



Universidad Nacional Autónoma de México

Facultad de Ingeniería



División de Ingeniería Eléctrica

Laboratorio de Redes y Seguridad

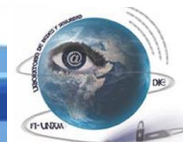
*CCNP ENCOR*

## **TOPOLOGÍA FINAL**

**Instructor:** Ing. José Antonio Macías García.

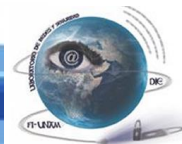
**Alumno:** Jiménez Juárez Jesús

JULIO 2021



## Índice

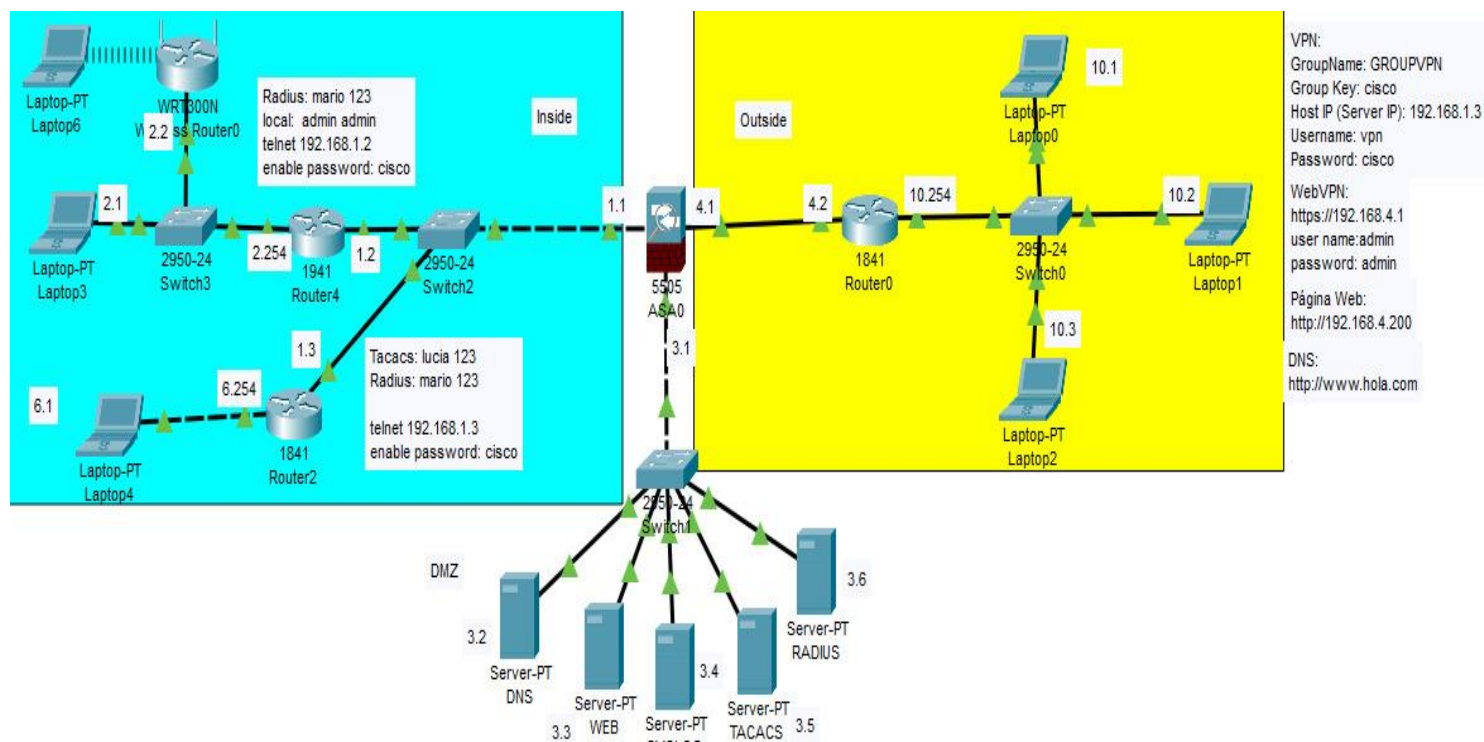
1.- Configurar lo siguiente:.....	2
2.-Adjuntar en este documento capturas de pantalla para la evidencia de cada configuración realizada y que está funcionando como se solicita.....	4
*Protocolo de enrutamiento libre. ....	4
*Acceso a R4 por Radius y de manera local .....	6
*Acceso a R2 por Tacacs y Radius .....	7
*Conexión de host a router inalámbrico por medio de Radius .....	10
*Configuración de zonas inside, outside y DMZ en ASA .....	12
*Configuración de webVPN para que los hosts de outside entren a la página web .....	14
*Acceso mediante VPN en Router2 para host de outside.....	16
*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. ....	18
*Servidor syslog funcionando (mandar mensajes desde cualquier dispositivo al servidor).....	20
*Configuración de un IPS en Router 4 denegando el ping .....	20
*Configuración de usuarios y vistas en Router 4: .....	22
Privilegios.....	22
usuario5 -> Nivel 5 de privilegios .....	22
usuario9 -> Nivel 9 de privilegios .....	23
usuario59 ->Nivel 15 de privilegios .....	24
usuario3 -> Nivel 3 de privilegios .....	25
usuario7 -> Nivel 7 de privilegios .....	26
usuario37 -> Nivel 15 de privilegios .....	27
Vistas.....	28
vista1.....	28
vista2.....	29
vista3.....	30
vista4.....	31
3.-Colocar conclusión general del curso.....	33



## TOPOLOGÍA FINAL CCNP

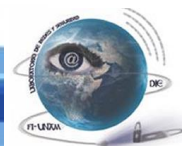
*Objetivo: Terminar la segunda parte del curso con conocimientos más sólidos de los temas vistos en el curso configurando la siguiente topología:*

*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](http://www.eselfingen21.com) aplicando NATeo estático con una IP virtual y colocando esa 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*

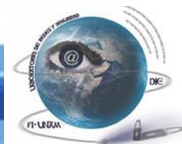
*\*ip dhcp pool*

*\*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**

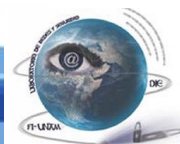
```
router rip
version 2
network 192.168.1.0
network 192.168.6.0
ex
```

