

SOLUCIÓN DE ESTUDIOS DE CASO BAJO EL USO DE TECNOLOGÍA
CISCO

HENRY ALBERTO ANGEL MORA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA

ECBTI – PROGRAMA DE INGENIERÍA DE SISTEMAS

DIPLOMADO DE PROFUNDIZACIÓN CCNA

BOGOTÁ

2019

SOLUCIÓN DE ESTUDIOS DE CASO BAJO EL USO DE TECNOLOGÍA
CISCO

HENRY ALBERTO ANGEL MORA

Diplomado de Profundización
CCNA

Director: Juan Carlos Vesga

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA

ECBTI – PROGRAMA DE INGENIERÍA DE SISTEMAS

DIPLOMADO DE PROFUNDIZACIÓN CCNA

BOGOTÁ

2019

CONTENIDO

| | pág. |
|--|------|
| GLOSARIO | 6 |
| INTRODUCCIÓN | 8 |
| 1. ESCENARIO 1 | 9 |
| 1.1 TOPOLOGÍA DE RED | 9 |
| 1.2 TABLA DE DIRECCIONAMIENTO ESCENARIO 1 | 9 |
| 1.3 DESCRIPCIÓN DEL ESCENARIO | 11 |
| 1.4 DESCRIPCIÓN DE LAS ACTIVIDADES..... | 11 |
| 1.4.1 Asignación de puertos de vlan en S1 y S2..... | 11 |
| 1.4.2 Deshabilitar los puertos no utilizados..... | 12 |
| 1.4.3 Configuración de las interfaces troncales..... | 13 |
| 1.4.4 Direccionamiento ip en los routers..... | 14 |
| 1.4.5 Realizar nat en R1..... | 17 |
| 1.4.6 Establecer ruta predeterminada a isp..... | 17 |
| 1.4.7 Establecer R2 como servidor dhcp..... | 18 |
| 1.4.8 Configuración ipv4 – ipv6 en R3..... | 20 |
| 1.4.9 Configurar ripv2 en los routers..... | 20 |
| 1.4.10 Verificaciones de conectividad..... | 21 |
| 2. ESCENARIO 2 | 26 |
| 2.1 TOPOLOGÍA DE RED | 26 |
| 2.2 TABLA DE DIRECCIONAMIENTO ESCENARIO 2 | 27 |
| 2.3 DESCRIPCIÓN DEL ESCENARIO..... | 27 |
| 2.4 DESCRIPCIÓN DE LAS ACTIVIDADES | 28 |
| 2.4.1 Configuración del direccionamiento ip en los dispositivos..... | 28 |
| 2.4.2 Configuraciones de vlan..... | 34 |
| 2.4.3 Configuraciones de seguridad 8021.q..... | 39 |
| 2.4.4 Configuraciones de ospfv2 área 0..... | 39 |
| 2.4.5 Verificaciones de ospfv2..... | 42 |
| 2.4.6 Implementación de dhcp en R1..... | 49 |
| 2.4.7 Implementación de nat en R2..... | 50 |
| 2.4.8 Configuración de listas de acceso..... | 50 |
| 2.4.9 Verificaciones de comunicación..... | 50 |

| | |
|----------------------|----|
| 3. CONCLUSIONES..... | 55 |
| BIBLIOGRAFÍA..... | 56 |

LISTA DE TABLAS

| | pág. |
|--|------|
| Tabla 1. Direccionamiento IP escenario 1 | 9 |
| Tabla 2. Asignación de VLAN y de puertos escenario 1 | 10 |
| Tabla 3. Enlaces troncales escenario 1 | 10 |
| Tabla 4. Direccionamiento IP escenario 2 | 27 |
| Tabla 5. Configuraciones VLAN escenario 2 | 34 |
| Tabla 6. Configuraciones de OSPFv2..... | 39 |
| Tabla 7. Implementación DHCP en R1 | 49 |

GLOSARIO

ACL: listas de control de acceso, son unas listas de instrucciones que controlan si un router descarta o envía paquetes y que se utilizan como mecanismo de seguridad para controlar el tráfico desde y hacia la red.

DHCP: es un protocolo de red que asigna automáticamente una dirección IP válida a un host.

ENLACE TRONCAL: es una conexión que se establece entre dos dispositivos de red para transportar tráfico de VLAN.

ENRUTAMIENTO: es el proceso que emplea un router para enviar paquetes a una red de destino escogiendo la mejor ruta.

INTERFAZ: es la conexión física entre dispositivos de red.

NAT: es Network Address Translation, que es un proceso realizado en los routers para permitir que las redes utilicen direcciones IPV4 privadas internamente y proporcionar la traducción a una dirección pública solo cuando sea necesario.

OSPF: es un protocolo de enrutamiento sin clase que utiliza el concepto de áreas para realizar la escalabilidad.

PROTOCOLO: se refiere al conjunto de reglas utilizadas por un router para comunicarse con otros routers.

PUERTO: es una interfaz que se utiliza para recibir y transmitir comunicación entre el dispositivo y las fuentes externas.

RIP: es Routing Information Protocol, que es un protocolo de enrutamiento dinámico utilizado por los routers para intercambiar y actualizar información de las redes conectadas.

ROUTER: dispositivo de red que se utiliza para conectar una red a otra red y es el responsable de la entrega de paquetes a través de distintas redes.

SWITCH: dispositivo de red que se utiliza para conectar otros dispositivos dentro de una misma red.

TOPOLOGÍA: es la representación gráfica de la forma como se encuentran conectados los dispositivos de una red, sea en forma lógica o en forma física.

VLAN: es Red de área local virtual o LAN virtual utilizada para agrupar dispositivos dentro de una red LAN, utilizando una conexión lógica y no física.

RESUMEN

Las redes han tenido que ir evolucionando para adaptarse a las necesidades del ser humano y sus organizaciones, de tal manera que se han ido implementando constantemente cambios que nos permiten la interacción de diferentes dispositivos como los switch y los router, que trabajando conjuntamente proporcionan conexiones adecuadas, rápidas, seguras y confiables aún entre puntos muy distantes y de forma remota.

El curso que hemos tomado en la plataforma CISCO, con la ayuda de PACKET TRACERT, nos ha permitido reconocer la importancia y la aplicación de una adecuada configuración de los dispositivos de red para lograr las conexiones esperadas en los diferentes escenarios de la vida real, desde las conexiones más sencillas de un hogar, hasta las más complejas de una gran empresa y de acuerdo con las necesidades de proveedores y usuarios.

Hemos podido apreciar la forma como se conforman las redes, la asignación de direcciones IP y la aplicación del enrutamiento estático y dinámico, según la necesidad de cada caso, las configuraciones y enrutamiento entre las redes de área local virtual (VLAN), y la implementación de los diferentes protocolos de enrutamiento tanto estático como dinámico como es el caso del RIPv2 y el OSPFv2, DHCP, la configuración de listas de control de acceso, y la implementación de NAT para la traducción de direcciones de red.

El estudio y la aplicación de estos conceptos adquiridos, nos permite estar en condiciones de plantear soluciones de redes adecuadas, de acuerdo a cada caso, con la ayuda de las herramientas que nos proporciona la tecnología CISCO.

INTRODUCCIÓN

La realización del presente trabajo tiene como fundamento plasmar los resultados de la aplicación práctica de los conocimientos adquiridos en redes, durante el curso del diplomado de profundización CCNA.

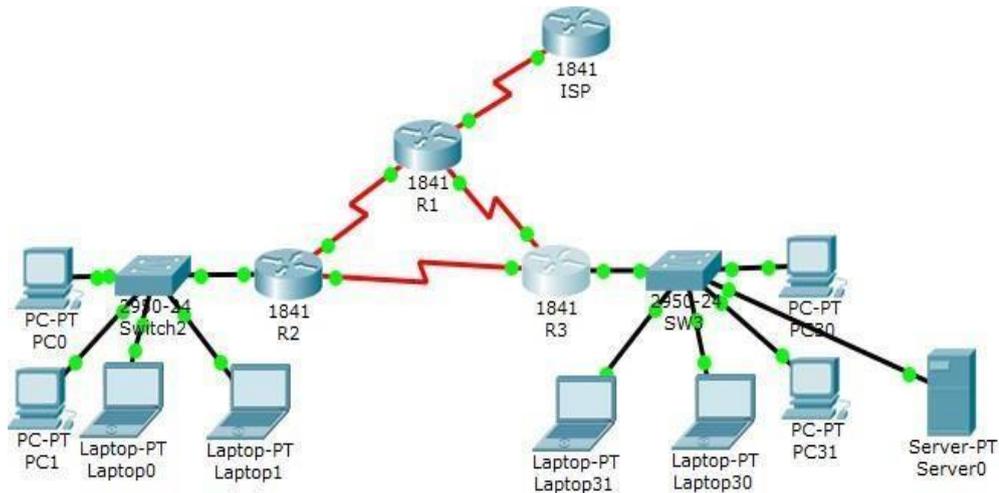
Específicamente se aplican temas como las configuraciones básicas y de direccionamiento IP en dispositivos como routers y en switches, las configuraciones de VLAN, deshabilitación de puertos, configuración de protocolos de enrutamiento como OSPFv2, NAT, RIPv2, DHCP, configuraciones de seguridad, listas de acceso y los comandos para verificar configuraciones y hacer pruebas de conectividad.

Para tal fin, se planteó el desarrollo de dos escenarios diferentes con sus respectivas topologías de red y tablas de direccionamiento IP, utilizando el programa de simulación de red PACKET TRACER para desarrollar la aplicación práctica.

1. ESCENARIO 1

1.1 TOPOLOGÍA DE RED

A continuación presentamos la topología de la red correspondiente al escenario 1 con base a la cual se irán desarrollando los requerimientos solicitados.



1.2 TABLA DE DIRECCIONAMIENTO IP ESCENARIO 1

A continuación presentamos la tabla de direccionamiento para el escenario 1 con base en la cual se harán las configuraciones IP de cada uno de los dispositivos.

Tabla 1. Direccionamiento IP escenario 1

| Administrador | Interface | Dirección IP | Máscara subred | de Gateway |
|---------------|-----------|---------------|-----------------|------------|
| ISP | S0/0/0 | 200.123.211.1 | 255.255.255.0 | N/D |
| R1 | Se0/0/0 | 200.123.211.2 | 255.255.255.0 | N/D |
| | Se0/1/0 | 10.0.0.1 | 255.255.255.252 | N/D |
| | Se0/1/1 | 10.0.0.5 | 255.255.255.252 | N/D |

| | | | | |
|----------|-----------|-----------------------|-----------------|------|
| R2 | Fa0/0.100 | 192.168.20.1 | 255.255.255.0 | N/D |
| | Fa0/0.200 | 192.168.21.1 | 255.255.255.0 | N/D |
| | Se0/0/0 | 10.0.0.2 | 255.255.255.252 | N/D |
| | Se0/0/1 | 10.0.0.9 | 255.255.255.252 | N/D |
| R3 | Fa0/0 | 192.168.30.1 | 255.255.255.0 | N/D |
| | | 2001:db8::9C0:80F:301 | /64 | N/D |
| | Se0/0/0 | 10.0.0.6 | 255.255.255.252 | N/D |
| | Se0/0/1 | 10.0.0.10 | 255.255.255.252 | N/D |
| SW2 | VLAN 100 | N/D | N/D | N/D |
| | VLAN 200 | N/D | N/D | N/D |
| SW3 | VLAN1 | N/D | N/D | N/D |
| PC20 | NIC | DHCP | DHCP | DHCP |
| PC21 | NIC | DHCP | DHCP | DHCP |
| PC30 | NIC | DHCP | DHCP | DHCP |
| PC31 | NIC | DHCP | DHCP | DHCP |
| Laptop20 | NIC | DHCP | DHCP | DHCP |
| Laptop21 | NIC | DHCP | DHCP | DHCP |
| Laptop30 | NIC | DHCP | DHCP | DHCP |
| Laptop31 | NIC | DHCP | DHCP | DHCP |

Tabla 2. Asignación de VLAN y de puertos escenario 1

| Dispositivo | VLAN | Nombre | Interfaz |
|-------------|------|----------|----------------------|
| SW2 | 100 | LAPTOPS | Fa0/2-3 |
| SW2 | 200 | DESKTOPS | Fa0/4-5 |
| SW3 | 1 | - | Todas las interfaces |

Tabla 3. Enlaces troncales escenario 1

| Dispositivo local | Interfaz local | Dispositivo remoto |
|-------------------|----------------|--------------------|
| SW2 | Fa0/2-3 | 100 |

1.3 DESCRIPCIÓN DEL ESCENARIO

En esta actividad, demostrará y reforzará su capacidad para implementar NAT, servidor de DHCP, RIPV2 y el routing entre VLAN, incluida la configuración de direcciones IP, las VLAN, los enlaces troncales y las subinterfaces. Todas las pruebas de alcance deben realizarse a través de ping únicamente.

