

Evaluación – Prueba de habilidades practica CCNA

Everth Alejandro Ramírez Duarte

Universidad Nacional Abierta y a Distancia – UNAD
Programa de Ingeniera de Sistemas
Diplomado de profundización CISCO (Diseño e Implementación de
Soluciones Integradas Lan/Wan)
Bogotá D.C.
2018

Evaluación – Prueba de habilidades practica CCNA

Everth Alejandro Ramírez Duarte

203092_9

Informe habilidades prácticas CCNA

Tutor: Efraín Alejandro Pérez

Universidad Nacional Abierta y a Distancia – UNAD
Programa de Ingeniera de Sistemas
Diplomado de profundización CISCO (Diseño e Implementación de
Soluciones Integradas Lan/Wan)
Bogotá D.C.
2018

Tabla de contenido

Introducción	6
Evaluación – Prueba de habilidades practica CCNA	7
Escenario 1	7
Topología original.....	7
Topología diseñada.....	8
Desarrollo del escenario.....	8
Escenario 2.....	18
Topología original.....	19
Topología diseñada.....	20
Desarrollo del escenario.....	20
Conclusiones	36
Glosario.....	37
Referencias bibliográficas	39

Tabla de contenido de ilustraciones

Tabla 1. OSPFv2 área 0	25
Tabla 2. Reservas de direcciones IP	32

Tabla de contenido de ilustraciones

Ilustración 1. Topología original Escenario 1	7
Ilustración 2. Topología diseñada Escenario 1	8
Ilustración 3. NAT con sobrecarga R1	12
Ilustración 4. Servidor IPv6 accesible – 1	14
Ilustración 5. Servidor IPv6 accesible – 2	15
Ilustración 6. Servidor IPv6 accesible – 2.2	15
Ilustración 7. Verificación de conectividad – 1	17
Ilustración 8. Verificación de conectividad – 2	18
Ilustración 9. Topología original Escenario 2	19
Ilustración 10. Topología diseñada del escenario 2	20
Ilustración 11. Static del PC de internet	21
Ilustración 12. DHCP del PC-A	22
Ilustración 13. DHCP del PC-C	23
Ilustración 14. Static para Web Server.....	24
Ilustración 15. Enrutamiento y routers conectados por OSPFv2.....	27
Ilustración 16. Interfaces por OSPF	28
Ilustración 17. Interfaces configuradas en cada router	29
Ilustración 18. Ping Internet PC	34
Ilustración 19. Ping Web Server.....	35

Introducción

Dentro del presente trabajo denominado *Evaluación – Prueba de habilidades CCNA* el cual hace parte de la etapa final del *diplomado de profundización CISCO (Diseño e Implementación de Soluciones Integradas Lan/Wan)* se da solución a dos escenarios completamente independientes entre sí, donde haremos uso de los conocimientos adquiridos dentro de las etapas anteriores al presente trabajo final.

Sobre cada uno de los escenarios que se resuelven dentro del presente informe se abordan técnicas básicas de la configuración de una red en la cual para que su funcionamiento sea óptimo y estable se hacen uso de comandos para cada uno de los dispositivos necesarios en la red como los son router, switch, servidores, computadores entre otros que son necesarios para lograr un buen enrutamiento dentro de la red correspondiente.

Para que cada uno de los dispositivos anteriores tengan una buena comunicación dentro de su red es necesario hacer uso del comando correspondiente a cada uno de los dispositivos como lo son: Vlans, configuraciones OSPF, implementación de los protocolos DHCP – NAT y su respectiva verificación de los ACL.

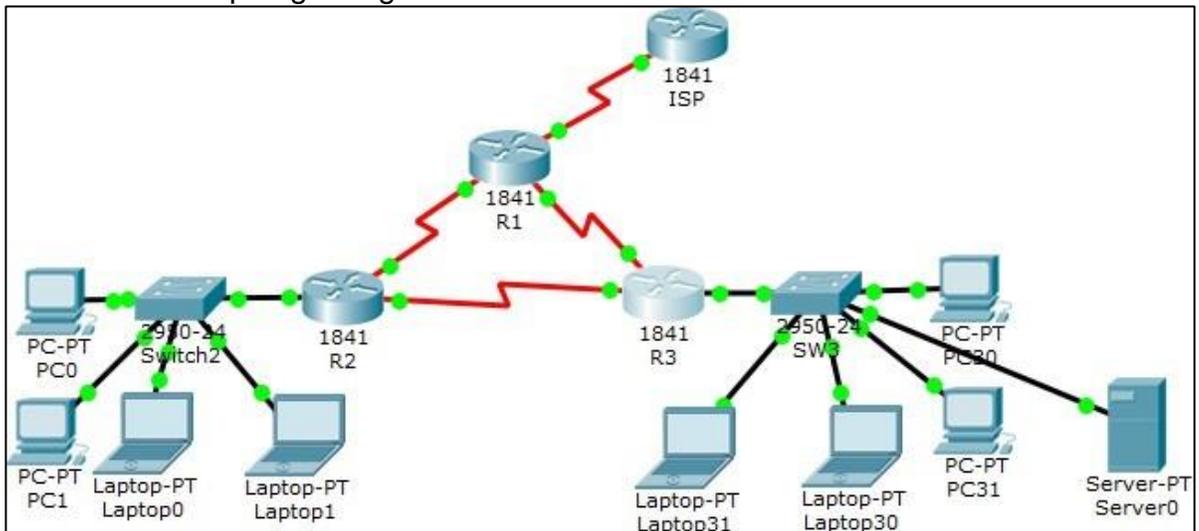
Evaluación – Prueba de habilidades practica CCNA

Escenario 1

Descripción: 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.

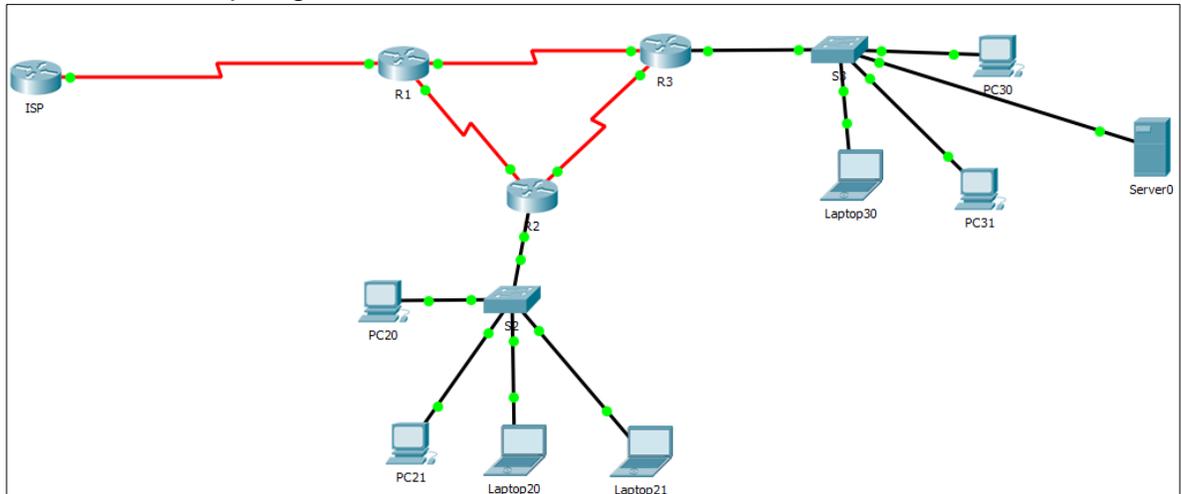
Topología original

Ilustración 1. Topología original Escenario 1



Topología diseñada

Ilustración 2. Topología diseñada Escenario 1



Desarrollo del escenario

1. **SW1** VLAN y las asignaciones de puertos de VLAN deben cumplir con la tabla 1.

