# SOLUCION DE DOS ESCENARIOS PRESENTES EN ENTORNOS CORPORATIVOS BAJO EL USO DE TECNOLOGIA CISCO

CAMILO HERNANDO MORA RUIZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
INGENIERÍA DE SISTEMAS
FUSAGASUGA
2021

# SOLUCION DE DOS ESCENARIOS PRESENTES EN ENTORNOS CORPORATIVOS BAJO EL USO DE TECNOLOGIA CISCO

CAMILO HERNANDO MORA RUIZ

Diplomado de opción de grado presentado para optar el título de INGENIERO DE SISTEMAS

TUTOR:
RAUL BAREÑO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DECIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
INGENIERÍA DE SISTEMAS
FUSAGASUGA
2021

NOTA DE ACEPTACIÓN

Firma del presidente del Jurado

Firma del Jurado

Firma del Jurado

Fusagasugá, 28 de noviembre de 2021

## AGRADECIMIENTOS

Estando a puertas de finalizar mi carrera profesional y después de haber pasado por muchas pruebas difícil en este camino, el camino del aprendizaje aun no finaliza, primero que todo quiero agradecer a Dios y a mi familia por apoyarme en este largo camino lleno de dificultades, igualmente a todos mis tutores que pasaron por este tiempo en la universidad y me brindaron su conocimiento, mis compañeros y demás personas que ayudaron a que ese sueño se convirtiera en realidad.

Infinitas gracias a todos y cada uno de ustedes, espero verlos pronto en algún punto de mi vida

**CONTENIDO**

## LISTA DE TABLAS

## LISTA DE FIGURAS

## GLOSARIO

**Subneting**: Definido de la forma más simple, el término subnetting hace referencia a la subdivisión de una red en varias subredes**.** El subneteo permite a los administradores de red, por ejemplo, dividir una red empresarial en varias subredes sin hacerlo público en Internet

**IPV4**: Un protocolo de interconexión de redes basados en Internet, y que fue la primera versión implementada en 1983 para la producción de ARPANET. Definida en el RFC 791, el IPv4 usa direcciones de 32 bits.

**IPv6:** Es una actualización al protocolo IPv4, diseñado para resolver el problema de agotamiento de direcciones.

**LAN:** Una red de área local o LAN (por las siglas en inglés de Local Area Network) es una red de computadoras que abarca un área reducida a una casa, un departamento o un edificio.

**SSH:** Es el nombre de un protocolo y del programa que lo implementa cuya principal función es el acceso remoto a un servidor por medio de un canal seguro en el que toda la información está cifrada.

## RESUMEN

La presente práctica mide las capacidades de interpretar una red mediante la plataforma de simulación Cisco Packet Tracert, siguiendo las indicaciones de la guía de aprendizaje para el avance al proyecto final.

Durante el desarrollo de los dos escenarios se trabajó según la teoría suministrada en el diplomado , donde podemos observar enrutamiento estático , Vlans , direccionamiento dinámico y acl, nat , pat , gestión de equipos de red, entre otras generalidades aplicadas durante su desarrollo, se observa el pleno como seria la correcta administración de equipos en una red grande simulada, dándonos así una idea de cómo se puede proyectar y sacar el máximo provecho reduciendo gastos y optimizando una red adecuadamente, Se puede observar la transición de configuraciones básicas en una red pequeña y hasta las configuraciones de redes y vlans en infraestructura más amplia , siendo esto perfecto para aplicar las configuraciones que más se pueden llegar a encontrar iniciando la vida laboral ,



Palabras clave: CISCO, Enrutamiento, Vlans, Nat ,LAN

## ABSTRACT

This practice measures the capabilities of interpreting a network using the Cisco Packet Tracert simulation platform, following the instructions in the learning guide to advance to the final project.

During the development of the two scenarios, we worked according to the theory provided in the diploma, where we can observe static routing, Vlans, dynamic addressing and acl, nat, pat, network equipment management, among other generalities applied during its development, it is observed the full as would be the correct management of equipment in a simulated large network, thus giving us an idea of how it can be planned and get the most out of reducing expenses and optimizing a network properly, You can see the transition of basic configurations in a small network and up to network configurations and vlans in broader infrastructure, this being perfect for applying the configurations that can be found most at the beginning of working life,



Keywords: CISCO, Switch, Router, Subneting, LAN

## INTRODUCCION

Mediante el siguiente trabajo se exponen los métodos necesarios para subnetear una red pequeña, configurar dispositivos por medio de conexión de consola y probar seguridad de SSH

El escenario uno consta de una topología de red, conformada por dos PC, un switch y un router, los cuales se configuraron por medio de subneting a la dirección ip 192.168.82.0 donde los dos penúltimos dígitos corresponden al número de mi documento, en donde se emplearon LANs extraidas de la dirección de red principal, cada dispositivo se configuro y se probó su conectividad, se concluye lo observado al finalizar la actividad

## DESARROLLO

### 1.1 ESCENARIO 1

Figura 1 Topologia de red


Fuente : Prueba de habilidades CISCO CCNAII

En este primer escenario se configurarán los dispositivos de una red pequeña. Debe configurar un router, un switch y equipos, diseñar el esquema de direccionamiento IPv4 para las LAN propuestas. El router y el switch también deben administrarse de forma segura.

**Objetivos**

Parte 1: Construir en el simulador la Red

Parte 2: Desarrollar el esquema de direccionamiento IP para la LAN1 y la LAN2
Parte 3: Configurar los aspectos básicos de los dispositivos de la Red propuesta.
Parte 4: Configurar los ajustes básicos de seguridad en el R1 y S1

Parte 4: Configurar los hosts y verificar la conectividad entre los equipos

**Aspectos básicos/situación**

En el desarrollo del caso de estudio usted implementa la topología mostrada en la figura y configura el Router R1 y el swich S1, y los PCs. Con la dirección suministrada realizará el subnetting y cumplirá el requerimiento para la LAN1 (100 host) y la LAN2 (50 hosts).

**Parte 1: Construya la Red**

En el simulador construya la red de acuerdo con la topología lógica que se plantea en la figura 1, cablee conforme se indica en la topología, y conecte los equipos de cómputo.

**Parte 2: Desarrolle el esquema de direccionamiento IP**

Desarrolle el esquema de direccionamiento IP. Para la dirección IPv4 cree las dos subredes con la cantidad requerida de hosts. Asigne las direcciones de acuerdo con los requisitos mencionados en la tabla de direccionamiento.

Cada estudiante tomará el direccionamiento 192.168.82.0 donde X corresponde a los últimos dos dígitos de su cédula.

Tabla 1 Direccionamiento

| ITEM | REQUERIMIENTO |
|---|---|
| Dirección de Red | 192.168.82.0 donde X corresponde a los últimos dos dígitos de su cédula. |
| Requerimiento de host Subred LAN1 | 100 |
| Requerimiento de host Subred LAN2 | 50 |
| R1 G0/0/1 | Primera dirección de host de la subred LAN1<br>192.168.82.1 |
| R1 G0/0/0 | Primera dirección de host de la subred LAN2<br>192.168.82.129 |
| S1 SVI | Segunda dirección de host de la subred LAN1<br>192.168.82.2 |
| PC-A | Última dirección de host de la subred LAN1<br>192.168.82.126 |
| PC-B | Última dirección de host de la subred LAN2<br>192.168.82.190 |

Fuente : Prueba de habilidades CISCO CCNAII

Tabla 2 Subneteo

| LAN | N# HOST | IP DE RED | MASCARA | HOST INICIAL | HOST FINAL | BROADCAST |
|---|---|---|---|---|---|---|
| 1 | 126 | 192.168.82 .0 / 25 | 255.255.255 .128 | 192.168.82 .1 | 192.168.82 .126 | 192.168.82 .127 |
| 2 | 62 | 192.168.82 .128 / 26 | 192.168.82. 128 | 192.168.82 .129 | 192.168.82 .190 | 192.168.82 .191 |

Fuente : Prueba de habilidades CISCO CCNAII

**Parte 3: Configure aspectos básicos**

Los dispositivos de red (S1 y R1) se configuran mediante conexión de consola.

**Paso 1: configurar los ajustes básicos**

Las tareas de configuración para R1 incluyen las siguientes:

**A. Desactivar la búsqueda DNS**

```
Router>enable ---> Inicio modo privilegiado
Router#config t ---> Ingreso Modo configuración
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#no ip domain-lookup ---> Desactivar búsqueda
DNS
Router(config)#
```

**B. Establecer R1 Nombre del router**

```
Router#config t ---> Ingreso Modo configuración
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname R1 ---> Renombrar Dispositivo
R1(config)#
```

**C. Nombre de dominio ccna-lab.com**

```
R1(config)#ip domain-name ccna-lab.com ---> Establecer Nombre
de Dominio
R1(config)#
```

**D. Contraseña cifrada para el modo EXEC privilegiado ciscoenpass**

```
R1(config)#enable secret ciscoenpass --->Establecer
Contraseña para modo privilegiado cifrada
R1(config)#
```

**E. Contraseña de acceso a la consola ciscoconpass**

R1(config)#line console 0 ---> **Modo de configuracion linea de consola 0 como primera**
R1(config-line)#password ciscoconpass---> **Se establece la contraseña de inicio de consola**
R1(config-line) #login ---> **activar autenticación al iniciar dispositivo**

**F. Establecer la longitud mínima para las contraseñas 10 caracteres**

R1(config)#security password min-length 10 ---> **Establece mínimo de 10 caracteres para una contraseña**

R1(config)#

**G. Crear un usuario administrativo en la base de datos local Usuario admin y password admin1pass**

R1(config)#username admin password admin1pass ---> **crear usuario para ingreso al dispositivo con contraseña**
R1(config)#

**H. Configurar el inicio de sesión en las líneas VTY para que use la base de datos local**

R1(config)#line console 0 ---> **Modo de configuracion linea de consola 0 como primera**
R1(config-line)#login local --->**Establece el usuario creado para iniciar el dispositivo**
R1(config-line)#
R1(config)#line vty 0 4 ---> **Ingreso a config line vty 0 4 para acceso telnet**
R1(config-line)#login local**--->Establece el usuario creado para iniciar el dispositivo desde telnet**

**I. Configurar VTY solo aceptando SSH**

```
R1(config-line)#transport input ssh ---> Establece que solo
acepten conexión SSH dentro de las líneas vty
R1(config-line)#
```

**J. Cifrar las contraseñas de texto no cifrado**

```
R1(config)#Service password-encryption--->Cifra las
contraseñas de texto
R1(config)#
```

**K. Configure un MOTD Banner**

```
R1(config)#banner motd #El acceso no autorizado esta
prohibido!# ---> Banner de mensaje de alerta al iniciar el
dispositivo
R1(config)#
```

**L. Configurar interfaz G0/0/0 establecer la direccioon IPv4 y activar la interfaz**

```
R1(config)#interface g0/0/0 --->Ingreso a la interface
R1(config-if)#ip address 192.168.82.129 255.255.255.192 --->
Configuracion de direccionamiento sobre la interface
R1(config-if)#no shutdown ---> Activar la interface
```

**M. Configurar interfaz G0/0/1 establecer la direccioon IPv4 y activar la interfaz**

```
R1(config-if)#interface g0/0/1 ---> Ingreso a la interface
R1(config-if)#ip address 192.168.82.1 255.255.255.128 --->
Configuracion de direccionamiento sobre la interface
R1(config-if)#no shutdown ---> Activar la interface
```

**N. Generar una clave de cifrado RSA Modulo de 1024 bits**

Se establece en 1024 bits en el módulo de cifrado

```
R1(config)#ip domain-name ccna-lab.com --->Establecer Nombre
de Dominio
R1(config)#crypto key generate rsa ---> Crear clave de
encryption RSA
The name for the keys will be: R1.ccna-lab.com
Choose the size of the key modulus in the range of 360 to
2048 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 ---> Establecer el
tamaño del modulo en 1024 bits
% Generating 1024 bit RSA keys, keys will be non-
exportable...[OK]
```

### Paso 2: configurar los ajustes básicos en el S1

Las tareas de configuración para S1 incluyen las siguientes:

**A. Desactivar la búsqueda DNS**

```
Switch>enable ---> Inicio modo privilegiado
Switch#config t ---> Ingreso Modo configuración
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#no ip domain-lookup ---> Desactivar búsqueda
DNS
Switch(config)#
```

**B. Establecer S1 Nombre del Switch**

```
Switch(config)#hostname S1 ---> Renombrar Dispositivo
S1(config)#
```

**C. Nombre de dominio ccna-lab.com**

```
S1(config)#ip domain-name ccna-lab.com ---> Establecer Nombre
de Dominio
S1 (config)#
```

**D. Contraseña cifrada para el modo EXEC privilegiado ciscoenpass**

Contraseña Exec cifrada por medio del comando

```
S1(config)#enable secret ciscoenpass ---> Establecer
```

**Contraseña Modo privilegiado cifrada**

**E. Contraseña de acceso a la consola ciscoconpass**

Se habilita la contraseña enable y se establece como se indica

```
S1(config)#line console 0 ---> Modo de configuracion linea de
consola 0 como primera
S1 (config-line)#password ciscoconpass ---> Se establece la
contraseña de inicio de consola
```

```
S1(config-line)# Login ---> activar autenticación al iniciar dispositivo
```