1.4 DESCRIPCIÓN DE LAS ACTIVIDADES

A continuación se enumeran y se describen cada una de las actividades a realizar en este escenario.

1.4.1 Asignación de puertos de vlan en S1 y S2. En primer lugar, se procede a dar nombre a cada una de las VLAN en S1 de acuerdo a los parámetros establecidos en la tabla de asignación de VLAN

```
S2(config)#vlan 100
S2(config-vlan)#name LAPTOPS
S2(config-vlan)#exit
S2(config)#vlan 200
S2(config-vlan)#name DESKTOPS
S2(config-vlan)#exit
S2(config)#
```

En segundo lugar, se habilitan y se asignan los puertos indicados a cada VLAN de acuerdo con los parámetros establecidos en la tabla de asignación de VLAN.

Se habilitan los puertos VLAN 100 y 200 en S2 utilizando el comando **switch por mode access** y se asignan utilizando el comando **switchport access vlan** y especificando el rango de interfaces para las cuales se asignará cada una

```
S2#config t
Enter configuration commands, one per line. End with CNTL/Z.
S2(config)#int range f0/2-3
S2(config-if-range)#switch port mode access
^
% Invalid input detected at '^' marker.
S2(config-if-range)#switchport mode access
S2(config-if-range)#switchport access valn 100
^
% Invalid input detected at '^' marker.
S2(config-if-range)#switchport access vlan 100
S2(config-if-range)#int range f0/4-5
S2(config-if-range)#switchport mode access
S2(config-if-range)#switchport access vlan 200
S2(config-if-range)#exit
S2(config)#exit
S2#
%SYS-5-CONFIG_I: Configured from console by console

S2#wr
Building configuration...
[OK]
```

Se habilitan los puertos VLAN 1 en S3 utilizando el comando **switch por mode access** y se asignan utilizando el comando **switchport access vlan** y especificando el rango de interfaces para el cual se va asignar

```
S3>enable
S3#config t
Enter configuration commands, one per line. End with CNTL/Z.
S3(config)#vlan 1
S3(config-vlan)#int range f0/1-24
S3(config-if-range)#switchport mode access
S3(config-if-range)#switchport access vlan 1
S3(config-if-range)#exit
S3(config)#exit
S3#
%SYS-5-CONFIG_I: Configured from console by console

S3#wr
Building configuration...
[OK]
```

1.4.2 Deshabilitar los puertos no utilizados. Por razones de seguridad se recomienda deshabilitar los puertos que no se van a utilizar.

Por tanto se procede a deshabilitar los puertos que no se van a utilizar en el S3 especificando el rango y aplicando el comando **shutdown**.

```
S3#config t
Enter configuration commands, one per line. End with CNTL/Z.
S3(config)#int range f0/6-23
S3(config-if-range)#shutdown

%LINK-5-CHANGED: Interface FastEthernet0/6, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/7, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/8, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/9, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/10, changed state to administratively
down
```

Se procede a deshabilitar los puertos que no se van a utilizar en el S2 especificando el rango y utilizando el comando **shutdown**.

```
S2>enable
S2#config t
Enter configuration commands, one per line.  End with CNTL/Z.
S2(config)#int range f0/6-24
S2(config-if-range)#shutdown

%LINK-5-CHANGED: Interface FastEthernet0/6, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/7, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/8, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/9, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/10, changed state to administratively down
```

1.4.3 Configuración de las interfaces troncales. Es necesario hacer la configuración de las interfaces troncales para permitir el tráfico entre switches y routers. Esto se hace utilizando el comando **switchport mode trunk**

Por tanto se configura la interfaz F0/1 en S2 como interfaz troncal para permitir el tráfico del S2 al R2

```
S2#config t
Enter configuration commands, one per line.  End with CNTL/Z.
S2(config)#int f0/1
S2(config-if)#switchport mode trunk
```

También se configura la interfaz F0/1 en S3 como interfaz troncal para permitir el tráfico del S3 al R3

```
S3(config)#int f0/1
S3(config-if)#switchport mode trunk
S3(config-if)#exit
```

1.4.4 Direcccionamiento ip en los routers. Se procede a realizar el direccionamiento IP de cada uno de los routers con base en la tabla de direccionamiento IP.

Procedemos a asignar la IP 200.123.211.2 a la interfaz S0/0/0 en el router R1

```
R1(config)#interfa s0/0/0
R1(config-if)#ip address 200.123.211.2 255.255.255.0
R1(config-if)#no shutdown
```

Procedemos a asignar la IP a las interfaces S0/1/0 y S0/1/1 en R1 de acuerdo con la tabla de direccionamiento.

```
Router>enable
Router#config t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname R1
R1(config)#int s0/1/0
R1(config-if)#ip address 10.0.0.1 255.255.255.252
R1(config-if)#no shutdown

%LINK-5-CHANGED: Interface Serial0/1/0, changed state to down
R1(config-if)#
R1(config-if)#exit
R1(config)#interface s0/1/1
R1(config-if)#ip address 10.0.0.5 255.255.255.252
R1(config-if)#no shutdown
```

Procedemos a configurar la IP a las interfaces F0/0 y S0/0/0 en **R2** de acuerdo con la tabla de direccionamiento, teniendo en cuenta que F0/0 es una interfaz troncal que hace parte de las VLAN 100 Y 200.

Para lo cual utilizamos el comando **encapsulation dot1Q** y el nombre de cada interfaz y procedemos a habilitarlas con el comando **no shutdown**.

```
R2#config t
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#interface f0/0.100
R2(config-subif)#
R2(config-subif)#encapsulation dot1Q 100
R2(config-subif)#ip address 192.168.20.1 255.255.255.0
R2(config-subif)#no shutdown
R2(config-subif)#exit
R2(config)#interface f0/0.200
R2(config-subif)#encapsulation dot1Q 200
R2(config-subif)#ip address 192.168.21.1 255.255.255.0
R2(config-subif)#exit
R2(config)#int s0/0/0
R2(config-if)#ip address 10.0.0.2 255.255.255.252
R2(config-if)#no shutdown

%LINK-5-CHANGED: Interface Serial0/0/0, changed state to down
R2(config-if)#exit
R2(config)#int s0/0/1
R2(config-if)#ip address 10.0.0.9 255.255.255.252
R2(config-if)#no shutdown

R2(config-if)#
%LINK-5-CHANGED: Interface Serial0/0/1, changed state to up

R2(config-if)#exit
R2(config)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1, changed state to up
```

Se procede a configurar las IP en las interfaces F0/0, S0/0/0 y S0/0/1 del **R3** utilizando el comando **ip address** y activando cada interfaz con el comando **no shutdown**

Se configuran y se habilitan las interfaces F0/0, S0/0/0 en el **R3**

```
R3>enable
R3#config t
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#int f0/0
R3(config-if)#ip address 192.168.30.1 255.255.255.0
R3(config-if)#ipv6 address 2001:db8:130::9C0:80F:301/64
R3(config-if)#no shutdown

R3(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to
up

R3(config-if)#exit
R3(config)#int s0/0/0 10.0.0.6 255.255.255.252
      ^
% Invalid input detected at '^' marker.

R3(config)#int s0/0/0
R3(config-if)#ip address 10.0.0.6 255.255.255.252
R3(config-if)#no shutdown
```

Se configura la interfaz S0/0/1 del **R3**

```
R3(config)#int s0/0/1
R3(config-if)#ip address 10.0.0.10 255.255.255.252
R3(config-if)#no shutdown

R3(config-if)#
%LINK-5-CHANGED: Interface Serial0/0/1, changed state to up

R3(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1, changed state to up
```

1.4.5 Realizar nat en R1. R1 debe realizar una NAT con sobrecarga sobre una dirección IPv4 pública. Asegúrese de que todos los terminales pueden comunicarse con Internet pública (haga ping a la dirección ISP) y la lista de acceso estándar se llama INSIDE-DEVS.

La configuración con NAT se realiza para que los terminales de una red privada puedan comunicarse con internet pública.

Para habilitar NAT se utiliza el comando **ip nat inside**

```
R1(config)#int s0/0/1
R1(config-if)#ip nat inside
R1(config-if)#exit
R1(config)#int s0/1/0
R1(config-if)#ip nat inside
R1(config-if)#exit
R1(config)#int s0/0/0
R1(config-if)#ip nat outside
R1(config-if)#exit
R1(config)#ip nat pool INSIDE-DEVS 200.123.211.2 200.123.211.128 netmask
255.255.255.0
R1(config)#access-list 1 permit 192.168.0.0 0.0.255.255
R1(config)#access-list 1 permit 10.0.0.0 0.255.255.255
R1(config)#ip nat inside source list 1 interface s0/0/0 overload
R1(config)#
```

1.4.6 Establecer ruta predeterminada a isp. R1 debe tener una ruta estática predeterminada al ISP que se configuró y que incluye esa ruta en el dominio RIPv2.

Se configura la ruta estática en R1

```
R1(config)#
R1(config)#ip nat inside source static tcp 192.168.30.6 80 200.123.211.1 80
R1(config)#ip nat inside source static tcp 192.168.30.6 80 200.123.211.1 80
R1(config)#
```

Se configura el RIPV2

```
R1(config)#router rip
R1(config-router)#version 2
R1(config-router)#network 10.0.0.0
R1(config-router)#
R1(config-router)#exit
```

Se verifica con los comandos **show ip nat translations** y **show ip nat statistics**

```
R1#show ip nat translations
Pro Inside global      Inside local      Outside local      Outside global
tcp 200.123.211.1:80   192.168.30.6:80   ---                ---

R1#show ip nat statics
^
% Invalid input detected at '^' marker.

R1#show ip nat statistics
Total translations: 1 (1 static, 0 dynamic, 1 extended)
Outside Interfaces: Serial0/0/0
Inside Interfaces: Serial0/0/1 , Serial0/1/0
Hits: 0 Misses: 0
Expired translations: 0
Dynamic mappings:
```

1.4.7 **Establecer R2 como servidor dhcp.** R2 es un servidor de DHCP para los dispositivos conectados al puerto FastEthernet0/0.

Por tanto se configura R2 como servidor DHCP con **ip dhcp pool**

```
R2(config)#ip dhcp excluded-address 10.0.0.2 10.0.0.9
R2(config)#ip dhcp pool INSIDE-DEVS
R2(dhcp-config)#network 192.168.20.1 255.255.255.0
R2(dhcp-config)#network 192.168.21.1 255.255.255.0
R2(dhcp-config)#default-router 192.168.1.1
R2(dhcp-config)#dns-server 0.0.0.0
```

R2 debe, además de enrutamiento a otras partes de la red, tener una ruta entre las VLAN 100 y 200, por tanto se configura el enrutamiento a las VLAN 100 y 200

```
R2(config)#int vlan 100
R2(config-if)#ip address 192.168.20.1 255.255.255.0
% 192.168.20.0 overlaps with FastEthernet0/0.100
R2(config-if)#exit
R2(config)#int vlan 200
R2(config-if)#ip address 192.168.21.1 255.255.255.0
% 192.168.21.0 overlaps with FastEthernet0/0.200
R2(config-if)#exit
```

El Servidor0 es sólo un servidor IPv6 y solo debe ser accesible para los dispositivos en R3 (ping). Por lo cual hacemos una verificación de ping desde la laptop 31 conectada al R3.

Se hace ping desde el laptop 31

```
Packet Tracer PC Command Line 1.0
PC>ping 169.254.108.139

Pinging 169.254.108.139 with 32 bytes of data:

Reply from 169.254.108.139: bytes=32 time=0ms TTL=128

Ping statistics for 169.254.108.139:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

1.4.8 **Configuración ipv4 – ipv6 en R3.** La interfaz FastEthernet 0/0 del R3 también debe tener direcciones IPv4 e IPv6 configuradas (dual- stack).

Por tanto se procede a configurar IPV6 en R3 primero habilitando el routing IPV6 con el comando **ipv6 unicast-routing** y luego asignado la IP correspondiente de acuerdo a la tabla de direccionamiento.