- **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**



```
Laptop3
Physical Config Desktop Programming Attributes
Command Prompt
Packet Tracer PC Command Line 1.0
C:\>ping 192.168.6.1

Pinging 192.168.6.1 with 32 bytes of data:

Reply from 192.168.6.1: bytes=32 time<1ms TTL=126
Reply from 192.168.6.1: bytes=32 time<1ms TTL=126
Reply from 192.168.6.1: bytes=32 time=1ms TTL=126
Reply from 192.168.6.1: bytes=32 time=1ms TTL=126

Ping statistics for 192.168.6.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>
```

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

```
Laptop3
Physical Config Desktop Programming Attributes
Command Prompt
C:\>ping 192.168.10.2

Pinging 192.168.10.2 with 32 bytes of data:

Request timed out.
Request timed out.
Reply from 192.168.10.2: bytes=32 time=1ms TTL=125
Reply from 192.168.10.2: bytes=32 time<1ms TTL=125

Ping statistics for 192.168.10.2:
    Packets: Sent = 4, Received = 2, Lost = 2 (50% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
```

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.

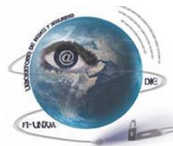
The screenshot shows the RADIUS configuration interface with the following details:

- Services:** AAA is selected in the left sidebar.
- AAA Configuration:**
  - Service: ☒ On ☐ Off
  - Radius Port: 1645
- Network Configuration:**

Client Name	Client IP	Server Type	Key
1 R4	192.168.1.2	Radius	cisco
2 R2	192.168.1.3	Radius	cisco2
3 CCNP	192.168.2.2	Radius	cisco
- User Setup:**

Username	Password
1 jesus	123
2 jimenez	pass123

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

The network diagram shows a topology with several devices including routers (R1, R2, R3, R4), switches (S1, S2, S3, S4), and servers (Server-PT-32, Server-PT-33, Server-PT-34, Server-PT-35, Server-PT-36). A user named 'jesus' is connected to a laptop. The terminal window shows the following commands and output:

```
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>telnet 192.168.1.2
Trying 192.168.1.2 ...Open

User Access Verification

Username: jesus
Password:
R4>
R4>
R4>
R4>
R4>
R4>
R4>
R4>
R4>
R4>
R4>
R4>
```

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

The network diagram shows the same topology as before. The terminal window shows the following commands and output:

```
C:\>
C:\>
C:\>
C:\>telnet 192.168.1.2
Trying 192.168.1.2 ...Open

User Access Verification

Username: local
Password:
R4>
R4>
R4>
R4>
R4>
R4>
R4>
R4>
R4>
R4>
R4>
R4>
```

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.

The screenshot shows the TACACS configuration window with the following details:

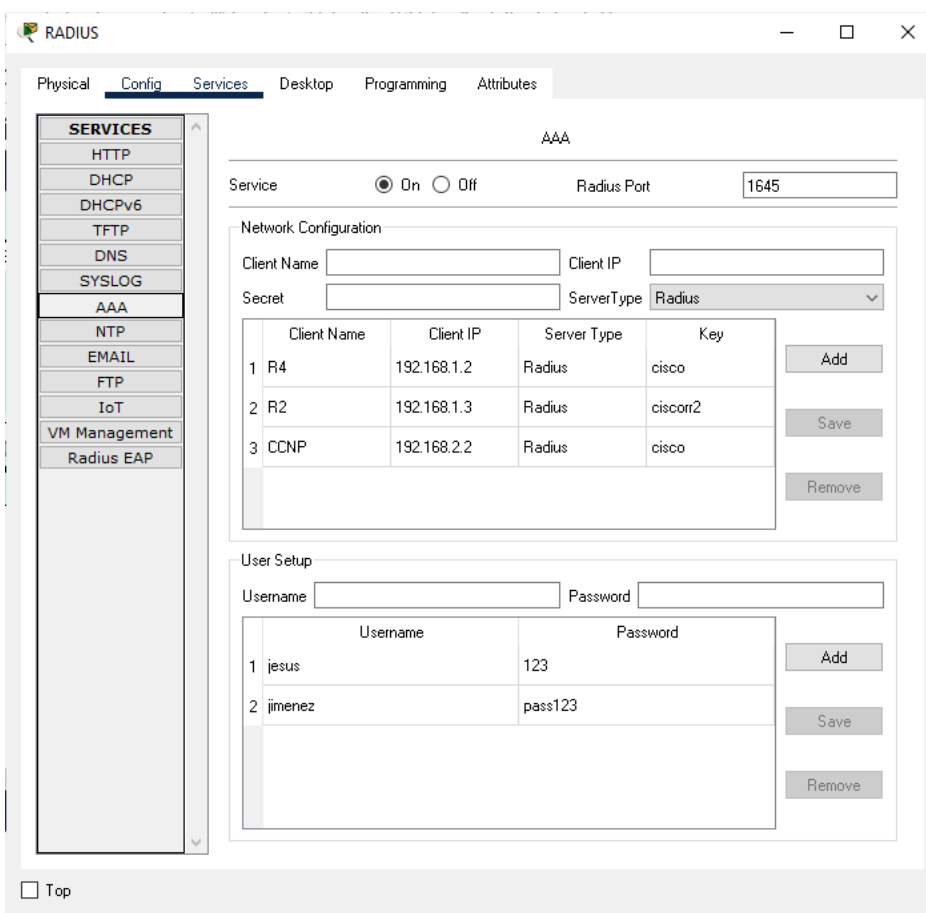
- Services Tab:** AAA is selected in the left sidebar.
- AAA Configuration:**
  - Service: ☒ On ☐ Off
  - Radius Port: 1645
- Network Configuration:**
  - Client Name:
  - Client IP:
  - Secret:
  - ServerType: Radius (dropdown)
  - Table:

	Client Name	Client IP	Server Type	Key
1	R2	192.168.1.3	Tacacs	ciscotr2
- User Setup:**
  - Username:
  - Password:
  - Table:

