.2 (10.1.2.2)' can't be established.
RSA key fingerprint is SHA256:A1Qd5nb5w7zFft+rc/qL8yN9i9GuF3xGGEFZFUI9VzA.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.1.2.2' (RSA) to the list of known hosts.
Password:

P2-R2>show runni
P2-R2>show runni/
P2-R2>show runnin
P2-R2>show runnin
P2-R2>show running-config
^
% Invalid input detected at '^' marker.

P2-R2>enable
% No password set
P2-R2>show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2

```

Como se puede ver no me permite hacer cambios de forma remota aún, para ello debo ejecutar lo siguiente en el router:

```

P2-R2(config)#enable password r2acr-config
P2-R2(config)#exit
P2-R2#
*Sep 15 16:58:56.667: %SYS-5-CONFIG_I: Configured from console
P2-R2#

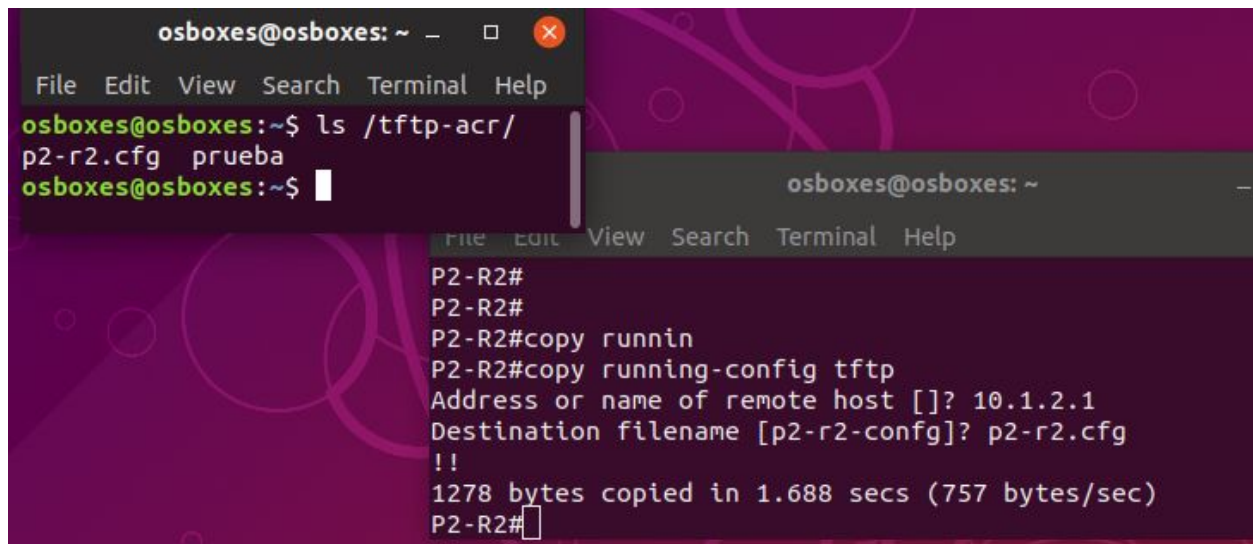
```

Ahora, después de esto ya puedo acceder de forma remota al router:

```
Password:
P2-R2#show running-c
P2-R2#show running-config
Building configuration...

Current configuration : 1278 bytes
!
upgrade fpd auto
version 12.4
```

Copiemos la configuración actual en el servidor de manera remota:

The image shows a terminal window titled 'osboxes@osboxes: ~'. The terminal has a menu bar with 'File', 'Edit', 'View', 'Search', 'Terminal', and 'Help'. The command prompt is 'osboxes@osboxes:~\$'. The user enters 'ls /tftp-acr/' and the output is 'p2-r2.cfg prueba'. Then, the user enters 'osboxes@osboxes:~\$' followed by a cursor. In the background, another terminal window is visible, showing the router's configuration being copied to a local file. The background terminal shows: 'P2-R2#', 'P2-R2#', 'P2-R2#copy runnin', 'P2-R2#copy running-config tftp', 'Address or name of remote host []? 10.1.2.1', 'Destination filename [p2-r2-config]? p2-r2.cfg', '!!', '1278 bytes copied in 1.688 secs (757 bytes/sec)', and 'P2-R2#' with a cursor.