**F. Crear un usuario administrativo en la base de datos local Usuario admin y password admin1pass**

```
S1(config)#username admin password admin1pass ---> crear usuario para ingreso al dispositivo con contraseña
S1(config)#
```

**G. Configurar el inicio de sesión en las líneas VTY para que use la base de datos local**

```
S1(config)#line console 0 ---> Modo de configuracion linea de consola 0 como primera
S1(config-line)#login local Establece el usuario creado para iniciar el dispositivo
S1(config-line)#exit ---> salir de modo de linea de consola 0
S1(config)#line vty 0 4 ---> Ingreso a config line vty 0 4 para acceso telnet
S1(config-line)#login local --->Establece el usuario creado para iniciar el dispositivo desde telnet
S1(config-line)#
```

**H. Configurar VTY solo aceptando SSH**

Configuración para que solo se acepte la conexión SSH

```
S1(config) line vty 0 4---> Ingreso a config line vty 0 4
S1(config-line)#transport input ssh ---> Establece que solo acepten conexión SSH dentro de las líneas vty
```

**I. Cifrar las contraseñas de texto no cifrado**

Se cifran las contraseñas para que aumente la seguridad con el comando

```
S1(config)#service password-encryption ---> Cifra las contraseñas de texto

S1(config)#
```

**J. Configure un MOTD Banner**

Se establece el banner MOTD con el mensaje de prohibido el acceso no autorizado

```
S1(config)#banner motd #El acceso no autorizado está
prohibido!# ---> Banner de mensaje de alerta al iniciar el
dispositivo
S1(config)#
```

**K. Generar una clave de cifrado RSA Modulo de 1024 bits**

Se establece en 1024 bits en el módulo de cifrado

```
S1(config)#ip domain-name ccna-lab.com ---> Establecer Nombre
de Dominio
S1(config)#crypto key generate rsa ---> Crear clave de
encryption RSA
The name for the keys will be: S1.ccna-lab.com
Choose the size of the key modulus in the range of 360 to
2048 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 ---> Establecer el
tamaño del modulo en 1024 bits
% Generating 1024 bit RSA keys, keys will be non-
exportable...[OK]
S1(config)#
```

**L. Configurar interfaz VLAN 1 establecer la direccioon IPv4 y activar la interfaz**

```
S1(config)#interface vlan 1---> Ingresar al modo de
configuracion Vlan 1
*Mar 1 0:54:40.329: %SSH-5-ENABLED: SSH 1.99 has been enabled
S1(config-if)#ip address 192.168.82.2 255.255.255.128 --->
Configuracion de direccionamiento sobre la vlan
S1(config-if)#
```

**M. Configuración del Gateway predeterminado**

```
S1(config)#ip default-gateway 192.168.82.1 ---> establece un
gateway predeterminado en el dispositivo
S1(config)#
```

**Paso 3: Configurar los equipos**

Configure los equipos host PC-A y PC-B conforme a la tabla de direccionamiento, registre las configuraciones de red del host con el comando **ipconfig /all**.

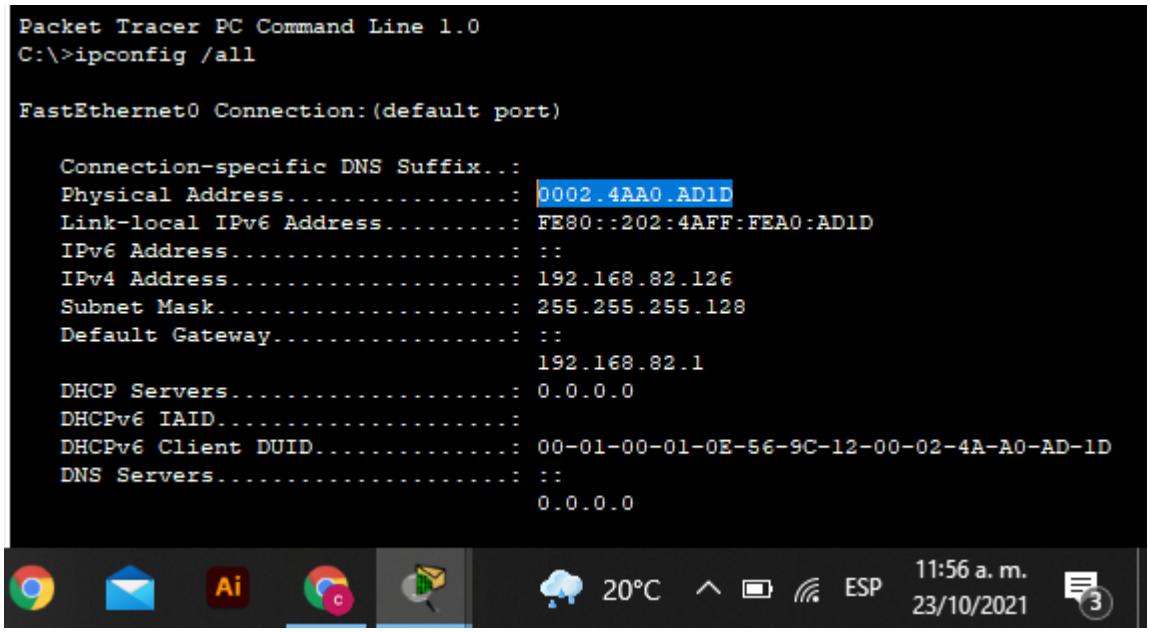
Se establecen las direcciones para los equipos de acuerdo al subneting realizado y se hace la prueba de conexión SSH y ping entre dispositivos

Tabla 3 PC-A Configuracion de Red

| **Descripción** | FastEthernet0 Connection:(default port) |
|---|---|
| **Dirección física** | 0002.4AA0.AD1D |
| **Dirección IP** | 192.168.82.126 |
| **Máscara de subred** | 255.255.255.128 |
| **Gateway predeterminado** | 192.168.82.1 |

Fuente : Prueba de habilidades CISCO CCNAII

Figura 2 Informacion red PC-A



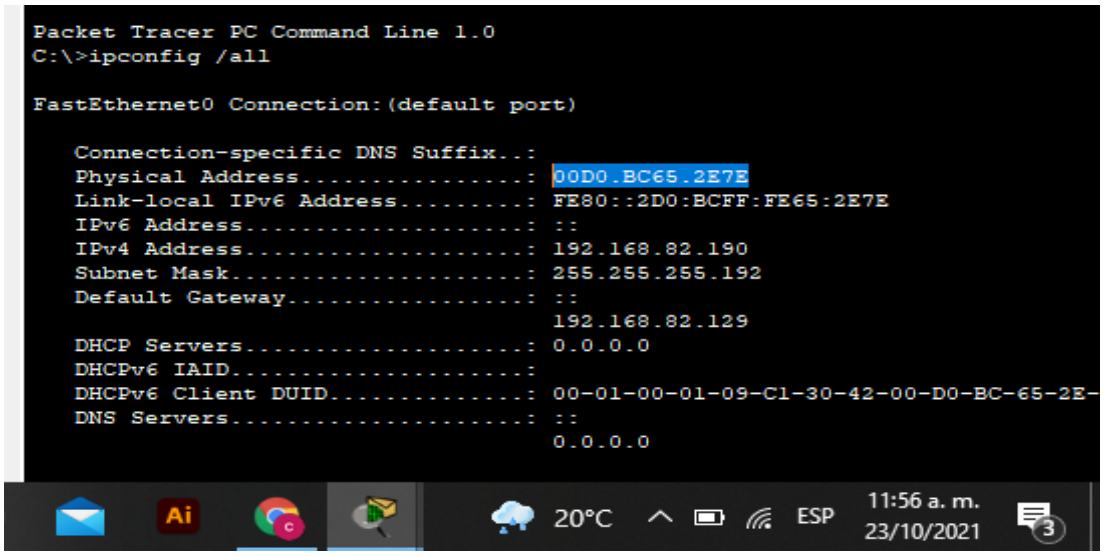

Fuente : Propia

Tabla 4 PC-B Configuracion de red

| **Descripción** | FastEthernet0 Connection:(default port) |
|---|---|
| **Dirección física** | 00D0.BC65.2E7E |
| **Dirección IP** | 192.168.82.126 |
| **Máscara de subred** | 255.255.255.128 |
| **Gateway** | 192.168.82.1 |

