Eje 3: Implementando Soluciones de Seguridad en Router

Melqui A. Romero y

Karolaine Z. Villero

Fundación Universitaria del Área Andina

Facultad De Ingeniería y Ciencias Básicas, Ingeniería en Sistemas,

Seguridad en Redes

Ing. Ricardo A. López Bulla

02 de marzo del 2025

1. Introducción

La seguridad en redes es un aspecto esencial en el diseño y administración de infraestructuras tecnológicas. En la actualidad, las redes son cada vez más complejas y vulnerables a ataques que buscan comprometer la confidencialidad, integridad y disponibilidad de la información. Por ello, la implementación de protocolos y herramientas adecuadas resulta fundamental para garantizar la protección de la red.

En este documento se desarrollará la configuración de routers utilizando el protocolo OSPF (Open Shortest Path First) con autenticación, así como la implementación de Listas de Control de Acceso (ACL) para filtrar el tráfico no deseado. La finalidad es asegurar el acceso a los dispositivos y proteger la red contra amenazas externas, brindando así una infraestructura más robusta y confiable para la comunicación de datos (Lopez, 2025)

Tabla de contenido

2. Tabla de Figuras

3. Seguridad de Routers

La seguridad en redes es un aspecto fundamental que abarca diversas técnicas y herramientas diseñadas para proteger la integridad, confidencialidad y disponibilidad de la información transmitida a través de la red. Los routers desempeñan un papel esencial en la seguridad al actuar como dispositivos que regulan el tráfico que entra y sale de la red. Las medidas de seguridad implementadas en estos dispositivos deben ser adecuadas para prevenir accesos no autorizados y garantizar la comunicación segura entre los dispositivos conectados.

Protocolo OSPF (Open Shortest Path First): OSPF es un protocolo de enrutamiento de estado de enlace que se utiliza principalmente en redes grandes y complejas debido a su capacidad para calcular rutas óptimas basadas en la menor métrica de costo. La autenticación en OSPF garantiza que sólo dispositivos autorizados puedan participar en el proceso de intercambio de información de enrutamiento, evitando ataques como la falsificación de rutas. Este protocolo es fundamental en la implementación de redes seguras, ya que su configuración adecuada permite garantizar la confiabilidad de las rutas establecidas (Netseccloud, 2025)

SSH (Secure Shell): El protocolo SSH se utiliza para asegurar la administración remota de dispositivos de red. A diferencia de Telnet, que transmite datos en texto plano, SSH proporciona un canal seguro que encripta toda la comunicación entre el cliente y el servidor. La autenticación se realiza mediante credenciales o certificados, y la integridad de la conexión se garantiza mediante el uso de algoritmos criptográficos avanzados (Microsoft Corporation. , s.f.)

Listas de Control de Acceso (ACL): Las ACL son un conjunto de reglas que permiten o deniegan el tráfico en función de criterios como direcciones IP, protocolos y puertos. Las ACL estándar se utilizan principalmente para filtrar tráfico basándose únicamente en la dirección IP de origen, mientras que las ACL extendidas permiten especificar múltiples criterios, como el tipo de tráfico (HTTP, ICMP, etc.) y la dirección IP de destino. Implementar ACL adecuadas contribuye significativamente a la protección de la red al restringir el acceso no autorizado y minimizar posibles ataques (QNAP, s.f.)

Importancia de la Seguridad en Redes: La seguridad en redes se fundamenta en la implementación de políticas adecuadas que aseguren el acceso autorizado y protejan la infraestructura contra posibles amenazas. El uso de protocolos seguros como OSPF con autenticación y SSH para acceso remoto contribuye a fortalecer la protección de la red. Además, las ACL desempeñan un papel crucial al definir reglas que permiten o bloquean ciertos tipos de tráfico, mejorando así la seguridad de la red (Lopez, 2025)

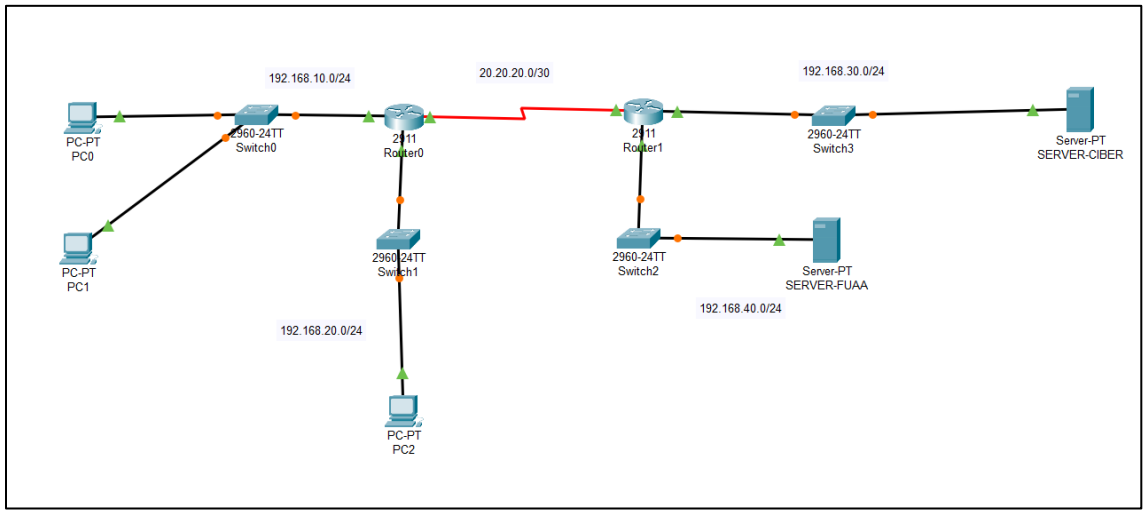
4. Diseñar e implementar la configuración básica del router.

Se configuro los routers para mejorar la protección de la red y los datos, verificando la seguridad, al asignarle contraseña y que autentifique con las bases de datos a cada usuario, enviando un mensaje de advertencia, con máximo 2 intentos de autentificación y midiendo el tiempo de inactividad el cual tiene como límite 90 segundos, gracias a configurar el acceso remoto SSH, las llaves y la configuración de la línea VTY 0 4, se comprobaran con el acceso remoto de SSH.

Figura 1 Tabla de direccionamiento
Con esta tabla implementaremos el Packet Tracer

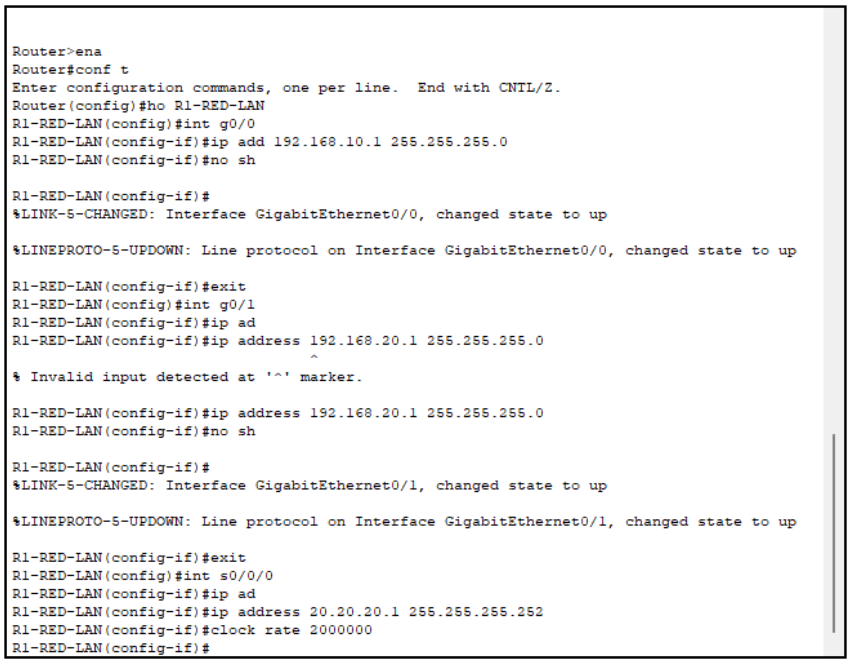
Dispositivo	Interfaz	Dirección IP	Máscara	Gateway
R1-RED-LAN	G0/0/0	192.168.10.1	255.255.255.0	N/A
	G0/0/1	192.168.20.1	255.255.255.0	N/A
	S0/1/0	20.20.20.1	255.255.255.252	N/A
R2-SERVER	S0/1/0	20.20.20.2	255.255.255.252	N/A
	G0/0/0	192.168.30.1	255.255.255.0	N/A
	G0/0/1	192.168.40.1	255.255.255.252	N/A
Server-CiberSax	NIC	192.168.30.2	255.255.255.0	192.168.30.1
Server-FUAA	NIC	192.168.40.2	255.255.255.0	192.168.40.1
PC0	NIC	192.168.10.10	255.255.255.0	192.168.10.1
PC1	NIC	192.168.10.11	255.255.255.0	192.168.10.1
PC6	NIC	192.168.20.10	255.255.255.0	192.168.20.1