```
R3>enable
R3#config t
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#ipv6 unicast-routing
R3(config)#int f0/0
R3(config-if)#ipv6 enable
R3(config-if)#ip address 192.168.30.1
% Incomplete command.
R3(config-if)#ip address 192.168.30.1 255.255.255.0
R3(config-if)#ipv6 address 2001:db8:130::9C0:80F:301/64
R3(config-if)#no shutdown
```

1.4.9 **Configurar ripv2 en los routers.** R1, R2 y R3 intercambian información de routing mediante RIP versión 2.

Por tanto se procede a configurar RIP versión 2 en cada uno de los routers mediante los comandos **router rip, versión 2.**

Se configura RIP versión 2 en R1

```
R1(config)#router rip
R1(config-router)#version 2
R1(config-router)#do show ip route connected
C 10.0.0.0/30 is directly connected, Serial0/1/0
C 10.0.0.4/30 is directly connected, Serial0/1/1
C 200.123.211.0/24 is directly connected, Serial0/0/0
R1(config-router)#network 10.0.0.0
R1(config-router)#network 10.0.0.4
```

Se configura RIP versión 2 en R2

```
R2(config)#router rip
R2(config-router)#version 2
R2(config-router)#do show ip route connected
C 10.0.0.0/30 is directly connected, Serial0/0/0
C 10.0.0.8/30 is directly connected, Serial0/0/1
R2(config-router)#network 10.0.0.0
R2(config-router)#network 10.0.0.8
```

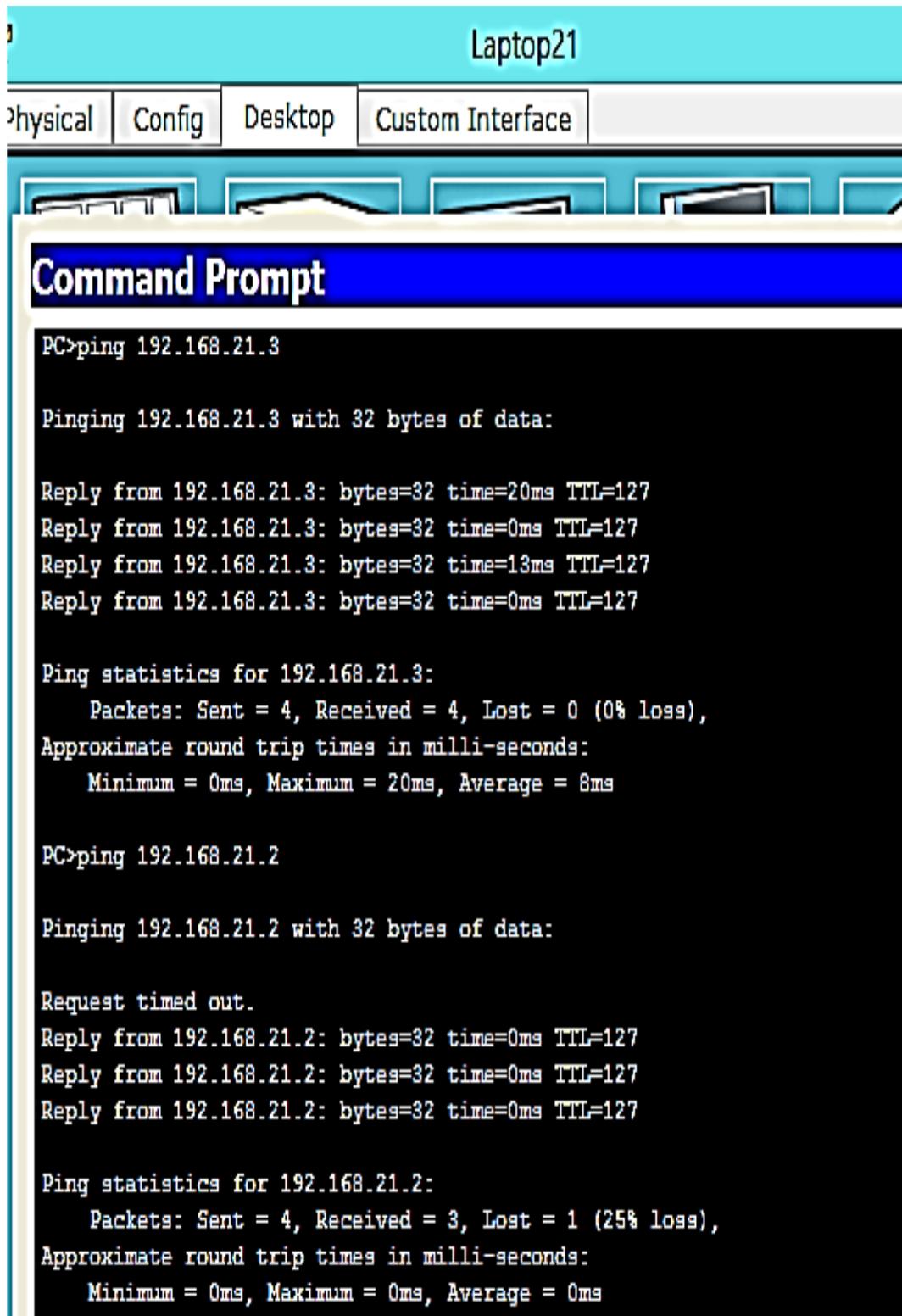
Se configura RIP versión 2 en R3

```
R3(config)#router rip
R3(config-router)#version 2
R3(config-router)#do show ip route connected
C 10.0.0.4/30 is directly connected, Serial0/0/0
C 10.0.0.8/30 is directly connected, Serial0/0/1
C 192.168.30.0/24 is directly connected, FastEthernet0/0
R3(config-router)#network 10.0.0.4
R3(config-router)#network 10.0.0.8
R3(config-router)#exit
```

1.4.10 Verificaciones de conectividad. Por último procedemos a realizar las verificaciones de conectividad pertinentes.

Comprobamos conectividad entre terminales de la misma red, por tanto hacemos ping de la laptop 21 a la PC20.

Ping de la laptop 21 a la PC20



```
Laptop21
Physical Config Desktop Custom Interface

Command Prompt
PC>ping 192.168.21.3

Pinging 192.168.21.3 with 32 bytes of data:

Reply from 192.168.21.3: bytes=32 time=20ms TTL=127
Reply from 192.168.21.3: bytes=32 time=0ms TTL=127
Reply from 192.168.21.3: bytes=32 time=13ms TTL=127
Reply from 192.168.21.3: bytes=32 time=0ms TTL=127

Ping statistics for 192.168.21.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 20ms, Average = 8ms

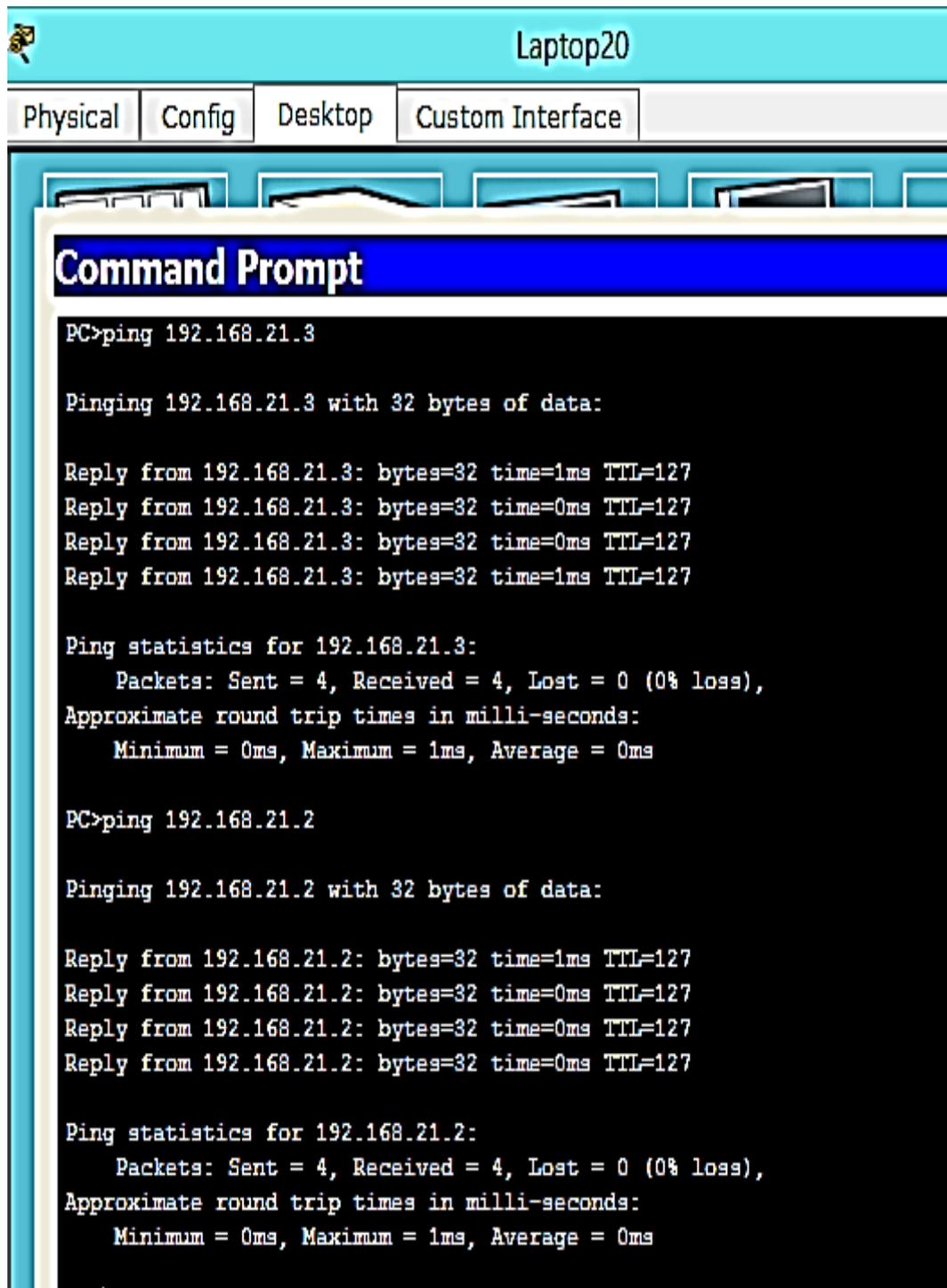
PC>ping 192.168.21.2

Pinging 192.168.21.2 with 32 bytes of data:

Request timed out.
Reply from 192.168.21.2: bytes=32 time=0ms TTL=127
Reply from 192.168.21.2: bytes=32 time=0ms TTL=127
Reply from 192.168.21.2: bytes=32 time=0ms TTL=127

Ping statistics for 192.168.21.2:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Comprobamos conectividad de la laptop 20 a la PC21



```
PC>ping 192.168.21.3

Pinging 192.168.21.3 with 32 bytes of data:

Reply from 192.168.21.3: bytes=32 time=1ms TTL=127
Reply from 192.168.21.3: bytes=32 time=0ms TTL=127
Reply from 192.168.21.3: bytes=32 time=0ms TTL=127
Reply from 192.168.21.3: bytes=32 time=1ms TTL=127

Ping statistics for 192.168.21.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

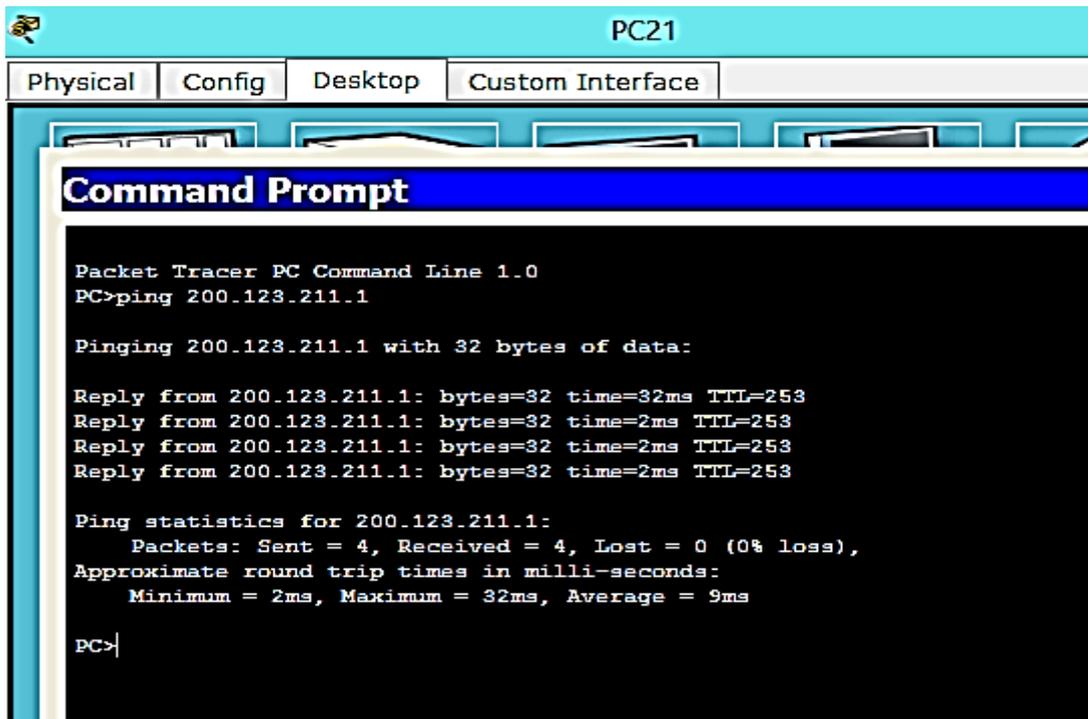
PC>ping 192.168.21.2

Pinging 192.168.21.2 with 32 bytes of data:

Reply from 192.168.21.2: bytes=32 time=1ms TTL=127
Reply from 192.168.21.2: bytes=32 time=0ms TTL=127
Reply from 192.168.21.2: bytes=32 time=0ms TTL=127
Reply from 192.168.21.2: bytes=32 time=0ms TTL=127

Ping statistics for 192.168.21.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

Hacemos Ping del PC21 al ISP