Para SW2

```
enable
```

```
config t
```

```
vlan 100
```

```
name LAPTOPS
```

```
vlan 200
```

```
name DESTOPS
```

```
interface range f0/2-3
```

```
switchport mode access
```

```
switchport access vlan 100
```

```
interface range f0/4-5
```

```
switchport mode access
```

```
switchport access vlan 200
```

```
interface f0/1
```

```
switchport mode trunk
```

Para SW3

```
enable
config t
vlan 1
interface range f0/1-24
switchport mode access
switchport access vlan 1
no shutdown
```

2. Los puertos de red que no se utilizan se deben deshabilitar.

```
interface range f0/6-24
shutdown
```

3. La información de dirección IP R1, R2 y R3 debe cumplir con la tabla 1.

Para R2

```
enable
config t
interface f0/0.100
encapsulation dot1Q 100
ip address 192.168.20.1 255.255.255.0
```

```
interface fastEthernet0/0.200
encapsulation dot1Q 200
ip address 192.168.21.1 255.255.255.0
```

```
interface fastEthernet0/0
no shutdown
```

```
interface serial 0/0/0
ip address 10.0.0.2 255.255.255.252
no shutdown
interface serial 0/0/1
ip address 10.0.0.9 255.255.255.252
no shutdown
```

Para R1

```
enable
config t
interface serial 0/0/0
ip address 200.123.211.2 255.255.255.0
no shutdown
```

```
interface serial 0/1/0
ip address 10.0.0.1 255.255.255.252
no shutdown
```

```
interface serial 0/1/1
ip address 10.0.0.5 255.255.255.252
no shutdown
```

Para R3

```
enable
config t
ipv6 unicast-routing
```

```
interface fastEthernet0/0
ip address 192.168.30.1 255.255.255.0
ipv6 address 2001:db8:130::9C0:80F:301/64
no shutdown
```

```
ipv6 dhcp server vlan_1
ipv6 nd other-config-flag
no shutdown
```

```
interface serial 0/0/0
ip address 10.0.0.6 255.255.255.252
no shutdown
interface serial 0/0/1
ip address 10.0.0.10 255.255.255.252
no shutdown
```

4. **Laptop20, Laptop21, PC20, PC21, Laptop30, Laptop31, PC30 y PC31** deben obtener información IPv4 del servidor DHCP.

Para R2

```
enable
config t
ip dhcp pool vlan_100
network 192.168.20.1 255.255.255.0
default-router 192.168.20.1
```

```
ip dhcp pool VLAN_200
network 192.168.21.1 255.255.255.0
default-router 192.168.21.1
exit
```

Para R3

```
enable
config t
ip dhcp pool vlan_1
network 192.168.30.1 255.255.255.0
default-router 192.168.30.1
```

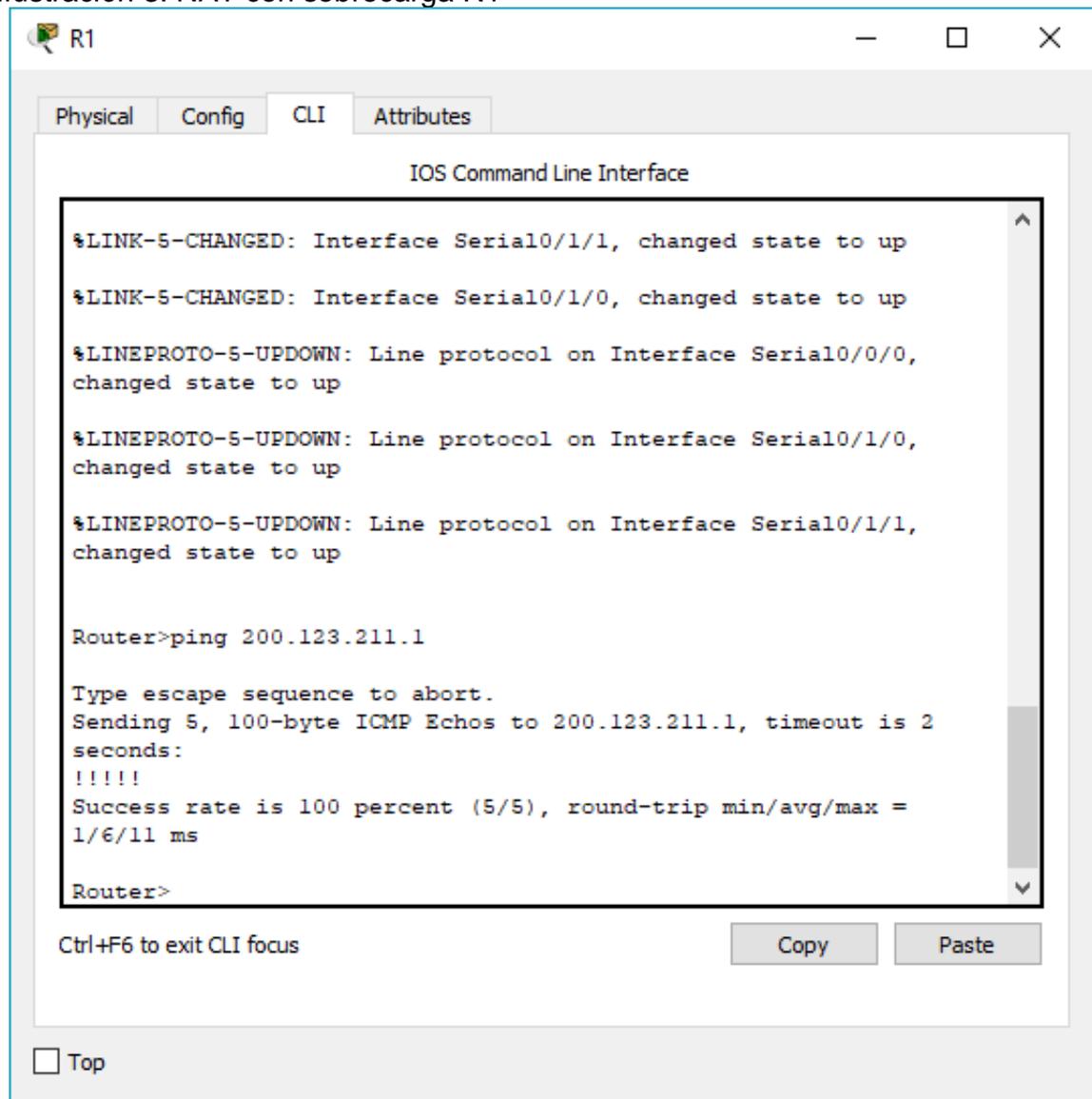
```
ipv6 dhcp pool vlan_1
dns-server 2001:db8:130::
exit
```