Fuente : Propia

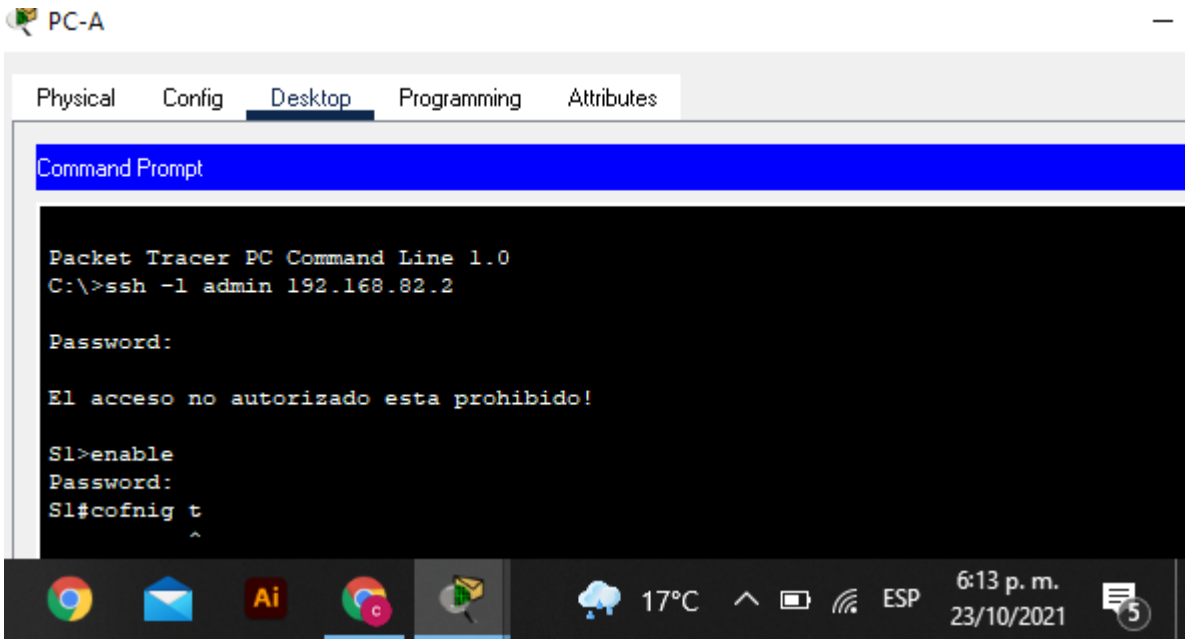
Figura 3 infomacion de red PC-B




Fuente : Propia

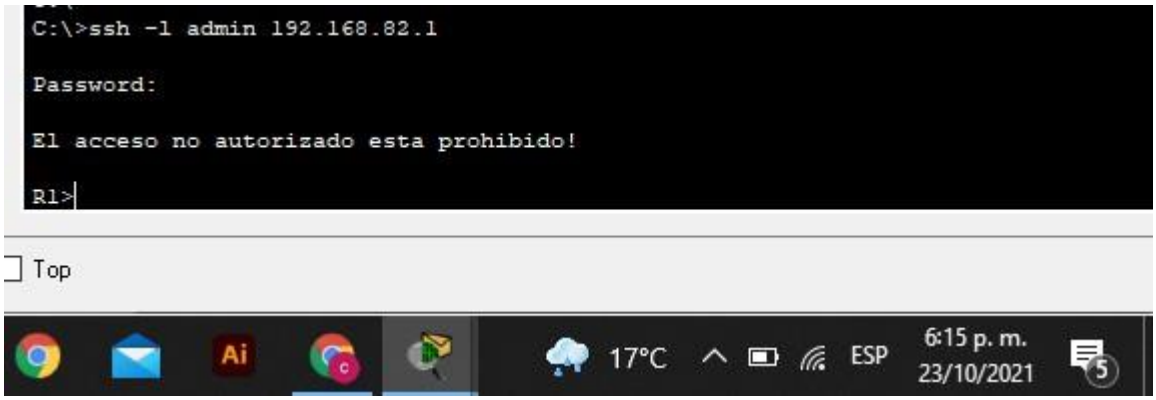
Prueba SSH PC-A a SW1 y R1

Figura 3 prueba SSH 1




Fuente : Propia

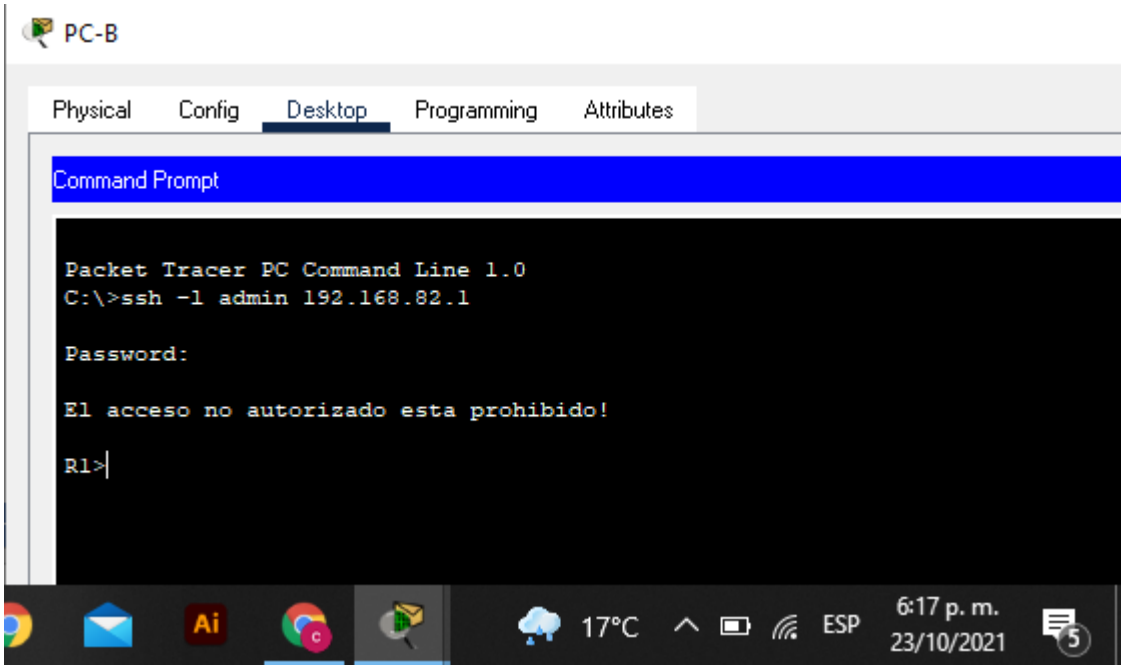
Figura 4 Prueba SSH 2




Fuente : Propia

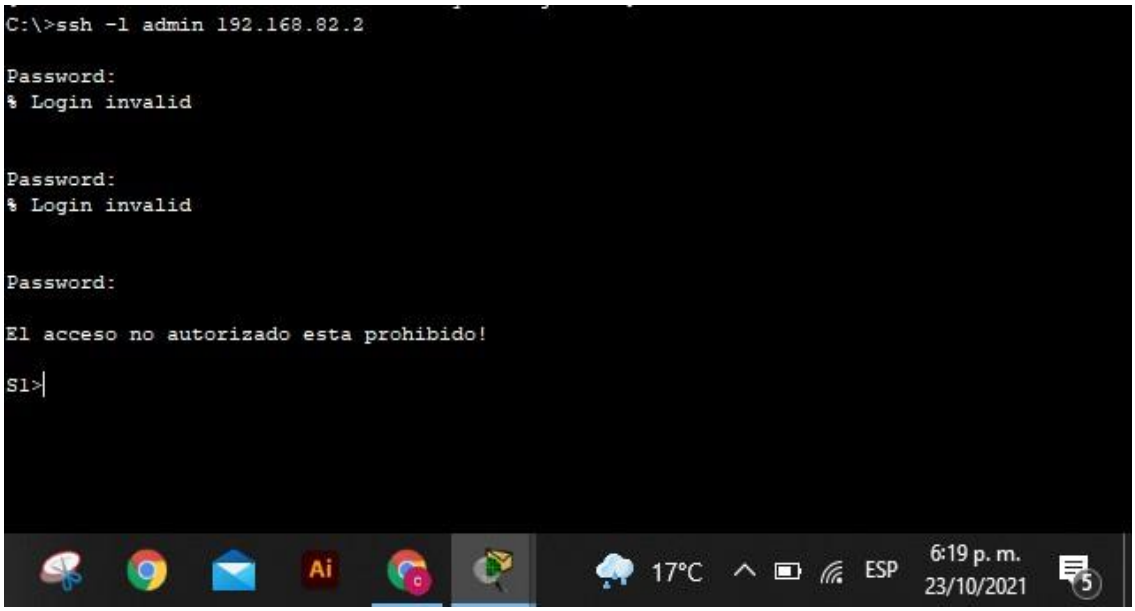
Prueba conexión PC-B a R1 y SW1

Figura 5 Prueba SSH 3




Fuente : Propia

Figura 6 Prueba SSH 4



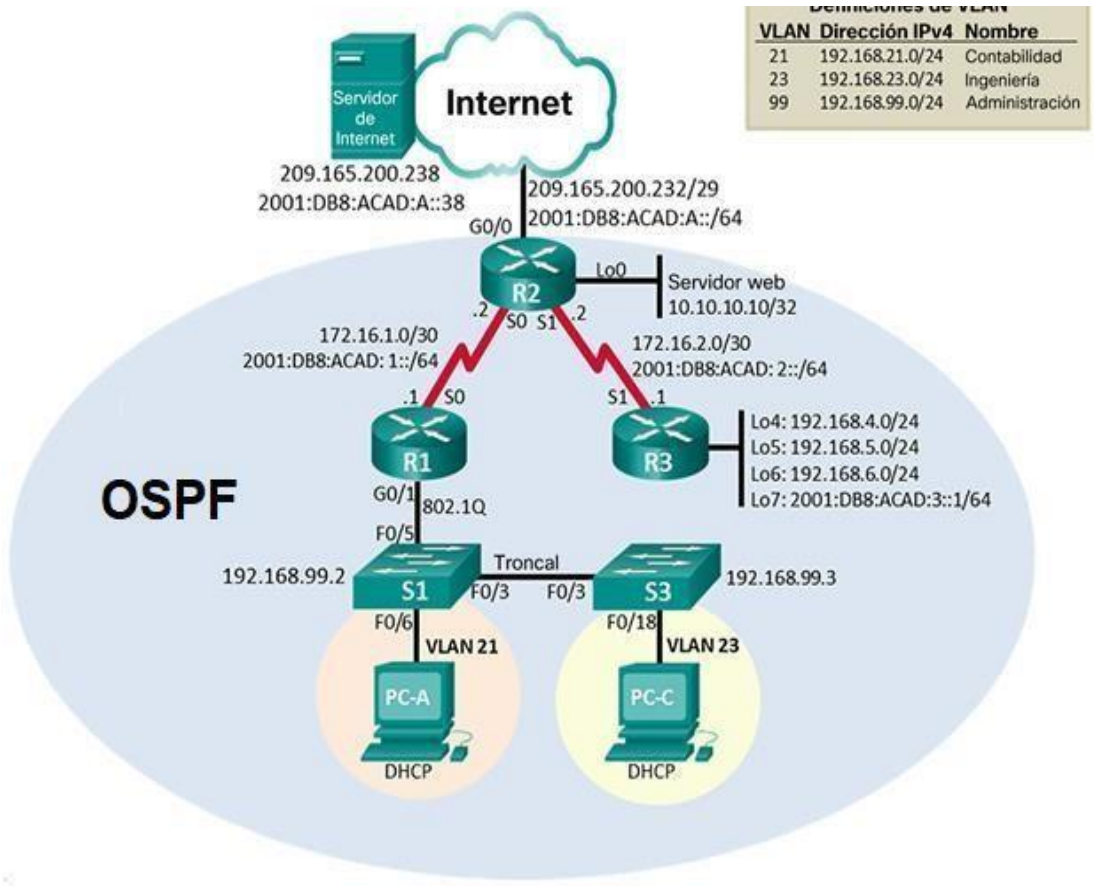

Fuente : Propia

## 1.2 ESCENARIO 2

Se debe configurar una red pequeña para que admita conectividad IPv4 e IPv6, seguridad de switches, routing entre VLAN, el protocolo de routing dinámico OSPF, el protocolo de configuración de hosts dinámicos (DHCP), la traducción de direcciones de red dinámicas y estáticas (NAT), listas de control de acceso (ACL) y el protocolo de tiempo de red (NTP) servidor/cliente. Durante la evaluación, probará y registrará la red mediante los comandos comunes de CLI.

**Topología**

Figura 7 Topología escenario 2




Fuente : Prueba de habilidades CCNA II

## Parte 1: Inicializar dispositivos

### Paso 1: Inicializar y volver a cargar los routers y los switches

Elimine las configuraciones de inicio y vuelva a cargar los dispositivos.

Antes de continuar, solicite al instructor que verifique la inicialización de los dispositivos.

**a. Eliminar el archivo startup-config de todos los routers**

```
Router#erase startup-config ---> Elimina la configuracion de
inicio del dispositivo
Erasing the nvram filesystem will remove all configuration
files! Continue? [confirm]
[OK]
Erase of nvram: complete
%SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram
```

**b. Volver a cargar todos los routers**

```
Router#reload ---> se cargan nuevamente las configuraciones de
inicio del dispositivo
Proceed with reload? [confirm]
System Bootstrap, Version 15.1(4)M4, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
```

**c. Eliminar el archivo startup-config de todos los switches y eliminar la base dedatos de VLAN anterior**

```
Switch>enable
Switch#erase startup-config --> Borrar contenidio de la NVRAM
Erasing the nvram filesystem will remove all configuration
files! Continue? [confirm]
[OK]
```

**d. Volver a cargar ambos switches**

```
Switch#reload ---> se cargan nuevamente las configuraciones de
inicio del dispositivo
Proceed with reload? [confirm]
C2960 Boot Loader (C2960-HBOOT-M) Version 12.2(25r)FX, RELEASE
SOFTWARE (fc4)
Cisco WS-C2960-24TT (RC32300) processor (revision C0) with
21039K bytes of memory.
```

e. **Verificar que la base de datos de VLAN noesté en la memoria flash en ambos switches**

`Switch#show flash` **---> Ver base de datos en el dispositivo**

Figura 8 Ver Vlan SW


Fuente : Propia

**Parte 2: Configurar los parámetros básicos de los dispositivos**

**Paso 1: Configurar la computadora de Internet**

Las tareas de configuración del servidor de Internet incluyen lo siguiente (para obtener información de las direcciones IP, consulte la topología):

Tabla 5 Direccionamiento 2

| Elemento o tarea de configuración | Especificación |
|---|---|
| Dirección IPv4 | 209.165.200.238 |
| Máscara de subred para IPv4 | 255.255.255.248 |
| Gateway predeterminado | 209.165.200.225 |
| Dirección IPv6/subred | 2001:DB8:200:238 |
| Gateway predeterminado IPv6 | 2001:DB8:ACAD:2::1 |

Fuente : Propia

**Paso 2: Configurar R1**

Las tareas de configuración para R1 incluyen las siguientes:

a. **Desactivar la búsqueda DNS**

```
Router>enable ---> Inicio modo privilegiado
Router#config t ---> Ingreso Modo configuración
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#no ip domain-lookup ---> Desactivar búsqueda
DNS
Router(config)#
```

b. **Nombre del router**

```
Router(config)#hostname R1 ---> Renombrar Dispositivo
R1(config)#
```

c. **Contraseña de exec privilegiado cifrada**

```
R1(config)#enable secret class ---> Establecer Contraseña
modo privilegiado cifrada
R1(config)#
```

d. **Contraseña de acceso a la consola**

```
R1(config)#line console 0 ---> Modo de configuracion linea de
consola 0 como primera
R1(config-line)#password cisco ---> Se establece la
contraseña de inicio de consola
R1(config-line)# login ---> activar autenticación al iniciar
dispositivo
```

e. **Contraseña de acceso Telnet**

```
R1(config)#line vty 0 4 ---> Ingreso a config line vty 0 4
para acceso telnet
R1(config-line)#password cisco ---> Se establece la
contraseña de inicio de consola desde telnet
R1(config-line)#login ---> activar autenticación al iniciar
dispositivo
R1(config-line)#
```

**f. Cifrar las contraseñas de texto no cifrado**

```
R1(config)#service password-encryption ---> Cifra las
contraseñas de texto
R1(config)#
```

**g. Mensaje MOTD**

```
R1(config)#banner motd #Se prohibe el acceso no autorizado!!#
---> Banner de mensaje de alerta al iniciar el dispositivo
R1(config)#
```

**h. Interfaz S0/0/0**

```
R1(config)#inter s0/0/0 ---> Ingreso a la interface
R1(config-if)#description Conexion hacia el R2 ---> Se añade
una descripción o etiqueta a la interface
R1(config-if)#ip address 172.16.1.1 255.255.255.252 --->
Configuracion de direccionamiento IPV4 sobre la interface
R1(config-if)#ipv6 address 2001:DB8:ACAD:1::1/64 --->
Configuracion de direccionamiento IPV6 sobre la interface
R1(config-if)#clock rate 128000 ---> activa la sincronización
y fija la velocidad de la trasnferencia a 128000 b/s
R1(config-if)#no shut ---> Activar la interface
```

**i. Rutas predeterminadas**

```
R1(config)#ip route 0.0.0.0 0.0.0.0 s0/0/0 ---> configura la
ruta predenterminada ipv4
%Default route without gateway, if not a point-to-point
interface, may impact performance
R1(config)#ipv6 route ::/0 s0/0/0 ---> configura la ruta
predenterminada ipv6
R1(config)#
```

**Paso 3: Configurar R2**

La configuración del R2 incluye las siguientes tareas:

**a. Desactivar la búsqueda DNS**

```
Router>enable ---> Inicio modo privilegiado
Router#config t ---> Ingreso Modo configuración
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#no ip domain-lookup ---> Desactivar búsqueda
DNS
```

**b. Nombre del router**

```
Router(config)#hostname R2 ---> Renombrar Dispositivo
R2(config)#
```

**c. Contraseña de exec privilegiado cifrada**

```
R2(config)#enable secret class ---> Establecer Contraseña
modo privilegiado cifrada
```