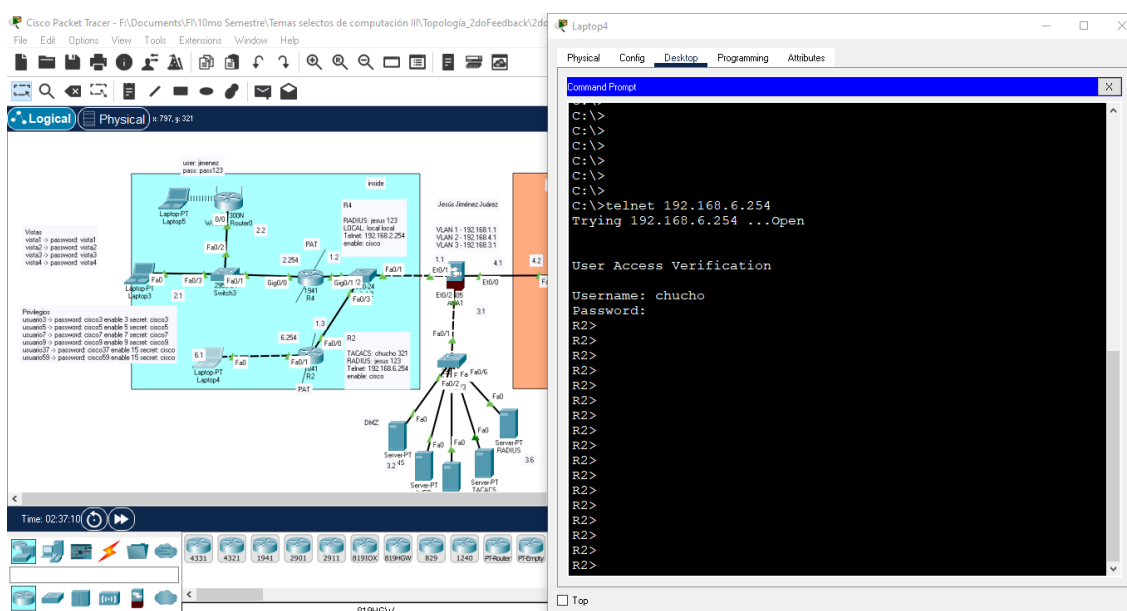
	Username	Password
1	chucho	321

- **Configuración en servidor Radius**

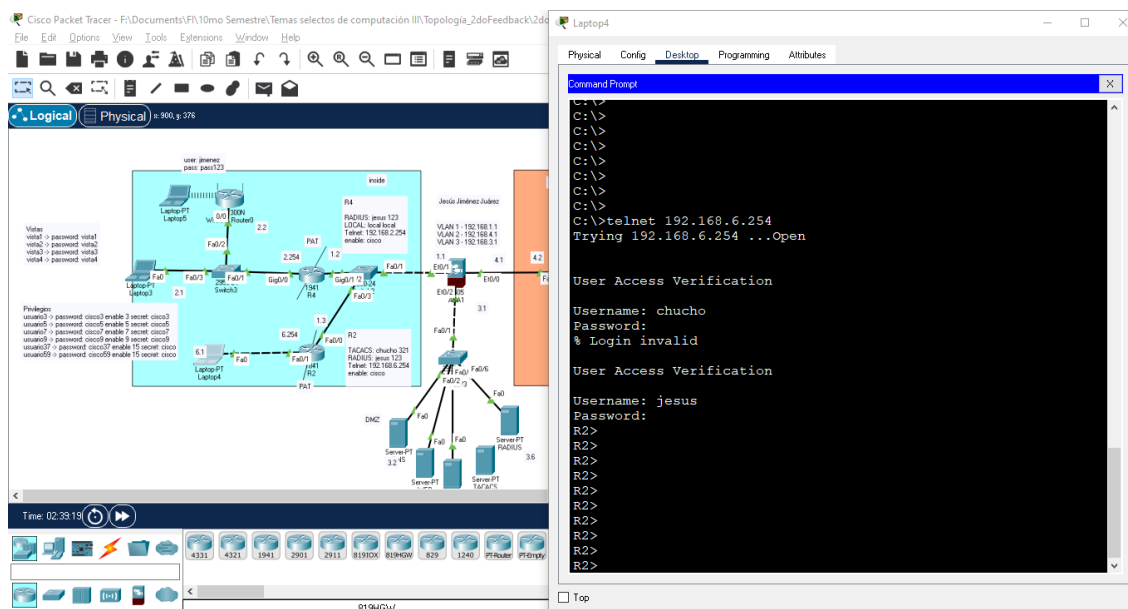
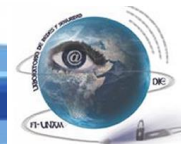
Hay que mencionar que se configuró con el *Client Name* R2 y el usuario que se usa es el de *jesus* con contraseña 123.



## Comprobación



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



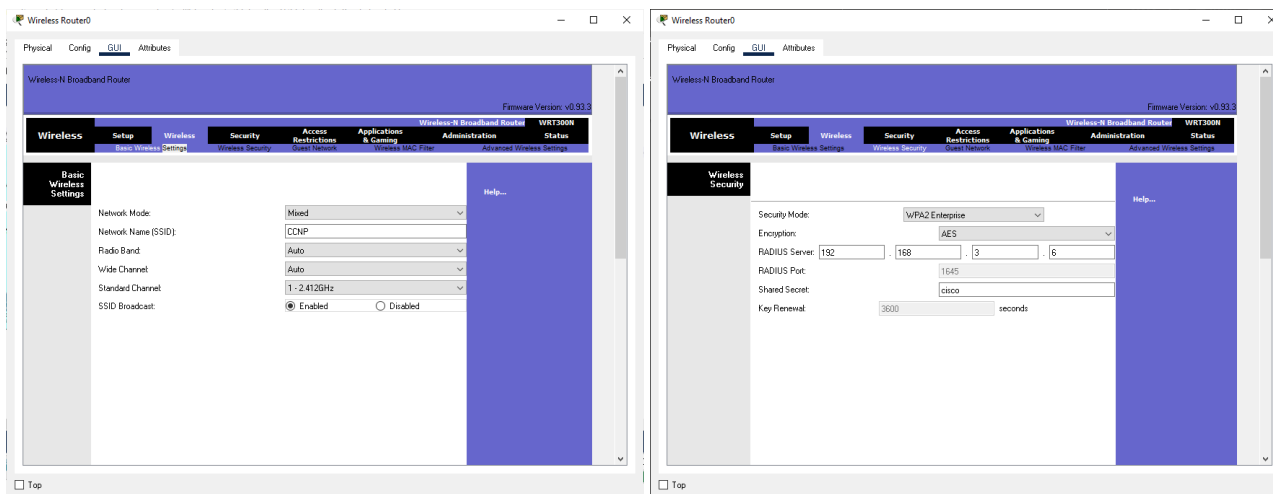
Realizando la conexión de Telnet autenticando con Radius (Usuario: *jesus* Pass: 123).

