s

Universidad Nacional Autónoma de México

Facultad de Ingeniería

División de Ingeniería Eléctrica

Laboratorio de Redes y Seguridad

CCNP ENCOR

TOPOLOGÍA FINAL

Instructor: Ing. José Antonio Macías García.

Alumno: Jiménez Juárez Jesús

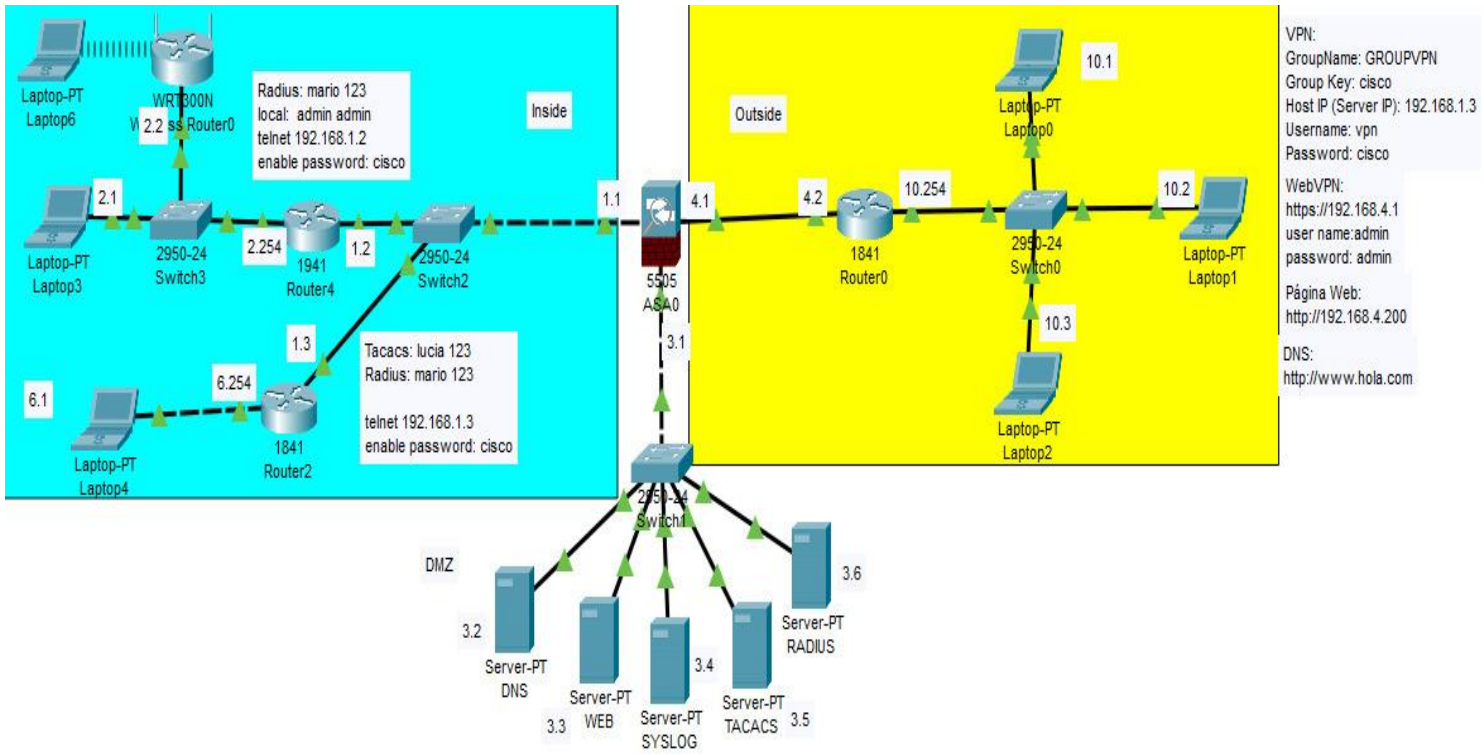
JULIO 2021

Índice

TOPOLOGÍA FINAL CCNP

Objetivo: Terminar la segunda parte del curso con conocimientos más sólidos de los temas vistos en el curso configurando la siguiente topología:

Dada la siguiente topología:



1.- Configurar lo siguiente:

***Protocolo de enrutamiento libre.**

***Acceso a R4 por Radius y de manera local**

***Acceso a R2 por Tacacs y Radius**

***Conexión de host a router inalámbrico por medio de Radius**

***Configuración de zonas inside, outside y DMZ en ASA**

***Configuración de webVPN para que los hosts de outside entren a la página web**

***Acceso mediante VPN en Router2 para host de outside**

***Acceso a página web mediante el DNS www.eselfingen21.com aplicando NATeo estático con una IP virtual y colocando es IP como DNS en los hosts.**

***Servidor syslog funcionando (mandar mensajes desde cualquier dispositivo al servidor).**

Configuración de un IPS en Router 4 denegando el ping

Configuración de usuarios y vistas en Router 4:

usuario5 -> Nivel 5 de privilegios

**ping*

**configure terminal*

**hostname*

usuario9 -> Nivel 9 de privilegios

**show running-config*

**interface fastethernet*

**ip address*

usuario59 ->Nivel 15 de privilegios

**Todos los comandos del sistema*

usuario3 -> Nivel 3 de privilegios

**show running-config*

**show ip route*

**show privilege*

usuario7 -> Nivel 7 de privilegios

**configure terminal*

**router rip*

**network (redes para el enrutamiento de rip)*

usuario37 -> Nivel 15 de privilegios

****Todos los comandos del sistema***

vista1

**configure terminal*

**ip dhcp pool*

**show ip route*

vista2

**clock set*

**show ip interface brief*

*show clock

vista3

*show cdp neighbors

*show version

*ping

vista4

*configure terminal

*logging host

*logging trap

2.-Adjuntar en este documento capturas de pantalla para la evidencia de cada configuración realizada y que está funcionando como se solicita.

*Protocolo de enrutamiento libre.

La configuración del protocolo se realizó con RIPv2 (Hay que mencionar que también se utilizó ruta estática, pero eso se explica en la configuración en zonas Inside, Outside y DMZ).

Configuración

- **Comandos para el Router2**

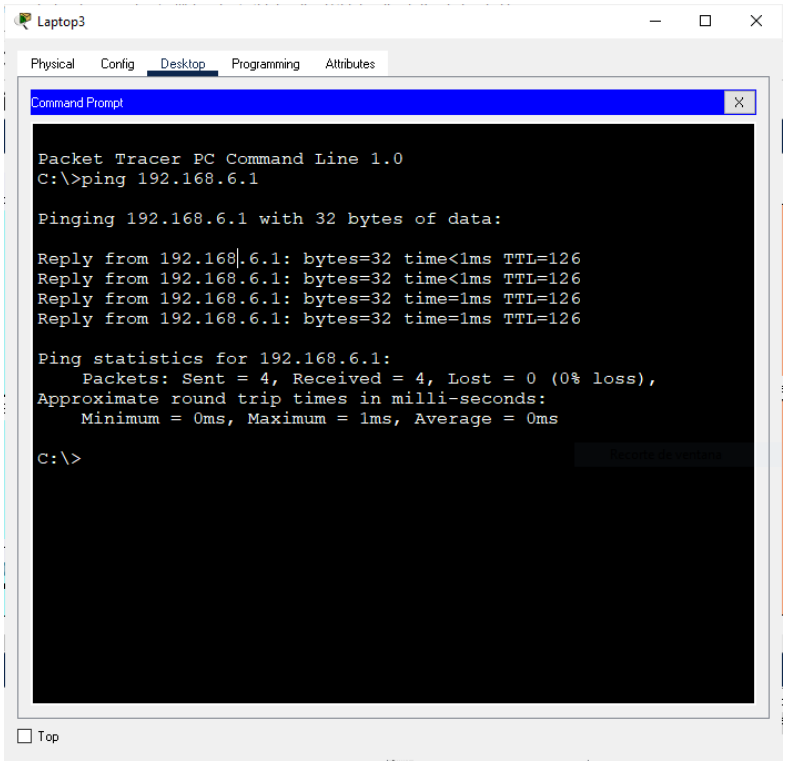
```
router rip
version 2
network 192.168.1.0
network 192.168.6.0
ex
```

- **Comandos para el Router4**

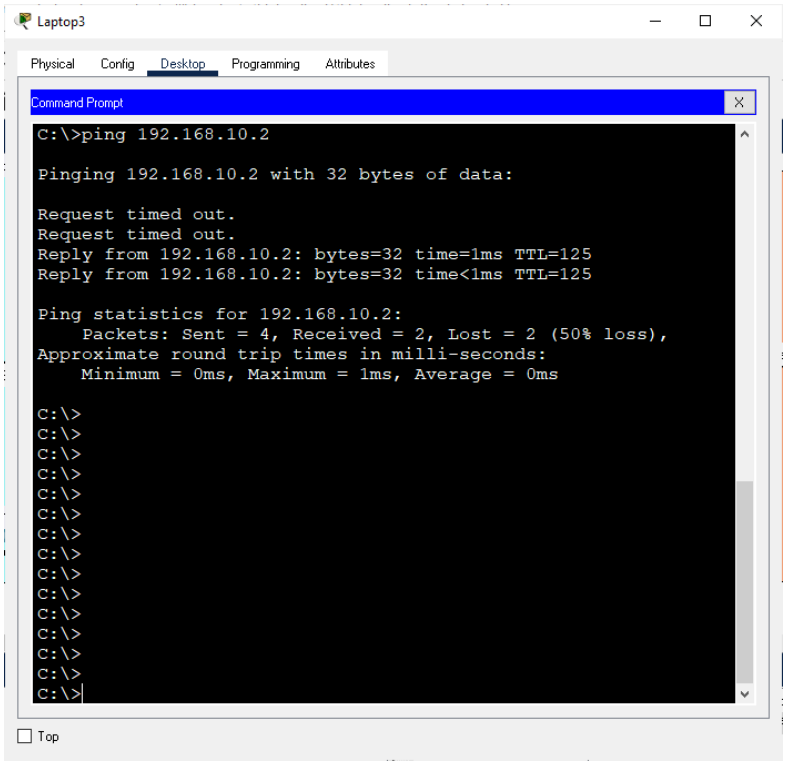
```
router rip
version 2
network 192.168.1.0
network 192.168.2.0
ex
```

En la topología se puede realizar un ping que comprueba que existe comunicación entre los dispositivos de la red.

Comprobación



Realizando ping del host 192.168.2.1 al 192.168.6.1, dando como exitosa la comunicación



Realizando ping del host 192.168.2.1 al 192.168.10.2, dando como exitosa la comunicación

*Acceso a R4 por Radius y de manera local

Se utilizó un servidor RADIUS con IP 192.168.3.6, el cual se encontraba en la zona DMZ donde se realizaron las configuraciones que se ven en las siguientes capturas de pantalla y comandos.