5. 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.

```
enable
config t
ip nat pool INSIDE-DEVS 200.123.211.2 200.123.211.128 netmask
255.255.255.0
access-list 1 permit 192.168.0.0 0.0.255.255
access-list 1 permit 10.0.0.0 0.0.0.255
ip nat inside source list 1 interface s0/0/0 overload
interface s0/1/0
ip nat inside
interface s0/1/1
ip nat inside

interface s0/0/0
ip nat outside
ping
```

Ilustración 3. NAT con sobrecarga R1



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

```
enable
config t
router r
version 2
router rip
version 2
network 10.0.0.0
```

```
default-information originate
ip route 0.0.0.0 0.0.0.0 serial 0/0/0
exit
```

7. R2 es un servidor de DHCP para los dispositivos conectados al puerto FastEthernet0/0.

```
config t
router rip
version 2
network 192.168.20.0
network 192.168.21.0
network 192.168.30.0
```

8. R2 debe, además de enrutamiento a otras partes de la red, ruta entre las VLAN 100 y 200.

```
enable
config t
ip dhcp pool vlan_100
network 192.168.20.1 255.255.255.0
default-router 192.168.20.1
```

```
ip dhcp pool VLAN_200
network 192.168.21.1 255.255.255.0
default-router 192.168.21.1
exit
```

9. El Servidor0 es sólo un servidor IPv6 y solo debe ser accesibles para los dispositivos en R3 (ping).

Ilustración 4. Servidor IPv6 accesible – 1

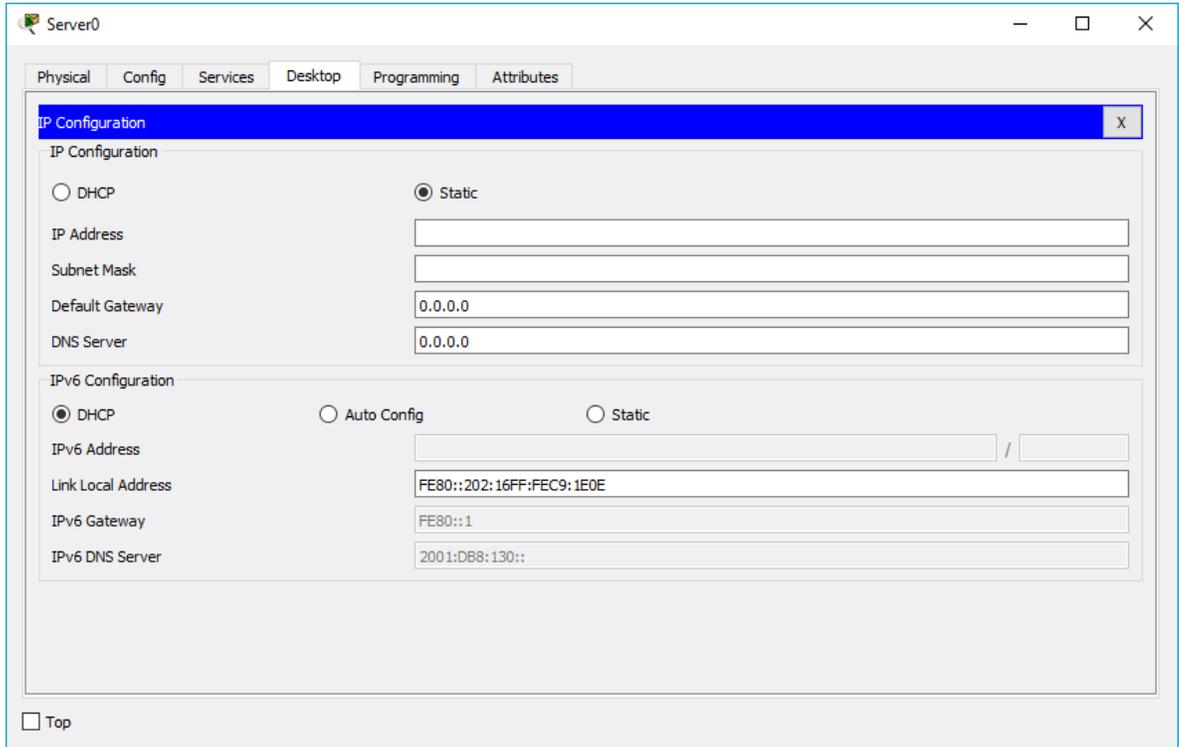


Ilustración 5. Servidor IPv6 accesible – 2

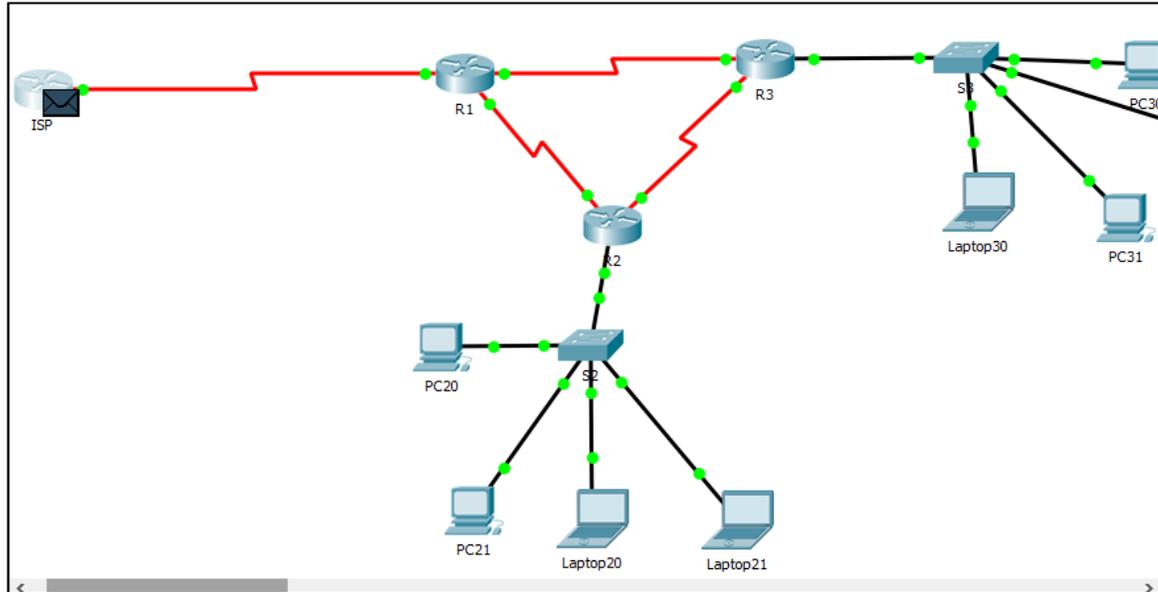


Ilustración 6. Servidor IPv6 accesible – 2.2

The screenshot shows a network simulation interface. On the left, a switch S3 is connected to Laptop30, PC31, and Server0. A 'Simulation Panel' window is open on the right, displaying an 'Event List' table. The table has columns for 'Vis.', 'Time(sec)', 'Last Device', 'At Device', 'Type', and 'Info'. The table shows several ICMP events occurring at 0.006 seconds.