### \*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.

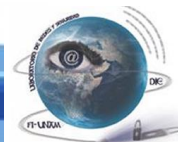
### Configuración

- 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*.



**RADIUS**

Physical **Config** Services Desktop Programming Attributes

**SERVICES**

- HTTP
- DHCP
- DHCPv6
- TFTP
- DNS
- SYSLOG
- AAA**
- NTP
- EMAIL
- FTP
- IoT
- VM Management
- Radius EAP

AAA

Service ☒ On ☐ Off Radius Port 1645

Network Configuration

Client Name  Client IP

Secret  Server Type Radius

	Client Name	Client IP	Server Type	Key	
1	R4	192.168.1.2	Radius	cisco	Add
2	R2	192.168.1.3	Radius	cisco2	Save
3	CCNP	192.168.2.2	Radius	cisco	Remove

User Setup

Username  Password

	Username	Password	
1	jesus	123	Add
2	jimenez	pass123	Save

☐ Top

- Configuración de laptop5 para conectarse al Router Inalámbrico.

**Laptop5**

Physical Config **Desktop** Programming Attributes

**Creating a Profile**

**Wireless Security - WPA2 Enterprise**

Authentication PEAP Please select the authentication method that you use to access your network.

Login Name jimenez Enter the Login Name used for authentication.

Password \*\*\*\*\* Enter the Password used for authentication.

Server Name Enter the Server Name used for authentication. (Optional)

Certificate Trust Any Please select the certificate used for authentication.

Inner Authen: TOKEN CARD Please select the inner authentication method used inside the PEAP tunnel.

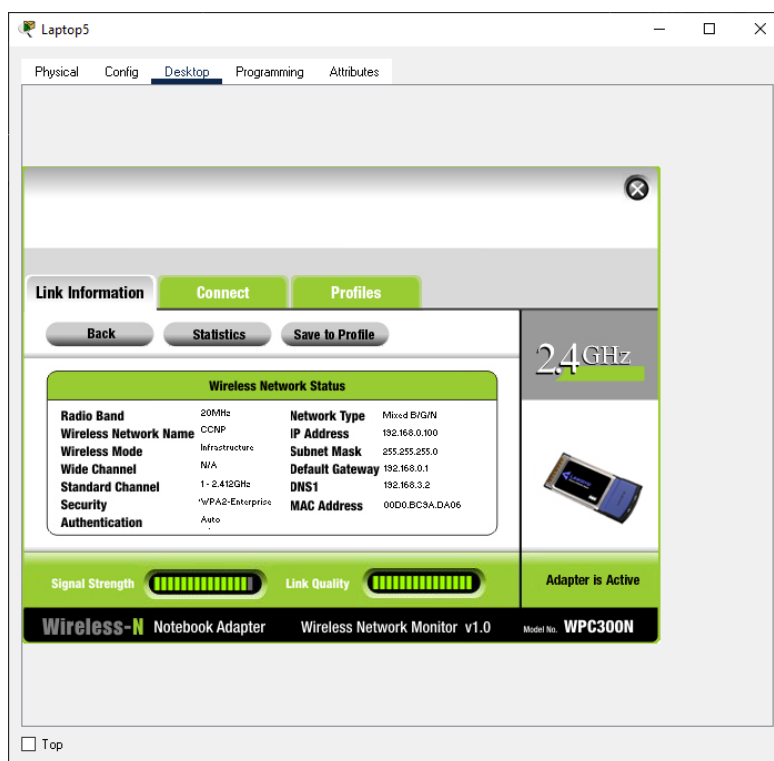
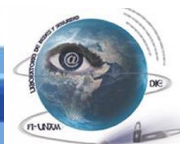
[Back](#) [Next](#)