```
PC21
Physical Config Desktop Custom Interface
Command Prompt
Packet Tracer PC Command Line 1.0
PC>ping 200.123.211.1

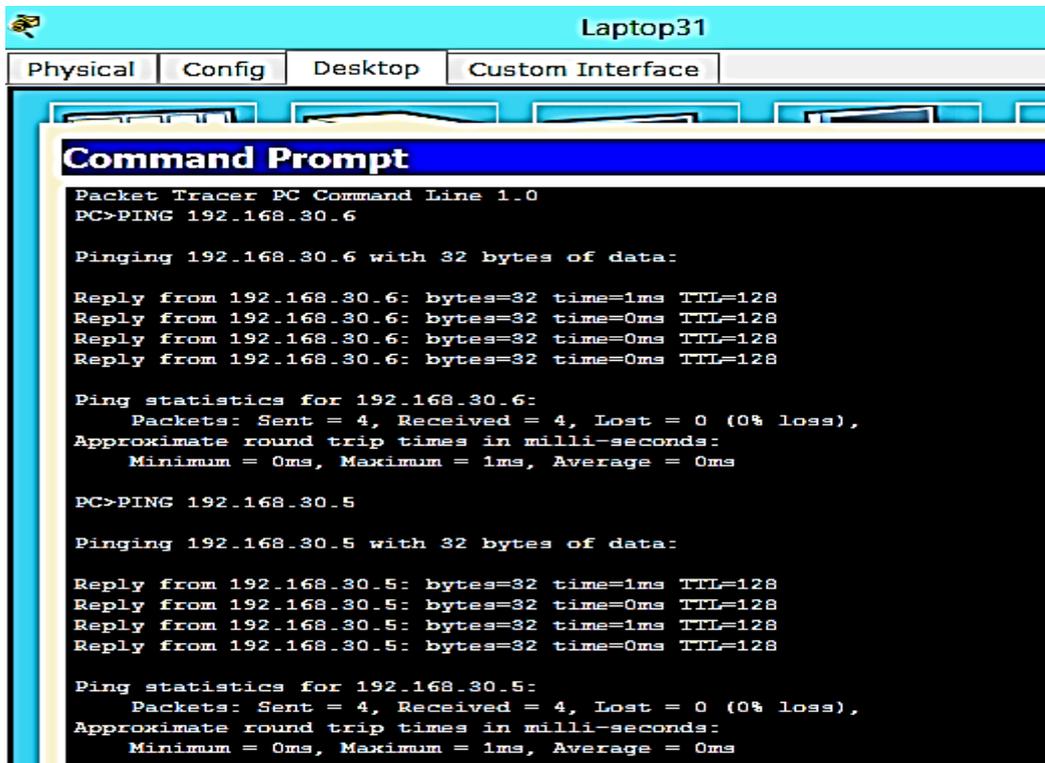
Pinging 200.123.211.1 with 32 bytes of data:

Reply from 200.123.211.1: bytes=32 time=32ms TTL=253
Reply from 200.123.211.1: bytes=32 time=2ms TTL=253
Reply from 200.123.211.1: bytes=32 time=2ms TTL=253
Reply from 200.123.211.1: bytes=32 time=2ms TTL=253

Ping statistics for 200.123.211.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 32ms, Average = 9ms

PC>
```

Hacemos prueba de conectividad de la laptop31 al PC30



```
Laptop31
Physical Config Desktop Custom Interface
Command Prompt
Packet Tracer PC Command Line 1.0
Laptop31>PING 192.168.30.6

Pinging 192.168.30.6 with 32 bytes of data:

Reply from 192.168.30.6: bytes=32 time=1ms TTL=128
Reply from 192.168.30.6: bytes=32 time=0ms TTL=128
Reply from 192.168.30.6: bytes=32 time=0ms TTL=128
Reply from 192.168.30.6: bytes=32 time=0ms TTL=128

Ping statistics for 192.168.30.6:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

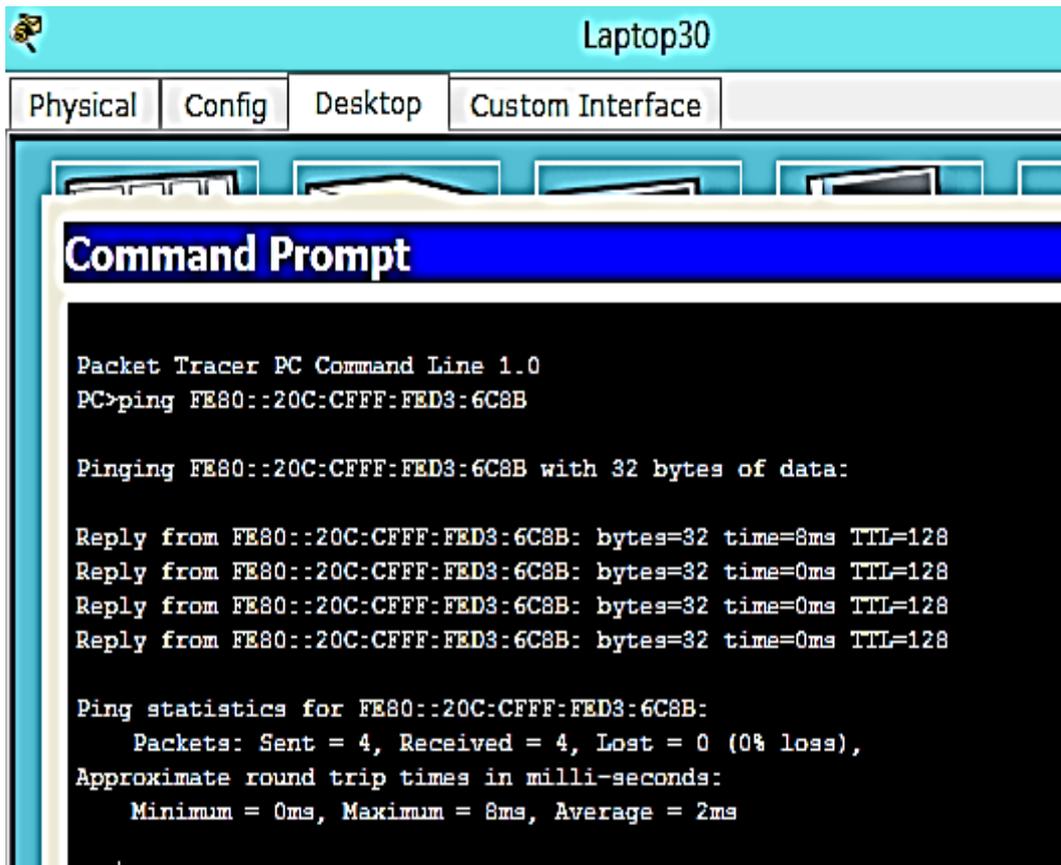
Laptop31>PING 192.168.30.5

Pinging 192.168.30.5 with 32 bytes of data:

Reply from 192.168.30.5: bytes=32 time=1ms TTL=128
Reply from 192.168.30.5: bytes=32 time=0ms TTL=128
Reply from 192.168.30.5: bytes=32 time=1ms TTL=128
Reply from 192.168.30.5: bytes=32 time=0ms TTL=128

Ping statistics for 192.168.30.5:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

Hacemos ping de la laptop 30 a la dirección IPV6 del servidor



The screenshot shows the Packet Tracer interface for Laptop30. The 'Command Prompt' window is open, displaying the following text:

```
Packet Tracer PC Command Line 1.0
PC>ping FE80::20C:CFFF:FED3:6C8B

Pinging FE80::20C:CFFF:FED3:6C8B with 32 bytes of data:

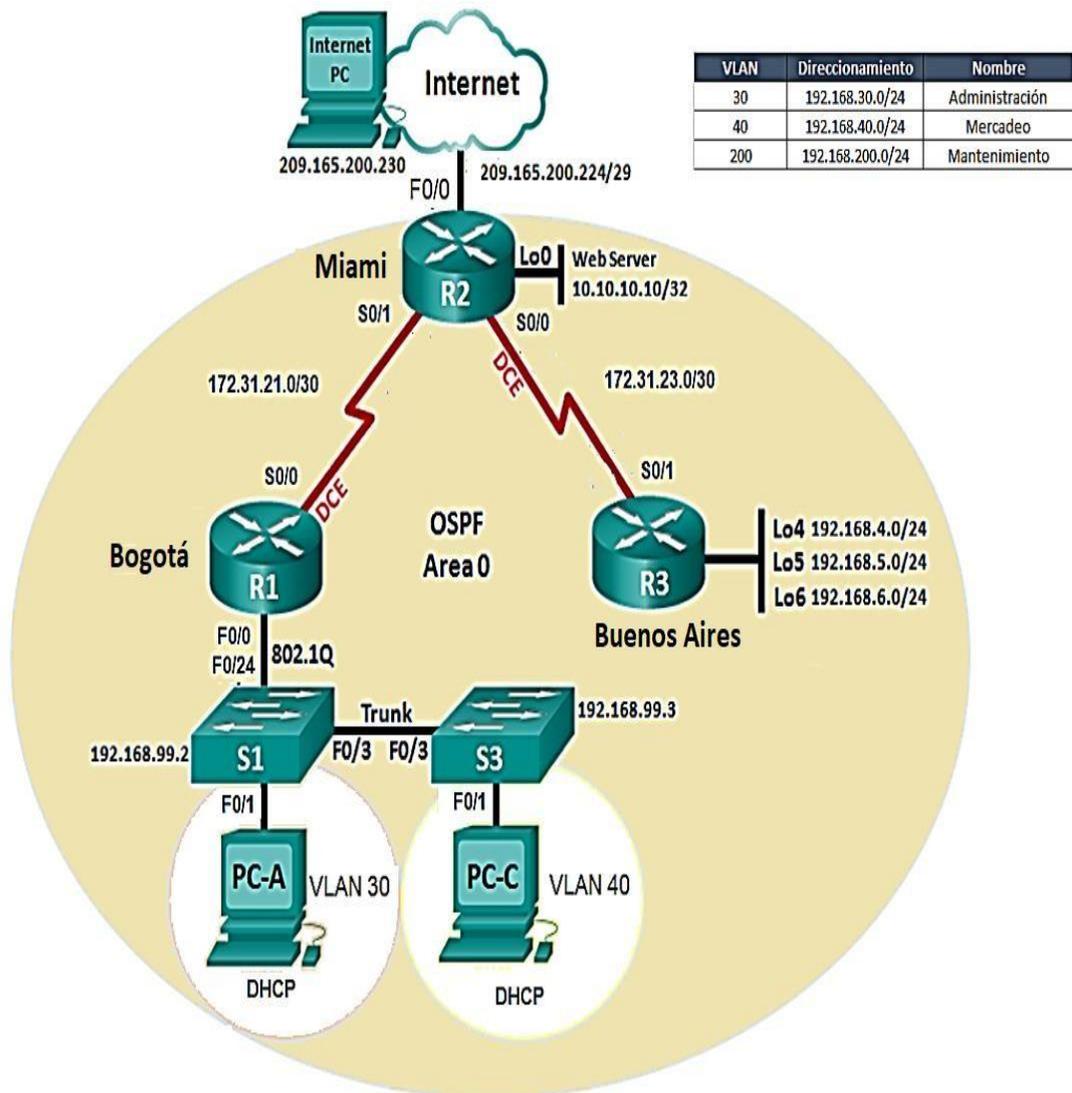
Reply from FE80::20C:CFFF:FED3:6C8B: bytes=32 time=8ms TTL=128
Reply from FE80::20C:CFFF:FED3:6C8B: bytes=32 time=0ms TTL=128
Reply from FE80::20C:CFFF:FED3:6C8B: bytes=32 time=0ms TTL=128
Reply from FE80::20C:CFFF:FED3:6C8B: bytes=32 time=0ms TTL=128

Ping statistics for FE80::20C:CFFF:FED3:6C8B:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 8ms, Average = 2ms
```

2. ESCENARIO 2

2.1 TOPOLOGÍA DE RED

A continuación se presenta la topología de red correspondiente al escenario 2 con base en la cual se desarrollarán los requerimientos solicitados.



