



Instituto Politécnico Nacional

IPN

Escuela Superior de Cómputo

ESCOM

Academia de Redes Aplicaciones para comunicaciones
en red

6CV2

Práctica 16

“Ejemplo Telnet en GNS3”

Alumna:

Navarrete Becerril Sharon Anette

Fecha de entrega: “ 16 - Diciembre - 2024”

Profesor: Ojeda Santillan Rodrigo

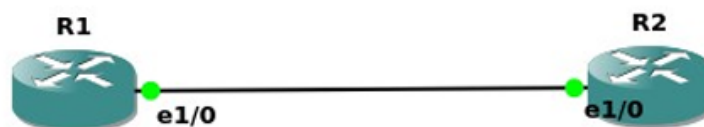
OBJETIVO

Familiarizarse con el uso del protocolo Telnet para administrar routers de forma remota en un entorno de red simulado utilizando GNS3. Esta práctica busca establecer una conexión Telnet desde Router 1 hacia Router 2, permitiendo el acceso a la configuración en tiempo real (show running-config) de Router 2.

INTRODUCCIÓN

El protocolo Telnet es una herramienta de administración remota que permite a los usuarios acceder a dispositivos de red y realizar configuraciones en tiempo real. En redes corporativas y entornos de prueba, Telnet es útil para gestionar dispositivos como routers y switches desde ubicaciones remotas. En esta práctica, se utilizará GNS3, una plataforma de simulación de redes, para configurar y probar la administración remota de routers.

La configuración se realiza en una topología simple en GNS3, con dos routers conectados mediante un enlace serial o Ethernet. Cada router se configura con una dirección IP única y se habilita el servicio Telnet para permitir la comunicación entre ellos. Esto facilita el acceso a la configuración y el monitoreo de Router 2 desde Router 1, simulando un entorno de administración remota en el que se pueden realizar ajustes en tiempo real y verificar el estado de la red.



DESARROLLO

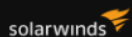
Creación de una topología simple en GNS3 con dos routers conectados mediante un enlace serial o Ethernet. Asignando direcciones IP a las interfaces de cada router para que puedan comunicarse entre sí. Por ejemplo:

- Router 1: 1.1.1.1 255.255.255.252
- Router 2: 1.1.1.2 255.255.255.252

Luego de construir la red como se indica en la imagen anterior, es necesario configurar los routers siguiendo los pasos detallados a continuación.

Una vez abiertas las consolas de Router 1 (R1) y Router 2 (R2), se deben ingresar los comandos correspondientes para asignar una dirección IP a cada router. Para Router 1, la configuración de la dirección IP se realiza de la siguiente manera:

```
R1#
R1#config terminal
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#int ethernet 1/0
R1(config-if)#exit
R1(config)#int ethernet 1/0
R1(config-if)#ip address 1.1.1.1 255.255.255.252
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#
```



Solar-PuTTY *free tool*

© 2019-2024 SolarWinds Worldwide, LLC. All rights reserved.

En el caso de Router 2, la configuración de la dirección IP se establece de la siguiente forma:

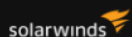
```
R2#
R2#config terminal
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#int ethernet 1/0
R2(config-if)#exit
R2(config)#int ethernet 1/0
R2(config-if)#ip address 1.1.1.2 255.255.255.252
R2(config-if)#no shutdown
R2(config-if)#ex
R2(config)#exit
R2#
```

A continuación, se recomienda ejecutar un ping desde Router 2 hacia Router 1 y viceversa, para verificar la conectividad entre ambos dispositivos.

Ping del Router 1 al Router 2

```
R1#
R1#ping 1.1.1.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 1.1.1.2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 64/64/68 ms
R1#
```



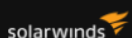
Solar-PuTTY *free tool*

© 2019-2024 SolarWinds Worldwide, LLC. All rights reserved.

Ping del Router 2 al Router 1

```
R2#ping 1.1.1.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 1.1.1.1, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 72/93/136 ms
R2#
```



Solar-PuTTY *free tool*

© 2019-2024 SolarWinds Worldwide, LLC. All rights reserved.