**Wireless-N** Notebook Adapter Wireless Network Monitor v 1.11 Model No. WPC300N

☐ Top

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 necesita 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
```

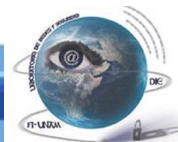
- **Comandos en el Router4**

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





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

The left screenshot shows the 'Bookmark Manager' configuration page. It has a table with columns 'Bookmark Title' and 'URL'. One entry is 'SITIO' with URL 'https://192.168.3.3'. Below the table are 'Add' and 'Remove' buttons. The right screenshot shows the 'User Manager' configuration page. It has fields for 'Username' (admin), 'Bookmark' (SITIO), 'Profile Name' (ACCESO), and 'Group Policy' (POLITICA). Below these is a 'Users' table with columns 'Username', 'Bookmark', 'Profile Name', and 'Group Policy'. One entry is 'admin', 'SITIO', 'ACCESO', 'POLITICA'. Both screenshots include a 'Equivalent ASA Commands' section at the bottom.

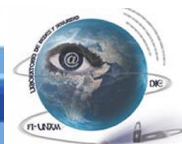
- Configuración en el servidor DNS

The screenshot shows the DNS configuration interface. The 'DNS Service' is turned 'On'. The 'Resource Records' section shows a table with columns 'No.', 'Name', 'Type', and 'Detail'. Two entries are listed: '0' for 'www.eselinger21.com' (A Record, 192.168.3.2) and '1' for 'www.hola.com' (A Record, 192.168.3.3). There are 'Add', 'Save', and 'Remove' buttons above the table. A 'DNS Cache' button is at the bottom.

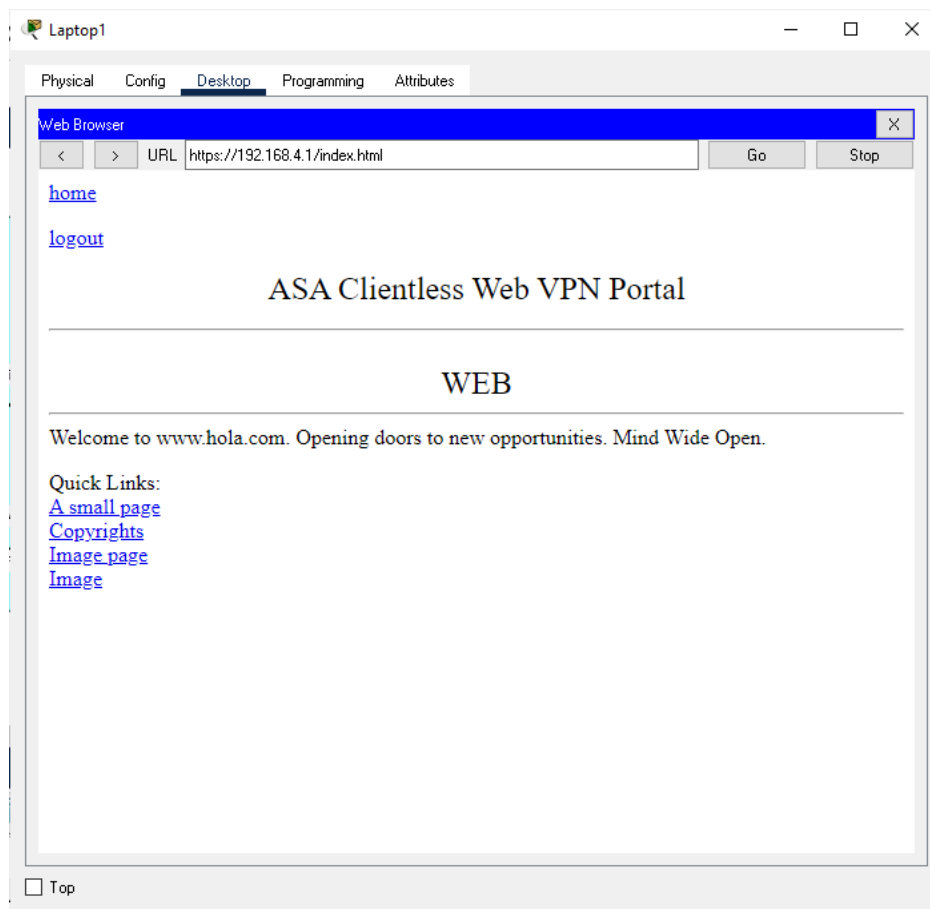
Se realizó desde uno de los hosts de la zona outside, se ingresaron los datos correspondientes para que pudiera corroborarse que se realizó la configuración de manera adecuada.

## 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.

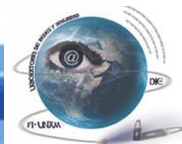
### \*Acceso mediante VPN en Router2 para host de outside

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**

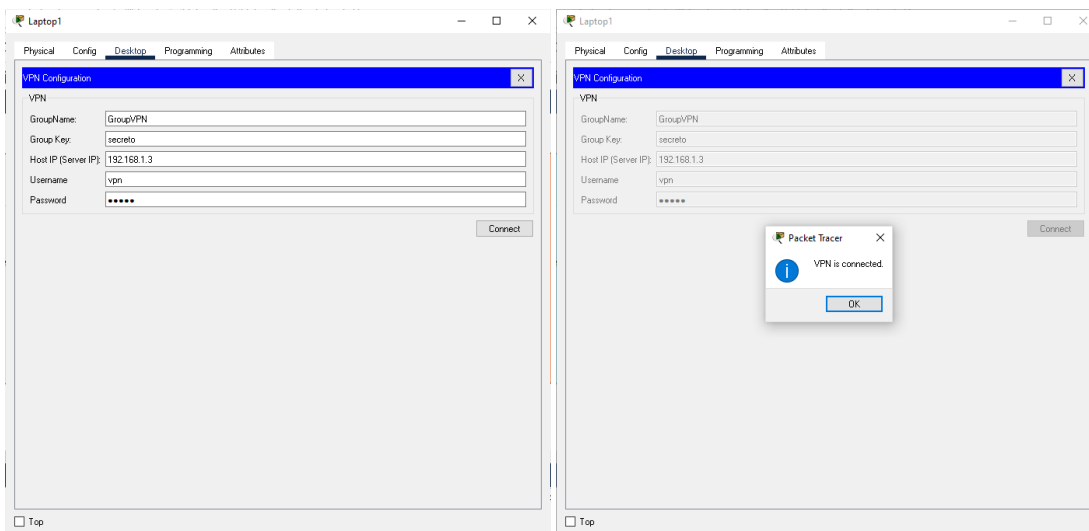
```
aaa new-model
aaa authentication login VPNUSER local
aaa authorization network GroupVPN local
username vpn secret cisco
crypto isakmp policy 10
encryption aes
```

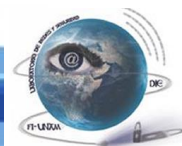


```
authentication pre-share
group 5
exit
crypto isakmp client configuration group GroupVPN
key secreto
pool POOLVPN
exit
ip local pool POOLVPN 192.168.6.10 192.168.6.20
crypto ipsec transform-set VPNSET esp-aes esp-sha-hmac
crypto dynamic-map VPNDINAMIC 10
set transform-set VPNSET
reverse-route
crypto 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.

```
Packet Tracer PC Command Line 1.0
C:\>ping 192.168.6.1

Pinging 192.168.6.1 with 32 bytes of data:

Request timed out.
Reply from 192.168.1.3: bytes=32 time=1ms TTL=127
Reply from 192.168.1.3: bytes=32 time=2ms TTL=127
Reply from 192.168.1.3: bytes=32 time=2ms TTL=127

Ping statistics for 192.168.6.1:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 2ms, Average = 1ms

C:\>
```

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](http://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](http://www.eselfingen21.com) para que pudiese funcionar, esté se encuentra activada en el servidor DNS.