**d. Contraseña de acceso a la consola**

```
R2(config)#line console 0 ---> Modo de configuracion linea de
consola 0 como primera
R2(config-line)#password cisco ---> Se establece la
contraseña de inicio de consola
R2(config-line)#login ---> activar autenticación al iniciar
dispositivo
R2(config-line)#exit
```

**e. Contraseña de acceso Telnet**

```
R2(config)#line vty 0 4 ---> Ingreso a config line vty 0 4
para acceso telnet
R2(config-line)#password cisco Se establece la contraseña de
inicio de consola para telnet
R2(config-line)#login ---> activar autenticación al iniciar
dispositivo
R2(config-line)#
```

**f. Cifrar las contraseñas de texto no cifrado**

```
R2(config)#service password-encryption ---> Cifra las
contraseñas de texto
R2(config)#
```

**g. Habilitar el servidor HTTP**

Comando no soportado por Packet Tracert

**h. Mensaje MOTD**

```
R2(config)#banner motd #Se prohibe el acceso no autorizado! #
---> Banner de mensaje de alerta al iniciar el dispositivo
R2(config)#
```

**i. Interfaz S0/0/0**

```
R2(config)#inter s0/0/0 ---> Ingreso a la interface
R2(config-if)#description Conexion hacia el R1 ---> Se añade
una descripción o etiqueta a la interface
R2(config-if)#ip address 172.16.1.2 255.255.255.252 --->
Configuracion de direccionamiento IPV4 sobre la interface
R2(config-if)#ipv6 address 2001:DB8:ACAD:1::2/64 --->
Configuracion de direccionamiento IPV6 sobre la interface
R2(config-if)#no shutdown ---> Activar la interface
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up
R2(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0,
changed state to up
```

**j. Interfaz S0/0/1**

```
R2(config)#interface s0/0/1 ---> Ingreso a la interface
R2(config-if)#description Conexion Hacia R3 ---> Se añade una
descripción o etiqueta a la interface
R2(config-if)#ip address 172.16.2.2 255.255.255.252 --->
Configuracion de direccionamiento IPV4 sobre la interface
R2(config-if)#ipv6 address 2001:DB8:ACAD:2::2/64 --->
Configuracion de direccionamiento IPV6 sobre la interface
R2(config-if)#clock rate 128000 ---> activa la sincronización
y fija la velocidad a 128000 b/s
R2(config-if)#no shutdown ---> Activar la interface
%LINK-5-CHANGED: Interface Serial0/0/1, changed state to down
R2(config-if)#
```

**k. Interfaz G0/0 (simulación de Internet)**

```
R2#config t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#interface g0/0 ---> Ingreso a la interface
R2(config-if)#description Conexion Hacia Servidor Internet --
-> Se añade una descripción o etiqueta a la interface
R2(config-if)#ip address 209.165.200.233 255.255.255.248 --->
Configuracion de direccionamiento IPV4 sobre la interface
R2(config-if)#ipv6 address 2001:DB8:ACAD:A::1/64 --->
Configuracion de direccionamiento IPV6 sobre la interface
R2(config-if)#no shutdown R2(config-if)#no shutdown --->
Activar la interface
%LINK-5-CHANGED: Interface GigabitEthernet0/0, cangad state
to up
```

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

**l. Interfaz loopback 0 (servidor web simulado)**

```
R2(config)#interface loopback 0 ---> Ingreso a la interface
virtual loopback 0
%LINK-5-CHANGED: Interface Loopback0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0,
changed state to up
R2(config-if)#ip address 10.10.10.10 255.255.255.255 --->
Configuracion de direccionamiento sobre la interface
R2(config-if)#description Simulacion de servidor WEB ---> Se
añade una descripción o etiqueta a la interface
R2(config-if)#
```

**m. Ruta predeterminada**

```
R2(config)#ip route 0.0.0.0 0.0.0.0 g0/0 ---> configura la
ruta predenterminada ipv4
%Default route without gateway, if not a point-to-point
interface, may impact performance
R2(config)#ipv6 route ::/0 g0/0 ---> configura la ruta
predenterminada ipv6
R2(config)#
```

### Paso 4: Configurar R3

La configuración del R3 incluye las siguientes tareas:

**a. Desactivar la búsqueda DNS**

```
Router(config)#no ip domain-lookup ---> Desactivar búsqueda
DNS
```

**b. Nombre del router**

```
Router(config)#hostname R3 ---> Renombrar Dispositivo
```

**c. Contraseña de exec privilegiado cifrada**

```
R3(config)#enable secret class ---> Establecer Contraseña
modo privilegiado cifrada
```

**d. Contraseña de acceso a la consola**

```
R3(config)#line console 0 ---> Modo de configuracion linea de
consola 0 como primera
R3(config-line)#password cisco ---> Se establece la
contraseña de inicio de consola
```

R3(config-line)#login **---> activar autenticación al iniciar dispositivo**

**e. Contraseña de acceso Telnet**

R3(config)#line vty 0 4 **---> Ingreso a config line vty 0 4 para acceso telnet**
R3(config-line)#password cisco **---> Se establece la contraseña de inicio de consola**
R3(config-line)#login **---> activar autenticación al iniciar dispositivo**
R3(config-line)#exit

**f. Cifrar las contraseñas de texto no cifrado**

R3(config)#service password-encryption **---> Cifra las contraseñas de texto**

**g. Mensaje MOTD**

R3(config)#banner motd #Se prohibe el acceso no autorizado!#

**---> Banner de mensaje de alerta al iniciar el dispositivo**

**h. Interfaz S0/0/1**

R3(config)#interface s0/0/1 **---> Ingreso a la interface**
R3(config-if)#description Conexion Hacia R2 **---> Se añade una descripción o etiqueta a la interface**
R3(config-if)#ip address 172.16.2.1 255.255.255.252 **---> Configuracion de direccionamiento IPV4 sobre la interface**
R3(config-if)#ipv6 address 2001:DB8:ACAD:2::1/64 **---> Configuracion de direccionamiento IPV6 sobre la interface**
R3(config-if)#no shutdown **---> Activar la interface**
%LINK-5-CHANGED: Interface Serial0/0/1, changed state to up

**i. Interfaz loopback 4**

R3(config)#interface loopback 4 **---> Ingreso a la interface virtual loopback 4**
%LINK-5-CHANGED: Interface Loopback4, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback4, changed state to up
R3(config-if)#ip address 192.168.4.1 255.255.255.0 **---> Configuracion de direccionamiento sobre la interface**

**j. Interfaz loopback 5**

```
R3(config)#interface loopback 5 ---> Ingreso a la interface
virtual loopback 5
%LINK-5-CHANGED: Interface Loopback5, changed state to up
R3(config-if)#ip address 192.168.5.1 255.255.255.0 --->
Configuracion de direccionamiento sobre la interface
```

**k. Interfaz loopback 6**

```
R3(config)#interface loopback 6 ---> Ingreso a la interface
virtual loopback 6
%LINK-5-CHANGED: Interface Loopback6, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback6,
changed state to up
R3(config-if)#ip address 192.168.6.1 255.255.255.0 --->
Configuracion de direccionamiento sobre la interface
```

**l. Interfaz loopback 7**

```
R3(config)#interface loopback 7 ---> Ingreso a la interface
virtual loopback 6
R3(config-if)#
%LINK-5-CHANGED: Interface Loopback7, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback7,
changed state to up
R3(config-if)#ipv6 address 2001:DB8:ACAD:3::1/64  --->
Configuracion de direccionamiento sobre la interface
```

**m. Rutas Predeterminadas**

```
R3(config)#ip route 0.0.0.0 0.0.0.0 serial0/0/1 --->
configura la ruta predenterminada ipv4
%Default route without gateway, if not a point-to-point
interface, may impact performance
R3(config)#ipv6 route ::/0 serial0/0/1 ---> configura la ruta
predenterminada ipv6
R3(config)#
```

### Paso 5: Configurar S1

La configuración del S1 incluye las siguientes tareas:

**a. Desactivar la búsqueda DNS**

```
Switch>enable ---> Inicio modo privilegiado
Switch#config t ---> Ingreso Modo configuración
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#no ip domain-lookup ---> Desactivar búsqueda
DNS
```

**b. Nombre del switch**

```
Switch(config)#hostname S1 ---> Renombrar Dispositivo
```

**c. Contraseña de exec privilegiado cifrada**

```
S1(config)#enable secret class ---> Establecer Contraseña

modo privilegiado cifrada
```

**d. Contraseña de acceso a la consola**

```
S1(config)#line console 0 ---> Modo de configuracion linea de
consola 0 como primera
S1(config-line)#password cisco ---> Se establece la
contraseña de inicio de consola
S1(config-line)#login ---> activar autenticación al iniciar
dispositivo
```

**e. Contraseña de acceso Telnet**

```
S1(config)#line vty 0 4 ---> Ingreso a config line vty 0 4
para acceso telnet
S1(config-line)#password cisco ---> Se establece la
contraseña de inicio de consola
S1(config-line)#login---> activar autenticación al iniciar
dispositivo
```

**f. Cifrar las contraseñas de texto no cifrado**

```
S1(config)#service password-encryption ---> Cifra las
contraseñas de texto
```

**g. Mensaje MOTD**

```
S1(config)#banner motd #Se prohibe el acceso no autorizado!!#
```

**---> Banner de mensaje de alerta al iniciar el dispositivo**

**Paso 6: Configurar el S3**

La configuración del S3 incluye las siguientes tareas:

**a. Desactivar la búsqueda DNS**

```
Switch(config)#no ip domain-lookup ---> Desactivar búsqueda DNS
```

**b. Nombre del switch**

```
Switch(config)#hostname S3 ---> Renombrar Dispositivo
S3(config)#
```

**c. Contraseña de exec privilegiado cifrada**

```
S3(config)#enable secret class ---> Establecer Contraseña modo privilegiado cifrada
S3(config)#
```

**d. Contraseña de acceso a la consola**

```
S3(config)#line console 0 ---> Modo de configuracion linea de consola 0 como primera
S3(config-line)#password cisco ---> Se establece la contraseña de inicio de consola
S3(config-line)#login ---> activar autenticación al iniciar dispositivo
```

**e. Contraseña de acceso Telnet**

```
S3(config)#line vty 0 4 ---> Ingreso a config line vty 0 4 para acceso telnet
S3(config-line)#password cisco ---> Se establece la contraseña de inicio de consola
S3(config-line)#login ---> activar autenticación al iniciar dispositivo
```

**f. Cifrar las contraseñas de texto no cifrado**

```
S3(config)#service password-encryption ---> Cifra las
contraseñas de texto
```

**g.** Mensaje MOTD

```
S3(config)#banner motd #Se prohibe el acceso no autorizado!!#
---> Banner de mensaje de alerta al iniciar el dispositivo
S3(config)#
```

**Paso 7: Verificar la conectividad de la red**

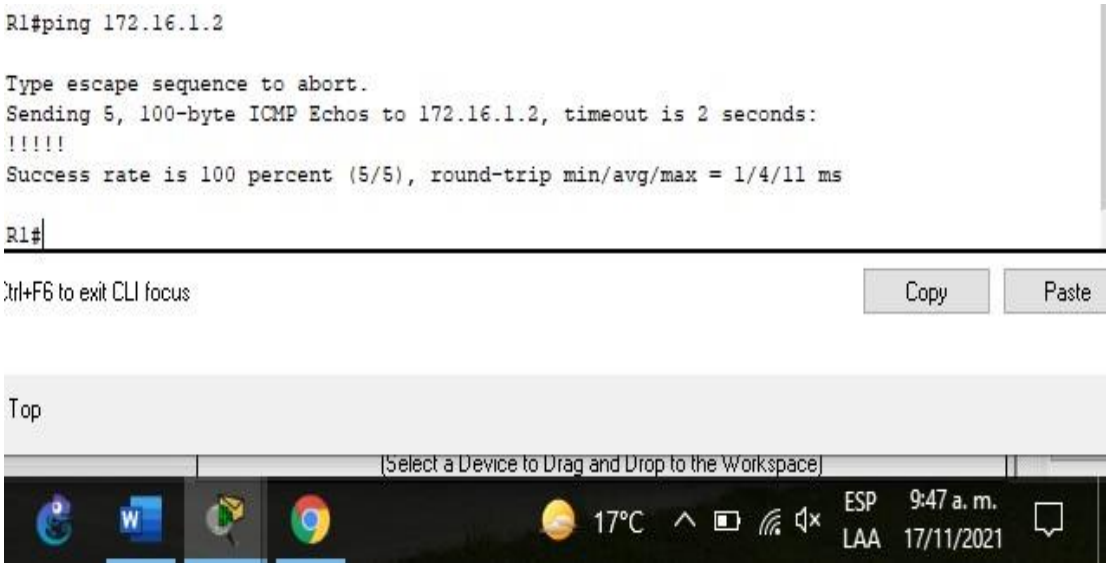
Utilice el comando ping para probar la conectividad entre los dispositivos de red.