```
osboxes@osboxes: ~
File Edit View Search Terminal Help
osboxes@osboxes:~$ ls /tftp-acr/
p2-r2.cfg prueba
osboxes@osboxes:~$

P2-R2#
P2-R2#
P2-R2#copy runnin
P2-R2#copy running-config tftp
Address or name of remote host []? 10.1.2.1
Destination filename [p2-r2-config]? p2-r2.cfg
!!
1278 bytes copied in 1.688 secs (757 bytes/sec)
P2-R2#
```

Automatización

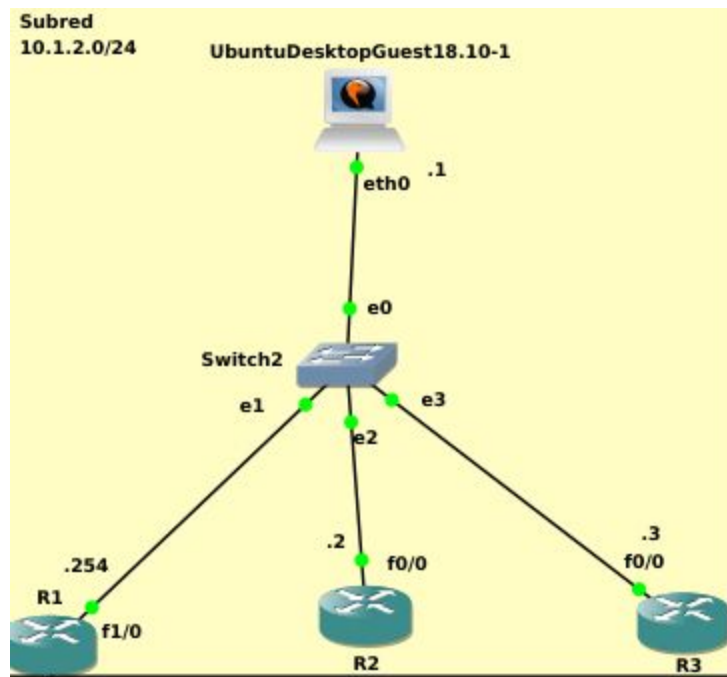
Para la automatización del proceso creé un script que tiene el siguiente cuerpo:

```

File Edit View Search Terminal Help
#!/bin/sh
ROUTERS=ip.lista
COMANDOS=ordenes.txt
while read IP
do
    #sudo rm -r /tftp-acr/$IP
    sudo mkdir /tftp-acr/$IP
    sudo chmod 777 /tftp-acr/$IP
    echo " copy running-config tftp ^M 10.1.2.1 ^M $IP/running.cfg " > $COMANDOS
    #echo " $IP ^M" >> $COMANDOS
    #echo " $IP/running.cfg ^M" >> $COMANDOS
    echo "\n exit " >> $COMANDOS
    sshpass -p escom ssh -c aes256-cbc mimir@$IP < $COMANDOS
done < "$ROUTERS"
~
"scriptf.sh" 14 lines, 408 characters

```

El script funciona de la siguiente manera: Hay una lista, **ROUTERS**, que contiene la ip de cada router a los que deseo hacer el respaldo, en este caso solamente son 3: 10.1.2.2, 10.1.2.3, 10.1.2.254



Cada línea en ese archivo es, entonces, una **IP** de esta forma creo una carpeta con el nombre de esa ip y luego otorgo permisos de escritura con **chmod** para que el router pueda escribir su archivo de configuración.

Luego creo un archivo que contiene los comandos que tiene que ejecutar el router. En este caso el router debe ejecutar el comando donde se conecte al servidor tftp y una vez ahí subirá su archivo de configuración en su respectiva carpeta.

Ese archivos de comando se tiene que pasar cuando realizo la conexión ssh que será en la respectiva IP, con usuario mimr y con la contraseña escom.

Probando nuestro script y vemos que logra hacer la configuración en automático:

```
osboxes@osboxes:~$ ./scriptf.sh
Pseudo-terminal will not be allocated because stdin is not a terminal.

P2-R2# copy running-config tftp
Address or name of remote host []? 10.1.2.1
Destination filename [p2-r2-config]? 10.1.2.2/running.cfg
!!
1370 bytes copied in 0.936 secs (1464 bytes/sec)
P2-R2#
P2-R2# exit
Connection to 10.1.2.2 closed by remote host.
```

Ahora verifiquemos que se hayan creado las carpeta y que el archivo se encuentre dentro de cada una:

```
osboxes@osboxes:~$ ls
comandos.txt  Downloads      Music          Public
Desktop       examples.desktop ordenes.txt    script2.
Documents     ip.lista       Pictures       script3.
osboxes@osboxes:~$ ls /tftp-acr/
10.1.2.2  10.1.2.254  10.1.2.3  p2-r2-config
osboxes@osboxes:~$ ls /tftp-acr/10.1.2.2
running.cfg
osboxes@osboxes:~$
```

Conclusiones

A pesar de que la explicación es sencilla, el desarrollo de esta práctica fue bastante tediosa y frustrante ya que tuve que investigar muchas cosas de configuración de los routers, así como podría automatizar el proceso. A su vez se presentaron muchas trabas como que al ser controlada remotamente el router mediante ssh había una parte donde debía introducir manualmente la confirmación del comando, no obstante me las ingenié y logré hacer funcionar todo. Puedo decir que adquirí más comprensión acerca de redes y como funcionan los dispositivos cisco.