Vis.	Time(sec)	Last Device	At Device	Type	Info
	0.005	R3	S3	ICMP	
	0.005	S3	PC31	ICMP	
	0.005	--	S3	ICMP	
	0.006	--	PC31	ICMP	
	0.006	PC31	S3	ICMP	
	0.006	S3	R3	ICMP	
	0.006	R3	S3	ICMP	
	0.006	S3	Laptop30	ICMP	
	0.006	--	S3	ICMP	

Below the table, there are controls for 'Reset Simulation', 'Constant Delay' (checked), and 'Captured to: 0.006 s'. There are also 'Play Controls' buttons: 'Back', 'Auto Capture / Play', and 'Capture / Forward'. At the bottom, there is a section for 'Event List Filters - Visible Events' with a list of protocols and a 'Show All/None' button.

10. La NIC instalado en direcciones IPv4 e IPv6 de Laptop30, de Laptop31, de PC30 y obligación de configurados PC31 simultáneas (dual-stack). Las direcciones se deben configurar mediante DHCP y DHCPv6.

11. La interfaz FastEthernet 0/0 del R3 también deben tener direcciones IPv4 e IPv6 configuradas (dual- stack).

```
enable
config t
interface fastEthernet 0/0
ip address 192.168.30.1 255.255.255.0
duplex auto
speed auto
ipv6 address FE80::1 link-local
ipv6 address 2001:DB8:130::9C0:80F:301/64
ipv6 nd other-config-flag
ipv6 dhcp server vlan_1
exit
ip access-list extended SERVER
```

12. R1, R2 y R3 intercambian información de routing mediante RIP versión 2.

Para R1

```
enable
config t
router rip
version 2
ip route 0.0.0.0 0.0.0.0 s0/0/0
router rip
version 2
network 10.0.0.4
network 10.0.0.0
default-information originate
```

Para R2

```
enable
config t
router rip
version 2
network 192.168.30.0
network 192.168.20.0
network 192.168.21.0
network 10.0.0.0
network 10.0.0.8
```

Para R3
 enable
 config t
 router rip
 version 2
 network 192.168.0.0
 network 10.0.0.8
 network 10.0.0.4

13. R1, R2 y R3 deben saber sobre las rutas de cada uno y la ruta predeterminada desde R1.

14. Verifique la conectividad. Todos los terminales deben poder hacer ping entre sí y a la dirección IP del ISP. Los terminales bajo el R3 deberían poder hacer IPv6-ping entre ellos y el servidor.

Ilustración 7. Verificación de conectividad – 1

The image shows a network simulation interface. On the left, a network diagram features a central switch 'S3' connected to three routers: 'R3' (left), 'R2' (top), and 'R1' (right). Under R3, there are two laptops labeled 'Laptop30' and 'Laptop31'. Under R2, there is a laptop labeled 'Laptop21'. Under R1, there is a PC labeled 'PC30'. A server labeled 'Server0' is connected to R1. On the right, a 'Simulation Panel' window displays an 'Event List' table with the following data:

Vis.	Time(sec)	Last Device	At Device	Type	Info
👁	0.004	--	Laptop21	ICMP	🟢
👁	0.004	--	Laptop21	ICMP	🟡
👁	0.004	--	Laptop21	ICMP	🟠
👁	0.004	--	PC31	ICMP	🟤
👁	0.004	PC31	S3	ICMP	🟢
👁	0.004	S3	R3	ICMP	🔴
👁	0.004	R3	S3	ICMP	🟡
👁	0.004	S3	Laptop30	ICMP	🟢
👁	0.004	--	S3	ICMP	🟠

Below the table, the 'Simulation Panel' includes a 'Reset Simulation' button, a checked 'Constant Delay' checkbox, and a 'Captured to: 0.004 s' indicator. The 'Play Controls' section has 'Back', 'Auto Capture / Play', and 'Capture / Forward' buttons. At the bottom, there are 'Event List Filters - Visible Events' and a list of protocols including ACL Filter, ARP, BGP, Bluetooth, CAPWAP, CDP, DHCP, DHCPv6, DNS, DTP, EIGRP, EIGRPv6, FTP, H.323, HSRP, HSRPv6, HTTP, HTTPS, ICMP, ICMPv6, IPSec, ISAKMP, IoT, IoT TCP, LACP, LLDP, NDP, NETFLOW, NTP, OSPF, OSPFv6, PAgP, POP3, PTP, RADIUS, REP, RIP, RIPng, RTP, SCCP, SMTP, SNMP, SSH, STP, SYSLOG, TACACS, TCP, TFTP, Telnet, UDP, USB, VTP. There are also 'Edit Filters' and 'Show All/None' buttons.

Ilustración 8. Verificación de conectividad – 2

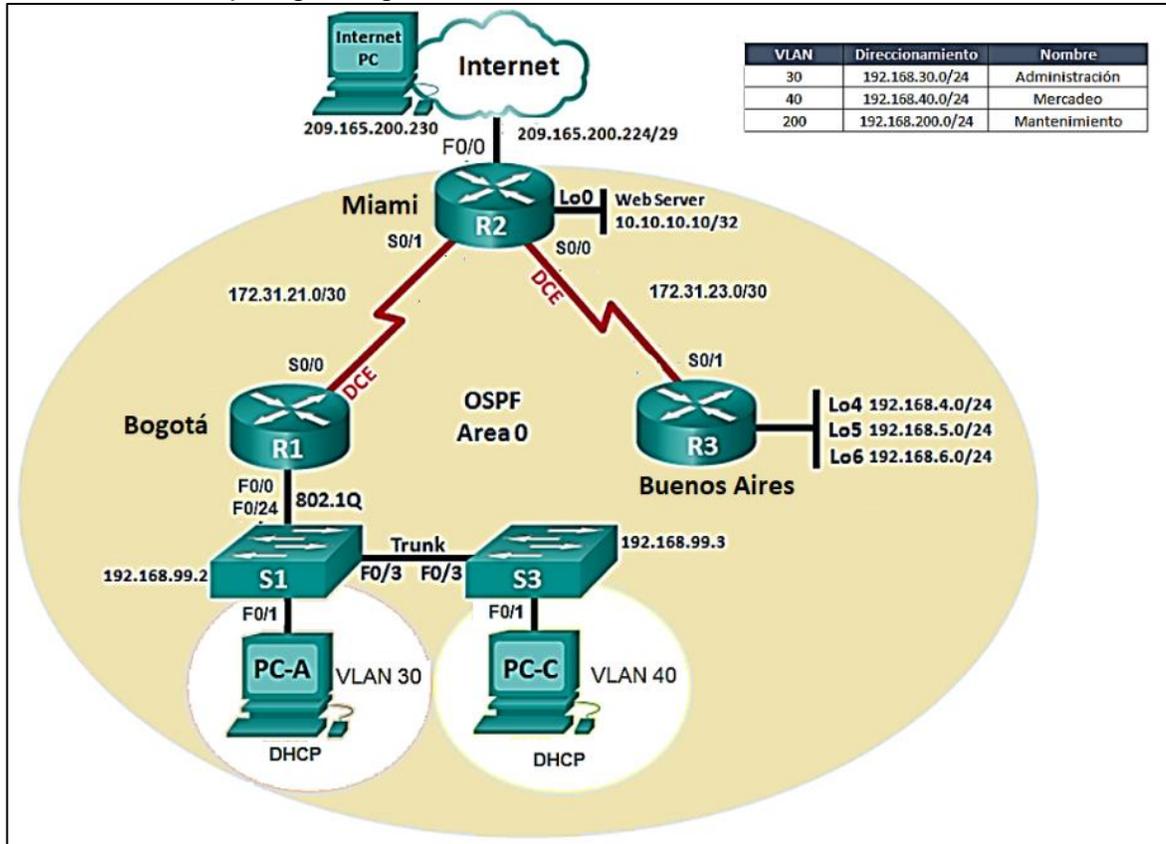
Vis.	Time(sec)	Last Device	At Device	Type	Info
	0.004	R3	S3	ICMP	
	0.004	S3	Laptop30	ICMP	
	0.004	--	S3	ICMP	
	0.005	--	PC31	ICMP	
	0.005	PC31	S3	ICMP	
	0.005	S3	R3	ICMP	
	0.005	R3	S3	ICMP	
	0.005	S3	PC31	ICMP	
	0.005	--	S3	ICMP	

Escenario 2

Descripción: 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.