1.1 TABLA DE DIRECCIONAMIENTO IP ESCENARIO 2

A continuación se presenta la tabla de direccionamiento IP correspondiente al escenario 2 con base en la cual se harán las configuraciones necesarias en cada uno de los dispositivos.

Tabla 4. Direccionamiento IP escenario 2

| Dispositivo | Dirección ip | Máscara de Subred | Default- gateway |
|-------------|-----------------|-------------------|------------------|
| R1 S0/0/0 | 172.31.21.1 | 255.255.255.252 | |
| R2 S0/0/0 | 172.31.23.1 | 255.255.255.252 | |
| R2 S0/0/1 | 172.31.21.2 | 255.255.255.252 | |
| R2 F0/0 | 209.165.200.225 | 255.255.255.248 | |
| R2 Lo0 | 10.10.10.10 | 255.255.255.255 | 0.0.0.0 0.0.0.0 |
| R3 S0/0/1 | 172.31.23.2 | 255.255.255.252 | |
| R3 Lo4 | 192.168.4.1 | 255.255.255.0 | 0.0.0.0 0.0.0.0 |
| R3 Lo5 | 192.168.5.1 | 255.255.255.0 | 0.0.0.0 0.0.0.0 |
| R3 Lo6 | 192.168.6.1 | 255.255.255.0 | 0.0.0.0 0.0.0.0 |
| S1 | 192.168.99.2 | 255.255.255.0 | |
| S3 | 192.168.99.3 | 255.255.255.0 | |
| R1 F0/0.30 | 192.168.30.1 | 255.255.255.0 | |
| R1 F0/0.40 | 192.168.40.1 | 255.255.255.0 | |
| R1 F0/0.200 | 192.168.200.1 | 255.255.255.0 | |
| Pc internet | 209.165.200.230 | 255.255.255.248 | 209.165.200.225 |

1.2 DESCRIPCIÓN DEL ESCENARIO

Una empresa de Tecnología posee tres sucursales distribuidas en las ciudades de Miami, Bogotá y Buenos Aires, en donde el estudiante será el administrador de la red, el cual deberá configurar e interconectar entre sí cada uno de los dispositivos que forman parte del escenario, acorde con los lineamientos establecidos para el direccionamiento IP, protocolos de enrutamiento y demás aspectos que forman parte de la topología de red.

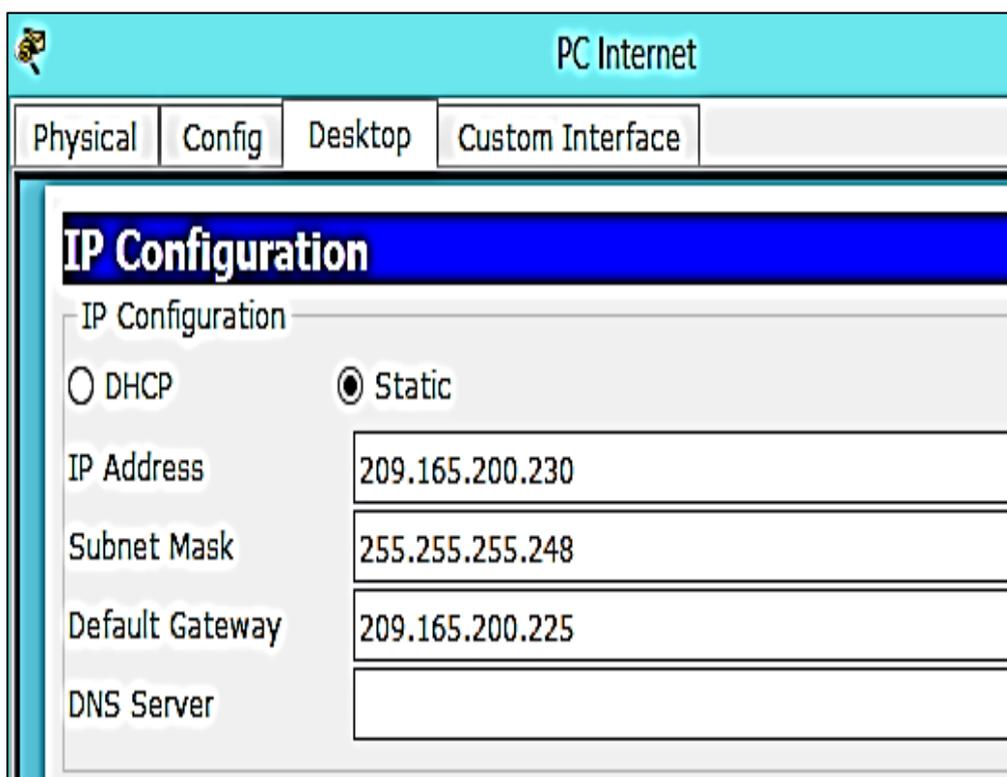
Par tal fin se emplearán los siguientes dispositivos:

3 Routers cisco 1841
2 Switch cisco 2960
PC con sistema operativo Windows
Cables serial y Ethernet

2.4 DESCRIPCIÓN DE LAS ACTIVIDADES

A continuación se enumeran y se describen cada una de las actividades que se desarrollarán para cumplir con los requerimientos solicitados.

2.4.1 **Configuración del direccionamiento ip en los dispositivos.** En primer lugar procedemos a configurar el PC Internet con la IP 209.165.200.230 de acuerdo con la tabla de direccionamiento.



The image shows a screenshot of a network configuration window titled "PC Internet". The window has four tabs: "Physical", "Config", "Desktop", and "Custom Interface". The "Config" tab is selected. Below the tabs, there is a section titled "IP Configuration" with a blue header. Under this section, there are two radio buttons: "DHCP" (unselected) and "Static" (selected). Below the radio buttons, there are four input fields: "IP Address" with the value "209.165.200.230", "Subnet Mask" with the value "255.255.255.248", "Default Gateway" with the value "209.165.200.225", and "DNS Server" which is empty.

Se hacen las configuraciones básicas en cada router y en cada switch asignando los nombres correspondientes a cada uno y estableciendo contraseñas, mensaje de seguridad y deshabilitando DNS look-up.

Los nombres asignados a los routers serán:

- R1 hostname Bogotá
- R2 hostname Miami
- R3 hostname Buenos Aires

Se procede a hacer las Configuraciones básicas en R1

```
Router>enable
Router#config t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname Bogota
Bogota(config)#no ip domain-lookup
Bogota(config)#enable secret class
Bogota(config)#line console 0
Bogota(config-line)#password cisco
Bogota(config-line)#login
Bogota(config-line)#line vty 0 5
Bogota(config-line)#password cisco
Bogota(config-line)#login
Bogota(config-line)#exit
Bogota(config)#service password-encryption
^
% Invalid input detected at '^' marker.

Bogota(config)#service password-encryption
Bogota(config)#banner motd #Prohibido el acceso no autorizado #
Bogota(config)#
```

Se procede a hacer las Configuraciones básicas en R2

```
Router>enable
Router#config t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname Miami
Miami(config)#no ip domain-lookup
Miami(config)#enable secret class
Miami(config)#line console 0
Miami(config-line)#password cisco
Miami(config-line)#login
Miami(config-line)#line vty 0 5
Miami(config-line)#password cisco
Miami(config-line)#login
Miami(config-line)#exit
Miami(config)#service password-encryption
Miami(config)#banner motd #Prohibido el acceso no autorizado #
Miami(config)#
```

Se procede a hacer las Configuraciones básicas en R3

```
Router>enable
Router#config t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname Miami
Miami(config)#no ip domain-lookup
Miami(config)#enable secret class
Miami(config)#line console 0
Miami(config-line)#password cisco
Miami(config-line)#login
Miami(config-line)#line vty 0 5
Miami(config-line)#password cisco
Miami(config-line)#login
Miami(config-line)#exit
Miami(config)#service password-encryption
Miami(config)#banner motd #Prohibido el acceso no autorizado #
Miami(config)#
```

Se procede a hacer las Configuraciones básicas en S1

```
S1>enable
S1#config t
Enter configuration commands, one per line. End with CNTL/Z.
S1(config)#no ip domain-lookup
S1(config)#enable secret class
S1(config)#line console 0
S1(config-line)#password cisco
S1(config-line)#login
S1(config-line)#exit
S1(config)#service password-encryption
S1(config)#banner motd #Prohibido el acceso no autorizado#
S1(config)#
```

Se procede a hacer las Configuraciones básicas en S1

```
S3>enable
S3#config t
Enter configuration commands, one per line. End with CNTL/Z.
S3(config)#no ip domain-lookup
S3(config)#enable secret class
S3(config)#line console 0
S3(config-line)#password cisco
S3(config-line)#login
S3(config-line)#exit
S3(config)#service password-encryption
S3(config)#banner motd #Prohibido el acceso no autorizado#
S3(config)#
```

Se configura el direccionamiento IP en cada uno de los routers de acuerdo a la topología

Se procede a configurar el direccionamiento IP el router R1

Se configura la Interface S0/0/0

```
Bogota>enable
Password:
Bogota#config t
Enter configuration commands, one per line. End with CNTL/Z.
Bogota(config)#interface s0/0/0
Bogota(config-if)#description connection to Miami
Bogota(config-if)#ip address 172.31.21.1 255.255.255.252
Bogota(config-if)#clock rate 128000
Bogota(config-if)#no shutdown
```

Se procede a configurar el direccionamiento IP en el router R2

Se configura la Interface S0/0/0

```
Miami>enable
Password:
Miami#config t
Enter configuration commands, one per line. End with CNTL/Z.
Miami(config)#interface s0/0/0
Miami(config-if)#description connection to BuenosAires
Miami(config-if)#ip address 172.31.23.1 255.255.255.252
Miami(config-if)#clock rate 128000
Miami(config-if)#no shutdown
```

Se configura la Interface S0/0/1

```
Miami(config-if)#  
Miami(config-if)#interface s0/0/1  
Miami(config-if)#description connection to Bogota  
Miami(config-if)#ip address 172.31.21.1 255.255.255.252  
Miami(config-if)#no shutdown  
  
Miami(config-if)#  
%LINK-5-CHANGED: Interface Serial0/0/1, changed state to up
```

Se configura la Interface F0/0

```
Miami(config-if)#interface f0/0  
Miami(config-if)#ip address 209.165.200.225 255.255.255.248  
Miami(config-if)#no shutdown  
  
Miami(config-if)#  
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up  
  
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to  
up
```

Se configura la interface Loopback 0

```
Miami(config-if)#interface lo0  
  
Miami(config-if)#  
%LINK-5-CHANGED: Interface Loopback0, changed state to up  
  
%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0, changed state to up  
  
Miami(config-if)#ip address 10.10.10.10 255.255.255.0  
Miami(config-if)#  
Miami(config-if)#no shutdown
```

Se procede a configurar el direccionamiento IP en R3

Se configura la Interface **S0/0/1**

```
BuenosAires(config)#interface s0/0/1
BuenosAires(config-if)#description connection to Miami
BuenosAires(config-if)#ip address 172.31.23.2 255.255.255.252
BuenosAires(config-if)#no shutdown

BuenosAires(config-if)#
%LINK-5-CHANGED: Interface Serial0/0/1, changed state to up
```

Se configura la interface **Loopback 4**

```
BuenosAires(config-if)#interface lo4

BuenosAires(config-if)#
%LINK-5-CHANGED: Interface Loopback4, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback4, changed state to up

BuenosAires(config-if)#ip address 192.168.4.1 255.255.255.0
BuenosAires(config-if)#no shutdown
```

Se configura la interface **Loopback 5**

```
BuenosAires(config-if)#interface lo5

BuenosAires(config-if)#
%LINK-5-CHANGED: Interface Loopback5, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback5, changed state to up

BuenosAires(config-if)#ip address 192.168.5.1 255.255.255.0
BuenosAires(config-if)#no shutdown
```

Se configura la interface **Loopback 6**

```
BuenosAires(config-if)#
%LINK-5-CHANGED: Interface Loopback6, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback6, changed state to up

BuenosAires(config-if)#ip address 192.168.6.1 255.255.255.0
BuenosAires(config-if)#no shutdown
```

2.4.2 **Configuraciones de vlan.** Se realizan las configuraciones VLAN según la siguiente tabla.