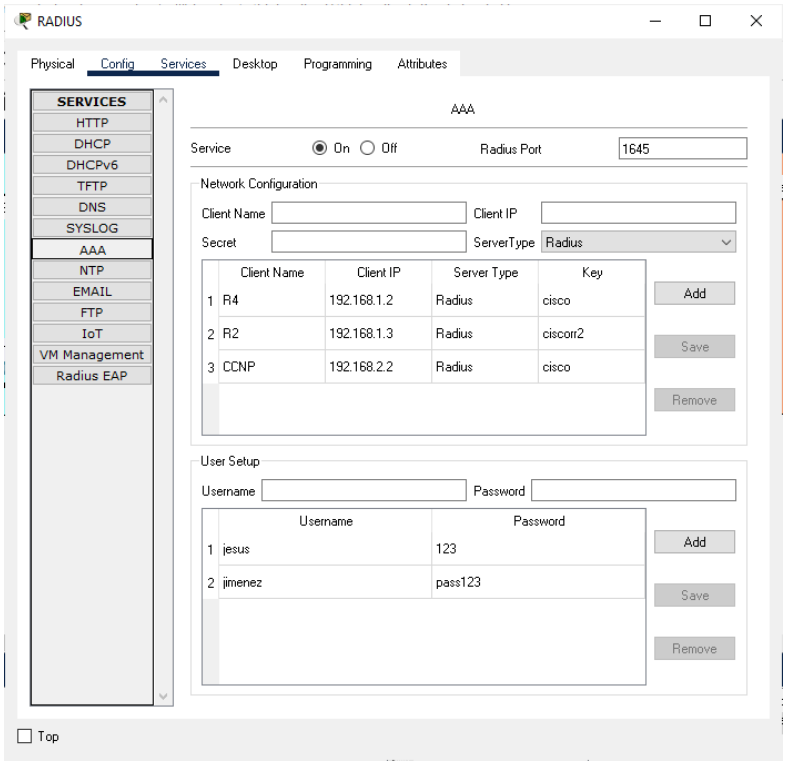
Configuración

- **Comandos para el Router4**

```
username local pass local
line vty 0 5
login local
aaa new-model
aaa authentication login default group radius local
aaa authentication enable default none
radius-server host 192.168.3.6
radius-server key cisco
```

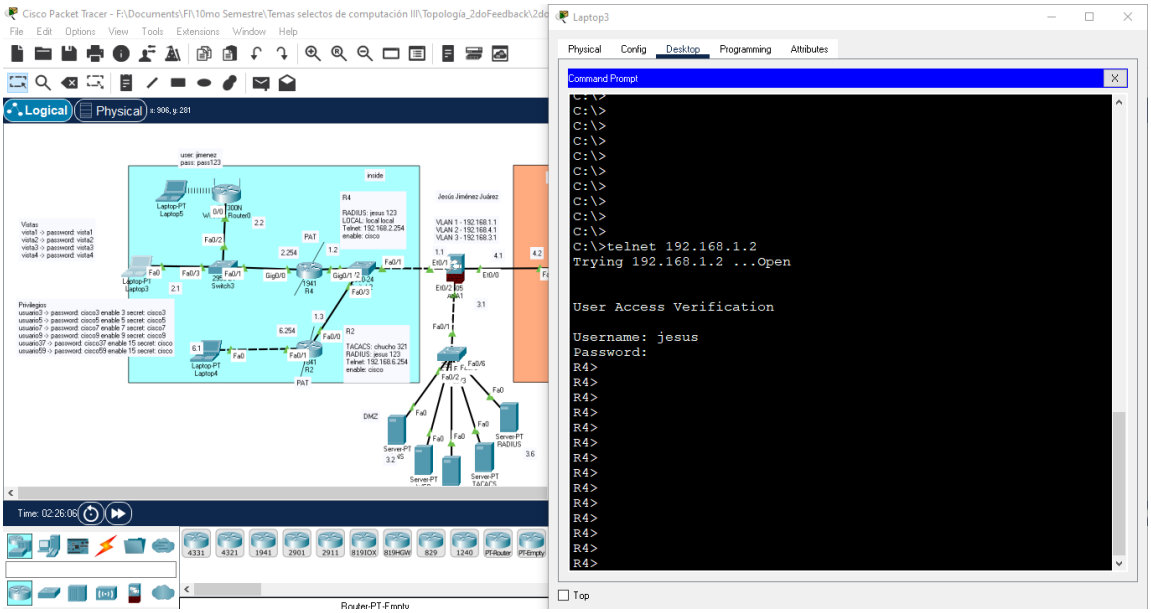
- **Configuración en servidor Radius**

Hay que mencionar que se configuró con el *Client Name* R4 y el usuario que se usa es el de *jesus* con contraseña *123*.

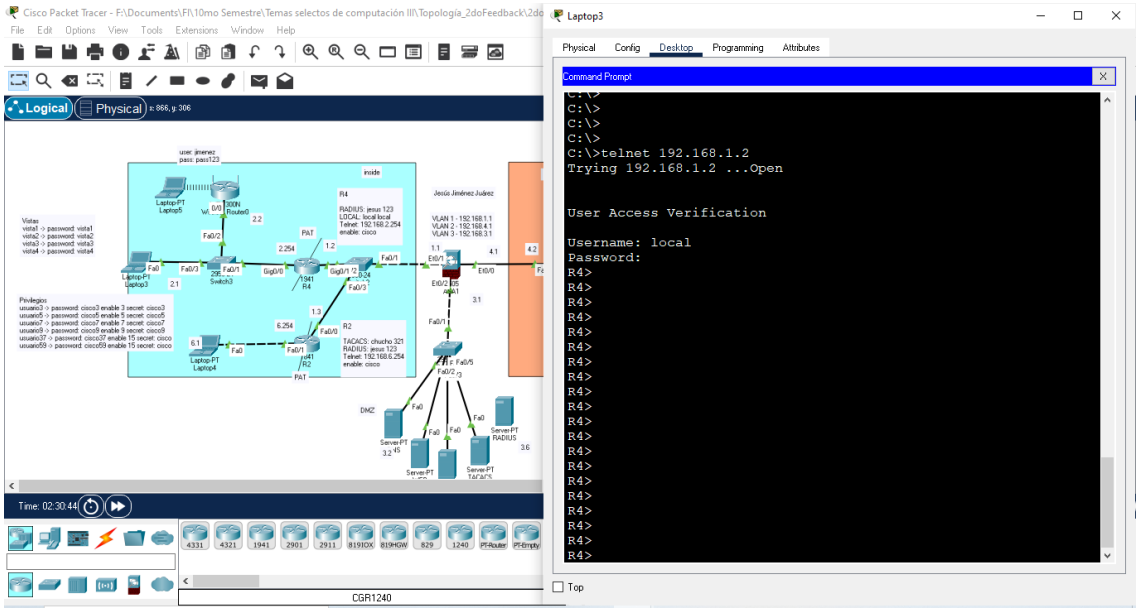


Para la comprobación se hizo uso de la laptop con IP 192.168.2.1 y se ingresó por medio de Telnet para corroborar que el acceso fuese ya sea por Radius o de manera local.

Comprobación



Realizando la conexión de Telnet autenticando con Radius (Usuario: *jesus* Pass: *123*).



Realizando la conexión de Telnet autenticando localmente, con el cable del servidor Radius desconectado de la red (Usuario: *local* Pass: *local*).

*Acceso a R2 por Tacacs y Radius

Se utilizaron dos servidores, TACACS+ con IP 192.168.3.5 y RADIUS con IP 192.168.3.6, los cuales se encontraban en DMZ donde se realizaron las configuraciones que se ven en las siguientes capturas de pantalla.

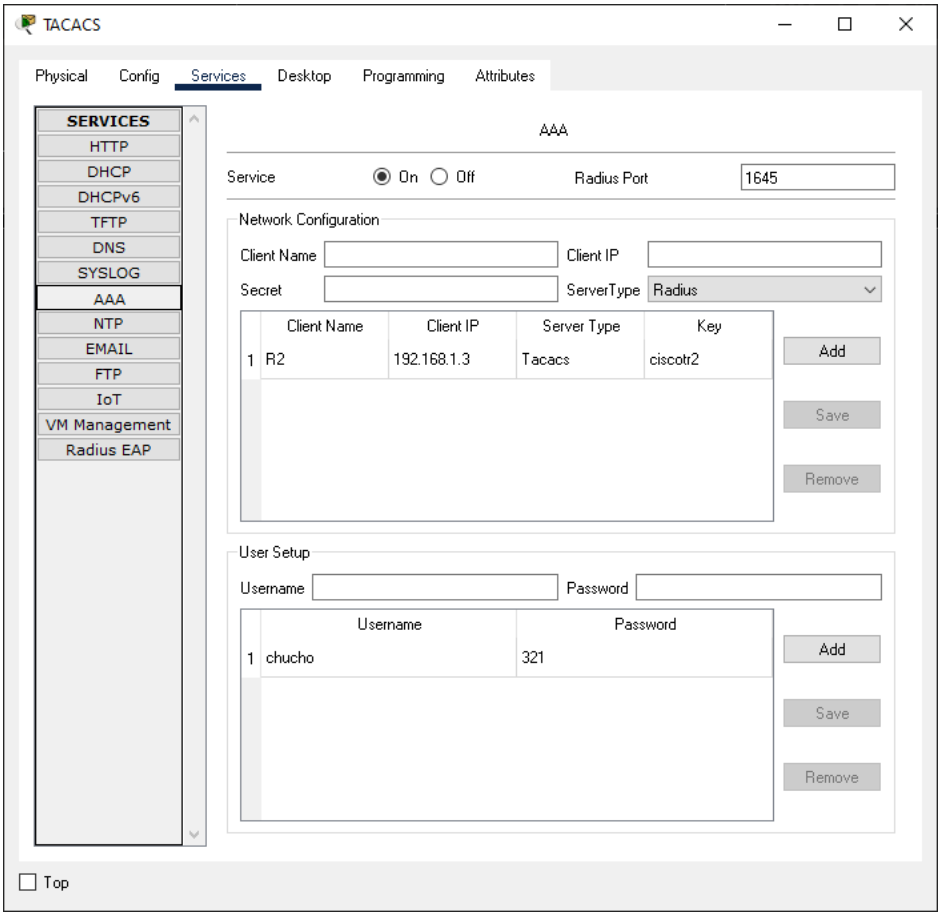
Configuración

- **Comandos en el Router2**

```
line vty 5 15
login local
aaa new-model
aaa authentication login default group tacacs+ group radius
tacacs-server host 192.168.3.5
tacacs-server key ciscotr2
radius-server host 192.168.3.6
radius-server key ciscorr2
```

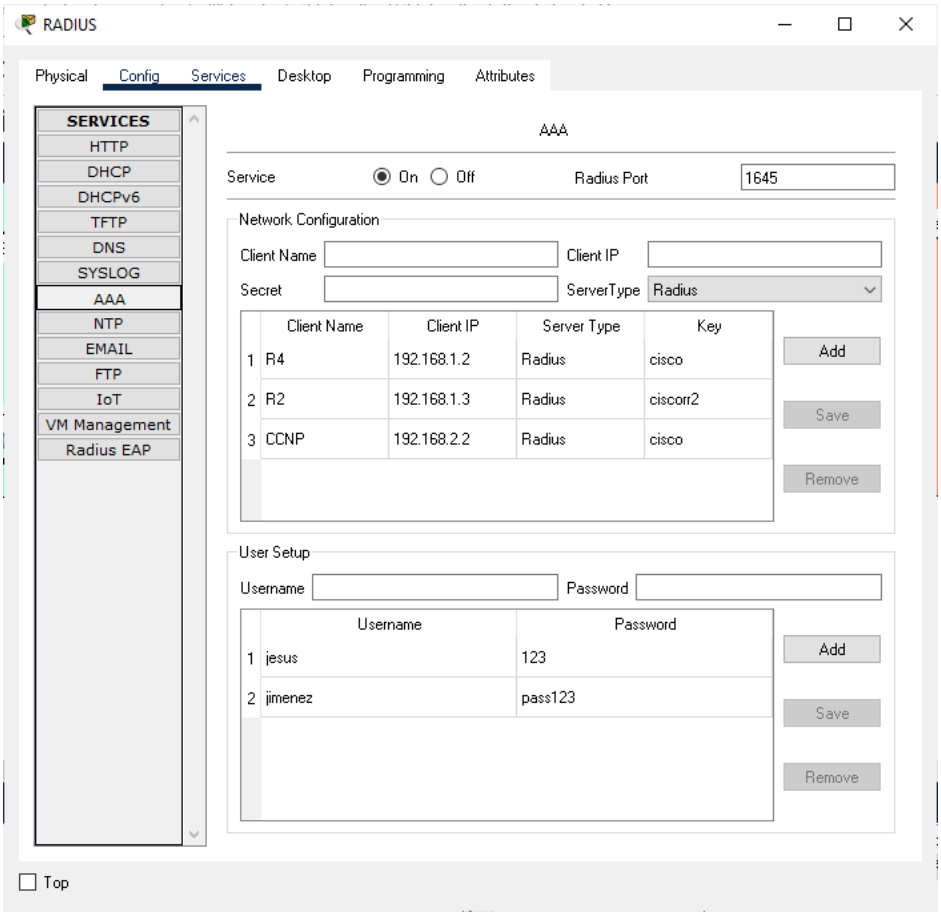
- **Configuración en servidor Tacacs**

Hay que mencionar que se configuró con el *Client Name* R2 y el usuario que se usa es el de *chucho* con contraseña *321*.