Posteriormente, se procede a configurar el acceso Telnet en uno de los routers; en este ejercicio, la configuración de Telnet se realizará en Router 2.

```
//Configuramos TELNET
R2#config terminal
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#line vty 0 15
R2(config-line)#password cisco
R2(config-line)#exit
//Tratar de ocupar ? para conocer los comandos
R2(config)#enable ?
last-resort Define enable action if no TACACS servers respond
password Assign the privileged level password (MAX of 25 characters)
secret Assign the privileged level secret (MAX of 25 characters)
use-tacacs Use TACACS to check enable passwords
R2(config)#enable password cisco
R2(config)#exit
R2#config terminal
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#line vty 0 15
R2(config-line)#no login
R2(config-line)#no password
R2(config-line)#login local
R2(config-line)#login ?
local Local password checking
<cr>
R2(config-line)#exit
R2(config)#exit
R2#config terminal
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#username escom password cisco
R2(config)#exit
R2#
```

```

R2#config terminal
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#line vty 0 15
R2(config-line)#password cisco
R2(config-line)#exit
R2(config)#enable ?
    last-resort  Define enable action if no TACACS servers respond
    password     Assign the privileged level password
    secret       Assign the privileged level secret
    use-tacacs   Use TACACS to check enable passwords

R2(config)#enable password cisco
R2(config)#exit
R2#ci
*Mar  1 00:10:32.571: %SYS-5-CONFIG_I: Configured from console by console
R2#config terminal
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#line vty 0 15
R2(config-line)#no login
R2(config-line)#no password
R2(config-line)#login local
R2(config-line)#login ?
    local      Local password checking
    <cr>

R2(config-line)#lexit
      ^
% Invalid input detected at '^' marker.

R2(config-line)#exit
R2(config)#exit
R2#config te
*Mar  1 00:11:11.351: %SYS-5-CONFIG_I: Configured from console by console
R2#config terminal
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#username escom password cisco
R2(config)#exit
R2#
*Mar  1 00:11:26.647: %SYS-5-CONFIG_I: Configured from console by console
R2#

```

Esta configuración permitirá que al conectarse mediante Telnet desde Router 1, se soliciten un nombre de usuario y una contraseña.

```

R1#telnet 1.1.1.2
Trying 1.1.1.2 ... Open

User Access Verification

Username: escom
Password:
R2>

```

Finalmente, uno de los beneficios de usar Telnet es la posibilidad de visualizar el archivo de configuración de Router 2, como se muestra en la imagen siguiente.

```
R2#show running
Building configuration...

Current configuration : 1594 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R2
!
boot-start-marker
boot-end-marker
!
enable password cisco
!
no aaa new-model
memory-size iomem 5
no ip icmp rate-limit unreachable
!
!
ip cef
no ip domain lookup
!
--More-- █
```

solarwinds  | Solar-PuTTY *free tool* © 2019-2024 SolarWinds Worldwide, LLC. All rights reserved.

Dado que la configuración principal se realiza en Router 2, los comandos necesarios en Router 1 son mínimos.

```
R1#config terminal
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#int ethernet 1/0
R1(config-if)#exit
R1(config)#int ethernet 1/0
R1(config-if)#ip address 1.1.1.1 255.255.255.252
R1(config-if)#no shutdown
R1(config-if)#exit
R1#ping 1.1.1.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 1.1.1.2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 8/9/12 ms
R1#telnet 1.1.1.2
Trying 1.1.1.2 ... Open
```

User Access Verification

Password:
//ENTRAMOS AL MODO USUARIO
R2>en
Password:
R2#
R2#show running
R2#show running-config

Building configuration...

Current configuration : 1247 bytes

!

upgrade fpd auto

version 12.4

service timestamps debug datetime msec

service timestamps log datetime msec

no service password-encryption

!

hostname R2

!

boot-start-marker

boot-end-marker

!

logging message-counter syslog

enable password cisco

!

no aaa new-model

ip source-route

no ip icmp rate-limit unreachable

ip cef

!

!

!

!

no ip domain lookup

no ipv6 cef

!

multilink bundle-name authenticated

!

!

!

!

!

!

--More--

[Connection to 1.1.1.2 closed by foreign host]

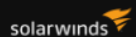
```
R1#telnet 1.1.1.2
Trying 1.1.1.2 ... Open

User Access Verification

Username: escom
Password:
% Login invalid

Username: escom
Password:
R2>en
Password:
R2#show running
Building configuration...

Current configuration : 1594 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R2
!
boot-start-marker
boot-end-marker
!
enable password cisco
!
no aaa new-model
memory-size iomem 5
no ip icmp rate-limit unreachable
!
!
ip cef
no ip domain lookup
!
R2#
```



Solar-PuTTY *free tool*

© 2019-2024 SolarWinds Worldwide, LLC. All rights reserved.

CONCLUSIONES

La administración remota mediante Telnet, una vez correctamente configurada, proporciona un acceso controlado y seguro, permitiendo a los administradores realizar ajustes en los routers desde ubicaciones remotas, lo cual optimiza la gestión de la red y la respuesta ante necesidades de configuración.

BIBLIOGRAFÍA

Stevens, W. Richard. Programación en red con Unix: La API de Sockets. Addison-Wesley Professional, 2003.

Forouzan, Behrouz A. Comunicaciones de Datos y Redes. McGraw-Hill, 2012. Tanenbaum, Andrew S., y David J. Wetherall. Redes de Computadoras. Pearson, 2010.

Comer, Douglas E. Internetworking con TCP/IP Volumen Uno. Prentice Hall, 2006. Kurose, James F., y Keith W. Ross. Redes de Computadoras: Un Enfoque Descendente. Pearson, 2017.