Tabla 5. Configuraciones VLAN escenario 2

| | Direccionamiento | Nombre |
|-----|------------------|----------------|
| 30 | 192.168.30.0/24 | Administración |
| 40 | 192.168.40.0/24 | Mercadeo |
| 200 | 192.168.200.0/24 | Mantenimiento |

Se realizan las configuraciones de VLAN necesarias en S1 asignando el nombre correspondiente a cada una según la tabla

```
S1>enable
Password:
S1#config t
Enter configuration commands, one per line. End with CNTL/Z.
S1(config)#vlan 30
S1(config-vlan)#name Administracion
S1(config-vlan)#vlan 40
S1(config-vlan)#name Mercado
S1(config-vlan)#vlan 200
S1(config-vlan)#name Mantenimiento
S1(config-vlan)#
```

Se habilitan los puertos troncales para recibir tráfico entre los switches y los routers.

Primero se hace la habilitación de los puertos troncales en S1

Se habilitan los puertos troncales en la Interface F0/3

```
S1(config)#interface f0/3
S1(config-if)#switchport mode trunk

S1(config-if)#
%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

S1(config-if)#switchport trunk native vlan1
^
% Invalid input detected at '^' marker.

S1(config-if)#switch port trunk native vlan 1
^
% Invalid input detected at '^' marker.

S1(config-if)#switchport trunk native vlan 1
```

Se habilitan los puertos troncales en la Interface F0/24

```
S1(config)#
S1(config)#interf f0/24
S1(config-if)#switchport mode trunk
S1(config-if)#switchport trunk native vlan 1
S1(config-if)#
```

Se configuran los puertos en modo access con el comando **switchport mode access**

```
S1>enable
Password:
S1#config t
Enter configuration commands, one per line. End with CNTL/Z.
S1(config)#interf f0/24
S1(config-if)#switchport trunk native vlan 1
S1(config-if)#int range fa0/1-2,fa0/4-24,g0/1-2
S1(config-if-range)#swichport mode access
^
% Invalid input detected at '^' marker.

S1(config-if-range)#switchport mode access
S1(config-if-range)#
```

Se asigna F0/1 a la VLAN 30, se activa la interfaz y se deshabilitan los demás puertos que no se van a utilizar.

```
S1(config)#int f0/1
S1(config-if)#switchport mode access
S1(config-if)#switchport access vlan 30
S1(config-if)#int range fa0/2,fa0/4-24,g0/1-2
S1(config-if-range)#shutdown

%LINK-5-CHANGED: Interface FastEthernet0/2, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/4, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/5, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/6, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/7, changed state to administratively down
```

Se configura la VLAN 200 (Mantenimiento) de acuerdo con la tabla de configuración

```
S1(config)#int vlan 200
S1(config-if)#
%LINK-5-CHANGED: Interface Vlan200, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan200, changed state to up

S1(config-if)#ip address 192.168.99.2 255.255.255.0
S1(config-if)#
```

Se hacen las configuraciones de VLAN en S3 según lo establecido en la tabla de VLAN

Primero que todo se asignan los nombres de cada VLAN

Se da nombre a cada una de las VLAN en el S3

```
S3>enable
Password:
S3#config t
Enter configuration commands, one per line. End with CNTL/Z.
S3(config)#vlan 30
S3(config-vlan)#name Administracion
S3(config-vlan)#vlan 40
S3(config-vlan)#name Mercado
S3(config-vlan)#vlan 200
S3(config-vlan)#name Mantenimiento
S3(config-vlan)#
```

Se configura la VLAN 200 (Mantenimiento)

```
S3>enable
Password:
S3#config t
Enter configuration commands, one per line. End with CNTL/Z.
S3(config)#int vlan 200
S3(config-if)#
%LINK-5-CHANGED: Interface Vlan200, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan200, changed state to up

S3(config-if)#ip address 192.168.99.3 255.255.255.0
S3(config-if)#
```

Se configura el Gateway predeterminado para permitir el tráfico de VLAN

```
S3(config)#
S3(config)#ip default-gateway 192.168.99.1
S3(config)#
```

Se habilita el modo troncal en la interfaz F0/3 para permitir el tráfico entre switch y router.

```
S3(config)#int f0/3
S3(config-if)#switchport mode access
S3(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan200, changed state to down
S3(config-if)#no shutdown
```

Se habilitan todos los puertos en modo access para permitir el tráfico de VLAN

```
S3(config-if)#no shutdown
S3(config-if)#int range fa0/1-2,fa0/4-24,g0/1-2
S3(config-if-range)#switchport mode access
S3(config-if-range)#exit
S3(config)#
```

Se asigna F0/1 a la VLAN 40 y se deshabilitan los puertos que quedan sin uso

```
S3(config)#int f0/1
S3(config-if)#switchport mode access
S3(config-if)#switchport access vlan 40
S3(config-if)#inrange fa0/2,fa0/4-24,g0/1-2
^
% Invalid input detected at '^' marker.
S3(config-if)#int range fa0/2,fa0/4-24,g0/1-2
S3(config-if-range)#shutdown
%LINK-5-CHANGED: Interface FastEthernet0/2, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/4, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/5, changed state to administratively down
```

2.4.3 **Configuraciones de seguridad 8021.q.** Se establece configuración de seguridad 8021.Q para activar la conexión hacia S1.

```

Bogota#config t
Enter configuration commands, one per line. End with CNTL/Z.
Bogota(config)#int f0/0.30
Bogota(config-subif)#description accounting LAN
Bogota(config-subif)#encapsulation dot1q 30
Bogota(config-subif)#ip address 192.168.30.1 255.255.255.0
Bogota(config-subif)#
Bogota(config-subif)#int f0/0.40
Bogota(config-subif)#description accounting LAN
Bogota(config-subif)#encapsulation dot1q 40
Bogota(config-subif)#ip address 192.168.40.1 255.255.255.0
Bogota(config-subif)#
Bogota(config-subif)#int f0/0.200
Bogota(config-subif)#description accounting LAN
Bogota(config-subif)#encapsulation dot1q 200
Bogota(config-subif)#ip address 192.168.200.1 255.255.255.0
Bogota(config-subif)#int f0/0
Bogota(config-if)#no shutdown

Bogota(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up

%LINK-5-CHANGED: Interface FastEthernet0/0.30, changed state to up

%LINK-5-CHANGED: Interface FastEthernet0/0.40, changed state to up

%LINK-5-CHANGED: Interface FastEthernet0/0.200, changed state to up

```

2.4.4 **Configuraciones de ospfv2 área 0.** Se hacen las configuraciones del protocolo de routing dinámico OSPFv2 en cada uno de los routers, asignado una ID a cada uno.

Tabla 6. Configuraciones de OSPFv2

| Configuración | Especificación |
|---|----------------|
| Router ID R1 | 1.1.1.1 |
| Router ID R2 | 5.5.5.5 |
| Router ID R3 | 8.8.8.8 |
| Configurar todas las interfaces LAN como pasivas | |
| Establecer el ancho de banda para enlaces seriales en | 256 Kb/s |
| Ajustar el costo en la métrica de S0/0 a | 9500 |

Se hacen las configuraciones de OSPFV2 en R1

Procedemos a crear un ospf en R1 con el comando **router ospf 1** y lo identificamos con la ID 1.1.1.1

```
Bogota>enable
Password:
Bogota#config t
Enter configuration commands, one per line. End with CNTL/Z.
Bogota(config)#router ospf 1
Bogota(config-router)#router-id 1.1.1.1
Bogota(config-router)#network 172.31.21.0 0.0.0.3 area 0
Bogota(config-router)#network 192.168.30.0 0.0.0.255 area0
^
% Invalid input detected at '^' marker.

Bogota(config-router)#network 192.168.30.0 0.0.0.255 area 0
Bogota(config-router)#network 192.168.40.0 0.0.0.255 area 0
Bogota(config-router)#network 192.168.200.0 0.0.0.255 area 0
Bogota(config-router)#
```

Se configuran las interfaces LAN como pasivas

```
Bogota(config-router)#
Bogota(config-router)#passive-interface f0/0.30
Bogota(config-router)#passive interface f0/0.40
^
% Invalid input detected at '^' marker.

Bogota(config-router)#passive-interface f0/0.40
Bogota(config-router)#passive-interface f0/0.200
Bogota(config-router)#
```

Se establecer el ancho de banda y costo de la métrica en s0/0/0

```
Bogota(config)#
Bogota(config)#int s0/0/0
Bogota(config-if)#bandwidth 256
Bogota(config-if)#ip ospf cost 9500
Bogota(config-if)#
```

Se hacen las configuraciones de OSPFV2 en R2

Se habilita OSPFV2 en R2 y se asigna la ID correspondiente

```
Miami>enable
Password:
Miami#config t
Enter configuration commands, one per line. End with CNTL/Z.
Miami(config)#router ospf 1
Miami(config-router)#router-id 5.5.5.5
Miami(config-router)#network 172.31.21.0 0.0.0.3 area 0
Miami(config-router)#
05:43:35: %OSPF-5-ADJCHG: Process 1, Nbr 1.1.1.1 on Serial0/0/1 from LOADING to
FULL, Loading Done

Miami(config-router)#network 172.31.23.0 0.0.0.3 area 0
Miami(config-router)#network 10.10.10.0 0.0.0.255 area 0
Miami(config-router)#passive-interface f0/1
Miami(config-router)#interface s0/0/0
Miami(config-if)#bandwidth 256
Miami(config-if)#ip ospf cost 9500
Miami(config-if)#
```

Se hacen las Configuraciones de OSPFV2 en R3

Se habilita el router con OSPFV2 y se asigna la ID correspondiente

```
BuenosAires>enable
Password:
BuenosAires#config t
Enter configuration commands, one per line. End with CNTL/Z.
BuenosAires(config)#router ospf 1
BuenosAires(config-router)#router-id 8.8.8.8
BuenosAires(config-router)#network 172.31.23.0 0.0.0.3 area 0
BuenosAires(config-router)#
00:07:00: %OSPF-5-ADJCHG: Process 1, Nbr 5.5.5.5 on Serial0/0/1 from LOADING to
FULL, Loading Done

BuenosAires(config-router)#network 192.168.4.0 0.0.3.255 area 0
BuenosAires(config-router)#passive-interface lo4
BuenosAires(config-router)#passive-interface lo5
BuenosAires(config-router)#paasive interface lo6
^
% Invalid input detected at '^' marker.

BuenosAires(config-router)#passive-interface lo6
BuenosAires(config-router)#exit
BuenosAires(config)#interface s0/0/1
BuenosAires(config-if)#bandwidth 256
BuenosAires(config-if)#ip ospf cost 9500
```

2.4.5 **Verificaciones de ospfv2.** Se hacen las verificaciones de OSPF en los routers utilizando los comandos **show ip route ospf** y **show ip ospf neighbors**.