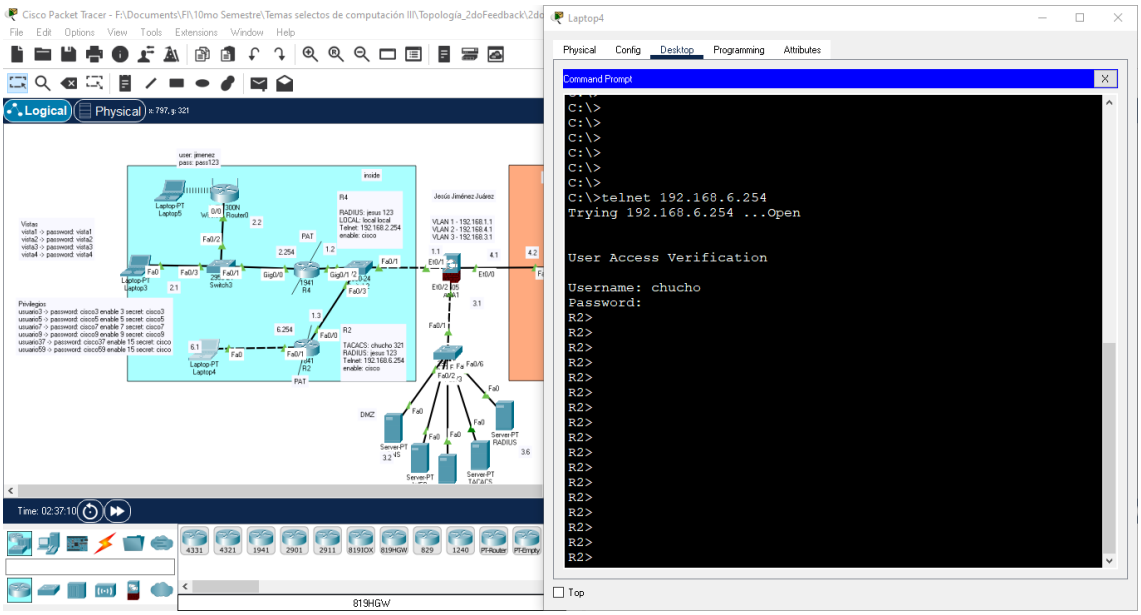
- **Configuración en servidor Radius**

Hay que mencionar que se configuró con el *Client Name* R2 y el usuario que se usa es el de *jesus* con contraseña *123*.

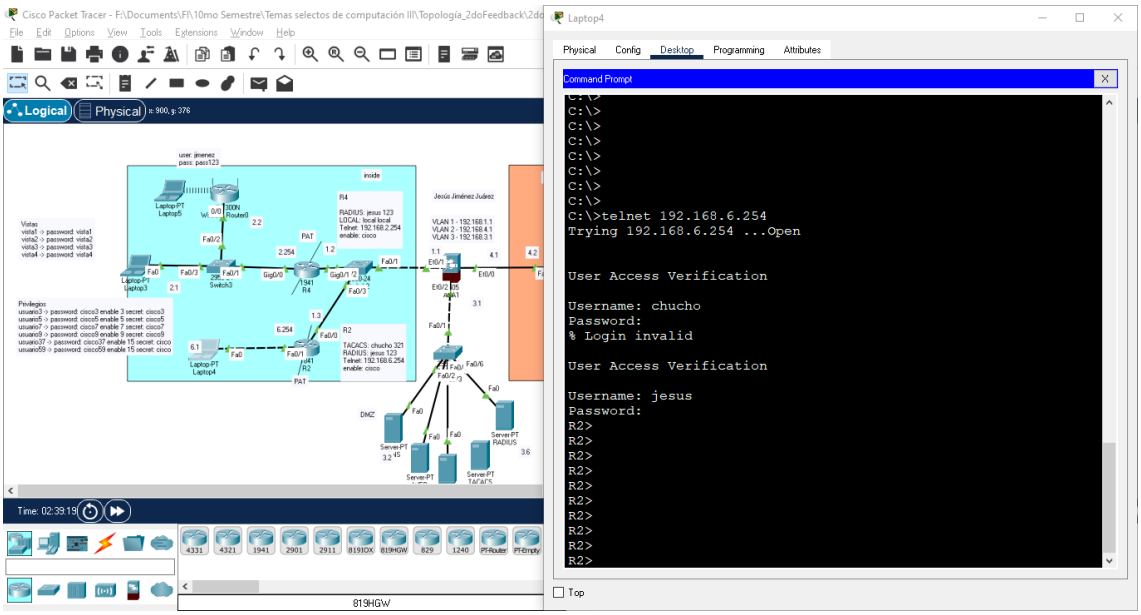


Para la comprobación se hizo uso de la laptop con IP 192.168.6.1 y se ingresó por medio de Telnet para corroborar que el acceso fuese ya sea por Tacacs o Radius

Comprobación



Realizando la conexión de Telnet autenticando con Tacacs (Usuario: *chucho* Pass: *321*).



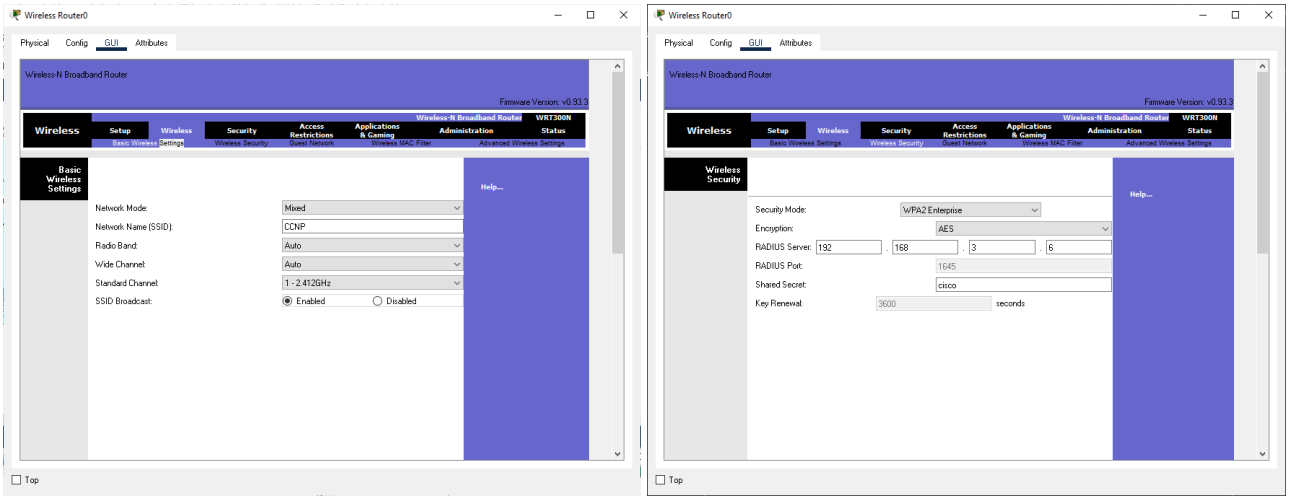
Realizando la conexión de Telnet autenticando con Radius (Usuario: *jesus* Pass: *123*).

*Conexión de host a router inalámbrico por medio de Radius

Se utilizó el Router Inalámbrico que está en la zona inside, así como una laptop para que se pudiera conectar.

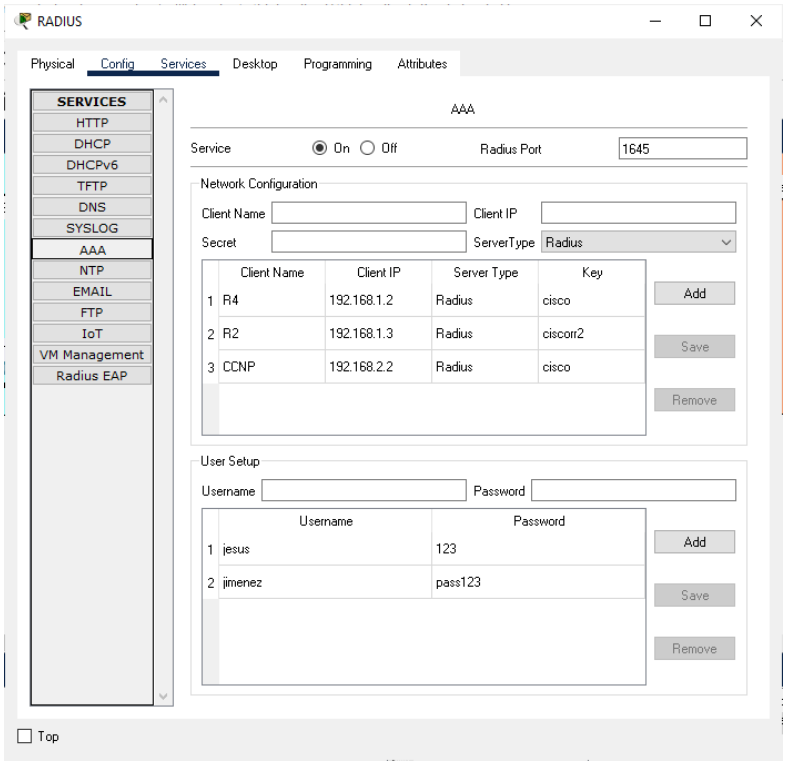
Configuración

- **Configuración del Router Inalámbrico**

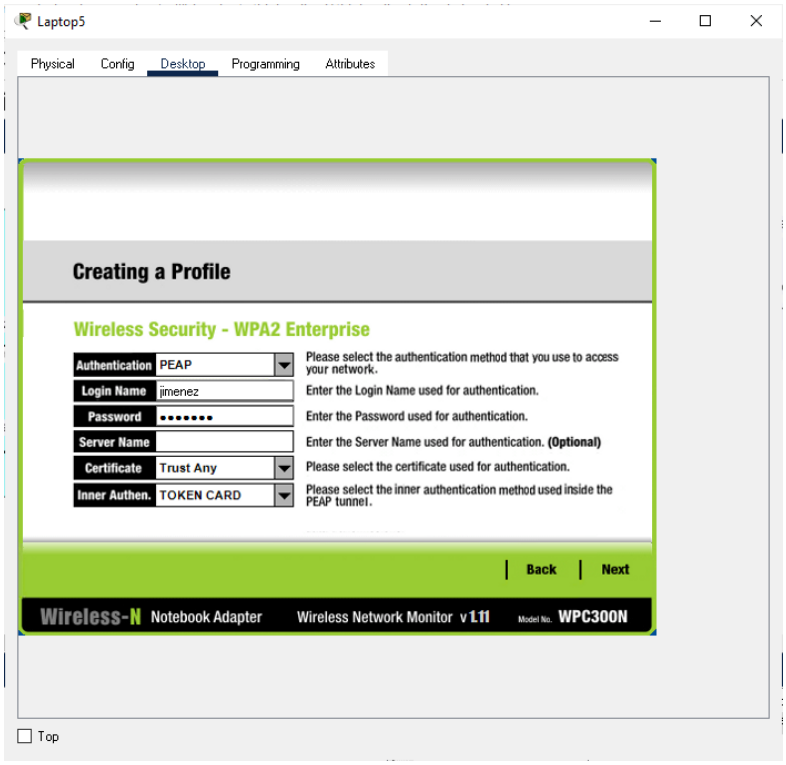


- **Configuración en el servidor Radius**

Hay que mencionar que se configuró con el *Client Name* CCNP y el usuario que se usa es el de *jimenez* con contraseña *pass123*.