Utilice la siguiente tabla para verificar metódicamente la conectividad con cada dispositivo de red. Tome medidas correctivas para establecer la conectividad si alguna de las pruebas falla:

**a. Ping desde R1 a R2 , S0/0/0 dirección 172.16.1.2**

Ping exitoso

Figura 9 Ping R1 a R3




Fuente : Propia

**b. Ping desde R2 a R3 , S0/0/1 dirección 172.16.2.1**

Ping exitoso

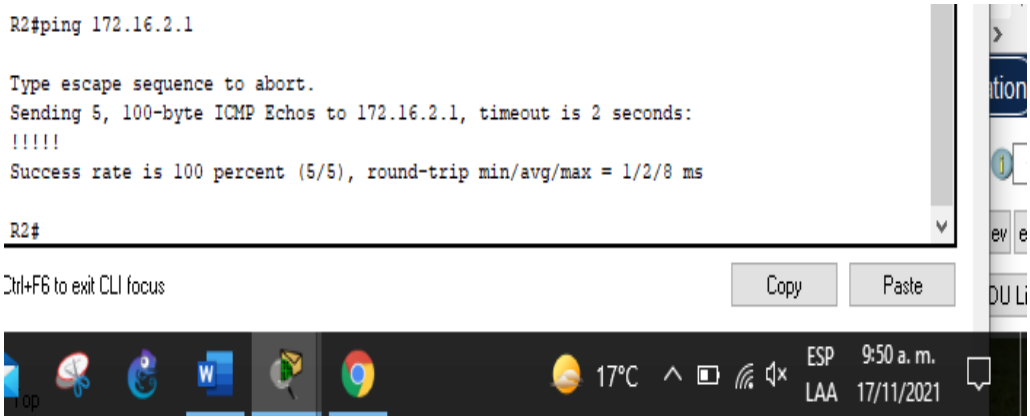
Figura 10 Ping R2 a R3


Fuente : Propia

**c. Ping desde Pc internet a Gateway predeterminado ,dirección 209.165.200.233**

Ping exitoso

Figura 11 Ping PC inter a Gateway




Fuente : Propia

## Parte 3: Configurar la seguridad del switch, las VLAN y el routing entre VLAN

### Paso 1: Configurar S1

La configuración del S1 incluye las siguientes tareas:

**a. Crear la base de datos de VLAN**

```
S1#config t ---> Ingreso Modo configuración
Enter configuration commands, one per line. End with CNTL/Z.
S1(config)#vlan 21 ---> Ingreso modo configuracion VLAN 21
S1(config-vlan)#name Contabilidad ---> Nombrar Vlan
S1(config-vlan)#vlan 23 -->Ingreso modo configuracion VLAN 26
S1(config-vlan)#name Ingenieria ---> Nombrar Vlan
S1(config-vlan)#vlan 99 -->Ingreso modo configuracion VLAN 99
S1(config-vlan)#name administración ---> Nombrar Vlan
```

**b. Asignar la dirección IP deadministración.**

```
S1(config)#interface vlan 99 ---> Ingreso modo configuracion
VLAN 99
S1(config-if)#
%LINK-5-CHANGED: Interface Vlan99, changed state to up
S1(config-if)#ip address 192.168.99.2 255.255.255.0 --->
Configuracion de direccionamiento sobre la vlan
S1(config-if)#no shut ---> Activar la interface
```

**c. Asignar el gateway predeterminado**

```
S1(config)#ip default-gateway 192.168.99.1 ---> establece un
gateway predeterminado en el dispositivo
```

**d. Forzar el enlace troncal en la interfaz F0/3**

```
S1(config)#interface f0/3 ---> Ingreso a la interface
S1(config-if)#switchport mode trunk ---> Establecer la
interface en modo troncal
%LINEPROTO-5-UPDOWN: Line protocol on Interface
FastEthernet0/3, changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface
FastEthernet0/3, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99,
changed state to up
S1(config-if)#switchport trunk native vlan 1 ---> Especifica
la vlan nativa para enlaces troncales
```

**e. Forzar el enlace troncal en la interfaz F0/5**

```
S1(config)#interface f0/5 ---> Ingreso a la interface
S1(config-if)#switchport mode trunk ---> Establecer la
interface en modo troncal
S1(config-if)#switchport trunk native vlan 1 ---> Especifica
la vlan nativa para enlaces troncales
S1(config-if)#
```

**f. Configurar el resto de los puertos comopuertos de acceso**

```
S1(config)#interface range f0/1-2,f0/4,f0/6-24,g0/1-2 --->
Selecciona las interfaces a la vez en rango que se requiera
S1(config-if-range)#switchport mode Access ---> se establece
el modo acceso en las interfaces seleccionadas
```

**g. Asignar F0/6 a la VLAN 21**

```
S1(config)#interface f0/6 ---> Ingreso a la interface
S1(config-if)#switchport access vlan 21 ---> se asigna la
interface a la vlan
S1(config-if)#
```

**h. Apagar todos los puertos sin usar**

```
S1(config)#interface range f0/1-2,f0/4,f0/7-24,g0/1-2 --->
Selecciona las interfaces a la vez en rango que se requiera
S1(config-if-range)#shutdown ---> se apagan las interfaces
seleccionadas
```

**Paso 2: Configurar el S3**

La configuración del S3 incluye las siguientes tareas:

**a. Crear la base de datos de VLAN**

```
S3(config)#vlan 21 ---> Ingresar al modo de configuracion
Vlan 21
S3(config-vlan)#name Contabilidad ---> Nombrar Vlan
S3(config-vlan)#vlan 23 ---> Ingresar al modo de
configuracion Vlan 23
S3(config-vlan)#name Ingenieria ---> Nombrar Vlan
S3(config-vlan)#vlan 99 ---> Ingresar al modo de
configuracion Vlan 23
S3(config-vlan)#name Administración ---> Nombrar Vlan
S3(config-vlan)#
```

**b. Asignar la dirección IP de administración**

```
S3(config)#interface vlan 99 ---> Ingreso modo configuracion
VLAN 21
S3(config-if)#
%LINK-5-CHANGED: Interface Vlan99, changed state to up
S3(config-if)#ip address 192.168.99.3 255.255.255.0 --->
Configuracion de direccionamiento sobre la vlan
```

**c. Asignar el gateway predeterminado.**

```
S3(config)#ip default-gateway 192.168.99.1 ---> establece un
gateway predeterminado en el dispositivo
S3(config)#
```

**d. Forzar el enlace troncal en la interfaz F0/3**

```
S3(config)#interface f0/3 ---> Ingreso a la interface
S3(config-if)#switchport mode trunk ---> Establecer la
interface en modo troncal
S3(config-if)#switchport trunk native vlan 1 ---> Especifica
la vlan nativa para enlaces troncales
S3(config-if)#
```

**e. Configurar el resto de los puertos comopuertos de acceso**

```
S3(config-if)#interface range f0/1-2,f0/4-24,g0/1-2 --->
Selecciona las interfaces a la vez en rango que se requiera
S3(config-if-range)#switchport mode access ---> se establece
el modo acceso en las interfaces seleccionadas
S3(config-if-range)#
```

**f. Asignar F0/18 a la VLAN 21**

```
S3(config)#interface f0/18 ---> Ingreso a la interface
S3(config-if)#switchport access vlan 21 ---> se asigna la
interface a la vlan
```

**g. Apagar todos los puertos sin usar**

```
S3(config)#interface range f0/1-2,f0/4-17,f0/19-24,g0/1-2---> Selecciona las interfaces a la vez en rango que se requiera
S3(config-if-range)#shutdown ---> Apagar las interfaces
%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/2, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/4, changed state to administratively down
```

**Paso 3: Configurar R1**

Las tareas de configuración para R1 incluyen las siguientes:

**a. Configurar la subinterfaz 802.1Q .21 enG0/1**

```
R1(config)#interface g0/1.21 ---> Ingresar al modo de configuracion de interface virtual

R1(config-subif)#description LAN Contabilidad ---> Se añade una descripción o etiqueta a la interface

R1(config-subif)#encapsulation dot1q 21 --->habilita 802.1Q y asocia una VLAN específica a la subinterfaz.

R1(config-subif)#ip address 192.168.21.1 255.255.255.0 ---> Configuracion de direccionamiento sobre la interface

R1(config-subif)#
```

**b. Configurar la subinterfaz 802.1Q .23 enG0/1**

```
R1(config)#interface g0/1.23 ---> Ingresar al modo de configuracion de interface virtual

R1(config-subif)#description LAN Ingenieria ---> Se añade una descripción o etiqueta a la interface

R1(config-subif)#encapsulation dot1q 23--->habilita 802.1Q y asocia una VLAN específica a la subinterfaz.

R1(config-subif)#ip address 192.168.23.1 255.255.255.0 ---> Configuracion de direccionamiento sobre la interface
```

c. **Configurar la subinterfaz 802.1Q .99 enG0/1**

```
R1(config-subif)#interface g0/1.99 ---> Ingresar al modo de
configuracion de interface virtual

R1(config-subif)#description LAN Administración ---> Se añade
una descripción o etiqueta a la interface

R1(config-subif)#encapsulation dot1q 99 --->habilita 802.1Q y
asocia una VLAN específica a la subinterfaz.

R1(config-subif)#ip address 192.168.99.1 255.255.255.0 --->
Configuracion de direccionamiento sobre la interface
```

d. **Activar la interfaz G0/1**

```
R1(config-subif)#interface g0/1 ---> Ingresar al modo de
configuracion de interface

R1(config-if)#no shutdown ---> Activar la interface

%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state
to up

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

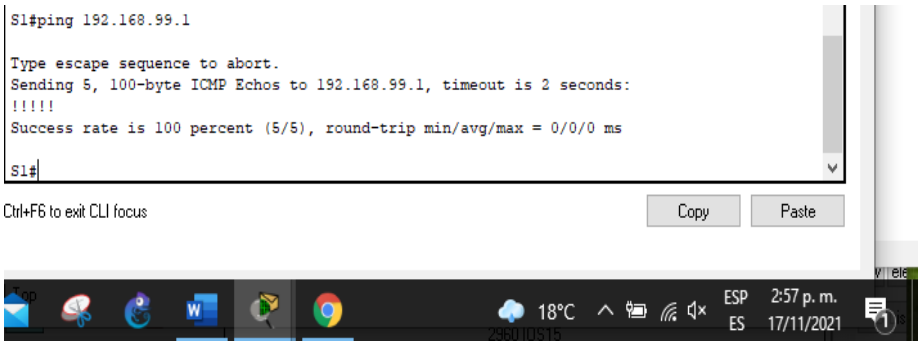
**Paso 4: Verificar la conectividad de la red**

Utilice el comando ping para probar la conectividad entre los switches y el R1.

a. **Ping desde S1 a R1, dirección VLAN 99 , IP 192.168.99.1**

**Ping exitoso**

Figura 12 Ping S1 A R1

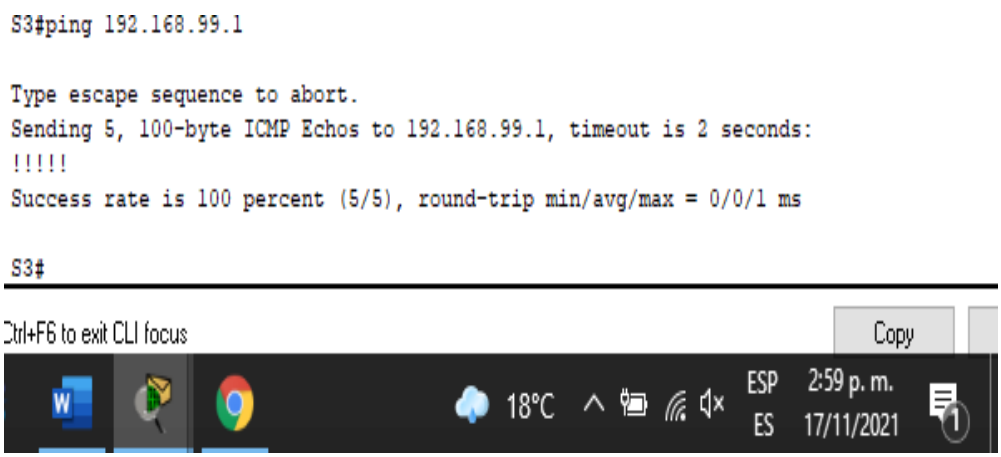



Fuente : Propia

**b.** Ping desde S3 a R1, dirección VLAN 99 , IP 192.168.99.1

**Ping exitoso**

Figura 13 Ping de S3 a R1

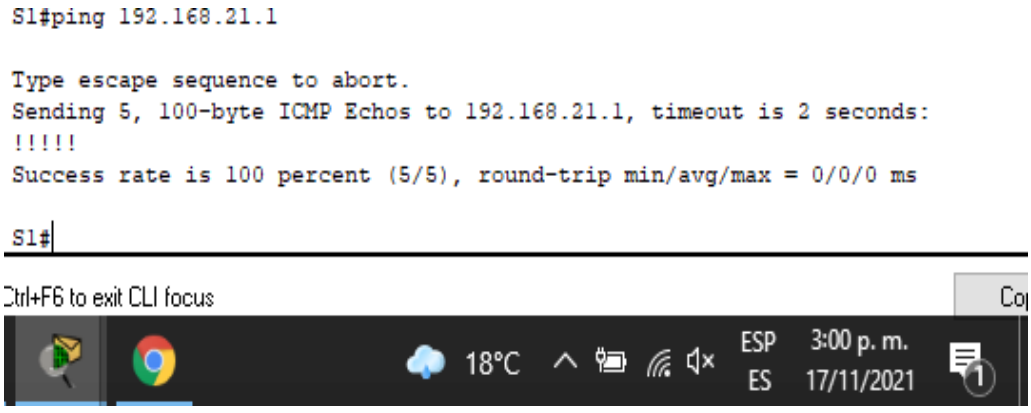



Fuente : Propia

**c.** Ping desde S1 a R1, dirección VLAN 21 , IP 192.168.21.1

**Ping exitoso**

Figura 14 Ping de S1 a R1




Fuente : Propia

**d.** Ping desde S3 a R1, dirección VLAN 23 , IP 192.168.23.1

**Ping exitoso**

Figura 15 Ping de S3 a R1


Fuente : Propia

## Parte 4: Configurar el protocolo de routing dinámico OSPF

### Paso 1: Configurar OSPF en el R1

Las tareas de configuración para R1 incluyen las siguientes:

**a. Configurar OSPF área 0**

**b. Anunciar las redes conectadas directamente**

**c. Establecer todas las interfaces LAN como pasivas**

**d. Desactive la sumarización automática**