Se hacen las verificaciones de OSPF en el R1

```
Bogota#show ip route ospf
      172.31.0.0/30 is subnetted, 2 subnets
O       172.31.23.0 [110/19000] via 172.31.21.1, 01:15:52, Serial0/0/0
      192.168.4.0/32 is subnetted, 1 subnets
O       192.168.4.1 [110/19001] via 172.31.21.1, 01:08:06, Serial0/0/0
      192.168.5.0/32 is subnetted, 1 subnets
O       192.168.5.1 [110/19001] via 172.31.21.1, 01:07:56, Serial0/0/0
      192.168.6.0/32 is subnetted, 1 subnets
O       192.168.6.1 [110/19001] via 172.31.21.1, 01:07:56, Serial0/0/0
```

Se hace verificación de los vecinos OSPF en R1 con **show ip ospf neighbor**

```
Bogota#show ip ospf neighbor

Neighbor ID   Pri  State           Dead Time   Address        Interface
5.5.5.5       0    FULL/ -         00:00:30    172.31.21.1    Serial0/0/0
Bogota#
```

Se hacen verificaciones de OSPF En R2 con el comando **show ip route ospf**

```
Miami#show ip route ospf
      192.168.4.0/32 is subnetted, 1 subnets
O       192.168.4.1 [110/9501] via 172.31.23.2, 01:09:55, Serial0/0/0
      192.168.5.0/32 is subnetted, 1 subnets
O       192.168.5.1 [110/9501] via 172.31.23.2, 01:09:55, Serial0/0/0
      192.168.6.0/32 is subnetted, 1 subnets
O       192.168.6.1 [110/9501] via 172.31.23.2, 01:09:55, Serial0/0/0
```

Se hacen verificaciones de OSPF En R2 con el comando **show ip ospf neighbor**

```
Miami#show ip ospf neighbor

Neighbor ID    Pri  State           Dead Time   Address      Interface
8.8.8.8        0    FULL/ -         00:00:35   172.31.23.2  Serial0/0/0
1.1.1.1        0    FULL/ -         00:00:34   172.31.21.1  Serial0/0/1
Miami#
```

Se hacen las verificaciones de OSPF En R3 con el comando **show ip route ospf**

```
BuenosAires#show ip route ospf
      172.31.0.0/30 is subnetted, 2 subnets
0       172.31.21.0 [110/9564] via 172.31.23.1, 01:07:37, Serial0/0/1
BuenosAires#
```

Se hacen las verificaciones de OSPF En R3 con el comando **show ip ospf Neighbor**

```
BuenosAires>enable
Password:
BuenosAires#show ip ospf neighbor

Neighbor ID    Pri  State           Dead Time   Address      Interface
5.5.5.5        0    FULL/ -         00:00:34   172.31.23.1  Serial0/0/1
BuenosAires#
```

Se requiere visualizar las tablas de enrutamiento y routers conectados por OSPFv2.

Por tanto se procede a ejecutar el comando **show ip route** en cada uno de los routers.

Se visualizan las tablas de enrutamiento con el comando **show ip route** en R1

```
Bogota>enable
Password:
Bogota#show ip route
Codes: C - connected, S - static, I - IGRP, 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 0.0.0.0 to network 0.0.0.0

    172.31.0.0/30 is subnetted, 2 subnets
C       172.31.21.0 is directly connected, Serial0/0/0
O       172.31.23.0 [110/19000] via 172.31.21.1, 00:32:38, Serial0/0/0
    192.168.4.0/32 is subnetted, 1 subnets
O       192.168.4.1 [110/19001] via 172.31.21.1, 00:24:53, Serial0/0/0
    192.168.5.0/32 is subnetted, 1 subnets
O       192.168.5.1 [110/19001] via 172.31.21.1, 00:24:43, Serial0/0/0
    192.168.6.0/32 is subnetted, 1 subnets
O       192.168.6.1 [110/19001] via 172.31.21.1, 00:24:43, Serial0/0/0
S*    0.0.0.0/0 is directly connected, Serial0/0/0
Bogota#
```

Se visualizan las tablas de enrutamiento con el comando **show ip route** en R2

```
Miami>enable
Password:
Miami#show ip route
Codes: C - connected, S - static, I - IGRP, 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

    172.31.0.0/30 is subnetted, 2 subnets
C       172.31.21.0 is directly connected, Serial0/0/1
C       172.31.23.0 is directly connected, Serial0/0/0
    192.168.4.0/32 is subnetted, 1 subnets
O       192.168.4.1 [110/9501] via 172.31.23.2, 00:28:54, Serial0/0/0
    192.168.5.0/32 is subnetted, 1 subnets
O       192.168.5.1 [110/9501] via 172.31.23.2, 00:28:54, Serial0/0/0
    192.168.6.0/32 is subnetted, 1 subnets
O       192.168.6.1 [110/9501] via 172.31.23.2, 00:28:54, Serial0/0/0
    209.165.200.0/29 is subnetted, 1 subnets
C       209.165.200.224 is directly connected, FastEthernet0/0
Miami#
```

Se visualizan las tablas de enrutamiento con el comando **show ip route** en R3

```
BuenosAires>enable
Password:
BuenosAires#show ip route
Codes: C - connected, S - static, I - IGRP, 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

172.31.0.0/30 is subnetted, 2 subnets
O       172.31.21.0 [110/9564] via 172.31.23.1, 00:27:55, Serial0/0/1
C       172.31.23.0 is directly connected, Serial0/0/1
C       192.168.4.0/24 is directly connected, Loopback4
C       192.168.5.0/24 is directly connected, Loopback5
C       192.168.6.0/24 is directly connected, Loopback6
```

Se requiere visualizar la lista resumida de interfaces por OSPF en donde se ilustre el costo de cada interface

Aplicamos el comando **show run** en R1

```
interface Serial0/0/0
description connection to Miami
bandwidth 256
ip address 172.31.21.1 255.255.255.252
ip ospf cost 9500
clock rate 128000
```

Aplicamos el comando **show run** en R2

```
*
interface Serial0/0/0
description connection to BuenosAires
bandwidth 256
ip address 172.31.23.1 255.255.255.252
ip ospf cost 9500
clock rate 128000
```

Aplicamos el comando **show run** en **R3**

```
interface Serial0/0/1
  description connection to Miami
  bandwidth 256
  ip address 172.31.23.2 255.255.255.252
  ip ospf cost 9500
  clock rate 2000000
!
```

Se requiere visualizar el OSPF Process ID, Router ID, Address summarizations, Routing Networks, and passive interfaces configuradas en cada router.

Aplicamos el comando **show run** en **R1**

```
!
router ospf 1
  router-id 1.1.1.1
  log-adjacency-changes
  passive-interface FastEthernet0/0.30
  passive-interface FastEthernet0/0.40
  passive-interface FastEthernet0/0.200
  network 172.31.21.0 0.0.0.3 area 0
  network 192.168.30.0 0.0.0.255 area 0
  network 192.168.40.0 0.0.0.255 area 0
  network 192.168.200.0 0.0.0.255 area 0
!
```

Aplicamos el comando **show run** en **R2**

```
router ospf 1
  router-id 5.5.5.5
  log-adjacency-changes
  passive-interface FastEthernet0/1
  passive-interface Loopback0
  network 172.31.21.0 0.0.0.3 area 0
  network 172.31.23.0 0.0.0.3 area 0
  network 10.10.10.0 0.0.0.255 area 0
!
```

Aplicamos el comando **show run** en **R3**

```
router ospf 1
  router-id 8.8.8.8
  log-adjacency-changes
  passive-interface Loopback4
  passive-interface Loopback5
  passive-interface Loopback6
  network 172.31.23.0 0.0.0.3 area 0
  network 192.168.4.0 0.0.3.255 area 0
!
```

Aplicamos el comando **show ip protocols** en **R1**

```
Bogota>enable
Password:
Bogota#show ip protocols

Routing Protocol is "ospf 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 1.1.1.1
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    172.31.21.0 0.0.0.3 area 0
    192.168.30.0 0.0.0.255 area 0
    192.168.40.0 0.0.0.255 area 0
    192.168.200.0 0.0.0.255 area 0
  Passive Interface(s):
    FastEthernet0/0.30
    FastEthernet0/0.40
    FastEthernet0/0.200
  Routing Information Sources:
    Gateway         Distance      Last Update
    1.1.1.1          110          00:06:26
    5.5.5.5          110          00:29:37
    8.8.8.8          110          00:25:16
  Distance: (default is 110)
```

Aplicamos el comando **show ip protocols** en **R2**

```
Miami>enable
Password:
Miami# show ip protocols

Routing Protocol is "ospf 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 5.5.5.5
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    172.31.21.0 0.0.0.3 area 0
    172.31.23.0 0.0.0.3 area 0
    10.10.10.0 0.0.0.255 area 0
  Passive Interface(s):
    FastEthernet0/1
    Loopback0
  Routing Information Sources:
    Gateway         Distance      Last Update
    1.1.1.1          110          00:11:02
    5.5.5.5          110          00:04:12
    8.8.8.8          110          00:29:52
  Distance: (default is 110)
```

Aplicamos el comando **show ip protocols** en **R3**

```
BuenosAires>enable
Password:
BuenosAires#show ip protocols

Routing Protocol is "ospf 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 8.8.8.8
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    172.31.23.0 0.0.0.3 area 0
    192.168.4.0 0.0.3.255 area 0
  Passive Interface(s):
    Loopback4
    Loopback5
    Loopback6
  Routing Information Sources:
    Gateway         Distance      Last Update
    1.1.1.1          110          00:12:19
    5.5.5.5          110          00:05:30
    8.8.8.8          110          00:01:08
  Distance: (default is 110)
```

2.4.6 **Implementación de DHCP en R1.** Se hace la implementación de DHCP para cada una de las LAN con el fin de permitir la asignación dinámica automática de IP a los host.

Tabla 7. Implementación DHCP en R1

| | |
|-----------------------------------|--|
| Configurar DHCP pool para VLAN 30 | Name: ADMINISTRACION DNS-Server: 10.10.10.11 Domain-Name: ccna-unad.com Establecer default - gateway. |
| Configurar DHCP pool para VLAN 40 | Name: MERCADEO DNS-Server: 10.10.10.11 Domain-Name: ccna-unad.com Establecer default- gateway. |

En R1 se reservan las primeras 30 direcciones en la VLAN 30 y en la VLAN 40 Aplicando el comando **ip dhcp excluded- address**

```
Bogota>enable
Password:
Bogota#config t
Enter configuration commands, one per line. End with CNTL/Z.
Bogota(config)#ip dhcp excluded address
Bogota(config)#ip dhcp excluded-address 192.168.30.1 192.168.30.30
Bogota(config)#ip dhcp excluded-address 192.168.40.1 192.168.40.30
Bogota(config)#
```

Se procede a configurar DHCP pool en la VLAN 30

```
Bogota(config)#ip dhcp pool Administracion
Bogota(dhcp-config)#dns-server 10.10.10.11
Bogota(dhcp-config)#default-router 192.168.30.1
Bogota(dhcp-config)#network 192.168.30.0 255.255.255.0
Bogota(dhcp-config)#
```

Se procede a configurar DHCP pool en la VLAN 40

```
Bogota#config t
Enter configuration commands, one per line. End with CNTL/Z.
Bogota(config)#ip dhcp pool Mercado
Bogota(dhcp-config)#dns-server 10.10.10.11
Bogota(dhcp-config)#default-router 192.168.40.1
Bogota(dhcp-config)#network 192.168.40.0 255.255.255.0
Bogota(dhcp-config)#exit
Bogota(config)#exit
Bogota#
```

2.4.7 Implementación de nat en R2. Se procede a implementar NAT en R2 utilizando los comandos **ip nat inside / ip nat outside**.

```
Miami(config)#ip nat inside source static 10.10.10.10 209.165.200.229
Miami(config)#int f0/0
Miami(config-if)#ip nat outside
Miami(config-if)#int f0/1
Miami(config-if)#ip nat inside
Miami(config-if)#
```

2.4.8 Configuración de listas de acceso. Se procede a hacer la configuración de las listas de acceso utilizando el comando **access-list permit**.

```
Miami(config)#access-list 1 permit 192.168.30.0 0.0.0.255
Miami(config)#access-list 1 permit 192.168.40.0 0.0.0.255
Miami(config)#access-list 1 permit 192.168.4.0 0.0.3.255
Miami(config)#ip nat pool INTERNET 209.165.200.225 209.165.200.229 netmask
255.255.255.248
```

2.4.9 Verificaciones de comunicación. Se hacen las verificaciones de comunicación pertinentes para comprobar que exista conexión entre las redes, utilizando el comando **PING**.