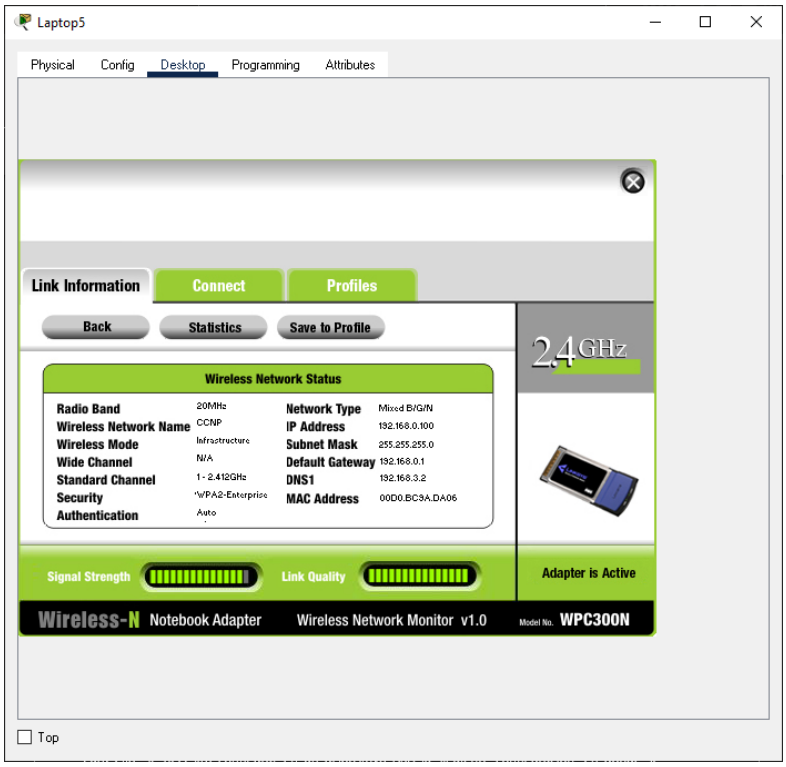


- **Configuración de laptop5 para conectarse al Router Inalámbrico.**



Viendo las ondas que manda el Router inalámbrico a la laptop nos podemos dar cuenta de que la conexión se realizó de manera exitosa.

Comprobación



Información de la conexión de la Laptop5.

*Configuración de zonas inside, outside y DMZ en ASA

Para ello, se necesito configurar en un dispositivo ASA la siguiente configuración, en donde se necesitó también de ruta estática para que hubiese comunicación entre las zonas.

Configuración

- **Comandos en el dispositivo ASA**

Se utilizaron los comandos vistos en clase, además de realizar un nateo en el outside para que se pudieran comunicar los dispositivos en la red.

```
interface vlan 2
ip address 192.168.4.1 255.255.255.0
no shutdown
exit
interface vlan 1
no shutdown
exit
interface vlan 3
no forward interface vlan 1
nameif DMZ
```

```
security-level 50
exit
interface Et0/2
switchport access vlan 3
exit
interface vlan 3
ip address 192.168.3.1 255.255.255.0
no shutdown
exit
route outside 0.0.0.0 0.0.0.0 192.168.4.2
```

- **Comandos en el Router2**

Para que haya comunicación entre los dispositivos de la red, lo que se debe de hacer es habilitar un nateo en el router, esto para traducir el segmento 192.168.6.0. Además, se utilizó ACLs, así como rutas estáticas, para que en algunos casos no se tradujeran los segmentos.

```
ip route 192.168.2.0 255.255.255.0 192.168.1.2
ip route 0.0.0.0 0.0.0.0 192.168.1.1
ip nat inside source list 100 interface FastEthernet0/0 overload
access-list 100 permit ip 192.168.6.0 0.0.0.255 host 192.168.1.1
access-list 100 deny ip 192.168.6.0 0.0.0.255 192.168.1.0 0.0.0.255
access-list 100 deny ip 192.168.6.0 0.0.0.255 192.168.2.0 0.0.0.255
access-list 100 permit ip 192.168.6.0 0.0.0.255 any
```

- **Comandos en el Router4**

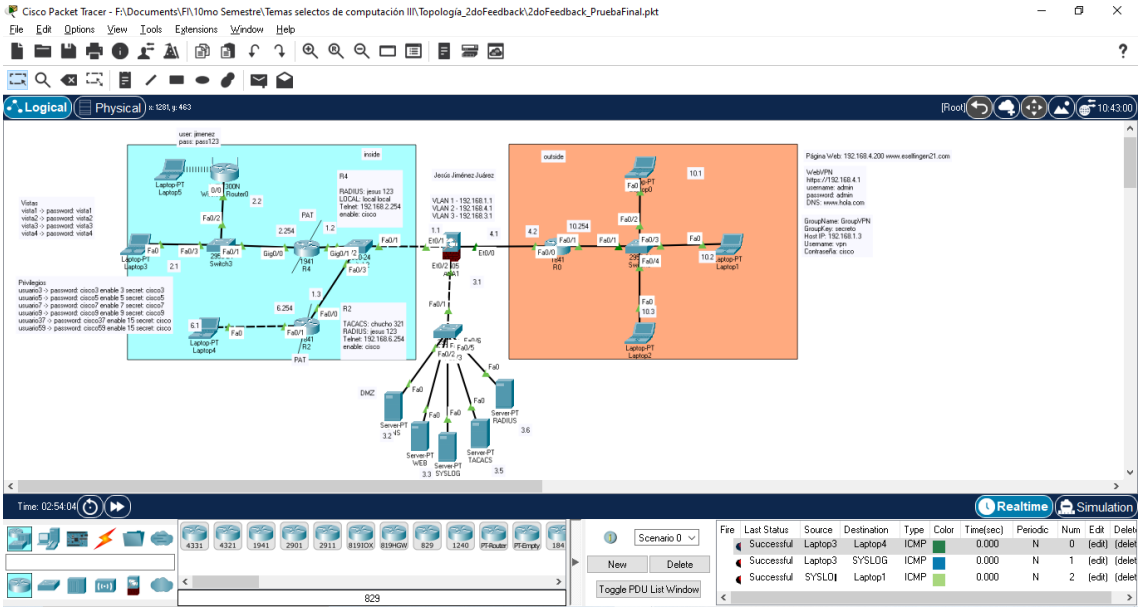
Para que haya comunicación entre los dispositivos de la red, lo que se debe de hacer es habilitar un nateo en el router, esto para traducir el segmento 192.168.2.0. Además, se utilizó de ACLs para que en algunos casos no se tradujeran los segmentos, así como de las rutas estáticas.

```
ip route 192.168.6.0 255.255.255.0 192.168.1.3
ip route 0.0.0.0 0.0.0.0 192.168.1.1
ip nat inside source list 100 interface GigabitEthernet0/1 overload
access-list 100 permit ip any host 192.168.1.1
access-list 100 deny ip any 192.168.1.0 0.0.0.255
access-list 100 deny ip any 192.168.6.0 0.0.0.255
access-list 100 permit ip any any
```

Se necesita realizar un ping de las zonas en donde se tiene mayor nivel de seguridad a las que son

menores, pero no de manera contraria.

Comprobación



Mandando ping desde los dispositivos de niveles más altos a los más bajos, corroborando que haya comunicación.

*Configuración de webVPN para que los hosts de outside entren a la página web

Dentro del dispositivo ASA, se tiene la posibilidad de realizar la configuración webVPN, además se utilizó una página web llamada www.hola.com para que pudiese funcionar, esté se encuentra activada en el servidor WEB.

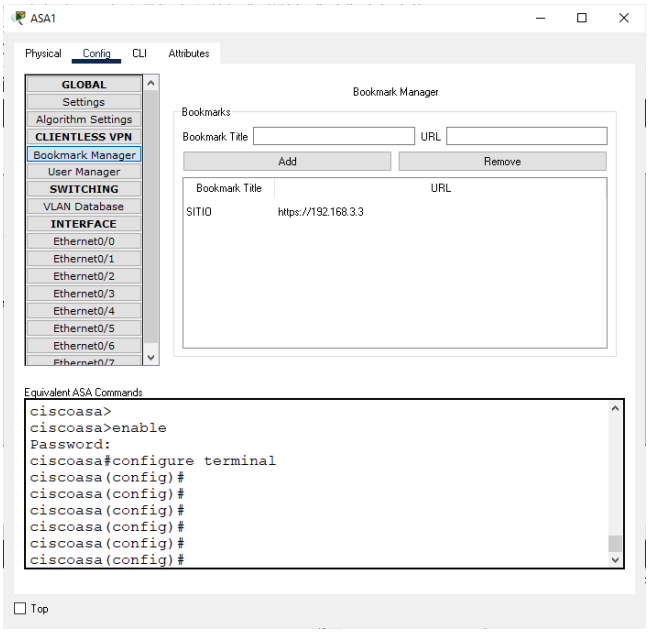
Configuración

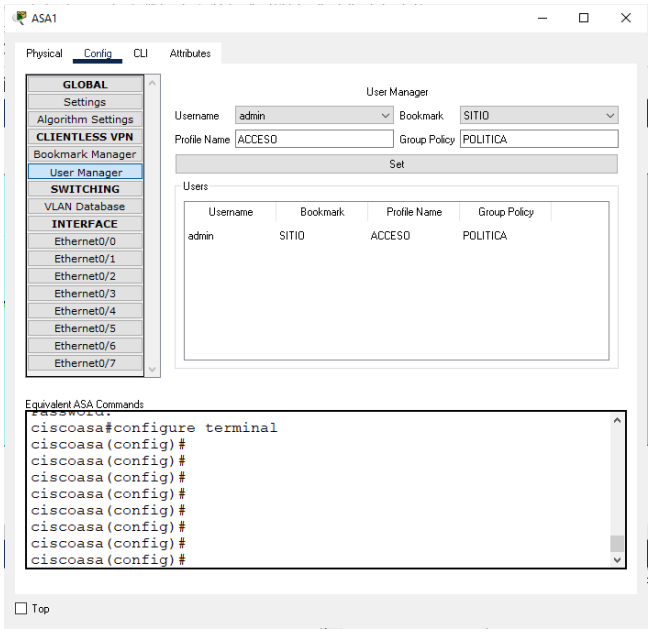
- **Configuración en ASA**

```
access-list 101 permit tcp any any eq 80
access-group 101 in interface outside
webvpn
enable outside
exit
username admin password admin
group-policy POLITICA internal
group-policy POLITICA attributes
webvpn
url-list value SITIO
exit
```