```
R1(config)#router ospf 1 ---> Habilitar enrutamiento OSPF en
el router
R1(config-router)#network 172.16.1.0 0.0.0.3 area 0 --->
habilitar el OSPF en las redes
R1(config-router)#network 192.168.21.0 0.0.0.255 area 0
R1(config-router)#network 192.168.23.0 0.0.0.255 area 0
R1(config-router)#network 192.168.24.0 0.0.0.255 area 0
R1(config-router)#passive-interface g0/1.21 ---> Evita la
transmisión de mensajes de routing a través de la interface
seleccionada
R1(config-router)#passive-interface g0/1.23
R1(config-router)#passive-interface g0/1.99

Comando auto summary no soportado para OSPF
```

**Paso 2: Configurar OSPF en el R2**

La configuración del R2 incluye las siguientes tareas:

a. **Configurar OSPF área 0**
b. **Anunciar las redes conectadas directamente**
c. **Establecer todas las interfaces LAN (loopback) como pasivas**
d. **Desactive la sumarización automática**

```
R2(config)#router ospf 1 ---> Habilitar enrutamiento OSPF en
el router
R2(config-router)#network 172.16.1.0 0.0.0.3 area 0 --->
habilitar el OSPF en las redes
R2(config-router)#network 172.16.1.0 0.0.0.3 area 0
06:58:23: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.99.1 on
Serial0/0/0 fr
R2(config-router)#network 172.16.2.0 0.0.0.3 area 0
R2(config-router)#network 172.16.2.0 0.0.0.3 area 0
06:58:53: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.6.1 on
Serial0/0/1 from LOADING to FULL, Loading Done
R2(config-router)#network 10.10.10.10 0.0.0.0 area 0
R2(config-router)#passive-interface loopback 0 ---> Evita la
transmisión de mensajes de routing a través de la interface
seleccionada
R2(config-router)#

Comando auto summary no soportado para OSPF
```

**Paso 3: Configurar OSPF en el R3**

La configuración del R3 incluye las siguientes tareas:

a. **Configurar OSPF área 0**
b. **Anunciar las redes IPv4 conectadas directamente**
c. **Establecer todas las interfaces LAN IPv4 (loopback) como pasivas**
d. **Desactive la sumarización automática**

```
R3(config)#router ospf 1 ---> Habilitar enrutamiento OSPF en
el router
R3(config-router)#network 172.16.2.0 0.0.0.3 area 0 --->
habilitar el OSPF en las redes
R3(config-router)#network 192.168.4.0 0.0.0.255 area 0
R3(config-router)#network 192.168.5.0 0.0.0.255 area 0
R3(config-router)#network 192.168.6.0 0.0.0.255 area 0
R3(config-router)#passive-interface loopback 4 ---> Evita la
transmisión de mensajes de routing a través de la interface
seleccionada
R3(config-router)#passive-interface loopback 5
R3(config-router)#passive-interface loopback 6
R3(config-router)#
06:58:53: %OSPF-5-ADJCHG: Process 1, Nbr 10.10.10.10 on
Serial0/0/1 from LOADING to FULL, Loading Done
```

**Paso 4: Verificar la información de OSPF**

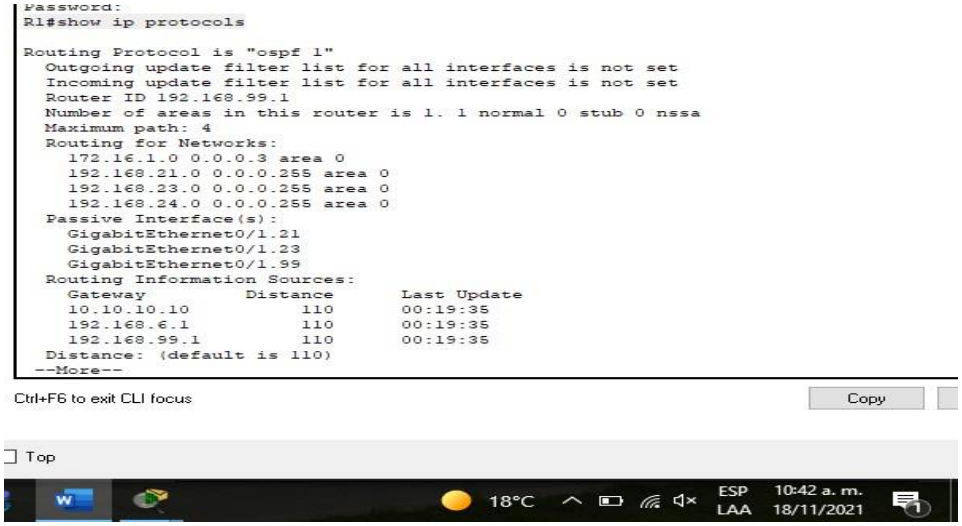
Verifique que OSPF esté funcionando como se espera. Introduzca el comando de CLI adecuado para obtener la siguiente información:

a. **¿Con qué comando se muestran la ID del proceso OSPF, la ID del router, las redes de routing y las interfaces pasivas configuradasen un router?**

   **Se utiliza el comando**

   ```
   R1#show ip protocols.
   ```

Figura 16 Ver Procesos OSPF



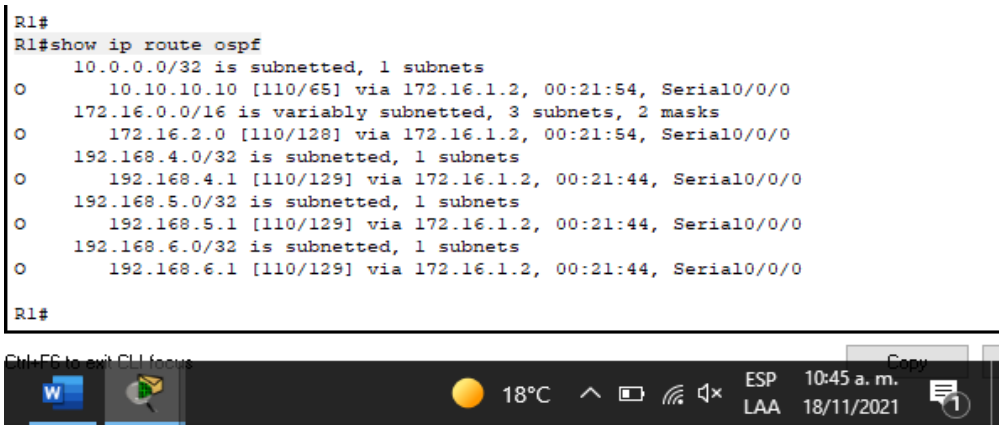

Fuente : Propia

**b. ¿Qué comando muestra solo las rutas OSPF?**

**Se utiliza el comando**

```
R1#show ip route ospf
```

Figura 17 Rutas OSPF

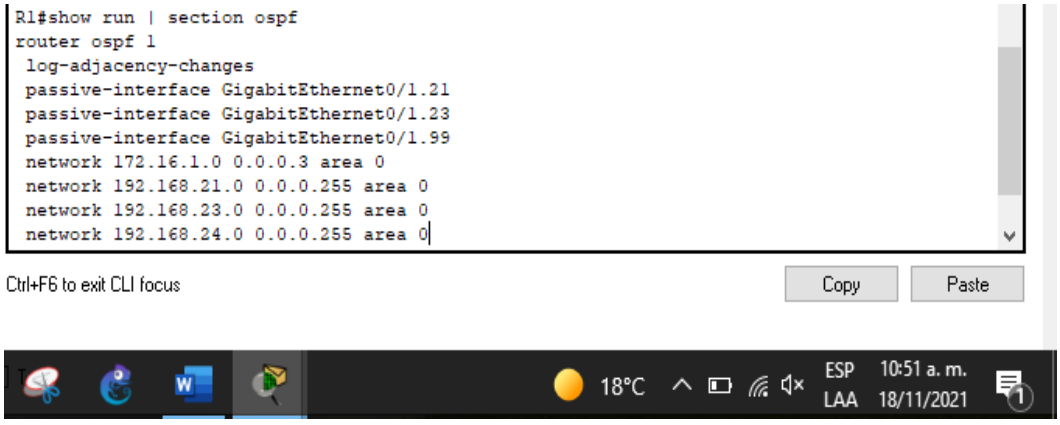



Fuente : Propia

**c. ¿Qué comando muestra la sección de OSPF de la configuraciónen ejecución?**

```
R1#show run | section ospf
router ospf 1
```

Figura 18 Sección OSPF




Fuente : Propia

**Parte 5: Implementar DHCP y NAT para IPv4**

**Paso 1: Configurar el R1 como servidor de DHCP para las VLAN 21 y 23**

Las tareas de configuración para R1 incluyen las siguientes:

a. **Reservar las primeras 20 direcciones IP enla VLAN 21 para configuraciones estáticas**

```
R1(config)#ip dhcp excluded-address 192.168.21.1
192.168.21.20 ---> se excluyen direcciones para reservarlas
en futuras configuraciones Vlan 21
```

b. **Reservar las primeras 20 direcciones IP enla VLAN 23 para configuraciones estáticas**

```
R1(config)#ip dhcp excluded-address 192.168.23.1 192.168.23.20 ---
> se excluyen direcciones para reservarlas en futuras
configuraciones Vlan 23
```

c. **Crear un pool de DHCP para la VLAN 21.**

```
R1(config)#ip dhcp pool ACCT ---> Crear pool dhcp y se nombra
R1(dhcp-config)#network 192.168.21.0 255.255.255.0 ---> se
establece la red de la vlan 21
R1(dhcp-config)#default-router 192.168.21.1 ---> establece un
gateway predeterminado al pool
R1(dhcp-config)#dns-server 10.10.10.10 ---> establece un dns
al pool
R1(dhcp-config)#ip domain-name ccna-sa.com ---> Establecer
Nombre de Dominio
R1(config)#
```

d. **Crear un pool de DHCP para la VLAN 23**

```
R1(config)#ip dhcp pool ENGNR ---> Crear pool dhcp y se
nombra
R1(dhcp-config)#network 192.168.23.0 255.255.255.0 ---> se
establece la red de la vlan 23
R1(dhcp-config)#default-router 192.168.23.1 ---> establece un
gateway predeterminado al pool
R1(dhcp-config)#dns-server 10.10.10.10 ---> establece un dns
al pool
R1(dhcp-config)#ip domain-name ccna-sa.com ---> Establecer
Nombre de Dominio
```

## 1 Paso 2: Configurar la NAT estática y dinámica en el R2

La configuración del R2 incluye las siguientes tareas:

### a. Crear una base de datos local con unacuenta de usuario

```
R2(config)#username webuser privilege 15 secret cisco12345
--> indica el nombre del usuario, el nivel de privilegio
del usuario y una clave secreta encriptada.
R2(config)#
```

### b. Habilitar el servicio del servidor HTTP

Comando no soportado

### c. Configurar el servidor HTTP para utilizar labase de datos local para la autenticación

Comando no soportado

### d. Crear una NAT estática al servidor web.