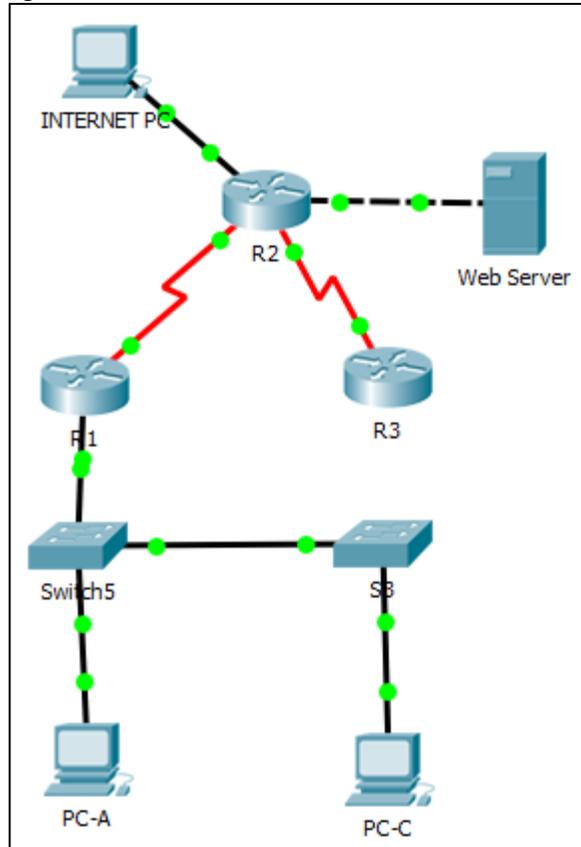
Topología original

Ilustración 9. Topología original Escenario 2



Topología diseñada

Ilustración 10. Topología diseñada del escenario 2



Desarrollo del escenario

1. Configurar el direccionamiento IP acorde con la topología de red para cada uno de los dispositivos que forman parte del escenario.

Para PC Internet

Ilustración 11. Static del PC de internet

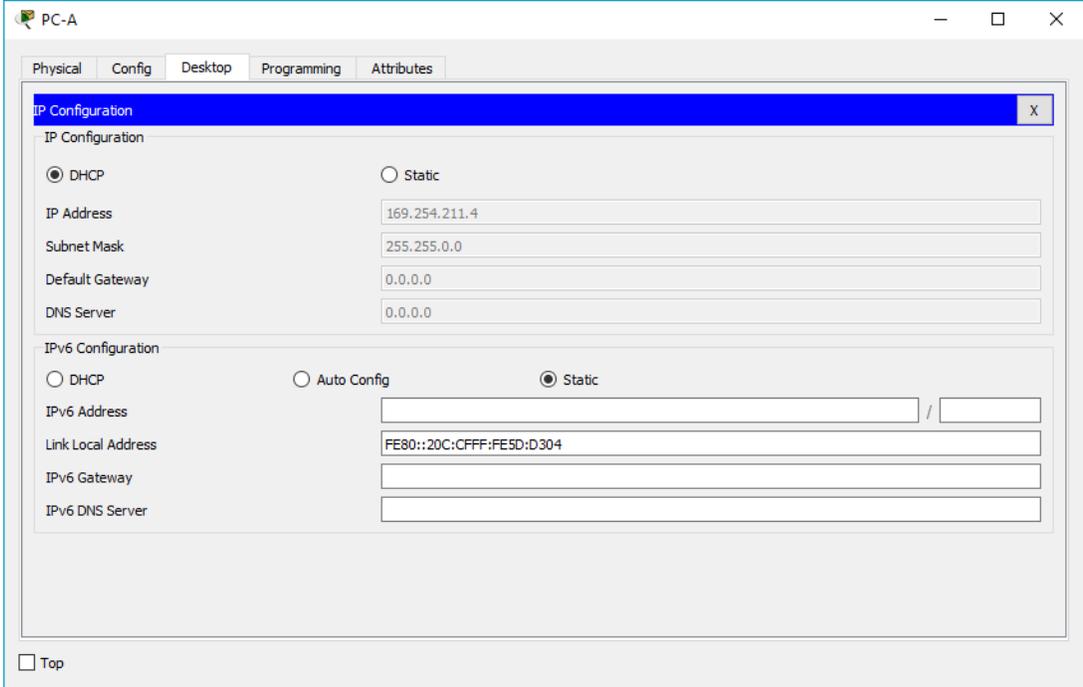
The screenshot shows a configuration window titled "INTERNET PC" with a tabbed interface. The "Config" tab is active, and the "IP Configuration" section is selected. The "Static" radio button is selected for both IPv4 and IPv6 configurations.

Field	Value
IP Address	209.165.200.230
Subnet Mask	255.255.255.248
Default Gateway	209.165.200.225
DNS Server	0.0.0.0
IPv6 Address	
Link Local Address	FE80::230:F2FF:FED4:B117
IPv6 Gateway	
IPv6 DNS Server	

At the bottom left of the window, there is a "Top" button with a checkbox.