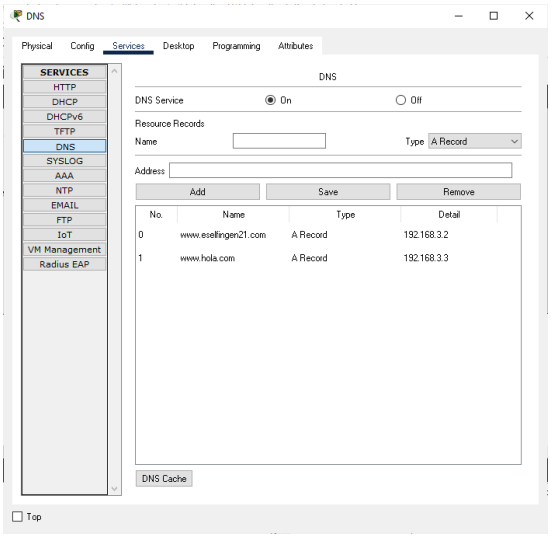
```
tunnel-group ACCESO type remote-access
tunnel-group ACCESO general-attributes
default-group-policy POLITICA
username admin attributes
vpn-group-policy POLITICA
```

- **Configuración en ASA**





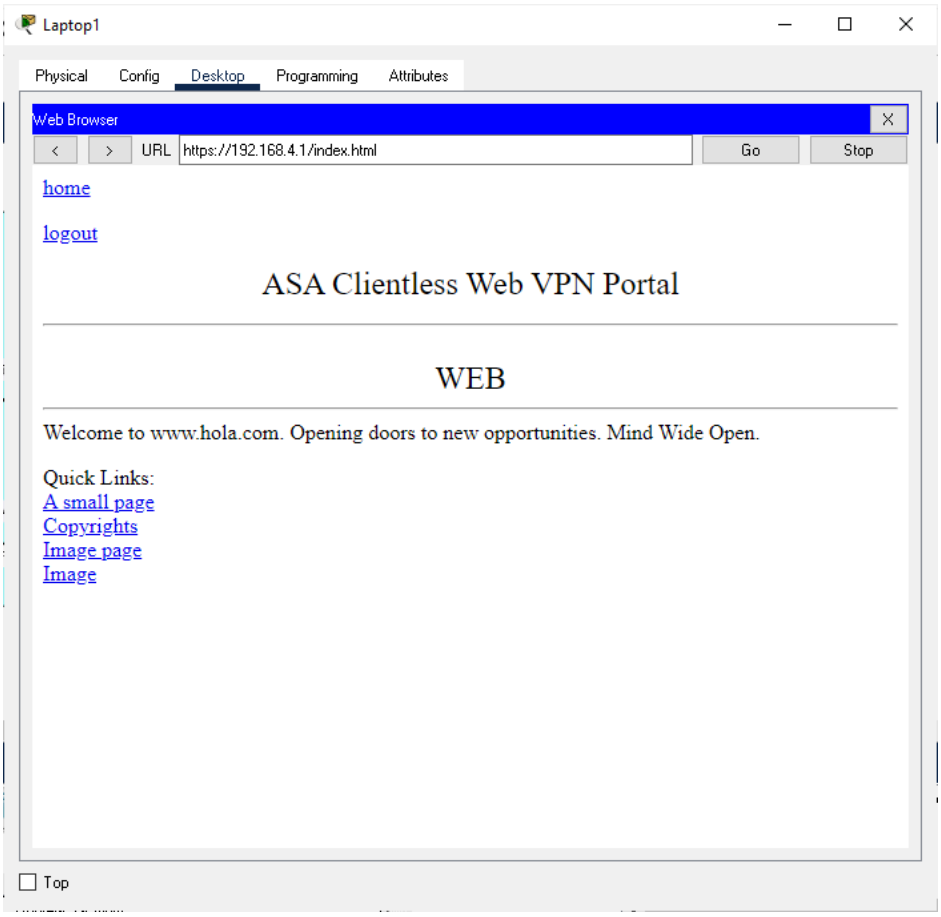
- **Configuración en el servidor DNS**



Se realizó desde uno de los hosts de la zona outside, se ingresaron los datos correspondientes para que pudiera corroborarse que se realizó la configuración de manera adecuada.

Comprobación

Ingresando https://192.168.4.1 a cualquiera de los hosts de la zona outside junto con las credenciales de acceso (admin/admin), tendremos el siguiente resultado.



Después de ingresar a https://192.168.4.1 y escribir las credenciales de acceso (admin/admin), aparece esta interfaz. Se puede realizar desde cualquier host de la zona outside.

*Acceso mediante VPN en Router2 para host de outside

Se hizo la configuración correspondiente para que cualquier host de la zona outside pudiera conectarse por medio de VPN al Router2.

Configuración

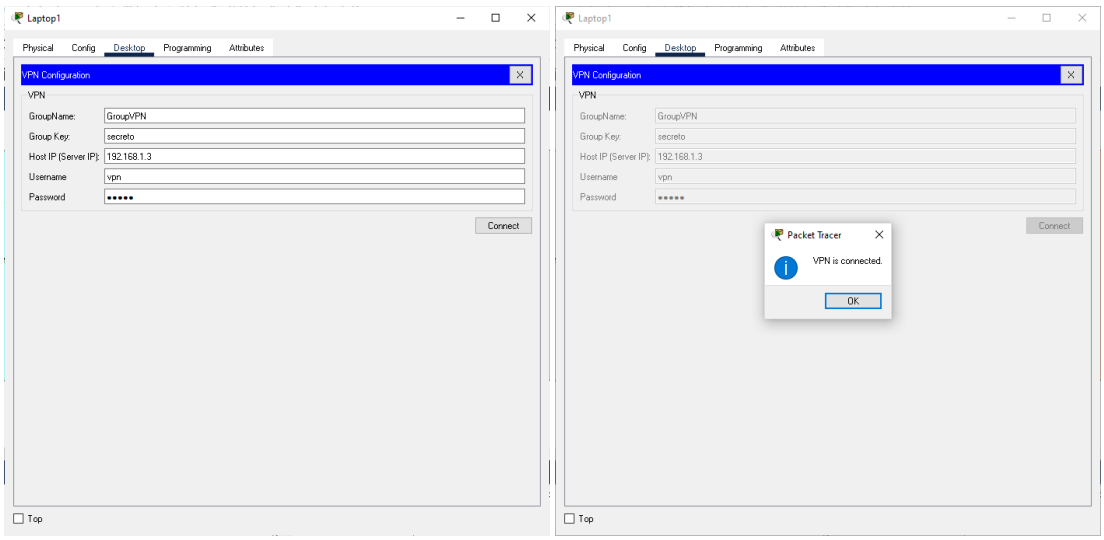
- **Comandos en Router2**

```
aaa new-model
aaa authentication login VPNUSER local
aaa authorization network GroupVPN local
username vpn secret cisco
crypto isakmp policy 10
encryption aes
```

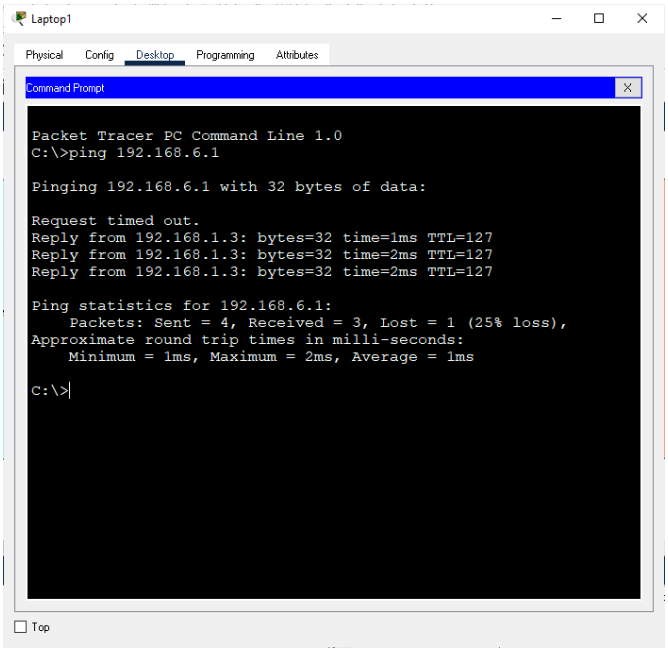
```
authentication pre-share
group 5
exit
crypto isakmp client configuration group GroupVPN
key secreto
pool POOLVPN
exit
ip local pool POOLVPN 192.168.6.10 192.168.6.20
crypto ipsec transform-set VPNSET esp-aes esp-sha-hmac
crypto dynamic-map VPNDINAMIC 10
set transform-set VPNSET
reverse-route
crypto map STATICMAP client authentication list VPNUSER
crypto map STATICMAP isakmp authorization list GroupVPN
crypto map STATICMAP client configuration address respond
crypto map STATICMAP 20 ipsec-isakmp dynamic VPNDINAMIC
interface fa0/0
crypto map STATICMAP
exit
```

Se ingresaron los datos para poder conectarse por medio de VPN al Router2 en uno de los hosts de la zona outside.

Comprobación



Los datos que se deben de ingresar son los que se muestran en la imagen izquierda en la sección *VPN* de la laptop. Deberá aparecer el mensaje como se ve en imagen derecha.



Si se desea mandar un ping desde una laptop con la VPN configurada a un dispositivo del segmento 192.168.6.0, tendrá éxito.

*Acceso a página web mediante el DNS www.eselfingen21.com aplicando NATeo estático con una IP virtual y colocando es IP como DNS en los hosts.

Dentro del dispositivo ASA, se tiene la posibilidad de realizar la configuración de nateo estático con una IP virtual, además se utilizó una página web llamada www.eselfingen21.com para que pudiese funcionar, esté se encuentra activada en el servidor DNS.

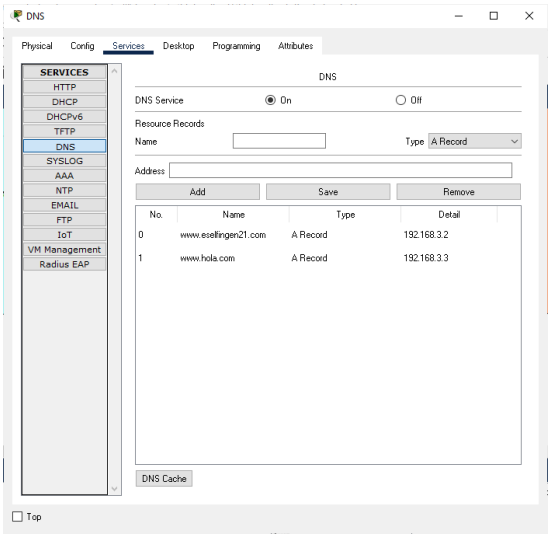
Configuración

- **Comandos para el dispositivo ASA**

```
class-map Inspector_estados
match default-inspection-traffic
exit
policy-map GLOBAL_POLICY
class Inspector_estados
inspect dns
inspect icmp
inspect http
service-policy GLOBAL_POLICY global
```

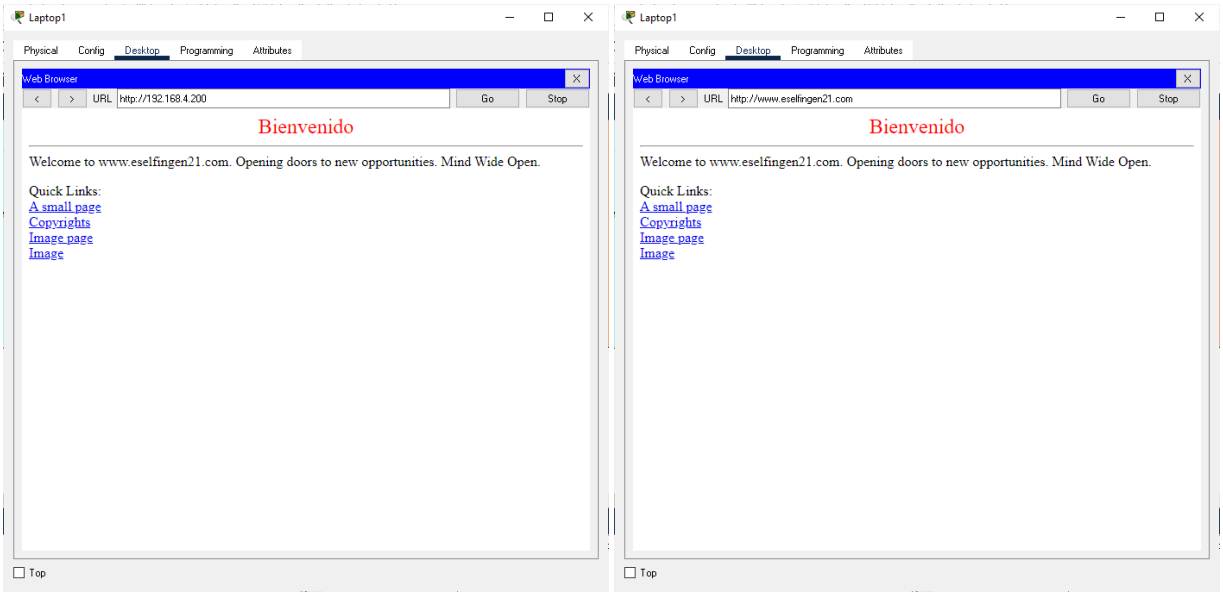
```
access-list ACL1 extended permit tcp any any
access-list ACL1 extended permit udp any any
access-group ACL1 in interface outside
object network OBJ1
host 192.168.3.2
nat (DMZ, outside) static 192.168.4.200
```

- **Configuración del servidor DNS**



Configurado lo anterior, se ingresa la dirección para verificar que puede acceder.