```
R2(config)#ip nat inside source static 10.10.10.10
209.165.200.237 ---> Establece la traducción estática
entre una dirección local interna y una dirección global
interna.
R2(config)#
```

### e. Asignar la interfaz interna y externa para la NAT estática

```
R2(config)#interface g0/0 ---> Ingreso a la interface
R2(config-if)#ip nat outside ---> Identificar la interfaz
como externa.
R2(config-if)#interface s0/0/0 ---> Ingreso a la interface
R2(config-if)#ip nat inside --> Identificar la interfaz como
interna
R2(config-if)#interface s0/0/1
R2(config-if)#ip nat inside
R2(config-if)#
```

**f. Configurar la NAT dinámica dentro de unaACL privada**

**Lista de acceso: 1**

Permitir la traducción de las redes de Contabilidad y de Ingeniería en el R1

Permitir la traducción de un resumen de las redes LAN

```
R2(config)#access-list 1 permit 192.168.21.0 0.0.0.255 --->se crea la lista y posteriormente se asocia a una interfaz entrante o saliente.
R2(config)#access-list 1 permit 192.168.23.0 0.0.0.255
R2(config)#access-list 1 permit 192.168.4.0 0.0.0.255
```

**g. Defina el pool de direcciones IP públicasutilizables.**

```
R2(config)#ip nat pool INTERNET 209.165.200.233 209.165.200.236 netmask 255.255.255.248 --->Definir el conjunto de direcciones globales que se debe usar para la traducción.
```

**h. Definir la traducción de NAT dinámica**

```
R2(config)#ip nat inside source list 1 pool INTERNET --->Especificar la lista de acceso y el conjunto que se definieron en los pasos anteriores para establecer la traducción dinámica de origen.
R2(config)#
```

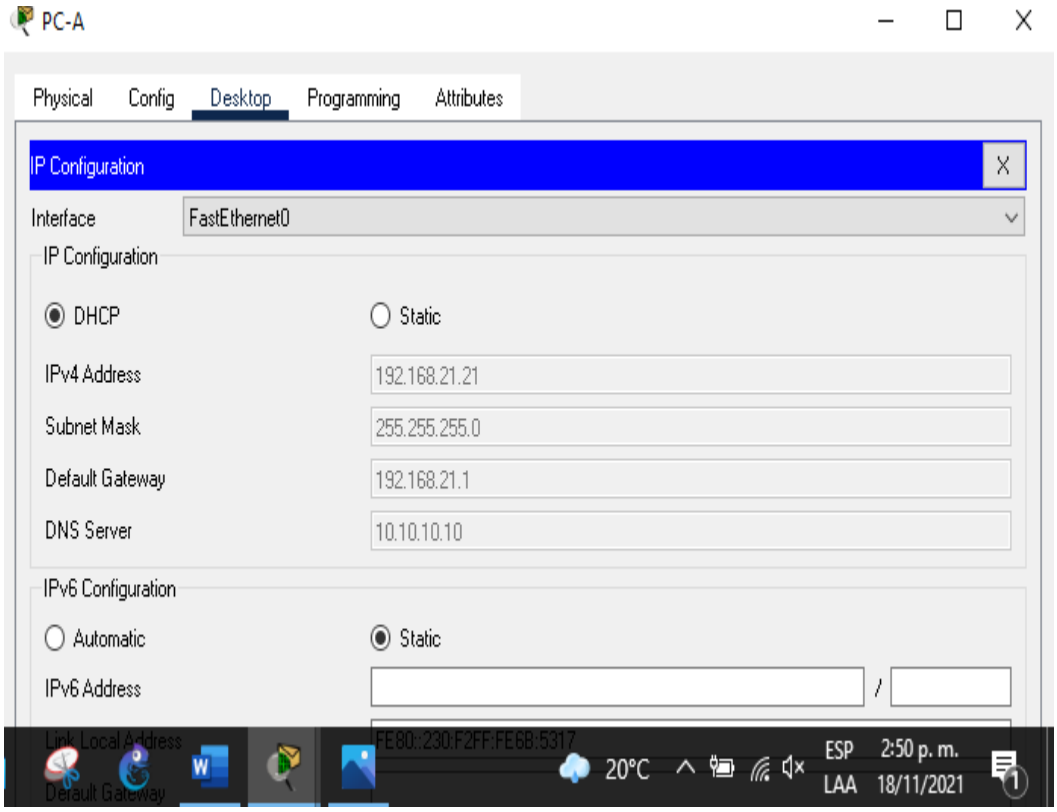
**Paso 3: Verificar el protocolo DHCP y la NAT estática**

Utilice las siguientes tareas para verificar que las configuraciones de DHCP y NAT estática funcionen de forma correcta. Quizá sea necesario deshabilitar el firewall de las computadoras para que los pingsse realicen correctamente.

a. **Verificar que la PC-A haya adquirido información de IP del servidor de DHCP**

**dhcp asignado con exito**

Figura 19 DHCP PC A

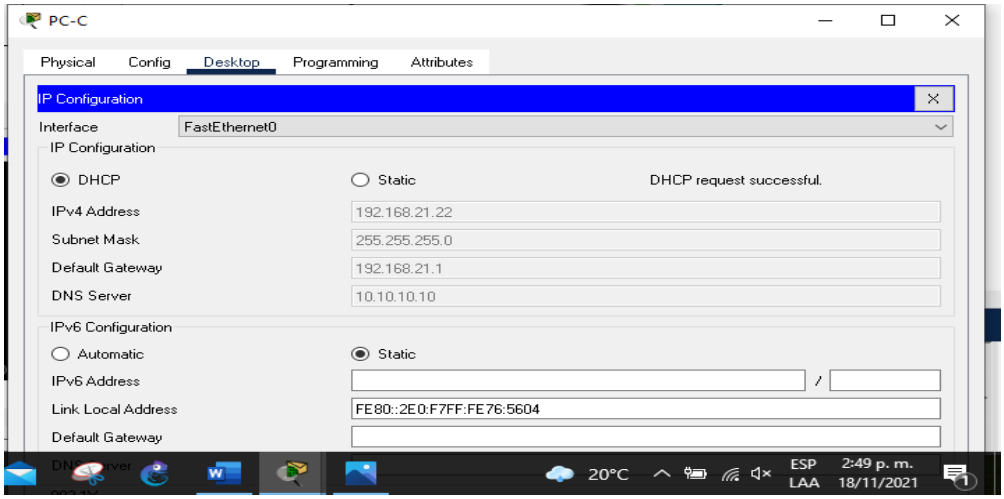



Fuente : Propia

**b. Verificar que la PC-C haya adquirido información de IP del servidor de DHCP**

**dhcp asignado con exito**

Figura 20 DHCP a PC-C

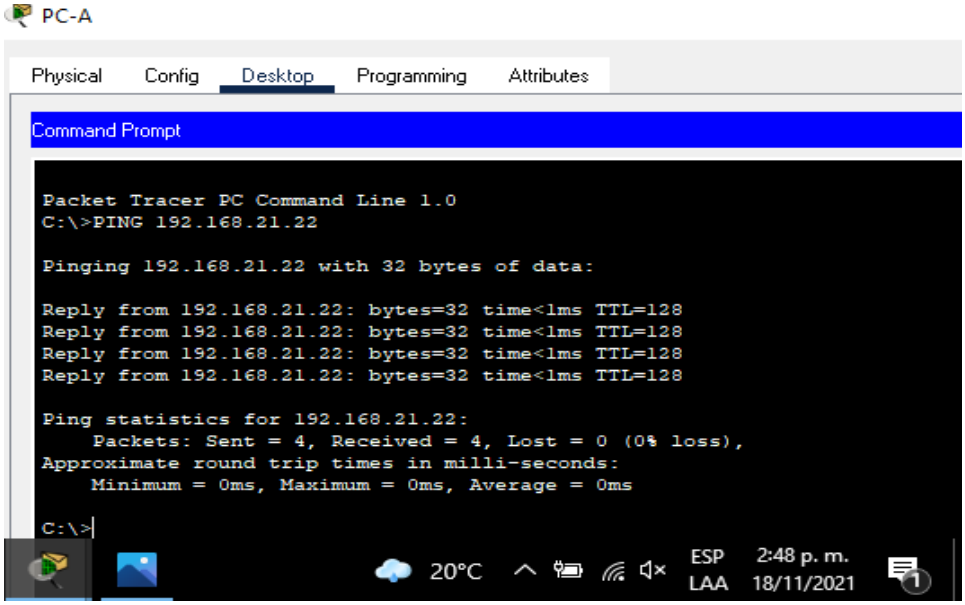



Fuente : Propia

**c. Verificar que la PC-A pueda hacer ping ala PC-C**

**Ping exitoso**

Figura 21 Ping de PC-A a PC-C

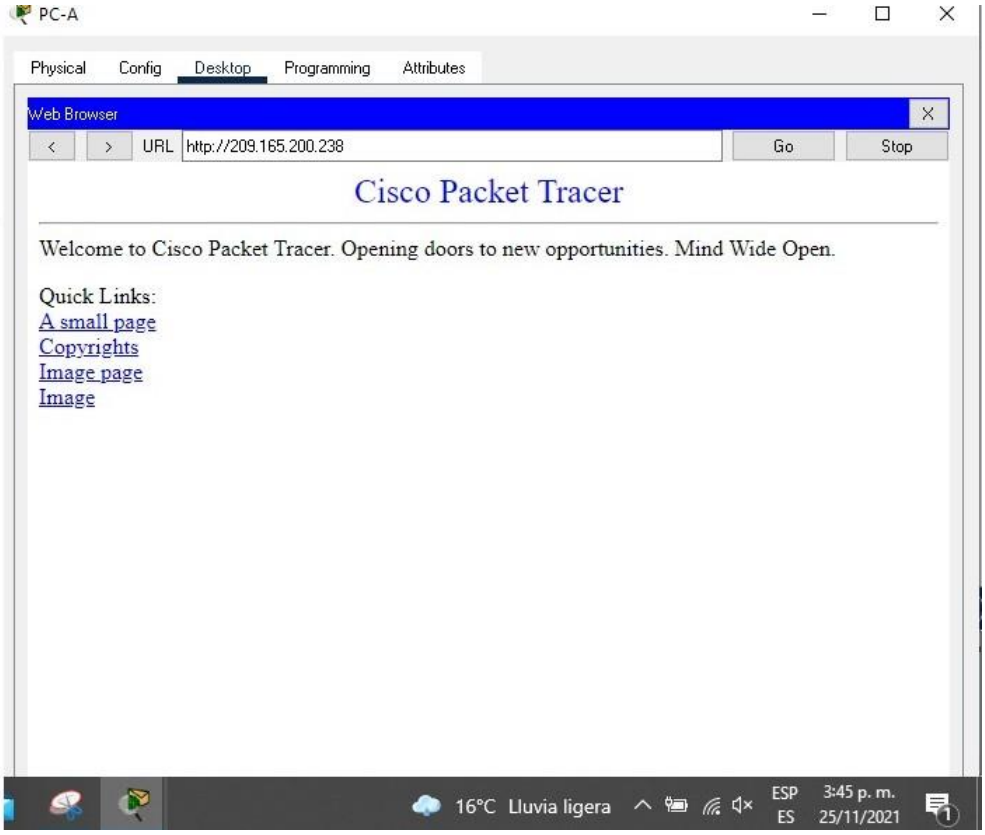



Fuente : Propia

**d. Utilizar un navegador web en la computadora de Internet para acceder alservidor web (209.165.200.237) Iniciar sesión con el nombre de usuario webuser y la contraseña cisco12345**

No solicita credenciales por el comando http no soportado , se prueba la conexión al servidor web desde la PC-A

Figura 22 Servidor Web




Fuente : Propia

**Parte 6: Configurar NTP**

**a. Ajuste la fecha y hora en R2.**

**5 de marzo de 2016, 9 a. m.**

```
R2#clock set 9:00:00 5 march 2016 ---> Establece la hora y fecha solicitada en el dispositivo
R2#
```

**b. Configure R2 como un maestro NTP.**

R2(config)#ntp master 5 **--->se establece el protocolo de tiempo de red en el R2 como maestro**

**c. Configurar R1 como un cliente NTP. Servidor R2**

R1(config)#ntp server 172.16.1.2 **---> se asigna el servidor R2 al R1 como master**
R1(config)#

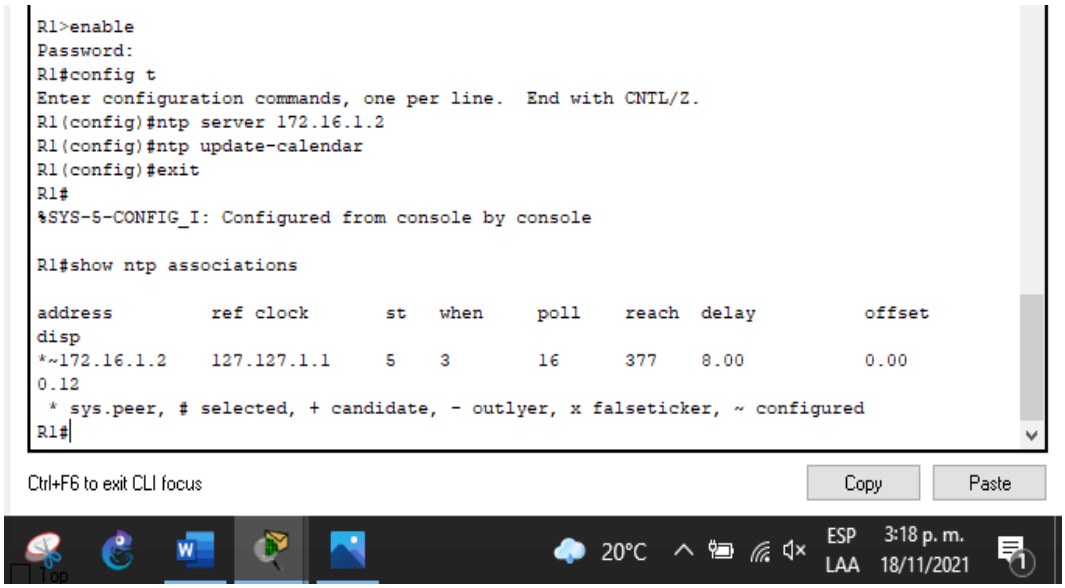
**d. Configure R1 para actualizaciones de calendario periódicas con hora NTP.**

R1(config)#ntp update-calendar **---> establece actualizaciones de calendario cada vez que la hora cambia**
R1(config)#

**e. Verifique la configuración de NTP en R1.**

R1#show ntp associations

Figura 23 ver configuracion NTP




Fuente : Propia

**Parte 7: Configurar y verificar las listas de control de acceso (ACL)**

**Paso 1: Restringir el acceso a las líneas VTY en el R2**

**a. Configurar una lista de acceso con nombre para permitir que solo R1 establezca una conexión Telnet con R2**

Nombre de la ACL: **ADMIN- MGT**