Figura 2 Ejercicio Packet Tracer
Ejercicio realizado y ejecutado en Packet Tracer



Ahora configuremos los parámetros básicos del router, iniciando con asignarle los nombres con la tabla de direccionamiento:

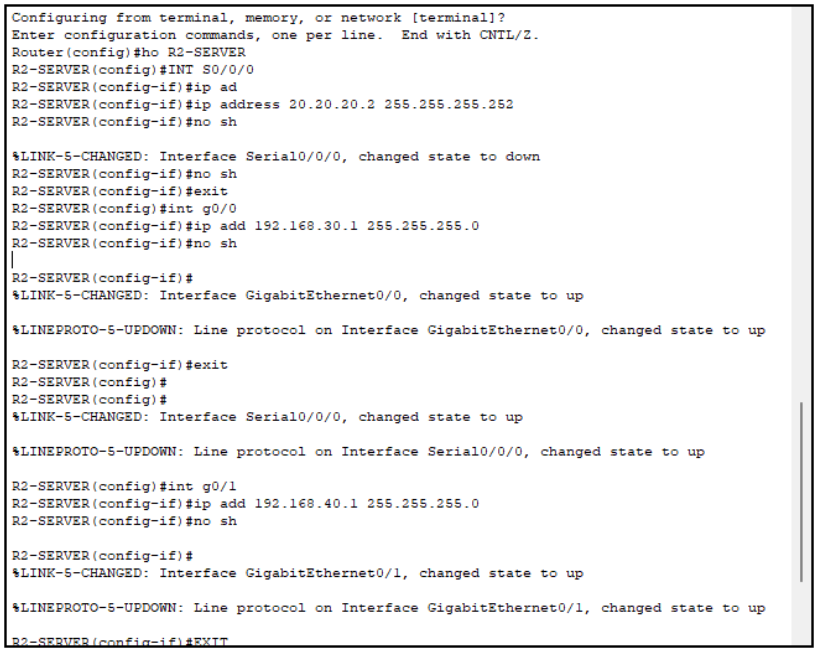
Figura 3 Configuración Router 1
Nombre del servidor y configuración de las redes del servidor que son: G0/0 - G0/1 - S0/0/0



```
Router>ena
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#ho R1-RED-LAN
R1-RED-LAN(config)#int g0/0
R1-RED-LAN(config-if)#ip add 192.168.10.1 255.255.255.0
R1-RED-LAN(config-if)#no sh

R1-RED-LAN(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to up

R1-RED-LAN(config-if)#exit
R1-RED-LAN(config)#int g0/1
R1-RED-LAN(config-if)#ip ad
R1-RED-LAN(config-if)#ip address 192.168.20.1 255.255.255.0
                                  ^
% Invalid input detected at '^' marker.

R1-RED-LAN(config-if)#ip address 192.168.20.1 255.255.255.0
R1-RED-LAN(config-if)#no sh

R1-RED-LAN(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to up

R1-RED-LAN(config-if)#exit
R1-RED-LAN(config)#int s0/0/0
R1-RED-LAN(config-if)#ip ad
R1-RED-LAN(config-if)#ip address 20.20.20.1 255.255.255.252
R1-RED-LAN(config-if)#clock rate 2000000
R1-RED-LAN(config-if)#
```

Figura 4 Configuración Router 2

nombre del servidor y configuración de las redes del servidor que son: G0/0 - G0/1 - S0/0/0



```
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#ho R2-SERVER
R2-SERVER(config)#INT S0/0/0
R2-SERVER(config-if)#ip ad
R2-SERVER(config-if)#ip address 20.20.20.2 255.255.255.252
R2-SERVER(config-if)#no sh

%LINK-5-CHANGED: Interface Serial0/0/0, changed state to down
R2-SERVER(config-if)#no sh
R2-SERVER(config-if)#exit
R2-SERVER(config)#int g0/0
R2-SERVER(config-if)#ip add 192.168.30.1 255.255.255.0
R2-SERVER(config-if)#no sh

R2-SERVER(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to up

R2-SERVER(config-if)#exit
R2-SERVER(config)#
R2-SERVER(config)#
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up

R2-SERVER(config)#int g0/1
R2-SERVER(config-if)#ip add 192.168.40.1 255.255.255.0
R2-SERVER(config-if)#no sh

R2-SERVER(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to up

R2-SERVER(config-if)#EXIT
```

Figura 5 Configuración servidor 1
Cibersax la Ip y default Gateway

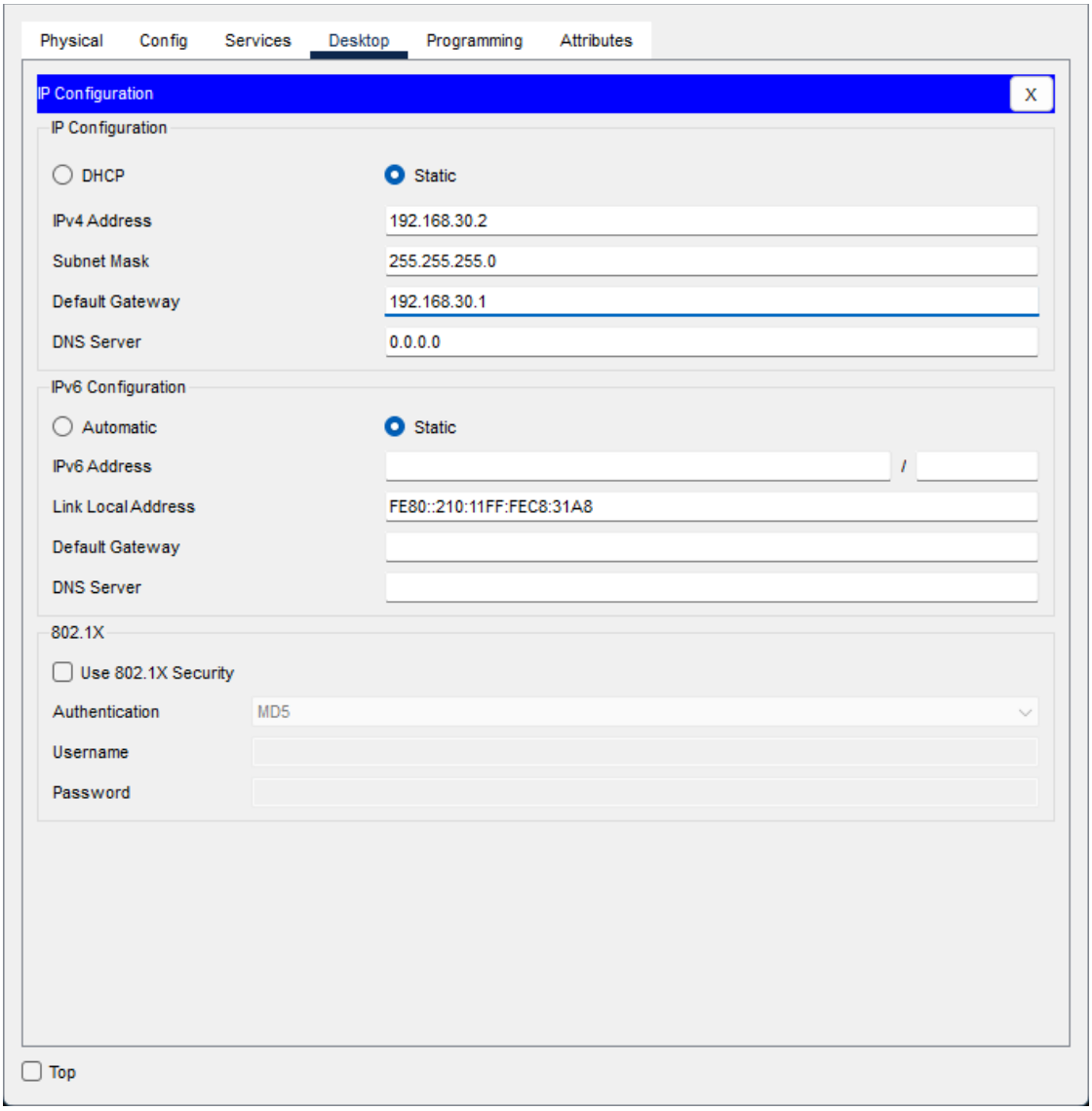

Physical
Config
Services
Desktop
Programming
Attributes
IP Configuration
X
IP Configuration
DHCP
Static
IPv4 Address
192.168.30.2
Subnet Mask
255.255.255.0
Default Gateway
192.168.30.1
DNS Server
0.0.0.0
IPv6 Configuration
Automatic
Static
IPv6 Address
/
Link Local Address
FE80::210:11FF:FEC8:31A8
Default Gateway
DNS Server
802.1X
Use 802.1X Security
Authentication
MD5
Username
Password
Top