Comprobación



Se puede ingresar a la página ya sea con la IP 192.168.4.200 o a través del dominio www.eselfingen21.com, sea cual sea el caso, vemos que se puede entrar.

*Servidor syslog funcionando (mandar mensajes desde cualquier dispositivo al servidor).

Se configura prácticamente el mismo comando en los routers y switches de la red.

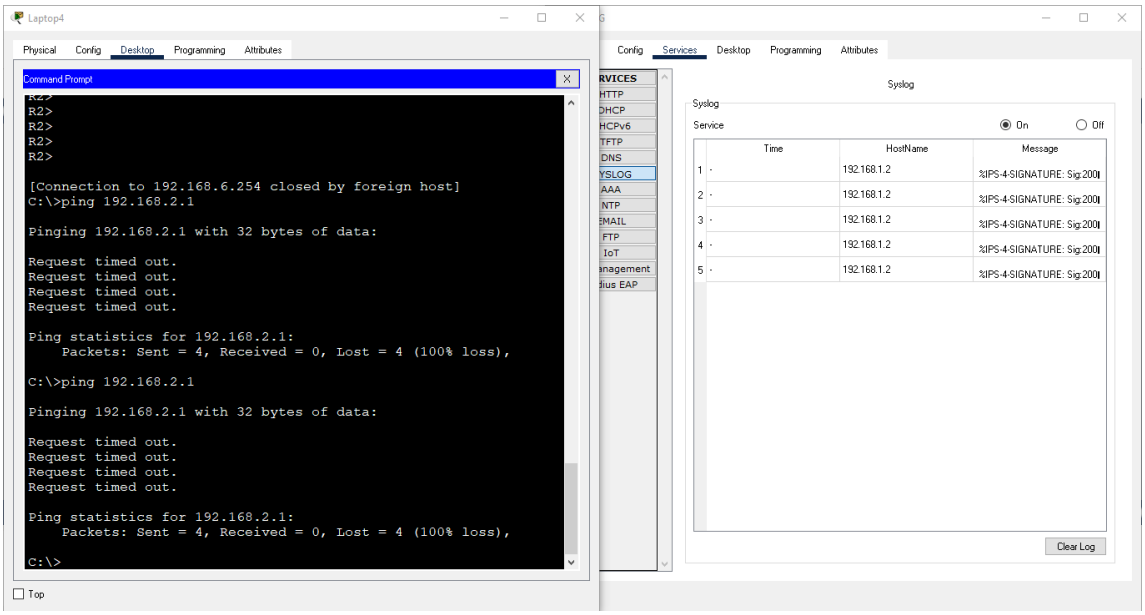
Configuración

- **Comandos en cualquier Router y Switch.**

```
logging host 192.168.3.4
logging trap debugging
```

Se puede comprobar con lo que se configuró en el Router4 al denegar los pings o realizando loopbacks para comprobar que realmente puede mandar mensajes al servidor.

Comprobación



Del lado izquierdo se está tratando de mandar un ping, pero como se denegó el ping hacia el segmento 192.168.2.0, entonces no se tendrá comunicación. Mientras que en el servidor syslog se muestran los mensajes.

*Configuración de un IPS en Router 4 denegando el ping

Se configuró en el Router4 para denegar el ping a todo aquel dispositivo de la red que desee comunicarse con el segmento de red 192.168.2.0.

Configuración

- **Comandos en el router 4**

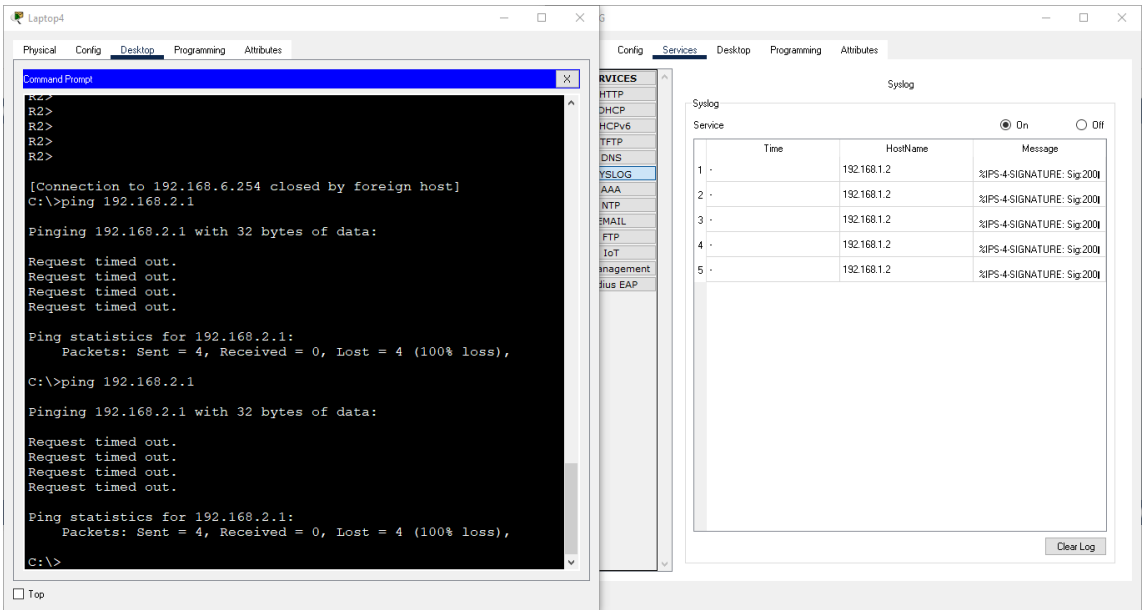
```
license boot module c1900 technology-package securityk9
yes
ex
wr
```

```
reload

ena
mkdir ipsdir
dir flash:
conf t
ip ips config location ipsdir
ip ips signature-category
category all
retired true
exit
category ios_ips basic
retired false
exit
exit
y
ip ips name iosips
interface gi0/0
ip ips iosips out
ip ips signature-definition
signature 2004 0
status
retired false
enabled true
exit
engine
event-action produce-alert
event-action deny-packet-inline
exit
exit
exit
```

Esto lo podemos comprobar con el punto anterior, dado que se tiene configurado syslog justamente para avisar cuándo se le está denegando un ping.

Comprobación



Del lado izquierdo se está tratando de mandar un ping, pero como se denegó el ping hacia el segmento 192.168.2.0, entonces no se tendrá comunicación. Mientras que en el servidor syslog se muestran los mensajes.

*Configuración de usuarios y vistas en Router 4:

Privilegios

usuario5 -> Nivel 5 de privilegios

***ping**

***configure terminal**

***hostname**

Se configuró al usuario5 dándole los privilegios que se enlistan, además de que ya viene heredando lo que en otros usuarios se le había asignado los comandos que podían utilizar.

Configuración

- **Comandos para el usuario5 en el Router4**

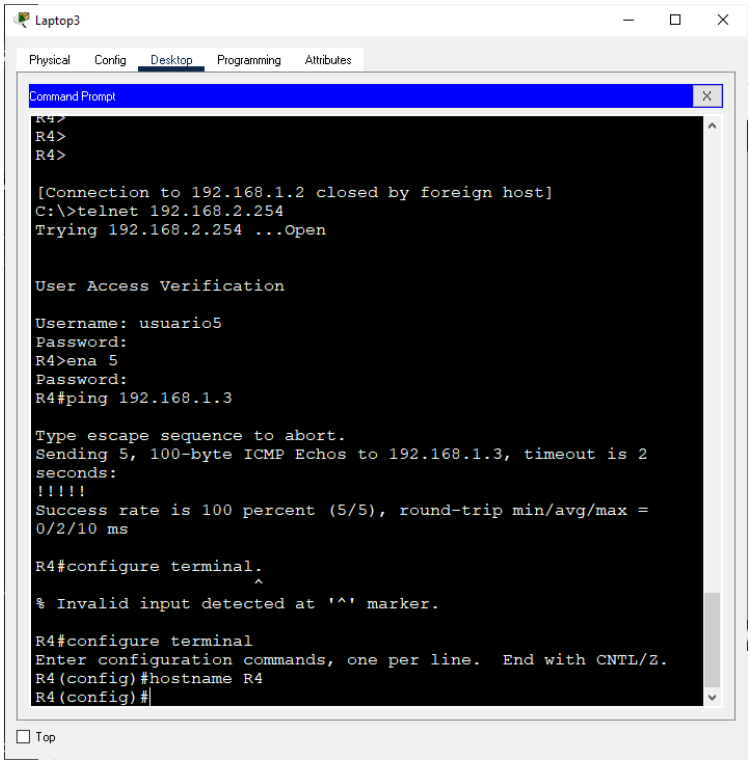
```
username usuario5 privilege 5 secret cisco5
privilege exec level 5 ping
privilege exec level 5 configure terminal
```

```
privilege configure level 5 hostname

enable secret level 5 cisco5
```

Se hace uso de Telnet, además de que se considera que no debe estar operando el servidor RADIUS, ya que se configuró la autenticación tanto con Radius como de manera local, pero con un mayor privilegio el primero mencionado.

Comprobación



Se muestra en la imagen que se tiene la posibilidad de usar los comandos *ping, configure terminal* y *hostname.*

usuario9 -> Nivel 9 de privilegios

**show running-config*

**interface fastethernet*

**ip address*

Se configuró al usuario9 dándole los privilegios que se enlistan, además de que ya viene heredando lo que en otros usuarios se le había asignado los comandos que podían utilizar.