Se comprueba la conectividad haciendo PING de R1 a R2

```
Bogota#ping 172.31.23.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.31.23.1, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/6/18 ms
```

Se comprueba la conectividad haciendo PING de R3 a R2

```
BuenosAires>enable
Password:
BuenosAires#ping 172.31.23.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.31.23.1, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/5/16 ms
```

Se comprueba la conectividad haciendo PING de R2 a R1

```
Miami>enable
Password:
Miami#ping 172.31.21.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.31.21.1, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/4/11 ms
```

Se comprueba la conectividad haciendo PING de R2 a R3

```
Miami#ping 172.31.23.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.31.23.2, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/4/18 ms
```

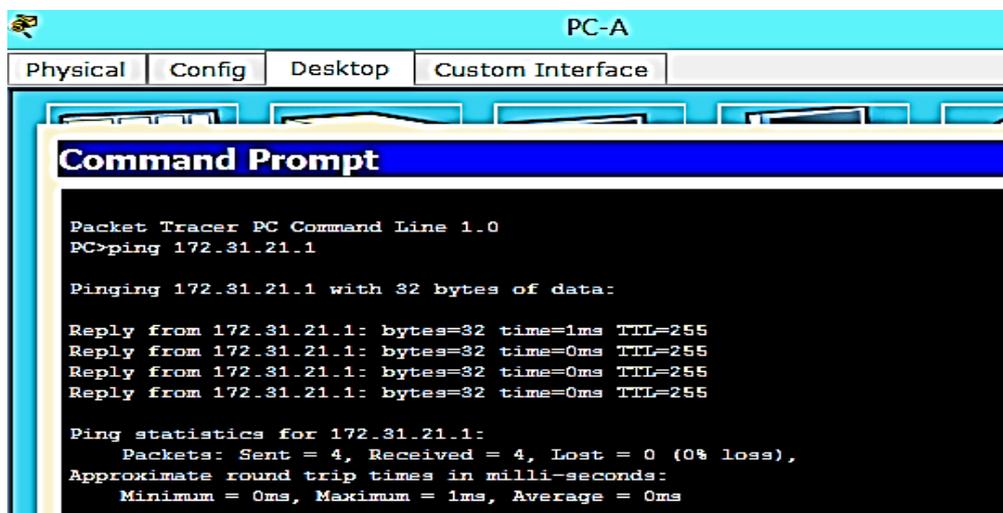
Se comprueba la conectividad haciendo PING de PC-C a R1

```
Pinging 172.31.21.1 with 32 bytes of data:

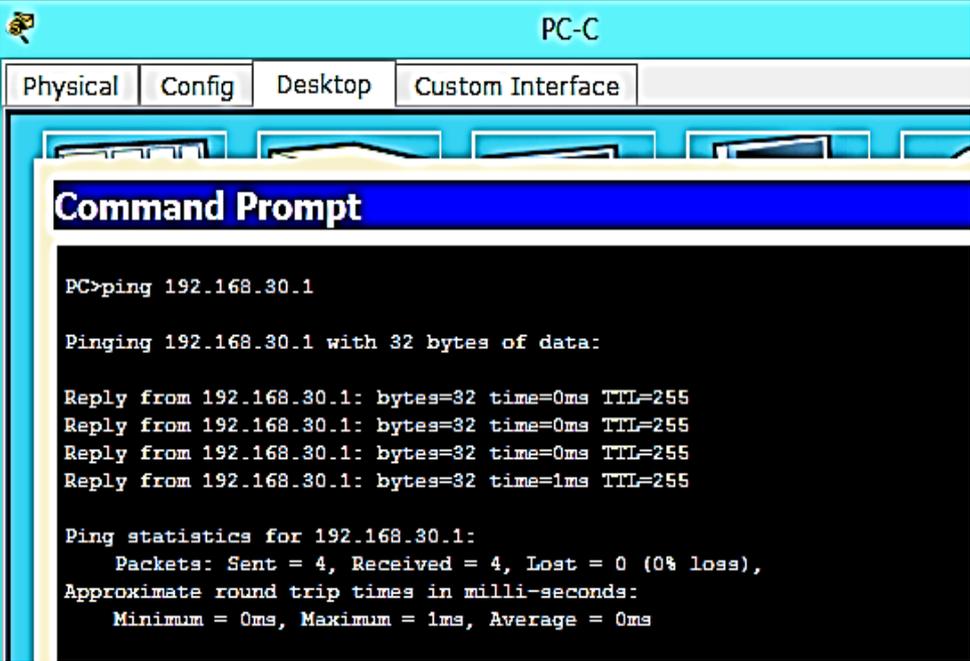
Reply from 172.31.21.1: bytes=32 time=14ms TTL=255
Reply from 172.31.21.1: bytes=32 time=0ms TTL=255
Reply from 172.31.21.1: bytes=32 time=0ms TTL=255
Reply from 172.31.21.1: bytes=32 time=0ms TTL=255

Ping statistics for 172.31.21.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 14ms, Average = 3ms
```

Se comprueba la conectividad haciendo PING de PC-A AL R1



Se comprueba la conectividad haciendo PING de PC-C a PC-A



```
PC-C
Physical Config Desktop Custom Interface

Command Prompt

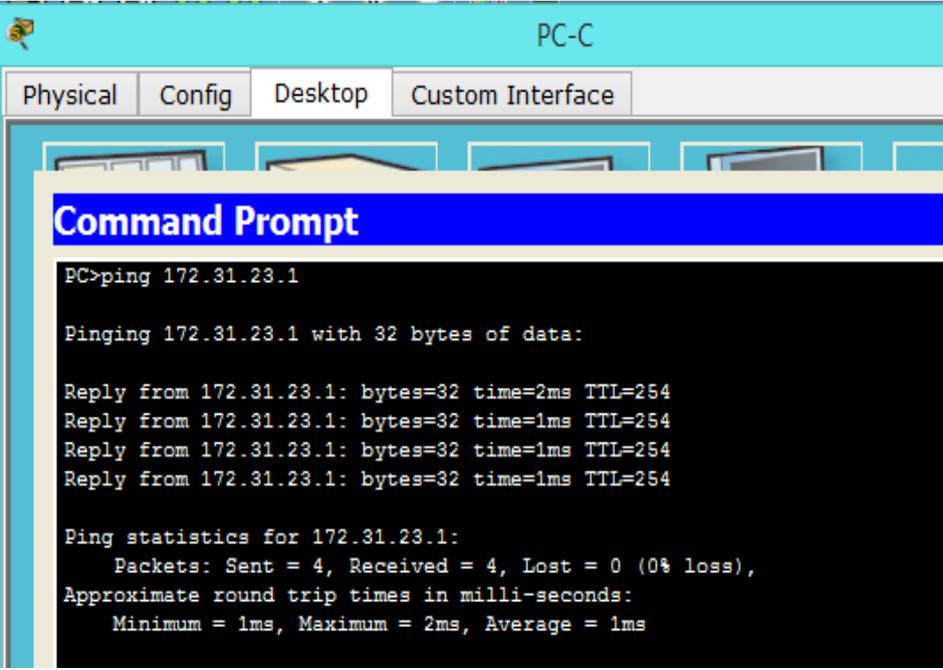
PC>ping 192.168.30.1

Pinging 192.168.30.1 with 32 bytes of data:

Reply from 192.168.30.1: bytes=32 time=0ms TTL=255
Reply from 192.168.30.1: bytes=32 time=0ms TTL=255
Reply from 192.168.30.1: bytes=32 time=0ms TTL=255
Reply from 192.168.30.1: bytes=32 time=1ms TTL=255

Ping statistics for 192.168.30.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

Se comprueba la conectividad haciendo PING de PC-C a R2



```
PC-C
Physical Config Desktop Custom Interface

Command Prompt

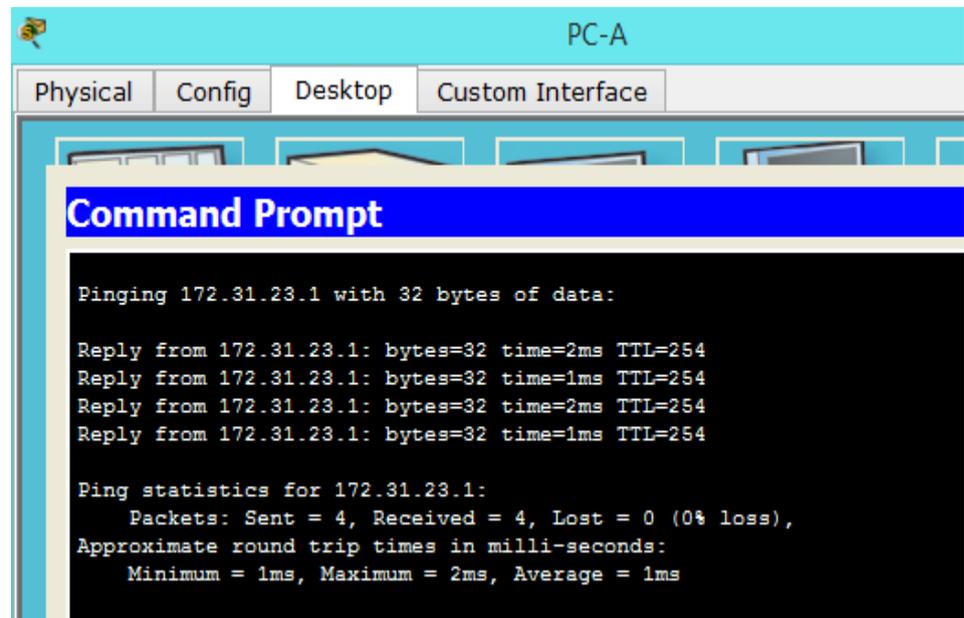
PC>ping 172.31.23.1

Pinging 172.31.23.1 with 32 bytes of data:

Reply from 172.31.23.1: bytes=32 time=2ms TTL=254
Reply from 172.31.23.1: bytes=32 time=1ms TTL=254
Reply from 172.31.23.1: bytes=32 time=1ms TTL=254
Reply from 172.31.23.1: bytes=32 time=1ms TTL=254

Ping statistics for 172.31.23.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 2ms, Average = 1ms
```

Se comprueba la conectividad haciendo PING de PC-A a R2



The screenshot shows a desktop environment for PC-A with tabs for Physical, Config, Desktop, and Custom Interface. A Command Prompt window is open, displaying the results of a ping command to 172.31.23.1. The output shows four successful replies with varying round-trip times (1ms and 2ms) and a TTL of 254. The statistics indicate 4 packets sent, 4 received, and 0% loss.

```
PC-A
Physical Config Desktop Custom Interface
Command Prompt
Pinging 172.31.23.1 with 32 bytes of data:

Reply from 172.31.23.1: bytes=32 time=2ms TTL=254
Reply from 172.31.23.1: bytes=32 time=1ms TTL=254
Reply from 172.31.23.1: bytes=32 time=2ms TTL=254
Reply from 172.31.23.1: bytes=32 time=1ms TTL=254

Ping statistics for 172.31.23.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 2ms, Average = 1ms
```

3. CONCLUSIONES

La realización del presente trabajo nos permitió realizar la aplicación práctica de configuración de switch y routers en redes.

La realización del presente trabajo nos permitió aplicar en forma práctica las configuraciones de VLAN necesarias para redes dinámicas, la habilitación de puertos troncales y deshabilitación de puertos no utilizados.

De la misma forma la realización de la actividad nos permitió reconocer la importancia y la aplicación de los protocolos de enrutamiento DHCP, OSPFv2, RIPv2 y la aplicación de NAT.

La realización del trabajo nos permitió reconocer la aplicación práctica de las Configuraciones de seguridad, y la configuración de las listas de control de acceso.

Así mismo nos permitió poner en práctica la aplicación de los comandos útiles en PACKET TRACER para hacer verificaciones de información, de configuración, de comunicación y de conectividad entre los diferentes dispositivos de una red.

BIBLIOGRAFÍA

CISCO. Configuración y conceptos básicos de switching. (2018). Disponible en: <https://static-course-assets.s3.amazonaws.com/RSE503/es/index.html#2>

CISCO. Conceptos de routing. (2018). Disponible en: <https://static-course-assets.s3.amazonaws.com/RSE503/es/index.html#4>

CISCO. Enrutamiento entre VLAN. (2018). Disponible en: <https://static-course-assets.s3.amazonaws.com/RSE503/es/index.html#5>

CISCO. Enrutamiento estático. (2018). Disponible en: <https://static-course-assets.s3.amazonaws.com/RSE503/es/index.html#6>

CISCO. Routing dinámico. (2018). Disponible en: <https://static-course-assets.s3.amazonaws.com/RSE503/es/index.html#7>

CISCO. Ospf de área única. (2018). Disponible en: <https://static-course-assets.s3.amazonaws.com/RSE503/es/index.html#8>

CISCO. Listas de control de acceso. (2018). Disponible en: <https://static-course-assets.s3.amazonaws.com/RSE503/es/index.html#9>

CISCO. DHCP. (2018). Disponible en: <https://static-course-assets.s3.amazonaws.com/RSE503/es/index.html#10>

CISCO. Traducción de direcciones de red para IPV4. (2018). Disponible en: <https://static-course-assets.s3.amazonaws.com/RSE503/es/index.html#11>