Para PC-A

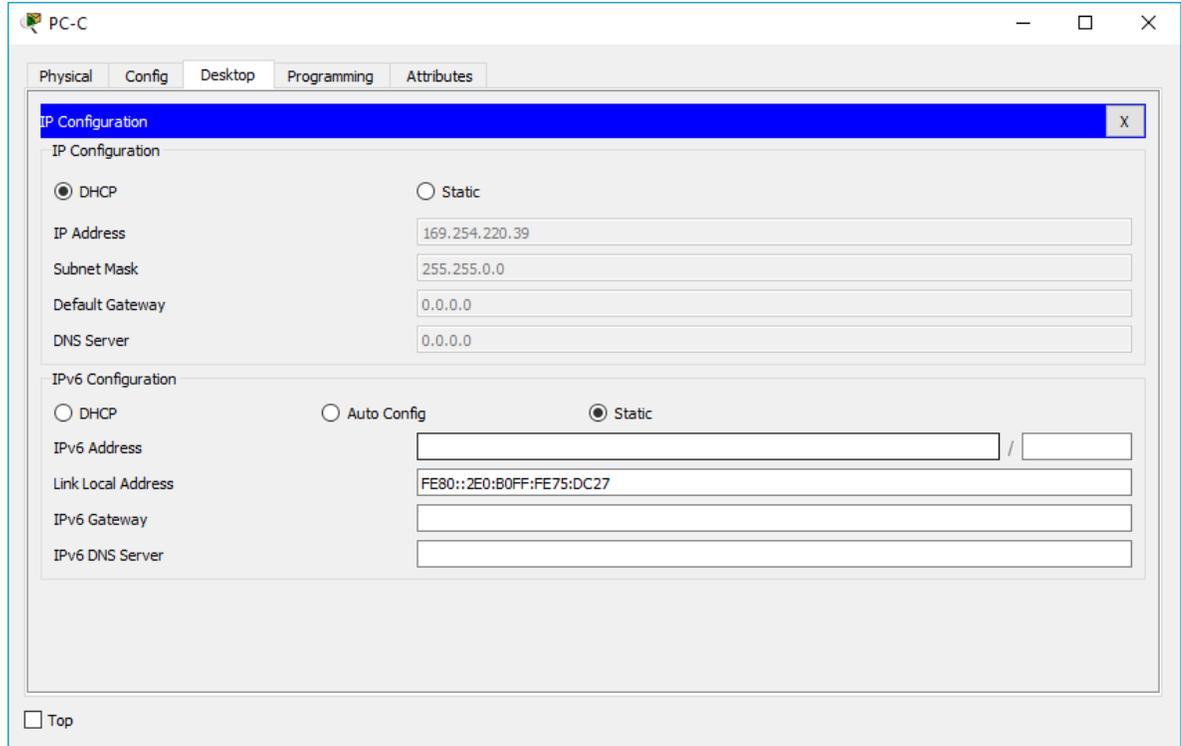
Ilustración 12. DHCP del PC-A



The screenshot shows the configuration window for PC-A, specifically the IP Configuration tab. The window has a title bar with 'PC-A' and standard window controls. Below the title bar are tabs for 'Physical', 'Config', 'Desktop', 'Programming', and 'Attributes'. The 'Config' tab is active, and the 'IP Configuration' sub-tab is selected, indicated by a blue header bar with an 'X' button. The configuration is divided into two sections: 'IP Configuration' and 'IPv6 Configuration'. In the 'IP Configuration' section, the 'DHCP' radio button is selected, and the 'Static' radio button is unselected. Below these are text input fields for 'IP Address' (169.254.211.4), 'Subnet Mask' (255.255.0.0), 'Default Gateway' (0.0.0.0), and 'DNS Server' (0.0.0.0). The 'IPv6 Configuration' section has three radio buttons: 'DHCP' (unselected), 'Auto Config' (unselected), and 'Static' (selected). Below these are text input fields for 'IPv6 Address' (empty), 'Link Local Address' (FE80::20C:CFFF:FE5D:D304), 'IPv6 Gateway' (empty), and 'IPv6 DNS Server' (empty). At the bottom left of the window is a 'Top' button with a small square icon.

Para PC-C

Ilustración 13. DHCP del PC-C



Para R1

```
enable
config t
interface serial 0/0/0
description connection to R2
ip address 172.31.21.1 255.255.255.252
no shutdown
exit
ipv6 route ::/0 s0/0/0
```

Para R2

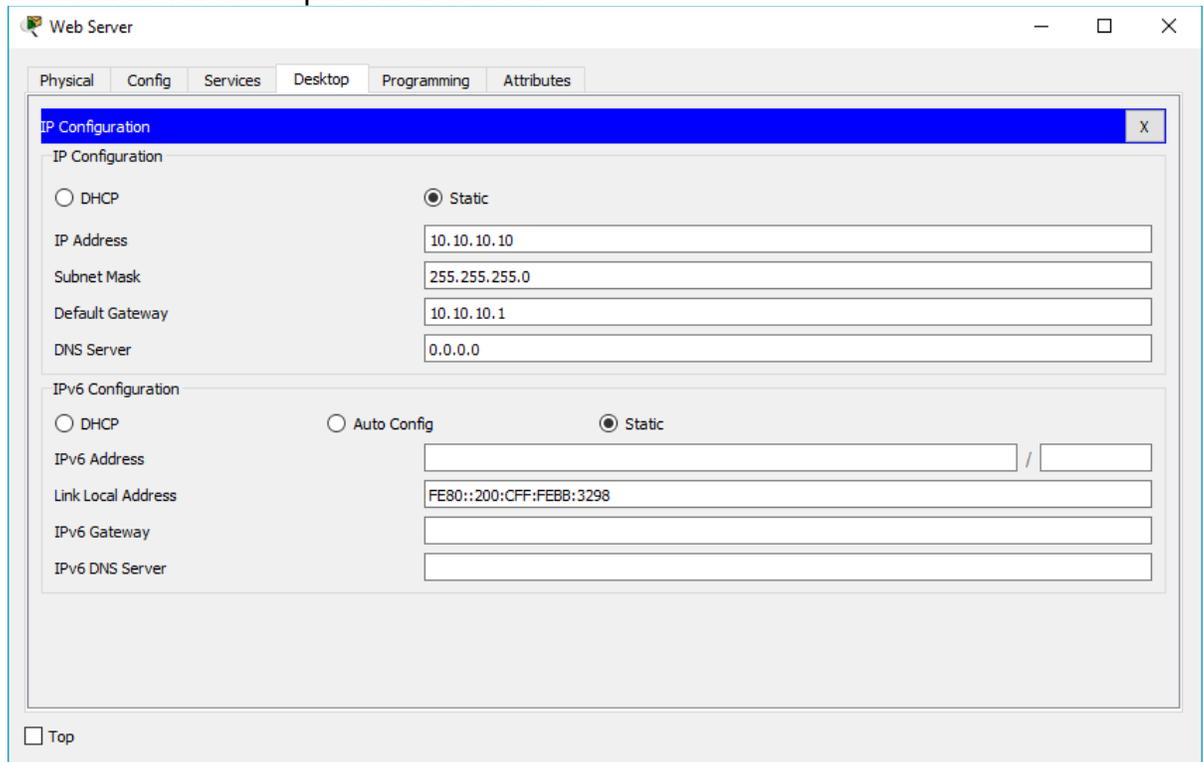
```
enable
config t
no ip domain-lookup
hostname R2
interface serial 0/0/0
ip address 172.31.21.2 255.255.255.252
no shutdown
```

```
interface serial 0/0/1
ip address 172.16.31.1 255.255.255.252
no shutdown
interface gigabitEthernet 0/1
description connection to internet
ip address 209.165.200.233 255.255.255.248
no shutdown
```

```
interface gigabitEthernet 0/0
description connection to Internet
ip address 209.165.200.225 255.255.255.248
no shutdown
ipv6 route ::/0 g0/1
```

Para Web Server

Ilustración 14. Static para Web Server



Para R3

```
enable
config t
interface serial 0/0/1
description connection to R2
ip address 172.31.23.2 255.255.255.252
no shutdown
interface loopback4
ip address 192.168.4.1 255.255.255.0
interface loopback 5
ip address 192.168.5.1 255.255.255.0
interface loopback 6
ip address 192.168.6.1 255.255.255.0
ipv6 route ::/0 s0/0/1
```