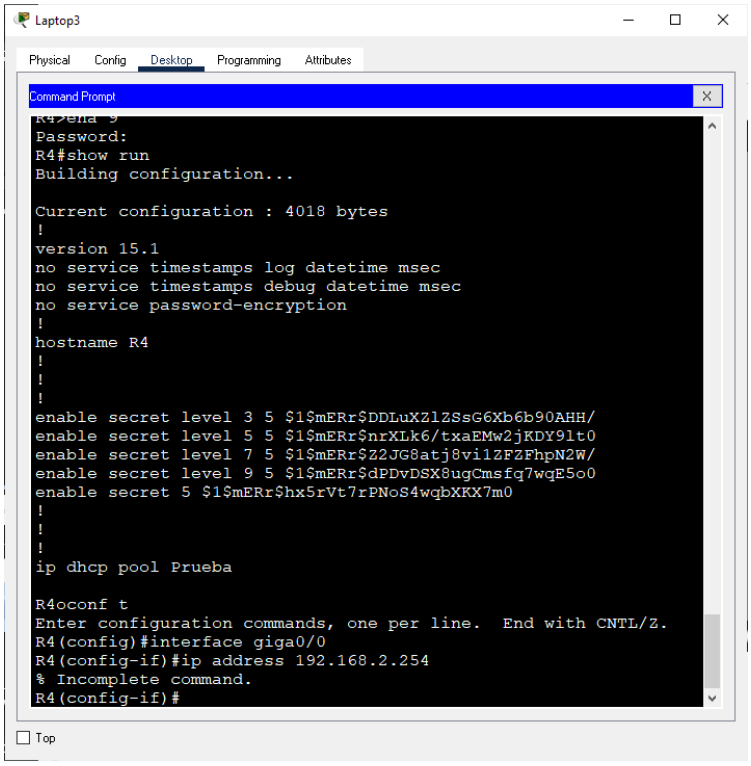
Configuración

- **Comandos para el usuario9 en el Router4**

```
username usuario9 privilege 9 secret cisco9
privilege exec level 9 show running-config
privilege configure level 9 interface fastethernet
privilege configure level 9 interface gigabitethernet
privilege interface level 9 ip address
enable secret level 9 cisco9
```

Se hace uso de Telnet, además de que se considera que no debe estar operando el servidor RADIUS, ya que se configuró la autenticación tanto con Radius como de manera local, pero con un mayor privilegio el primero mencionado.

Comprobación



Se muestra en la imagen que se tiene la posibilidad de usar los comandos *show running-config, interface GigabitEthernet* e *ip address.*

usuario59 ->Nivel 15 de privilegios

**Todos los comandos del sistema*

Se configuró al usuario59 dándole todos los privilegios del sistema únicamente creando al usuario, ya que es el que se tiene por default.

Configuración

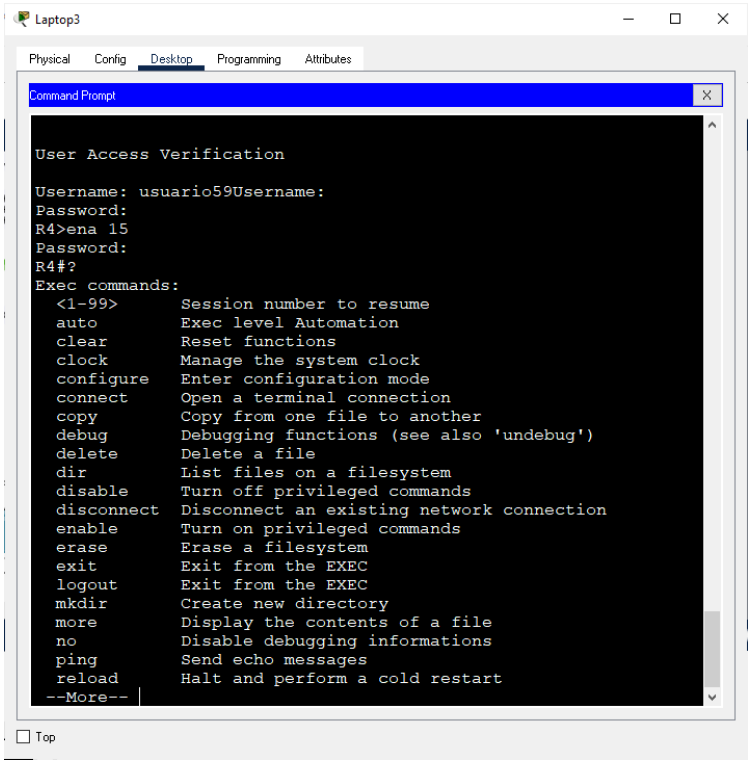
- **Comandos para el usuario59 en el Router4**

username usuario59 privilege 15 secret cisco59

enable secret level 15 cisco

Se hace uso de Telnet, además de que se considera que no debe estar operando el servidor RADIUS, ya que se configuró la autenticación tanto con Radius como de manera local, pero con un mayor privilegio el primero mencionado.

Comprobación



Se muestra en la imagen que se tiene la posibilidad de usar cualquier comando con tan solo escribir *?*.

usuario3 -> Nivel 3 de privilegios

**show running-config*

**show ip route*

**show privilege*

Se configuró al usuario3 dándole los privilegios que se enlistan. Hay que mencionar que es el de nivel más bajo de privilegios, por lo que no se le heredan comandos.

Configuración

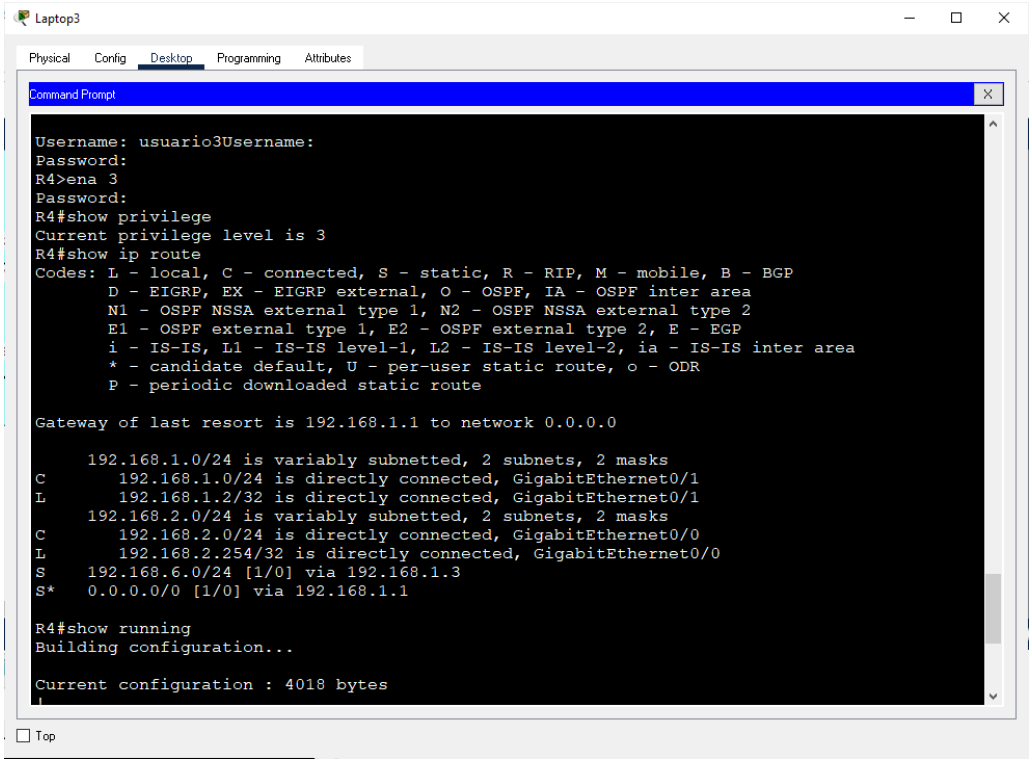
- **Comandos para el usuario3 en el Router4**

```
username usuario3 privilege 3 secret cisco3
```

```
privilege exec level 3 show running-config
privilege exec level 3 show ip route
privilege exec level 3 show privilege
enable secret level 3 cisco3
```

Se hace uso de Telnet, además de que se considera que no debe estar operando el servidor RADIUS, ya que se configuró la autenticación tanto con Radius como de manera local, pero con un mayor privilegio el primero mencionado.

Comprobación



Se muestra en la imagen que se tiene la posibilidad de usar los comandos *show privilege, show ip route y show running-config.*

usuario7 -> Nivel 7 de privilegios

**configure terminal*

**router rip*

**network (redes para el enrutamiento de rip)*

Se configuró al usuario7 dándole los privilegios que se enlistan, además de que ya viene heredando lo que en otros usuarios se le había asignado los comandos que podían utilizar.

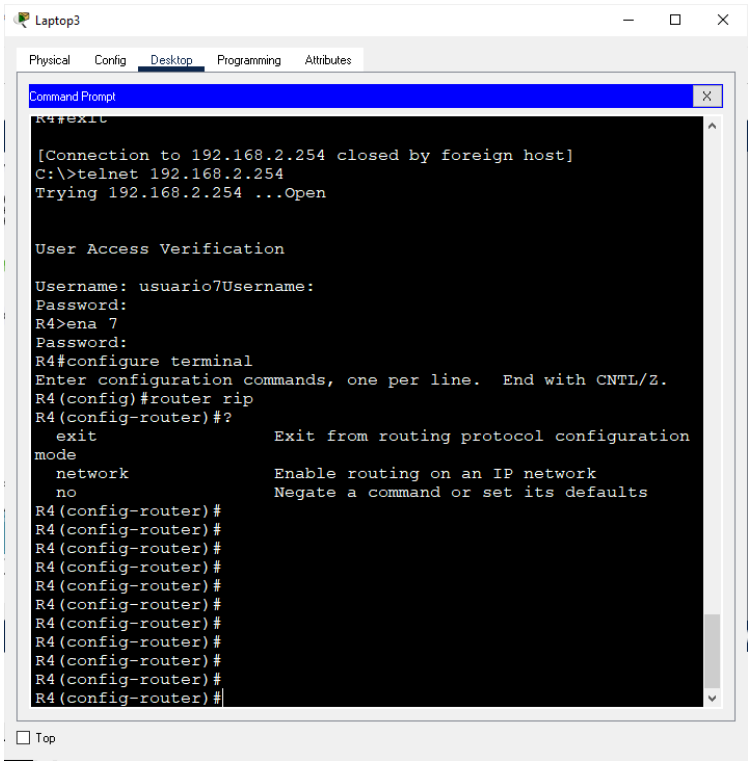
Configuración

- **Comandos para el usuario7 en el Router4**

```
username usuario7 privilege 7 secret cisco7
privilege exec level 7 configure terminal
privilege configure level 7 router rip
privilege router level 7 network
enable secret level 7 cisco7
```

Se hace uso de Telnet, además de que se considera que no debe estar operando el servidor RADIUS, ya que se configuró la autenticación tanto con Radius como de manera local, pero con un mayor privilegio el primero mencionado.

Comprobación



Se muestra en la imagen que se tiene la posibilidad de usar los comandos *configure terminal, router rip* y *network.*

usuario37 -> Nivel 15 de privilegios

Todos los comandos del sistema

Se configuró al usuario37 dándole todos los privilegios del sistema únicamente creando al usuario, ya que es el que se tiene por default.

Configuración

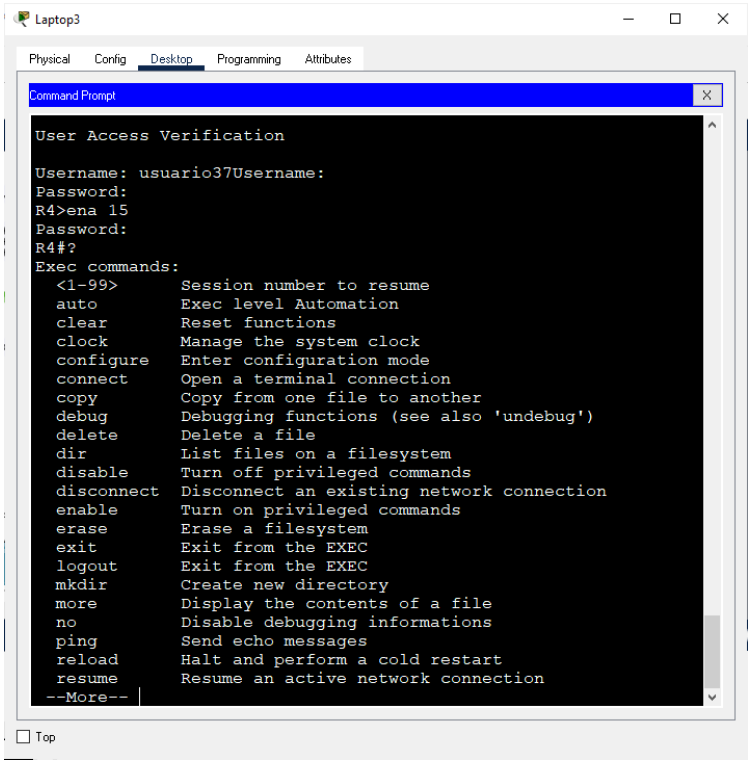
- **Comandos para el usuario7 en el Router4**

```
username usuario37 privilege 15 secret cisco37

enable secret level 15 cisco
```

Se hace uso de Telnet, además de que se considera que no debe estar operando el servidor RADIUS, ya que se configuró la autenticación tanto con Radius como de manera local, pero con un mayor privilegio el primero mencionado.