### Configuración

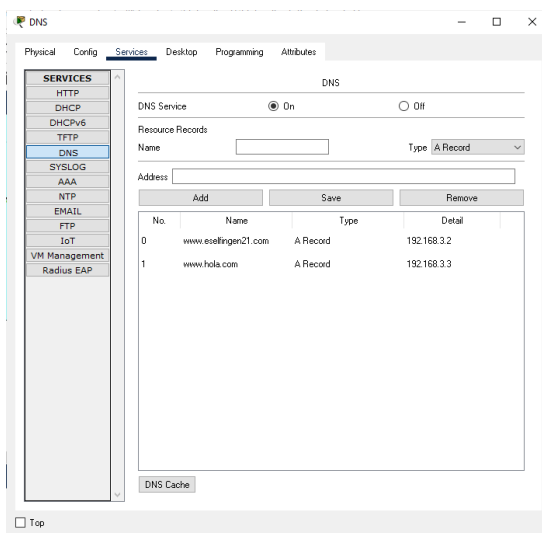
- **Comandos para el dispositivo ASA**

```
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
```



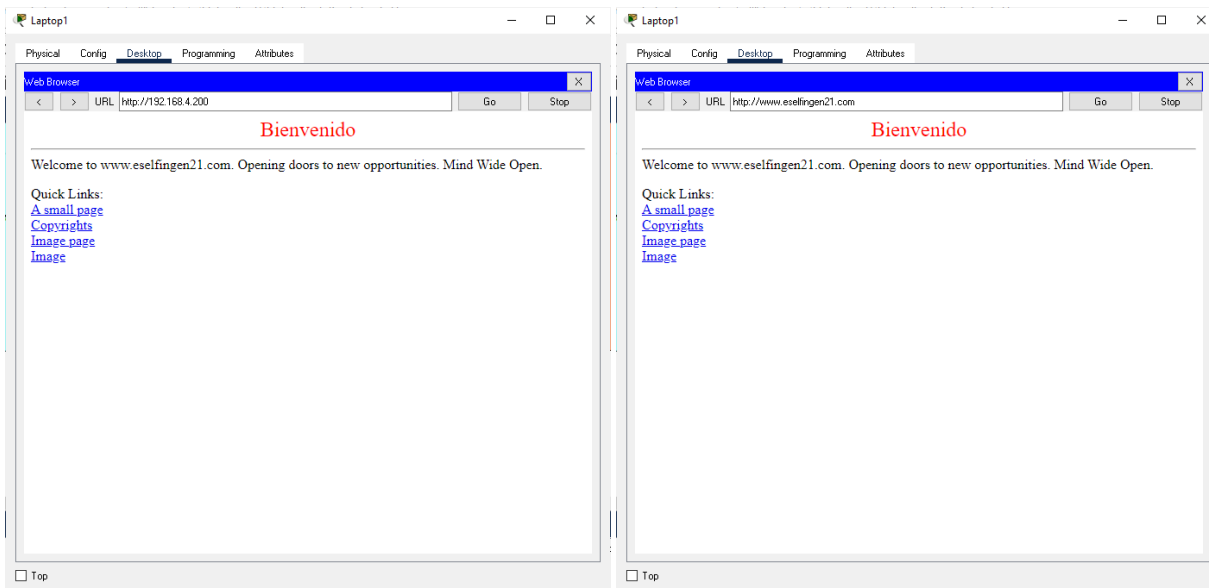
```
access-list ACL1 extended permit tcp any any
access-list ACL1 extended permit udp any any
access-group ACL1 in interface outside
object network OBJ1
host 192.168.3.2
nat (DMZ, outside) static 192.168.4.200
```

- **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](http://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

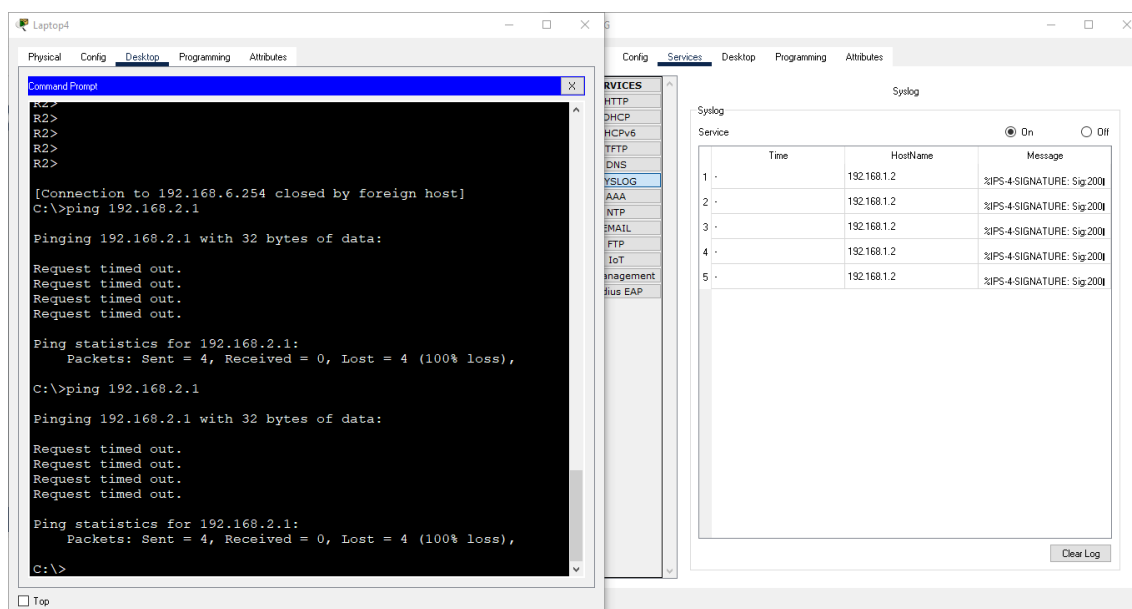
- **Comandos en cualquier Router y Switch.**

```
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

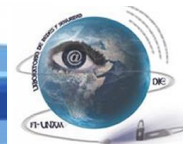
- **Comandos en el router 4**

```
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
```

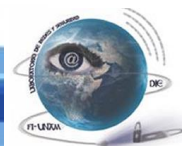
```
event-action produce-alert
```