2. Configurar el protocolo de enrutamiento OSPFv2 bajo los siguientes criterios:

OSPFv2 área 0

Tabla 1. OSPFv2 área 0

Configuration Item or Task	Specification
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

Para R1

```
enable
config t
router ospf 1
router-id 1.1.1.1
network 172.31.21.0 0.0.0.3 area 0
network 192.168.30.0 0.0.0.3 area 0
network 192.168.40.0 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
auto-cost reference-bandwidth 9500
```

```
exit
```

```
int s0/0/0  
bandwidth 256  
ip ospf cost 9500  
exit
```

Para R2

```
enable  
config t  
router ospf 1  
router-id 5.5.5.5  
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  
passive-interface g0/1  
auto-cost reference-bandwidth 9500
```

```
int s0/0/0  
bandwidth 256
```

```
int s0/0/1  
bandwidth 256  
ip ospf cost 9500  
exit
```

Para R3

```
enable  
config t  
router ospf 1  
router-id 8.8.8.8  
network 172.16.31.23 0.0.0.3 area 0  
network 192.168.4.0 0.0.3.255 area 0
```

```
passive-interface loopback 4  
passive-interface loopback 5  
passive-interface loopback 6  
auto-cost reference-bandwidth 9500
```

```
int s0/0/1  
bandwidth 256  
ip ospf cost 9500  
exit
```