Comprobación



Se muestra en la imagen que se tiene la posibilidad de usar cualquier comando con tan solo escribir *?*.

Vistas

vista1

**configure terminal*

**ip dhcp pool*

**show ip route*

Se configuró a vista1 dando únicamente estos comandos, donde no se hereda nada de las demás vistas.

Configuración

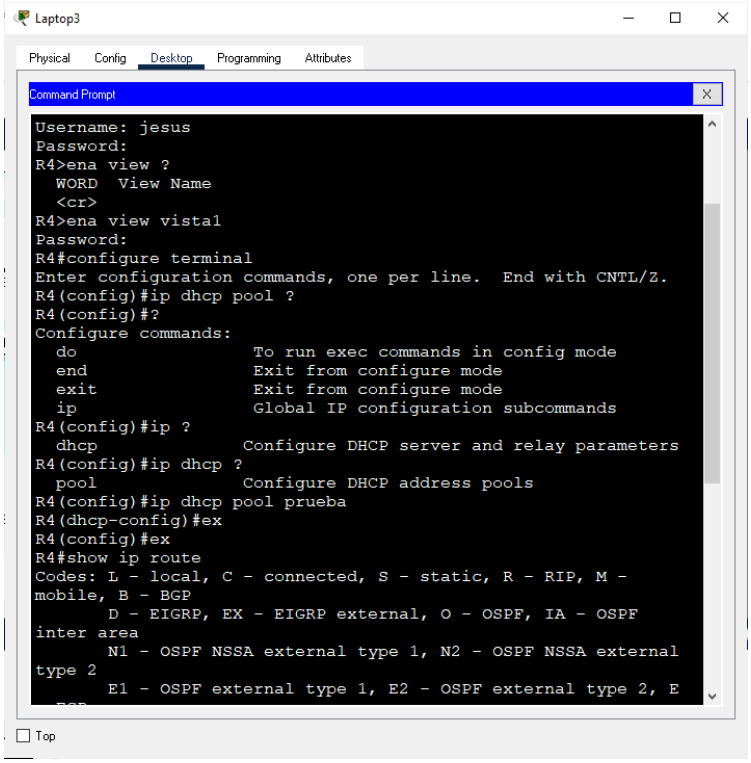
- **Comandos para la vista1 en el Router4**

```
parser view vista1
```

```
secret vista1
commands exec include configure terminal
commands exec include show ip route
commands configure include ip dhcp pool
exit
enable view vista1
```

En este caso, no se tiene que hacer nada más que entrar por medio de enable view y corroborar que se tienen los comandos configurados.

Comprobación



Se muestra en la imagen que se tiene la posibilidad de usar los comandos *configure terminal, ip dhcp pool* y *show ip route*

vista2

**clock set*

**show ip interface brief*

**show clock*

Se configuró a vista2 dando únicamente estos comandos, donde no se hereda nada de las demás vistas.

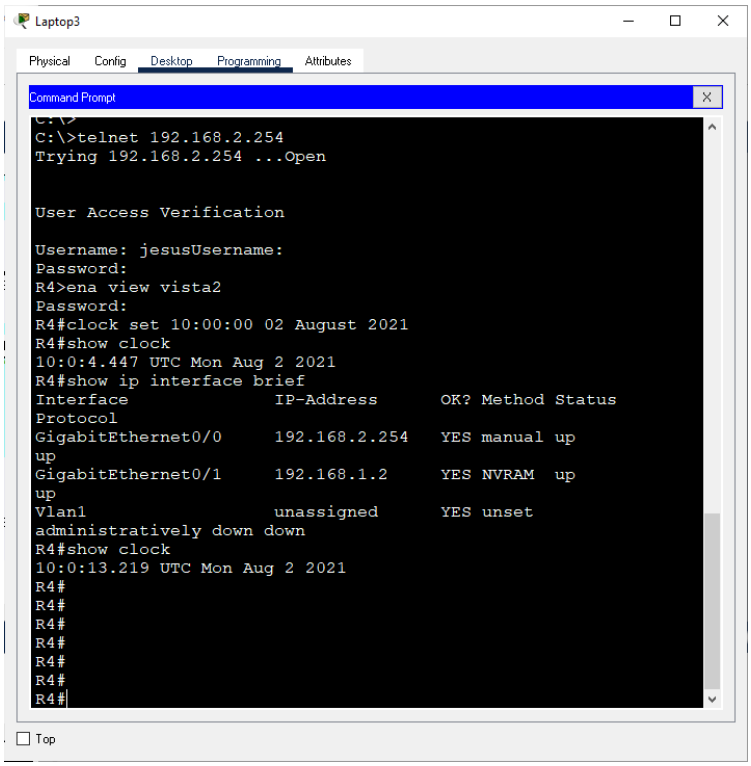
Configuración

- **Comandos para la vista2 en el Router4**

```
parser view vista2
secret vista2
commands exec include clock set
commands exec include show ip interface brief
commands exec include show clock
exit
enable view vista2
```

En este caso, no se tiene que hacer nada más que entrar por medio de enable view y corroborar que se tienen los comandos configurados.

Comprobación



Se muestra en la imagen que se tiene la posibilidad de usar los comandos *clock set, show ip interface brief* y *show clock.*

vista3

**show cdp neighbors*

**show version*

**ping*

Se configuró a vista3 dando únicamente estos comandos, donde no se hereda nada de las demás vistas.

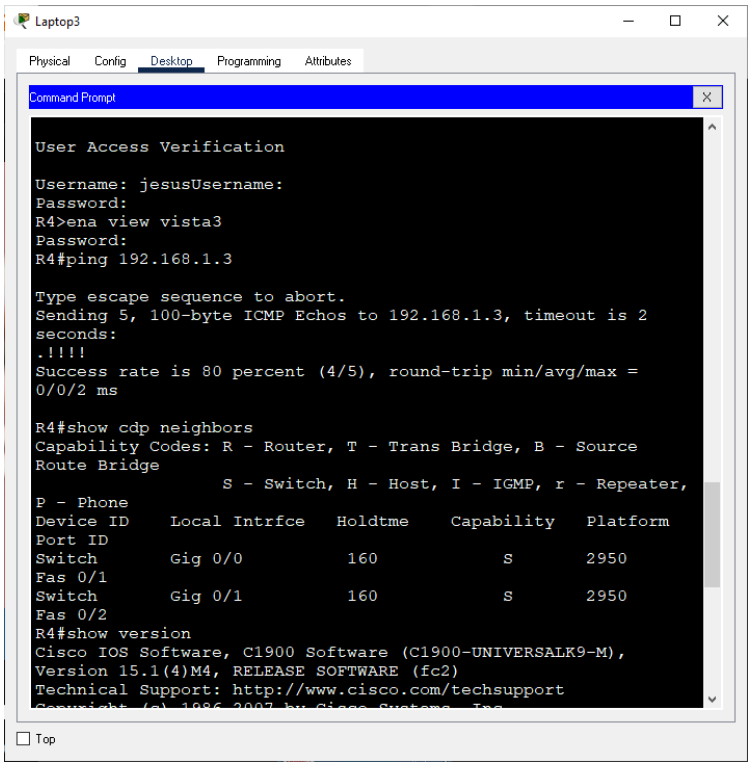
Configuración

- **Comandos para la vista3 en el Router4**

```
parser view vista3
secret vista3
commands exec include ping
commands exec include show cdp neighbors
commands exec include show versión
exit
enable view vista3
```

En este caso, no se tiene que hacer nada más que entrar por medio de enable view y corroborar que se tienen los comandos configurados.

Comprobación



Se muestra en la imagen que se tiene la posibilidad de usar los comandos *ping, show cdp neighbors, show version*

vista4

**configure terminal*

*logging host

*logging trap

Se configuró a vista1 dando únicamente estos comandos, donde no se hereda nada de las demás vistas.

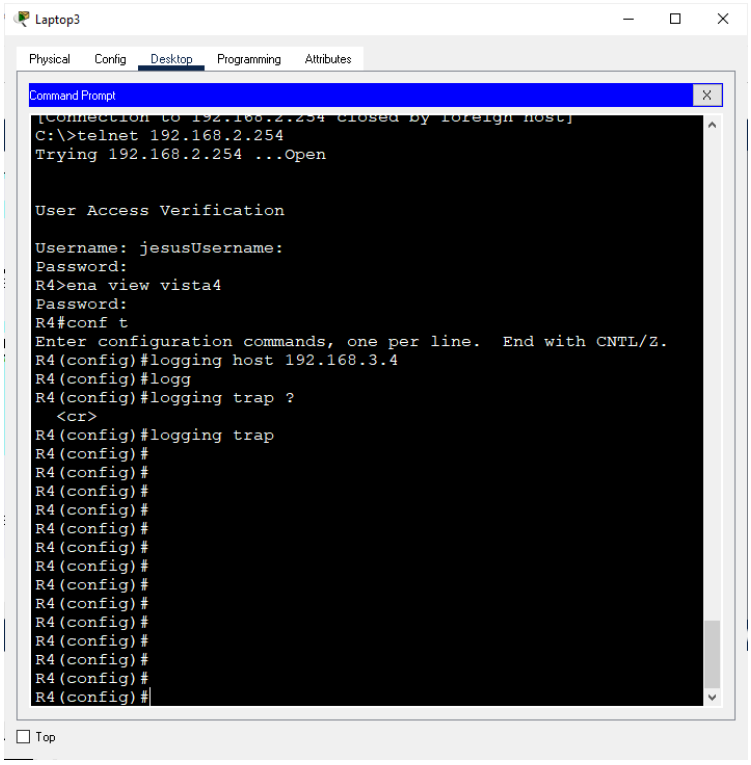
Configuración

- **Comandos para la vista4 en el Router4**

```
parser view vista4
secret vista4
commands exec include configure terminal
commands configure include logging host
commands configure include logging trap
exit
enable view vista4
```

En este caso, no se tiene que hacer nada más que entrar por medio de enable view y corroborar que se tienen los comandos configurados.

Comprobación



Se muestra en la imagen que se tiene la posibilidad de usar los comandos *configure terminal, logging host* y *logging trap*

3.-Colocar conclusión general del curso.

Me ha parecido un excelente curso a pesar de que hubo paro académico. Tener las clases grabadas y poder verlas en cualquier momento hacen más amena la enseñanza, ya que se puede repasar bastantes veces para poder tener un mejor aprendizaje. Además, las sesiones de dudas fueron de mucha ayuda con el fin de entender de una excelente manera los temas o para poder atender cualquier problema que se generan en las topologías que se debían realizar. Sin duda alguna es de las asignaturas que más he disfrutado aprender junto con Redes de Datos Seguras que cursé en semestres pasados justamente con usted.

Evaluación: feedback 2:

Simulación: 70%

Trabajo escrito: 30%