```
event-action deny-packet-inline
```

```
exit
```

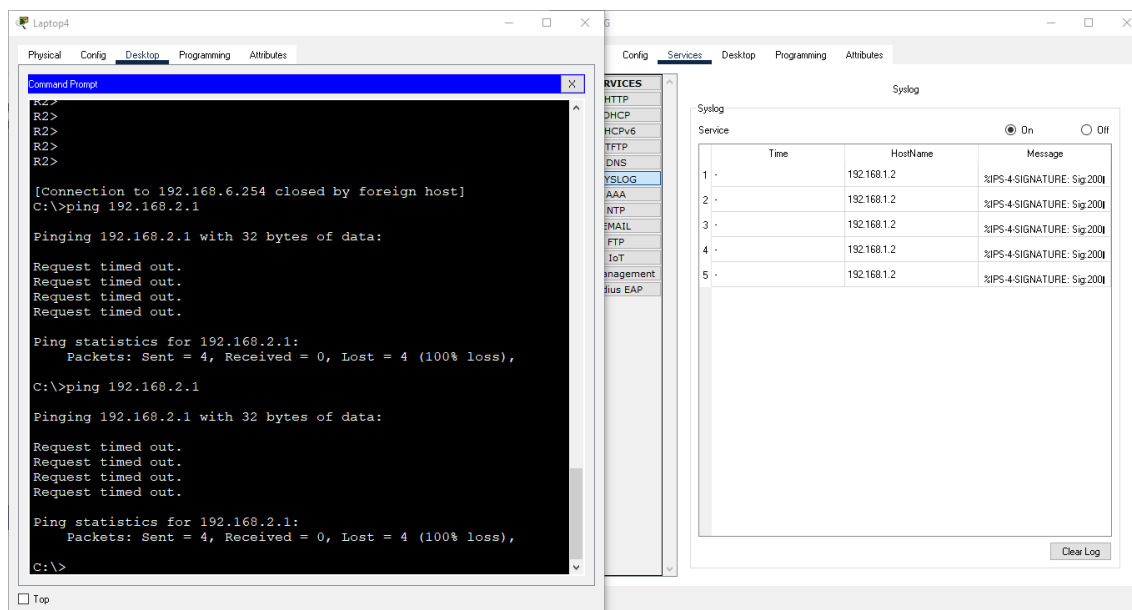
```
exit
```

```
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.

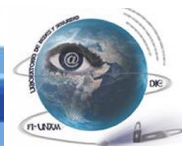
### **Configuración**

- **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

```
Laptop3
Physical Config Desktop Programming Attributes
Command Prompt
R4>
R4>
R4>

[Connection to 192.168.1.2 closed by foreign host]
C:\>telnet 192.168.2.254
Trying 192.168.2.254 ...Open

User Access Verification

Username: usuario5
Password:
R4>ena 5
Password:
R4#ping 192.168.1.3

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.3, timeout is 2
seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max =
0/2/10 ms

R4#configure terminal
^
% Invalid input detected at '^' marker.

R4#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R4(config)#hostname R4
R4(config)#
```

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*

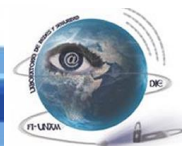
*\*ip address*

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

```
Command Prompt
R4>ena 9
Password:
R4#show run
Building configuration...

Current configuration : 4018 bytes
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname R4
!
!
!
enable secret level 3 5 $1$mERr$DDLxXz1ZSsG6Xb6b90AHH/
enable secret level 5 5 $1$mERr$nrXLk6/txaEMw2jKDY91t0
enable secret level 7 5 $1$mERr$Z2JG8atj8vil2FZFhpN2W/
enable secret level 9 5 $1$mERr$dPDvDSX8ugCmsfq7wqE5o0
enable secret 5 $1$mERr$hX5rVt7rPNoS4wqbXKX7m0
!
!
!
ip dhcp pool Prueba

R4oconf t
Enter configuration commands, one per line. End with CNTL/Z.
R4(config)#interface giga0/0
R4(config-if)#ip address 192.168.2.254
% Incomplete command.
R4(config-if)#
```

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

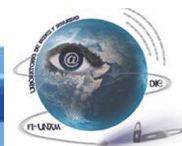
usuario59 -> Nivel 15 de privilegios

*\*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

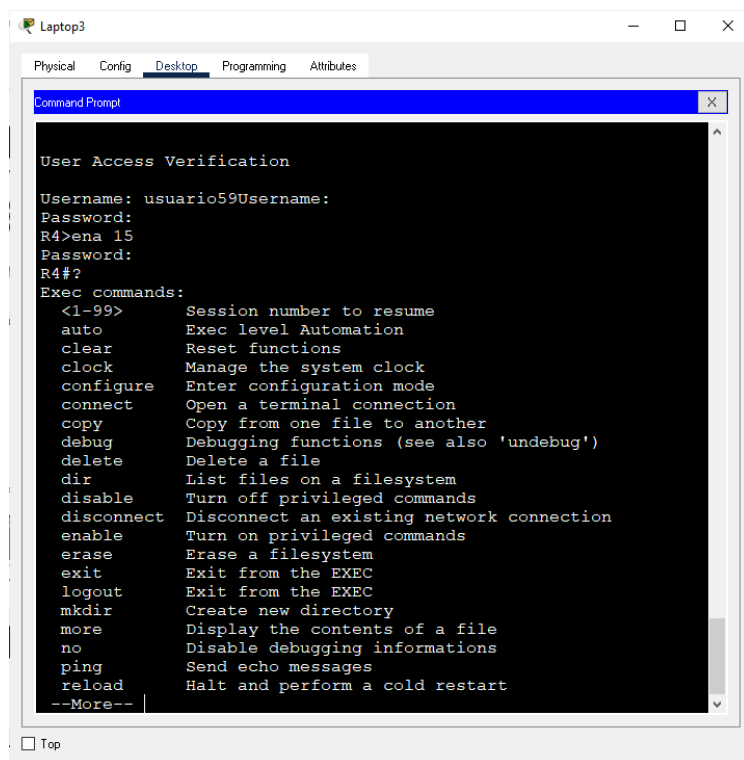


```
username usuario59 privilege 15 secret cisco59
```

```
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*

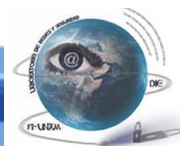
*\*show privilege*

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

```
Command Prompt
Username: usuario3
Password:
R4>ena 3
Password:
R4#show privilege
Current privilege level is 3
R4#show ip route
Codes: L - local, 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, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 192.168.1.1 to network 0.0.0.0

 192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
   C   192.168.1.0/24 is directly connected, GigabitEthernet0/1
   L   192.168.1.2/32 is directly connected, GigabitEthernet0/1
 192.168.2.0/24 is variably subnetted, 2 subnets, 2 masks
   C   192.168.2.0/24 is directly connected, GigabitEthernet0/0
   L   192.168.2.254/32 is directly connected, GigabitEthernet0/0
   S   192.168.6.0/24 [1/0] via 192.168.1.3
   S*  0.0.0.0/0 [1/0] via 192.168.1.1

R4#show running
Building configuration...