```
R2(config)#ip access-list standard ADMIN-MGT ---> se asigna el nombre a la ACL standar
R2(config-std-nacl)#permit host 172.16.1.1 ---> Se establece la dirección R1 permitir conexión Telnet a R2
```

**b. Aplicar la ACL con nombre a las líneas VTY**

```
R2(config)#line vty 0 15
R2(config-line)#access-class ADMIN-MGT in
```

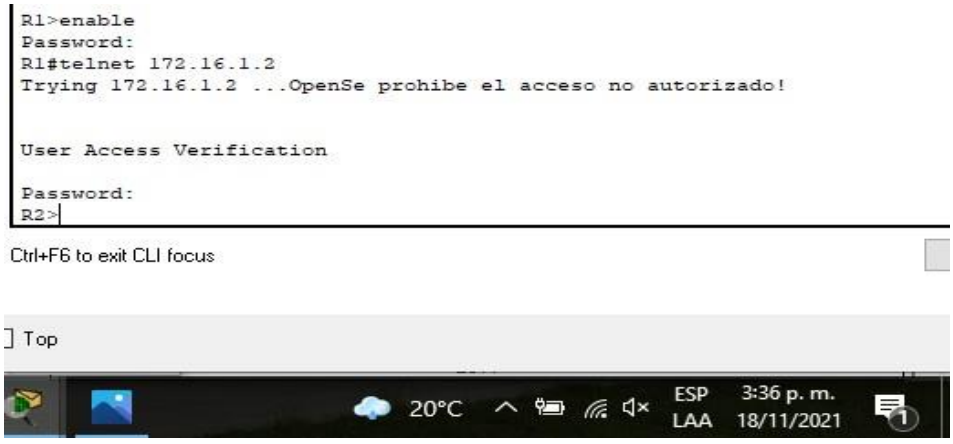
**c. Permitir acceso por Telnet a las líneas de VTY**

```
R2(config-line)#transport input telnet ---> Permite las conexiones Telnet en las líneas vty
R2(config-line)#
```

**d. Verificar que la ACL funcione como se espera**

Prueba de conexión desde R1 a R2 via telnet

Figura 24 Telnet R1 a R2




Fuente : Propia

Se intenta realizar conexión desde el R3 pero es rechazada por la lista de acceso

Figura 25 Error Telnet R3

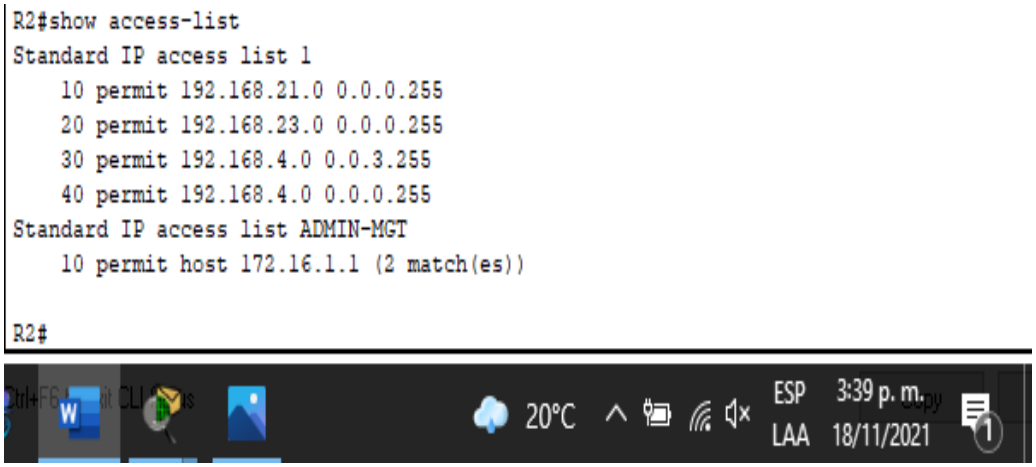

Fuente : Propia

**Paso 2: Introducir el comando de CLI adecuado que se necesita para mostrar lo siguiente**

a. **Mostrar las coincidencias recibidas poruna lista de acceso desde la última vez que se restableció**

`R2#show access-list ---> Muestra las ACL creadas`

Figura 26 Ver ACL




Fuente : Propia

**b. Restablecer los contadores de una listade acceso**

Comando no soportado en packet tracert

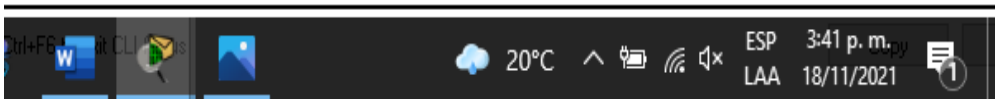
```
R2#Clear ip Access-list counters
```

**c. ¿Qué comando se usa para mostrar qué ACL se aplica a una interfaz y la dirección enque se aplica?**

Se utiliza el comando
`R2#show ip interface` **`---> se muestra información general sobre las interfaces , entre ellas las ACL aplicadas`**

Figura 27 Ver ACL

```
R2#show ip interface
GigabitEthernet0/0 is up, line protocol is up (connected)
  Internet address is 209.165.200.233/29
  Broadcast address is 255.255.255.255
  Address determined by setup command
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Outgoing access list is not set
  Inbound  access list is not set
  Proxy ARP is enabled
  Security level is default
  Split horizon is enabled
  ICMP redirects are always sent
  ICMP unreachables are always sent
  ICMP mask replies are never sent
  IP fast switching is disabled
  IP fast switching on the same interface is disabled
  IP Flow switching is disabled
  IP Fast switching turbo vector
  IP multicast fast switching is disabled
  IP multicast distributed fast switching is disabled
  Router Discovery is disabled
 --More--
```



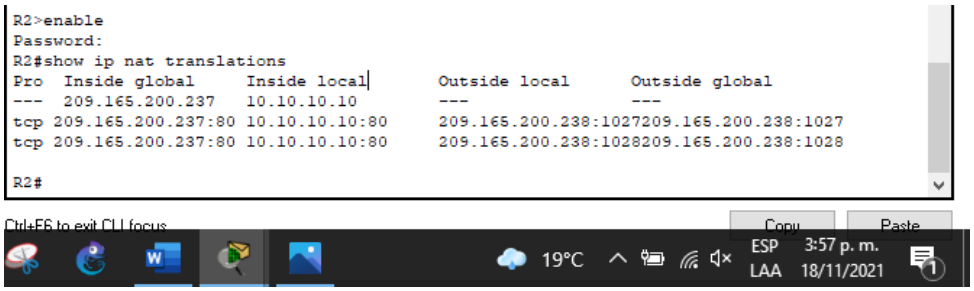

Fuente : Propia

**d. ¿Con qué comando se muestran las traducciones NAT?**

**El comando que se utiliza es**

`R2#show ip nat translations` **`--->Traducciones NAT`**
`R2#`

Figura 28 Traducciones Nat



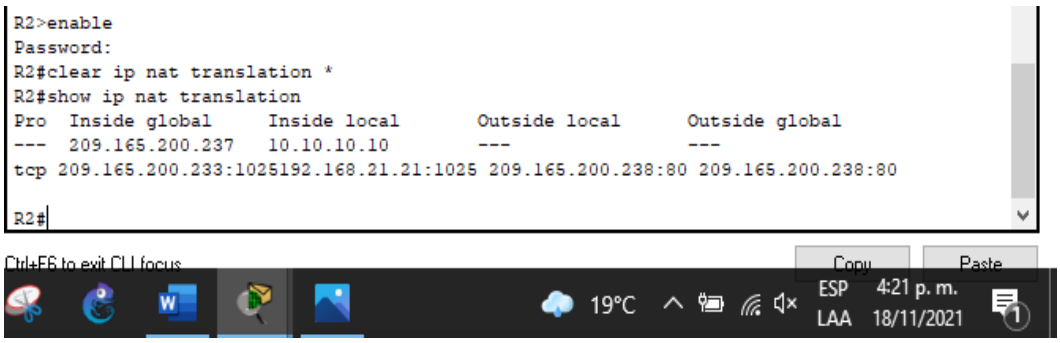

Fuente : Propia

**e.** ¿Qué comando se utiliza para eliminarlas traducciones de NAT dinámicas?

`R2#clear ip nat translation *` **`---> Se limpian las traducciones NAT configuradas`**

`R2#`

Figura 29 Traducción Nat




Fuente : Propia

## CONCLUSIONES

Los diferentes entornos de red y configuraciones vistos en este documento, nos enseñó que no solo existen comandos básicos , que hay una gran gama de configuración y acciones que se pueden realizar con un Router, Switch etc., a pesar de que cisco packet tracert no es completo , es muy práctico para iniciarnos ,

se pudo observar también mediante los laboratorios smartlab los comando que no funcionaban en cisco , se aplicaron ahí para ver su funcionamiento , espero poder en mi vida laborar encontrarme con equipos reales y poder aprender mucho más en este amplio mundo de las redes e infraestructura tecnologica

Entrando en un ambiente más global sobre que se realizó en los dos escenarios aprendí a conocer una red funcional, antes no habría llegado a imaginar cómo era posible que nos pudiéramos conectar a distancias tan lejanas , se pudo observar cómo se hace para realizar este proceso lo mejor es que esto se hizo practicando cada comando, cada conexión y cada equipo necesario para crear una topología de red funcional

No solo se aprendió a configurar una red ,comandos , equipos y demás , se reforzo la lógica y se aprendió a ser un poco más analítico siendo esto la esencia del Ingeniero , como podemos ver los errores cometidos en cada parte de la guía y así mismo como resolverlos para cumplir el objetivo que se nos solicitaba , todo esto ayudo bastante a ser meticuloso con cada cosa que hicimos y al final se ven los resultados con las pruebas satisfactorias

## BIBLIOGRAFIA

[1] GUTIERREZ, R. B., Núñez, W. N., Urrea, S. C., Osorio, H. S., & Acosta, N. D. (2016). Revisión de la seguridad en la implementación de servicios sobre IPv6. *Inge Cuc*, *12*(1), 86-93.

[2] GUTIERREZ, R. B., Urrea, S. C., Núñez, W. N., Sarmiento, H., Acosta, N. D., & Sánchez, G. G. V. (2015). Análisis de la seguridad en la implementación de servicios corporativos sobre el protocolo IPV. *Revista de Tecnología*, *14*(1), 127-138.

[3] BAREÑO, Gutiérrez, R., Sevillano, A. M. L., Díaz-Piraquive, F. N., & González-Crespo, R. (2021, July). Analysis of WEB Browsers of HSTS Security Under the MITM Management Environment. In *International Conference on Knowledge Management in Organizations* (pp. 331-344). Springer, Cham.

[4] BAREÑO, Gutiérrez, R., Cardenas-Urrea, S. E., Navarro-Nuñez, W., Sarmiento-Osorio, H., & Forero-Paez, N. (2017). Sistema de votación electrónico con características de seguridad SSL/TLS e IPsec en Colombia. *Revista UIS Ingenierías*, *16*(1), 75-84.

[5] BAREÑO Gutiérrez, R. (2013). Elaboración de un estado de arte sobre el protocolo IPV6; y su implementación sobre protocolos de enrutamiento dinámico como RIPNG, EIGRP y OSPF basado sobre la plataforma de equipos cisco.

[6] BAREÑO Raúl, G., & Sevillano, A. M. L. (2017, October). Services cloud under HSTS, Strengths and weakness before an attack of man in the middle MITM. In *2017 Congreso Internacional de Innovacion y Tendencias en Ingenieria (CONIITI)* (pp. 1-5). IEEE.

[7] MOJICA S. Felipe, Andrés, L. V. S., & Raúl, B. G. (2019, October). Risks Found in Electronic Payment Cards on Integrated Public Transport System Applying the ISO 27005 Standard. Case Study Sitp DC Colombia. In *2019 Congreso Internacional de Innovación y Tendencias en Ingenieria (CONIITI)* (pp. 1-6). IEEE

[8] Ali, A. N. A. (2012). Comparison study between IPV4 & IPV6. *International Journal of Computer Science Issues (IJCSI)*, *9*(3), 314.

[9 ]Aucapeña Macias, C. C. (2015). Diseño y simulación de una red que implemente enrutamiento estático para el protocolo de internet versión 4 y 6.

[10] Garimella, P., Sung, Y. W. E., Zhang, N., & Rao, S. (2007, August). Characterizing VLAN usage in an operational network. In *Proceedings of the 2007 SIGCOMM workshop on Internet network management* (pp. 305-306).

[11] Nguyen, V. G., & Kim, Y. H. (2016). SDN-based enterprise and campus networks: a case of VLAN management. *Journal of Information Processing Systems*, *12*(3), 511-524.

[12] Ortiz Arias, L. J. (2011). Topología de Red. *Redes de Comunicación I*.

[13] Vázquez Viejo, J. M. (2011). *Diseño y desarrollo de una aplicación para el estudio comparativo de topologías de red* (Bachelor's thesis).