Figura 6 servidor 2 FUAA la Ip y default Gateway

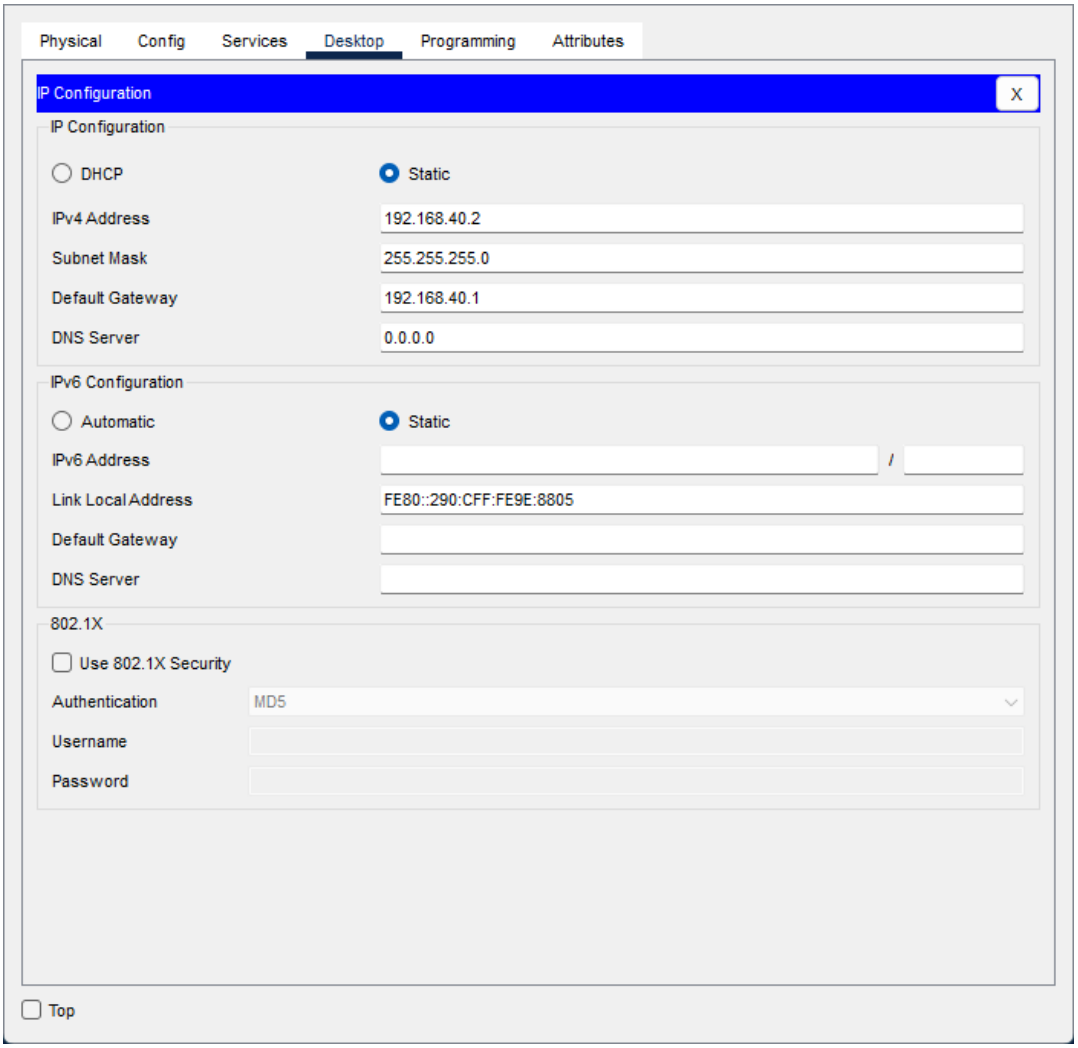


Figura 7 Configuración PC 0 la ip y el default Gateway

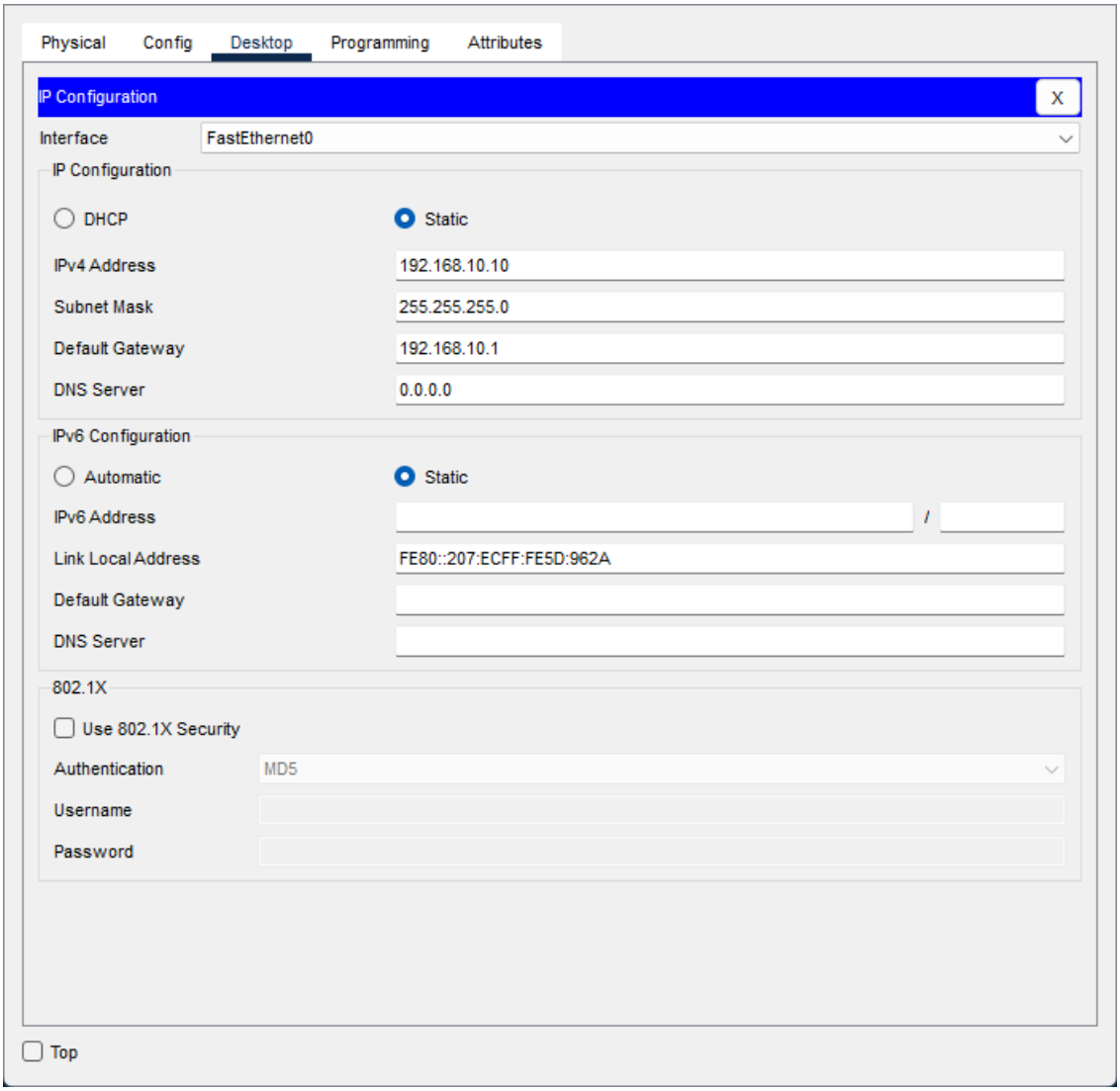


Figura 8 Configuración PC 1 la ip y el default Gateway

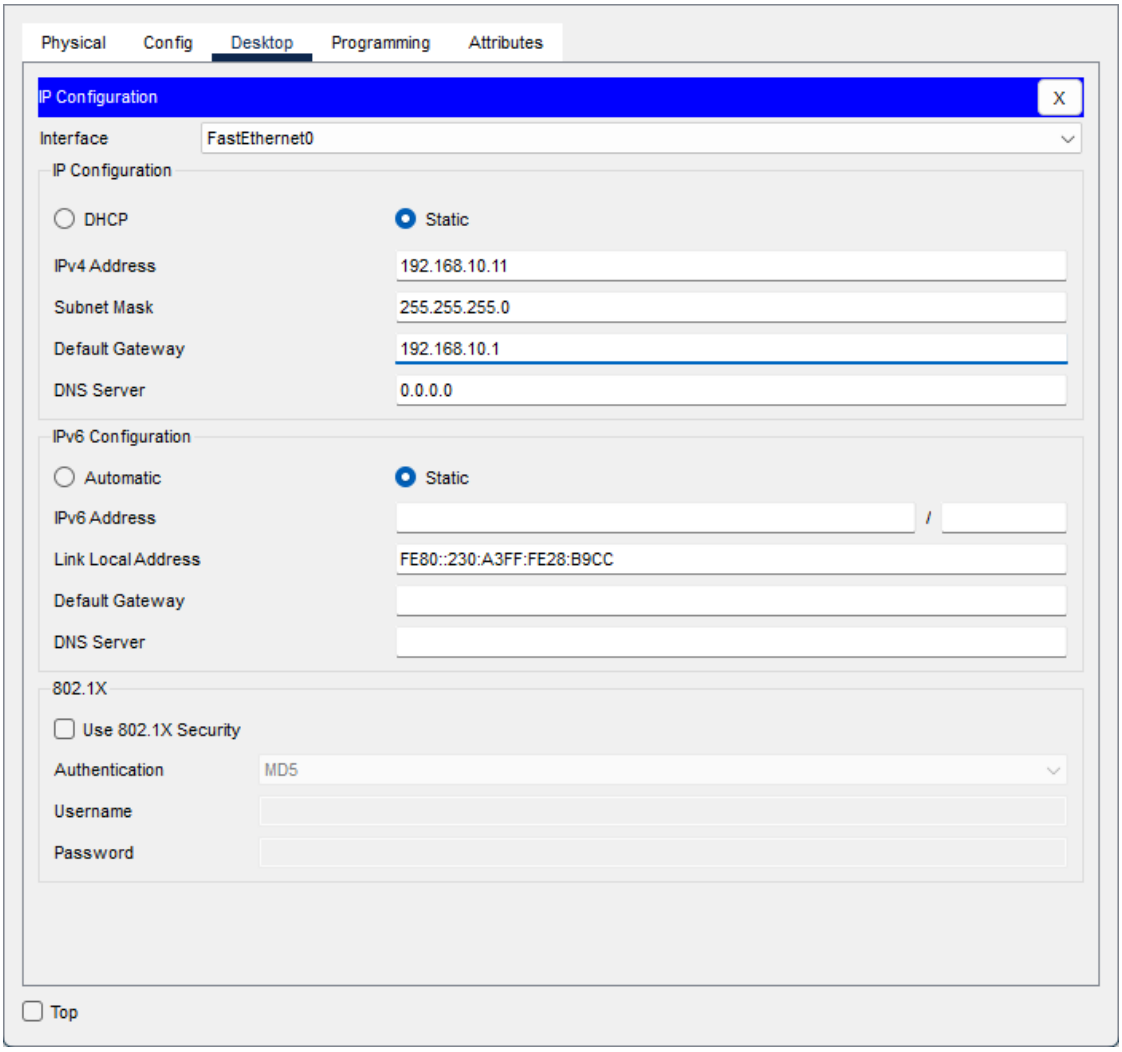


Figura 9 Configuración PC 2 la ip y el default Gateway

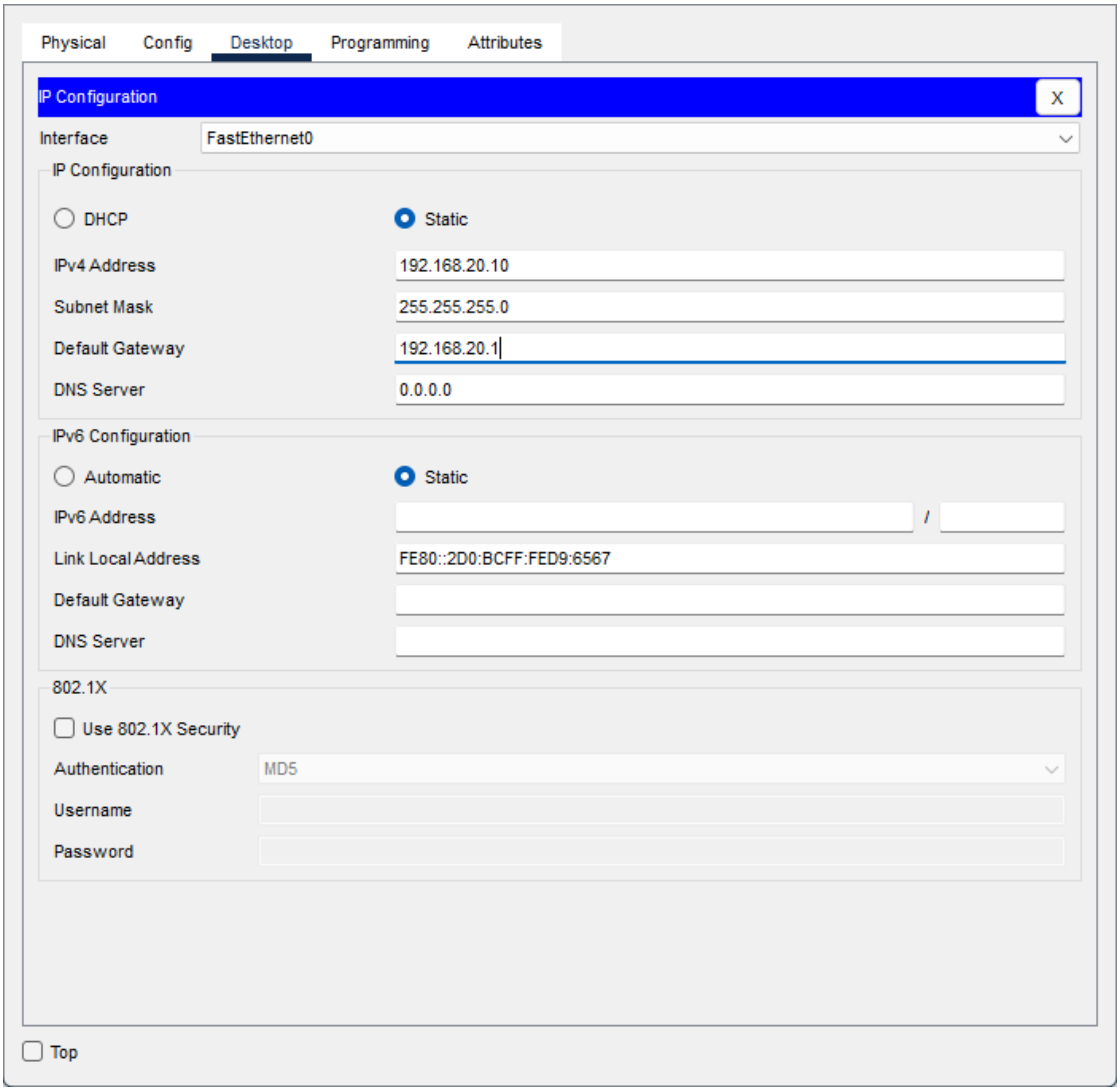
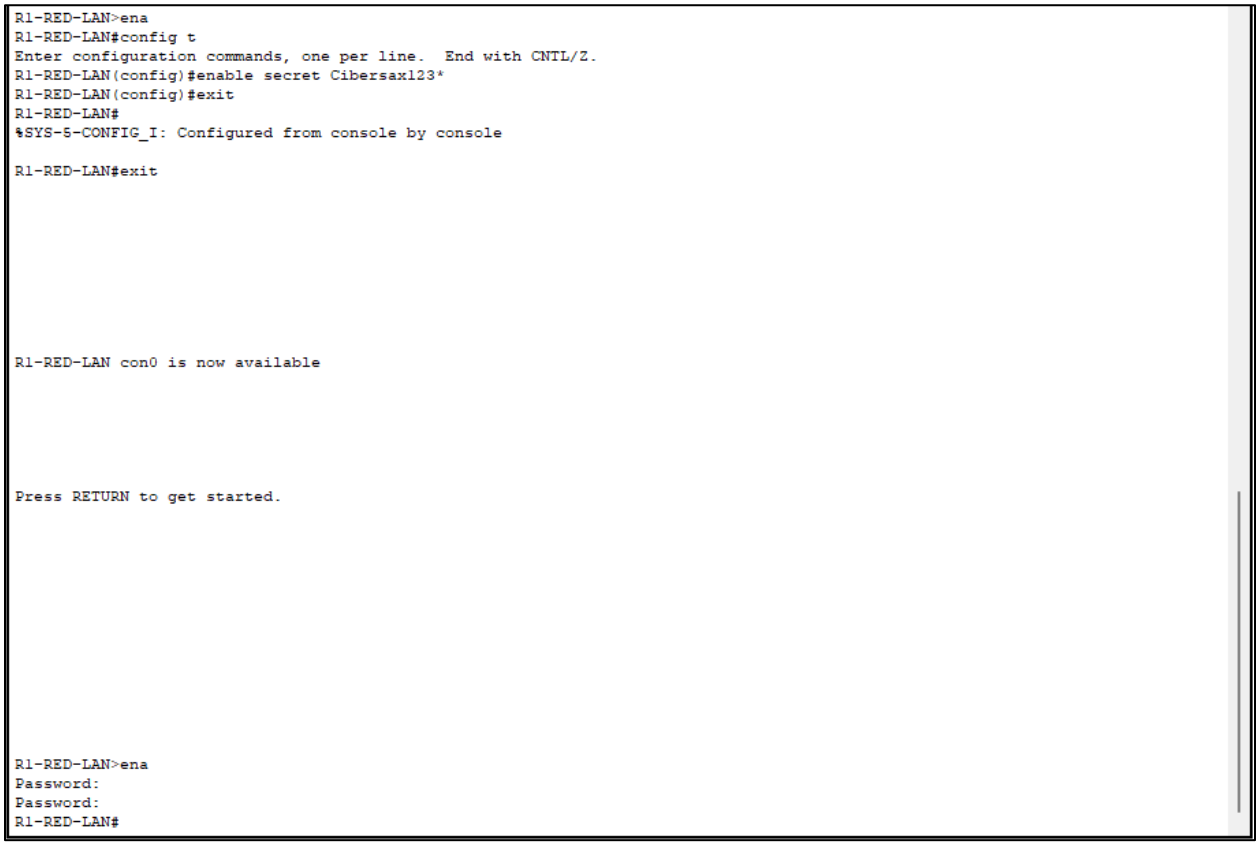
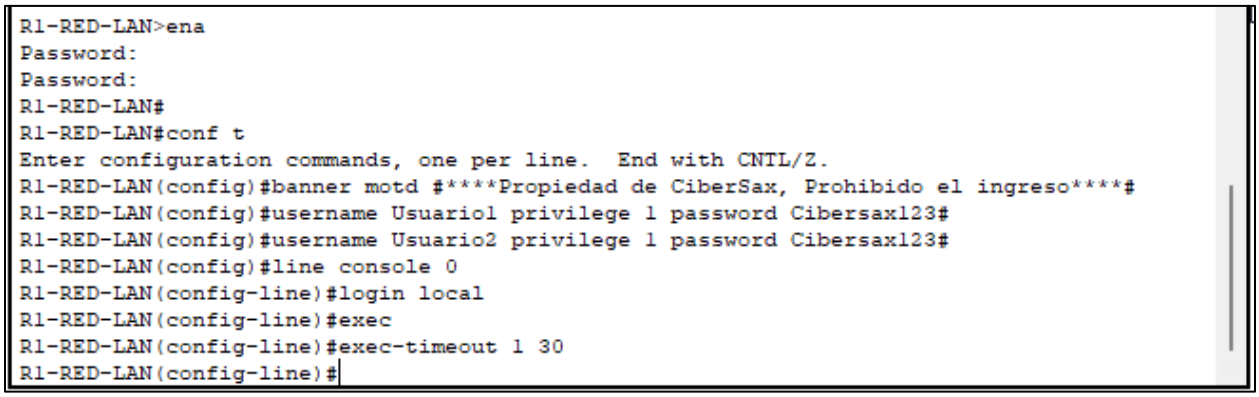