Current configuration : 4018 bytes
```

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

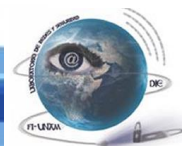
*\*configure terminal*

*\*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

```
Laptop3
Physical Config Desktop Programming Attributes
Command Prompt
R4#exit
[Connection to 192.168.2.254 closed by foreign host]
C:\>telnet 192.168.2.254
Trying 192.168.2.254 ...Open

User Access Verification

Username: usuario7Username:
Password:
R4>ena 7
Password:
R4#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R4(config)#router rip
R4(config-router)#?
    exit                Exit from routing protocol configuration
    mode
    network             Enable routing on an IP network
    no                  Negate a command or set its defaults
R4(config-router)#
R4(config-router)#
R4(config-router)#
R4(config-router)#
R4(config-router)#
R4(config-router)#
R4(config-router)#
R4(config-router)#
R4(config-router)#
R4(config-router)#
R4(config-router)#
```

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

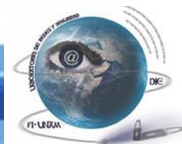
usuario37 -> Nivel 15 de privilegios

**\*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**

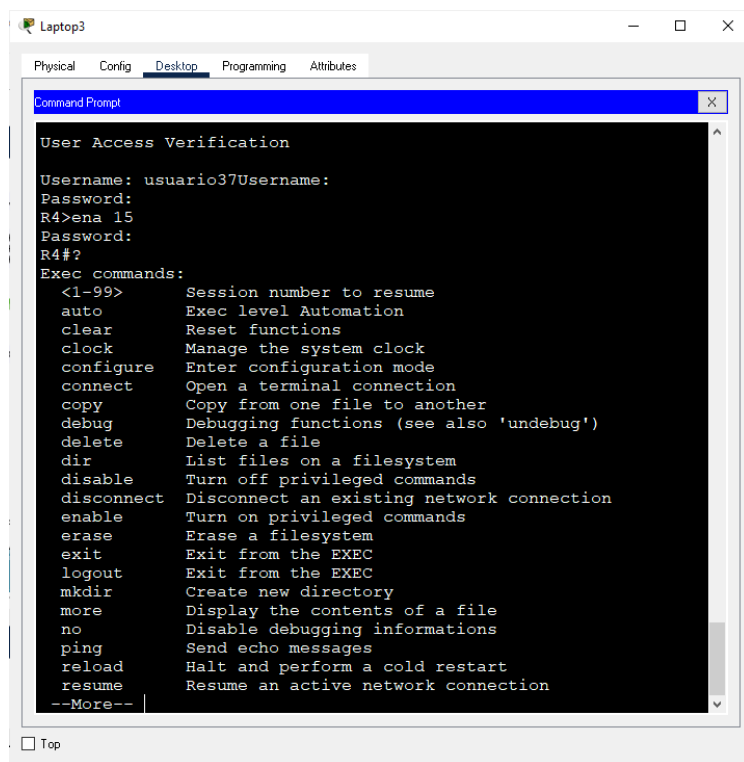


```
username usuario37 privilege 15 secret cisco37
```

```
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*

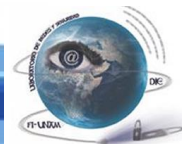
*\*show ip route*

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

```
Command Prompt  
Username: jesus  
Password:  
R4>ena view ?  
WORD View Name  
<cr>  
R4>ena view vista1  
Password:  
R4#configure terminal  
Enter configuration commands, one per line. End with CNTL/Z.  
R4(config)#ip dhcp pool ?  
R4(config)#?  
Configure commands:  
do To run exec commands in config mode  
end Exit from configure mode  
exit Exit from configure mode  
ip Global IP configuration subcommands  
R4(config)#ip ?  
dhcp Configure DHCP server and relay parameters  
R4(config)#ip dhcp ?  
pool Configure DHCP address pools  
R4(config)#ip dhcp pool prueba  
R4(dhcp-config)#ex  
R4(config)#ex  
R4#show ip route  
Codes: L - local, 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, E
```

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

```
Laptop3
Physical Config Desktop Programming Attributes
Command Prompt
C:\>telnet 192.168.2.254
Trying 192.168.2.254 ...Open

User Access Verification

Username: jesusUsername:
Password:
R4>ena view vista2
Password:
R4#clock set 10:00:00 02 August 2021
R4#show clock
10:0:4.447 UTC Mon Aug 2 2021
R4#show ip interface brief
Interface          IP-Address      OK? Method Status
Protocol
GigabitEthernet0/0  192.168.2.254   YES manual up
up
GigabitEthernet0/1  192.168.1.2     YES NVRAM  up
up
Vlan1               unassigned      YES unset
administratively down down
R4#show clock
10:0:13.219 UTC Mon Aug 2 2021
R4#
R4#
R4#
R4#
R4#
R4#
```

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

```
Laptop3
Physical Config Desktop Programming Attributes
Command Prompt
User Access Verification
Username: jesusUsername:
Password:
R4>ena view vista3
Password:
R4#ping 192.168.1.3

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.3, timeout is 2
seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max =
0/0/2 ms

R4#show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source
Route Bridge
                S - Switch, H - Host, I - IGMP, r - Repeater,
P - Phone
Device ID      Local Intrfce  Holdtme    Capability  Platform
Port ID
Switch         Gig 0/0        160        S           2950
Fas 0/1
Switch         Gig 0/1        160        S           2950
Fas 0/2

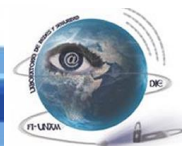
R4#show version
Cisco IOS Software, C1900 Software (C1900-UNIVERSALK9-M),
Version 15.1(4)M4, RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2007 by Cisco Systems, Inc.
```

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.

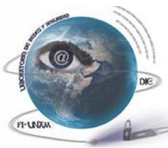
### Comprobación

```
Laptop3
Physical Config Desktop Programming Attributes
Command Prompt
[connection to 192.168.2.254 closed by foreign host]
C:\>telnet 192.168.2.254
Trying 192.168.2.254 ...Open

User Access Verification

Username: jesusUsername:
Password:
R4>ena view vista4
Password:
R4#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R4(config)#logging host 192.168.3.4
R4(config)#logg
R4(config)#logging trap ?
<cr>
R4(config)#logging trap
R4(config)#
R4(config)#
R4(config)#
R4(config)#
R4(config)#
R4(config)#
R4(config)#
R4(config)#
R4(config)#
R4(config)#
R4(config)#
R4(config)#
```

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%*