Figura 10 Acceder al Router



Configuración para que pida la contraseña al intentar acceder al router

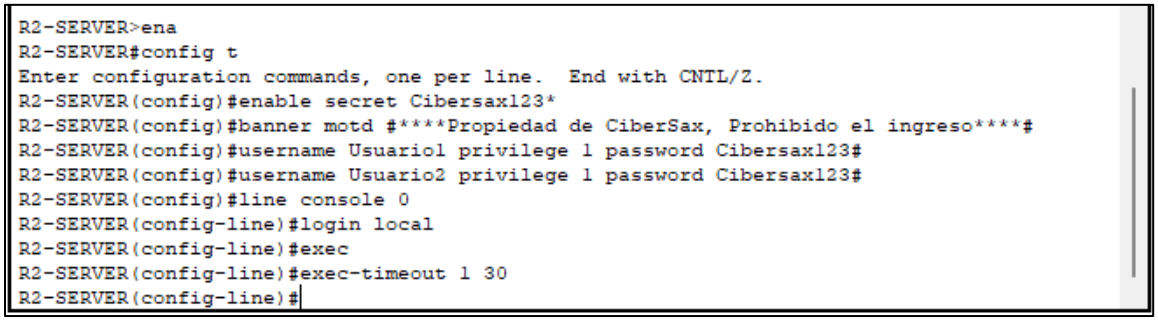
Figura 11 Mensaje de Alerta



Creación del mensaje de alerta, creación de los usuarios y además asegure la línea de consola de

manera que se autentique con las bases de datos de usuarios

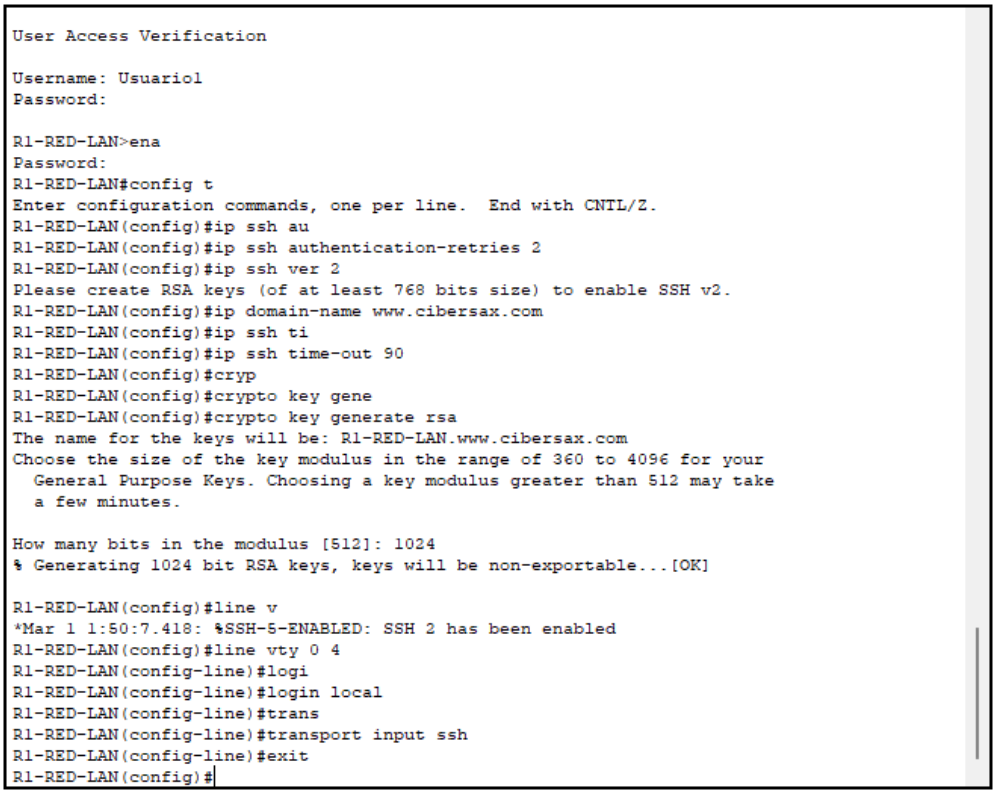
Figura 12 Configuración contraseña



```
R2-SERVER>ena
R2-SERVER#config t
Enter configuration commands, one per line.  End with CNTL/Z.
R2-SERVER(config)#enable secret Cibersax123*
R2-SERVER(config)#banner motd #****Propiedad de CiberSax, Prohibido el ingreso****#
R2-SERVER(config)#username Usuario1 privilege 1 password Cibersax123#
R2-SERVER(config)#username Usuario2 privilege 1 password Cibersax123#
R2-SERVER(config)#line console 0
R2-SERVER(config-line)#login local
R2-SERVER(config-line)#exec
R2-SERVER(config-line)#exec-timeout 1 30
R2-SERVER(config-line)#
```

Configuración de contraseña en modo privilegiado, creación del mensaje de alerta, creación de los usuarios y además asegure la línea de consola de manera que se autentique con las bases de datos de usuarios

Figura 13 Configuración Router 1 ssh, crypto key con rsa a 1024 bits y vty

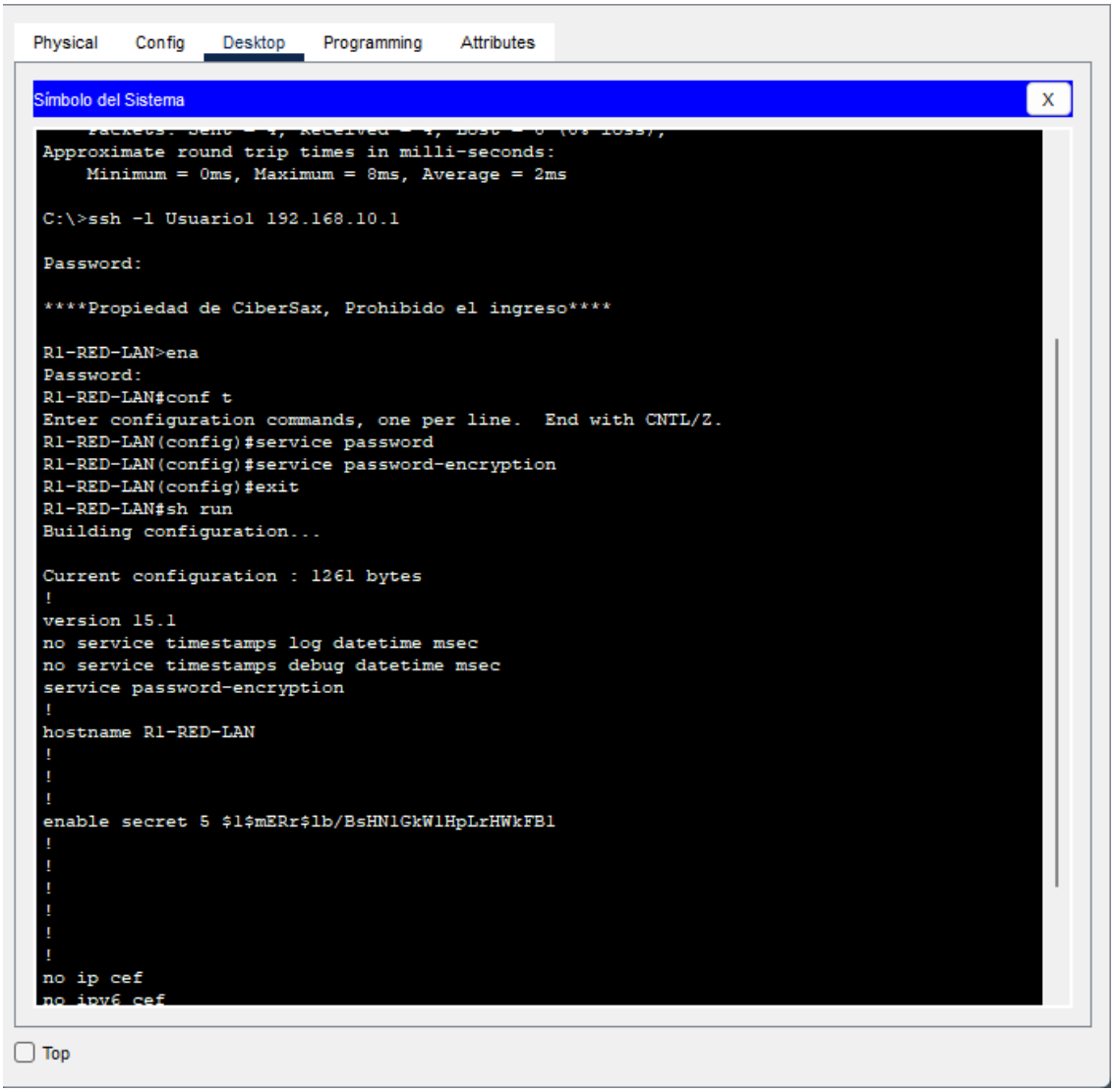


```
User Access Verification

Username: Usuario1
Password:

R1-RED-LAN>ena
Password:
R1-RED-LAN#config t
Enter configuration commands, one per line.  End with CNTL/Z.
R1-RED-LAN(config)#ip ssh au
R1-RED-LAN(config)#ip ssh authentication-retries 2
R1-RED-LAN(config)#ip ssh ver 2
Please create RSA keys (of at least 768 bits size) to enable SSH v2.
R1-RED-LAN(config)#ip domain-name www.cibersax.com
R1-RED-LAN(config)#ip ssh ti
R1-RED-LAN(config)#ip ssh time-out 90
R1-RED-LAN(config)#cryp
R1-RED-LAN(config)#crypto key gene
R1-RED-LAN(config)#crypto key generate rsa
The name for the keys will be: R1-RED-LAN.www.cibersax.com
Choose the size of the key modulus in the range of 360 to 4096 for your
  General Purpose Keys. Choosing a key modulus greater than 512 may take
  a few minutes.

How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

R1-RED-LAN(config)#line v
*Mar 1 1:50:7.418: %SSH-5-ENABLED: SSH 2 has been enabled
R1-RED-LAN(config)#line vty 0 4
R1-RED-LAN(config-line)#logi
R1-RED-LAN(config-line)#login local
R1-RED-LAN(config-line)#trans
R1-RED-LAN(config-line)#transport input ssh
R1-RED-LAN(config-line)#exit
R1-RED-LAN(config)#
```

Figura 14 Configuración Router 2 ssh, crypto key con rsa a 1024 bits y vty

```
Press RETURN to get started!

****Propiedad de CiberSax, Prohibido el ingreso****

User Access Verification

Username: Usuariol
Password:

R2-SERVER>ena
Password:
R2-SERVER#config t
Enter configuration commands, one per line.  End with CNTL/Z.
R2-SERVER(config)#ip ssh au
R2-SERVER(config)#ip ssh authentication-retries  2
R2-SERVER(config)#ip ssh ver 2
Please create RSA keys (of at least 768 bits size) to enable SSH v2.
R2-SERVER(config)#ip domain-name www.cibersax.com
R2-SERVER(config)#ip ssh tin
R2-SERVER(config)#ip ssh time
R2-SERVER(config)#ip ssh time-out 90
R2-SERVER(config)#crypto
R2-SERVER(config)#crypto ke
R2-SERVER(config)#crypto key gene
R2-SERVER(config)#crypto key generate rsa
R2-SERVER(config)#crypto key generate rsa
The name for the keys will be: R2-SERVER.www.cibersax.com
Choose the size of the key modulus in the range of 360 to 4096 for your
  General Purpose Keys. Choosing a key modulus greater than 512 may take
  a few minutes.

How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

R2-SERVER(config)#line vty 0 4
*Mar 1 1:55:27.230: %SSH-5-ENABLED: SSH 2 has been enabled
R2-SERVER(config-line)#login local
R2-SERVER(config-line)#trans
R2-SERVER(config-line)#transport input ssh
R2-SERVER(config-line)#exit
R2-SERVER(config)#
```

Figura 15 Comprobación del acceso remoto por SSH



5. Diseñar e implementar autenticación del protocolo de enrutamiento OSPF.

Se configuro el protocolo OSPF en los 2 router y se verificaran las tablas de rutas, así mismo comprobaremos la conexión entre las redes externas. Habilitamos la autenticación OSPF en las interfaces seriales de los routers.

Figura 16 Configuración de enrutamiento OSPF en el router 1

```
****Propiedad de CiberSax, Prohibido el ingreso****

User Access Verification

Username: Usuario 1
Password:
% Login invalid

Username: Usuario1
Password:

R1-RED-LAN>ena
Password:
R1-RED-LAN#net 192.168.10.0 0.0.0.255 area 0
             ^
% Invalid input detected at '^' marker.

R1-RED-LAN#config t
Enter configuration commands, one per line.  End with CNTL/Z.
R1-RED-LAN(config)#router ospf 1
R1-RED-LAN(config-router)#net 192.168.10.0 0.0.0.255 area 0
R1-RED-LAN(config-router)#net 192.168.20.0 0.0.0.255 area 0
R1-RED-LAN(config-router)#net 20.20.20.0 0.0.0.3 area 0
R1-RED-LAN(config-router)#
```

Figura 17 Configuración de enrutamiento OSPF en el router 2 y mensaje del proceso exitoso

```
****Propiedad de CiberSax, Prohibido el ingreso****

User Access Verification

Username: Usuario 1
Password:
% Login invalid

Username: Usuario1
Password:

R2-SERVER>ena
Password:
R2-SERVER#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R2-SERVER(config)#router ospf 1
R2-SERVER(config-router)#net 192.168.30.0 0.0.0.255 area 0
R2-SERVER(config-router)#net 192.168.40.0 0.0.0.255 area 0
R2-SERVER(config-router)#net 20.20.20.0 0.0.0.3 area 0
R2-SERVER(config-router)#
02:11:09: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.20.1 on Serial0/0/0 from LOADING to
FULL, Loading Done
```

Figura 18 Configuración autenticación OSPF router 1

```
****Propiedad de CiberSax, Prohibido el ingreso****

User Access Verification

Username: Usuario1
Password:

R1-RED-LAN>ena
Password:
R1-RED-LAN#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1-RED-LAN(config)#int s0/0/0
R1-RED-LAN(config-if)#ip ospf mess
R1-RED-LAN(config-if)#ip ospf message-digest-key 1 md5 FUAA123#
R1-RED-LAN(config-if)#ip ospf au
R1-RED-LAN(config-if)#ip ospf authentication mes
R1-RED-LAN(config-if)#ip ospf authentication message-digest
R1-RED-LAN(config-if)#exit
R1-RED-LAN(config)#
02:32:18: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.40.1 on Serial0/0/0 from FULL to DOWN,
Neighbor Down: Dead timer expired

02:32:18: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.40.1 on Serial0/0/0 from FULL to DOWN,
Neighbor Down: Interface down or detached

R1-RED-LAN(config)#area 0 authentication me
R1-RED-LAN(config)#area 0 authentication mess
R1-RED-LAN(config)#router ospf 1
R1-RED-LAN(config-router)#area 0 aut
R1-RED-LAN(config-router)#area 0 authentication mess
R1-RED-LAN(config-router)#area 0 authentication message-digest
R1-RED-LAN(config-router)#
```

Figura 19 Configuración autenticación OSPF router 1

```
Username: Usuario1
Password:

R2-SERVER>ena
Password:
R2-SERVER#config t
Enter configuration commands, one per line.  End with CNTL/Z.
R2-SERVER(config)#R2-SERVER(config)#
R2-SERVER(config)#int s0/0/0
R2-SERVER(config-if)#ip ospf meesa
R2-SERVER(config-if)#ip ospf meess
R2-SERVER(config-if)#ip ospf messa
R2-SERVER(config-if)#ip ospf message-digest-key 1 md5 FUAA123#
R2-SERVER(config-if)#ip ospf authentication messa
R2-SERVER(config-if)#ip ospf authentication message-digest
R2-SERVER(config-if)#exit
02:36:50: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.20.1 on Serial0/0/0 from LOADING to
FULL, Loading Done

R2-SERVER(config)#router ospf 1
R2-SERVER(config-router)#area 0 at
R2-SERVER(config-router)#area 0 auth
R2-SERVER(config-router)#area 0 authentication mess
R2-SERVER(config-router)#area 0 authentication message-digest
R2-SERVER(config-router)#exit
R2-SERVER(config)#exit
R2-SERVER#
%SYS-5-CONFIG_I: Configured from console by console
```

Figura 20 Comprobación de las tablas de direccionamiento con OSPF

```
R2-SERVER#
%SYS-5-CONFIG_I: Configured from console by console

R2-SERVER#sh 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 not set

     20.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C       20.20.20.0/30 is directly connected, Serial0/0/0
L       20.20.20.2/32 is directly connected, Serial0/0/0
O    192.168.10.0/24 [110/65] via 20.20.20.1, 00:00:37, Serial0/0/0
O    192.168.20.0/24 [110/65] via 20.20.20.1, 00:00:37, Serial0/0/0
     192.168.30.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.30.0/24 is directly connected, GigabitEthernet0/0
L       192.168.30.1/32 is directly connected, GigabitEthernet0/0
     192.168.40.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.40.0/24 is directly connected, GigabitEthernet0/1
L       192.168.40.1/32 is directly connected, GigabitEthernet0/1
```

6. Diseñar e implementar ACL estándar y ACL extendida.

Figura 21 Configuración de las ACL Extendidas

```
02:36:50: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.40.1 on Serial0/0/0 from LOADING to FULL, Loading
Done
****Propiedad de CiberSax, Prohibido el ingreso****

User Access Verification

Username: Usuario1
Password:

R1-RED-LAN>ena
Password:
R1-RED-LAN#acces
R1-RED-LAN#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1-RED-LAN(config)#accw
R1-RED-LAN(config)#acce
R1-RED-LAN(config)#access-list 101 permit TCP 192.168.10.0 0.0.0.255 192.168.40.0 0.0.0.255 eq www
R1-RED-LAN(config)#access-list 101 permit TCP 192.168.10.0 0.0.0.255 192.168.30.0 0.0.0.255 eq www
R1-RED-LAN(config)#acce
R1-RED-LAN(config)#access-list 101 deny ICMP 192.168.10.0 0.0.0.255 192.168.40.0 0.0.0.255
R1-RED-LAN(config)#access-list 101 deny ICMP 192.168.10.0 0.0.0.255 192.168.30.0 0.0.0.255
R1-RED-LAN(config)#int s0/0/0
R1-RED-LAN(config-if)#ip axx
R1-RED-LAN(config-if)#ip acc
R1-RED-LAN(config-if)#ip access-group 101 out
R1-RED-LAN(config-if)#exit
R1-RED-LAN(config)#exit
R1-RED-LAN#
%SYS-5-CONFIG_I: Configured from console by console

R1-RED-LAN#write memory
Building configuration...
[OK]
R1-RED-LAN#
```

Figura 22 Configuración de las ACL Estándar

```
****Propiedad de CiberSax, Prohibido el ingreso****

User Access Verification

Username: Usuario1
Password:

R2-SERVER>ena
Password:
R2-SERVER#config t
Enter configuration commands, one per line.  End with CNTL/Z.
R2-SERVER(config)#acces-list 1 permit 192.168.40.0 0.0.0.255
                   ^
% Invalid input detected at '^' marker.

R2-SERVER(config)#access-list 1 permit 192.168.40.0 0.0.0.255
R2-SERVER(config)#access-list 1 deny 192.168.20.0 0.0.0.255
R2-SERVER(config)#int g0/0
R2-SERVER(config-if)#ip acces
R2-SERVER(config-if)#ip access-group 1 out
R2-SERVER(config-if)#exit
R2-SERVER(config)#exit
R2-SERVER#
%SYS-5-CONFIG_I: Configured from console by console

R2-SERVER#write memory
Building configuration...
[OK]
R2-SERVER#
```

7. Análisis de Routers

La configuración de los routers y la implementación de las ACLs permitieron un control adecuado del tráfico en la red, garantizando que solo los dispositivos autorizados pudieran comunicarse. La autenticación OSPF impidió que routers externos no autorizados ingresaran al dominio de enrutamiento, mejorando así la seguridad. Además, la configuración de SSH como método exclusivo de acceso remoto aseguró que las conexiones se realizaran de manera encriptada. Las ACLs aplicadas brindaron un control granular sobre qué tráfico era permitido y cuál era bloqueado, cumpliendo con los objetivos establecidos.

https://drive.google.com/file/d/1QhGN-0rXb84p-jzkJ1p7GYLOD2yIU5IQ/view?usp=drive_link

Nota: Este mapa se realizó con la ayuda de (Lucidchard, s.f.)

mensajes de advertencia, autenticación SSH y dominios es esencial para evitar accesos no autorizados. Esto ayuda a establecer un control efectivo sobre quién accede al dispositivo y qué puede hacer, garantizando la seguridad de la red desde la configuración inicial.

Tabla 1 Protocolos de enrutamiento

Categoría	Protocolo	Características
Enrutamiento Estático	Rutas Estáticas	Configuración manual, adecuado para redes pequeñas.
Enrutamiento Dinámico	**Vector Distancia**	Envía periódicamente la tabla de rutas.
	RIP (Routing Information Protocol)	Usa el número de saltos como métrica (máx. 15 saltos).
	EIGRP (Enhanced Interior Gateway RP)	Propietario de Cisco, combina vector distancia y estado de enlace.
	Estado de Enlace	Crea un mapa completo de la red.
	OSPF (Open Shortest Path First)	Usa el algoritmo de Dijkstra, eficiente en redes grandes.
	IS-IS (Intermediate System to IS)	Similar a OSPF, utilizado en entornos ISP y grandes redes.
	Híbrido	Combinación de vector distancia y estado de enlace.
	EIGRP (Cisco)	Utiliza múltiples métricas y optimiza rutas más rápido.
Protocolos por Alcance	**IGP (Interior Gateway Protocols)**	Usados dentro de un sistema autónomo (AS).
	RIP, OSPF, EIGRP, IS-IS	Manejan el enrutamiento interno de una organización.
	EGP (Exterior Gateway Protocols)	Usados entre diferentes sistemas autónomos.
	BGP (Border Gateway Protocol)	Principal protocolo de enrutamiento en Internet.

La autenticación garantiza que solo dispositivos autorizados puedan intercambiar información de enrutamiento. Esto previene ataques como la falsificación de rutas y asegura la

integridad de las tablas de enrutamiento. La autenticación también proporciona un nivel adicional de control sobre la comunicación entre routers.

La autenticación garantiza que solo dispositivos autorizados puedan intercambiar información de enrutamiento. Esto previene ataques como la falsificación de rutas y asegura la integridad de las tablas de enrutamiento. La autenticación también proporciona un nivel adicional de control sobre la comunicación entre routers.

Tabla 2 Cuadro comparativo entre ACL estándar y ACL extendida.

Criterio	ACL Estándar	ACL Extendida
Rango de Números	1 - 99 (IPv4) y 1300 - 1999 (extendido)	100 - 199 (IPv4) y 2000 - 2699 (extendido)
Filtro basado en	Solo dirección IP de origen	Dirección IP de origen y destino, puerto y protocolo
Mayor Control	Menos específico	Más específico y flexible
Protocolos Filtrados	Solo IPv4	IPv4, TCP, UDP, ICMP, etc.
Ubicación en la Red	Cerca del destino	Cerca del origen
Ejemplo de Configuración	access-list 10 permit 192.168.1.0 0.0.0.255	access-list 110 permit tcp 192.168.1.0 0.0.0.255 any eq 80

Las políticas de seguridad propuestas buscan proteger la infraestructura de red mediante un enfoque integral que considere diferentes aspectos de seguridad. En primer lugar, es fundamental deshabilitar el uso de Telnet y permitir únicamente el acceso remoto mediante SSH versión 2, lo cual garantiza la protección de las credenciales y configuraciones críticas frente a ataques de intercepción. Asimismo, se debe implementar autenticación OSPF con claves de autenticación avanzadas como MD5 o SHA-256 en todas las interfaces seriales para prevenir la manipulación de rutas por agentes no autorizados.

También se recomienda configurar ACL estándar y extendidas para filtrar tráfico no deseado y permitir únicamente el tráfico necesario hacia redes críticas, mejorando

significativamente el control sobre el flujo de datos en la red. Además, debe establecerse un sistema de monitoreo constante que registre intentos de acceso fallidos y genere alertas en tiempo real, lo cual permitirá identificar amenazas potenciales y reaccionar a tiempo.

Por otro lado, realizar auditorías periódicas de la configuración de seguridad es esencial para garantizar que las políticas implementadas se mantengan actualizadas y efectivas. Estas auditorías deben complementarse con un plan de respuesta a incidentes que incluya procedimientos específicos para la identificación, análisis, contención y recuperación de ataques. Asimismo, se debe restringir el acceso a la configuración de routers mediante usuarios autenticados y privilegios específicos, asegurando que cada usuario tenga acceso limitado a sus funciones correspondientes.

Finalmente, aplicar actualizaciones regulares de software en los dispositivos de red es crucial para protegerlos contra vulnerabilidades conocidas y emergentes. La combinación de estas políticas permitirá establecer un entorno seguro y eficiente, capaz de enfrentar las amenazas actuales y futuras con un enfoque preventivo y proactivo.

8. Conclusiones

La implementación de mecanismos de seguridad en routers mediante la autenticación de protocolos de enrutamiento OSPF y la configuración de ACLs es esencial para garantizar la integridad, disponibilidad y confidencialidad de la red. La configuración adecuada de OSPF con autenticación permite proteger el intercambio de información de enrutamiento, asegurando que solo dispositivos autorizados puedan participar en este proceso. Asimismo, el uso de SSH para acceso remoto proporciona un canal seguro que evita la exposición de credenciales y configuraciones críticas durante la gestión de la red.

Las ACLs, tanto estándar como extendidas, son herramientas efectivas para controlar el tráfico de red, permitiendo o denegando accesos específicos según criterios definidos. Su correcta implementación contribuye a la protección contra ataques comunes como ICMP no deseado o accesos no autorizados desde subredes específicas.

Además, las políticas de seguridad propuestas proporcionan un enfoque integral que incluye monitoreo continuo, auditorías periódicas, actualización de dispositivos y planes de respuesta ante incidentes, elementos fundamentales para mantener la red protegida contra amenazas conocidas y emergentes. La implementación de estas medidas permite crear una infraestructura más robusta, confiable y preparada para enfrentar desafíos de seguridad actuales y futuros.

En conclusión, asegurar la red a través de protocolos adecuados y configuraciones sólidas es un proceso continuo que requiere análisis, implementación, monitoreo y mejora constante. La adopción de buenas prácticas de seguridad permitirá garantizar un funcionamiento eficiente y seguro de la red en todo momento.La implementación de mecanismos de seguridad en routers mediante la autenticación de protocolos de enrutamiento OSPF y la configuración de ACLs es esencial para garantizar la integridad y disponibilidad de la red. El uso de SSH en lugar de Telnet proporciona un método seguro para la administración remota, mientras que las ACLs permiten controlar el tráfico no deseado y proteger áreas críticas de la red. Además, las políticas de seguridad propuestas aseguran que la infraestructura permanezca protegida ante amenazas comunes. La adopción de medidas adecuadas y la realización de auditorías periódicas permiten mantener un entorno seguro y confiable, garantizando la operación continua y eficiente de la red.

Bibliografía

Lopez, R. A. (2025). *Seguridad en redes - Eje 2.* Obtenido de Fundación Universitaria del Área Andina.

Microsoft Corporation. . (s.f.). *Autenticación multifactor de Microsoft Entra.* Obtenido de Microsoft Corporation.: https://www.microsoft.com/es-es/security/business/identity-access/microsoft-entra-mfa-multi-factor-authentication

Netseccloud. (16 de marzo de 2025). *El impacto de las subredes y las VLAN en la seguridad de la red*. Obtenido de https://netseccloud.com/the-impact-of-subnets-and-vlans-on-network-security

QNAP. (s.f.). *Telnet/SSH.* . Obtenido de QNAP: https://docs.qnap.com/operating-system/qts/4.3.x/es-es/GUID-08E3AD8F-ADE3-4B16-85A4-F255E6F79ADB.html