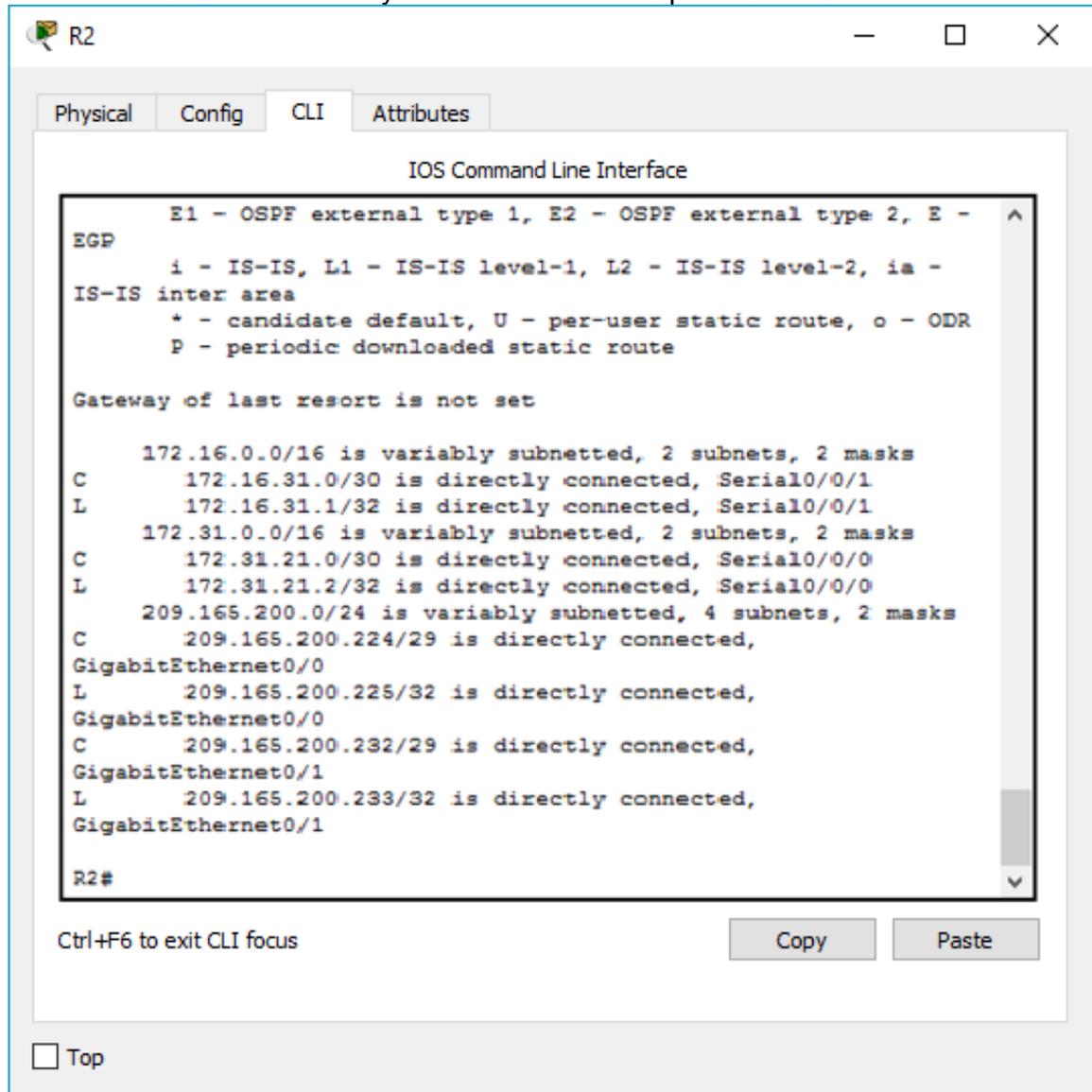
Verificar información de OSPF

- Visualizar tablas de enrutamiento y routers conectados por OSPFv2

Para R2

show ip route

Ilustración 15. Enrutamiento y routers conectados por OSPFv2



The screenshot shows a network device CLI window titled "R2" with tabs for "Physical", "Config", "CLI", and "Attributes". The "CLI" tab is active, displaying the output of the "show ip route" command. The output is as follows:

```
IOS Command Line Interface

      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

      172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
C       172.16.31.0/30 is directly connected, Serial0/0/1
L       172.16.31.1/32 is directly connected, Serial0/0/1
      172.31.0.0/16 is variably subnetted, 2 subnets, 2 masks
C       172.31.21.0/30 is directly connected, Serial0/0/0
L       172.31.21.2/32 is directly connected, Serial0/0/0
      209.165.200.0/24 is variably subnetted, 4 subnets, 2 masks
C       209.165.200.224/29 is directly connected,
GigabitEthernet0/0
L       209.165.200.225/32 is directly connected,
GigabitEthernet0/0
C       209.165.200.232/29 is directly connected,
GigabitEthernet0/1
L       209.165.200.233/32 is directly connected,
GigabitEthernet0/1

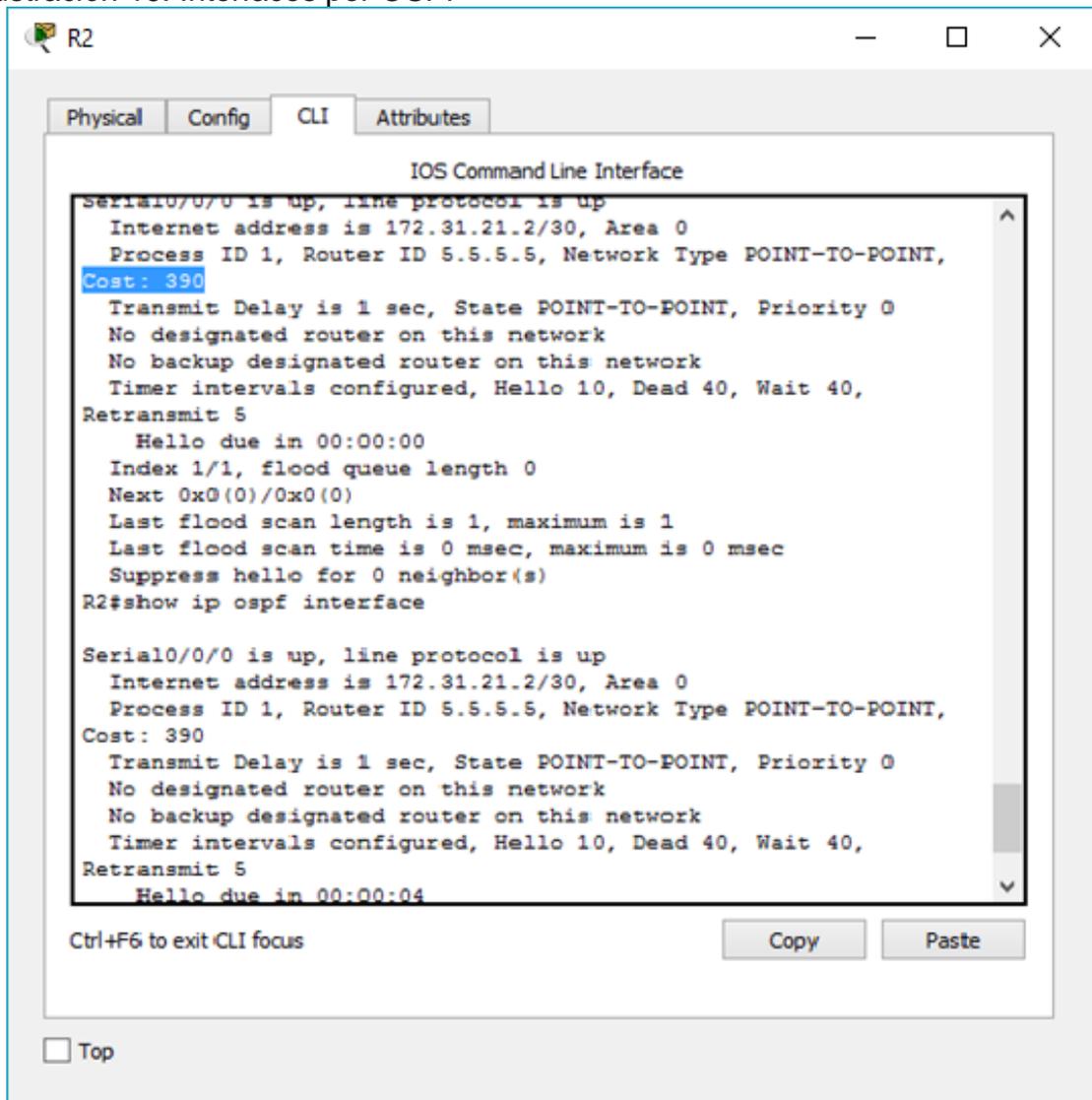
R2#
```

Below the CLI window, there is a "Ctrl+F6 to exit CLI focus" label and "Copy" and "Paste" buttons. At the bottom left, there is a "Top" button.

- Visualizar lista resumida de interfaces por OSPF en donde se ilustre el costo de cada interface.

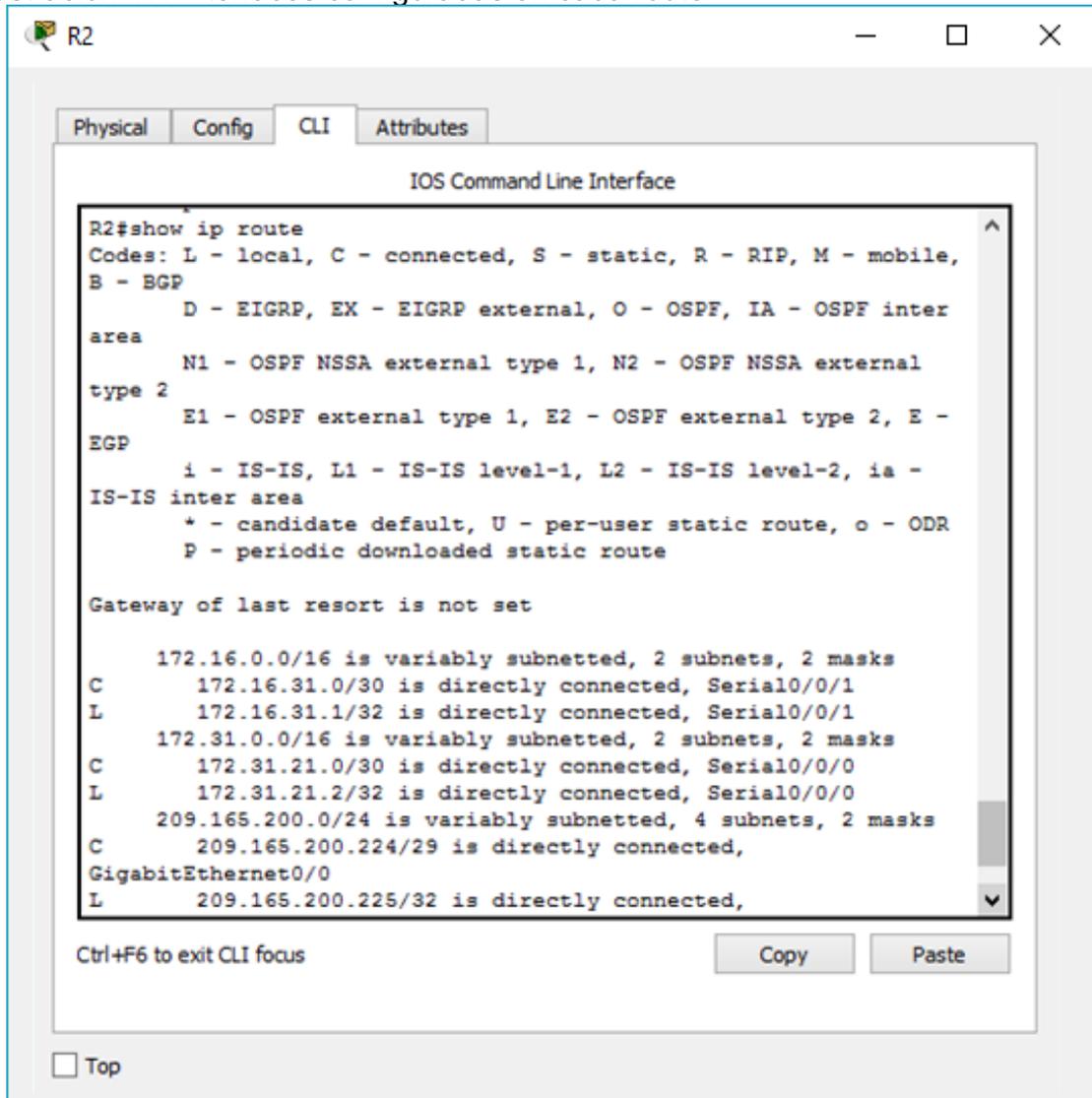
Para R2
show ip ospf interface

Ilustración 16. Interfaces por OSPF



- Visualizar el OSPF Process ID, Router ID, Address summarizations, Routing Networks, and passive interfaces configuradas en cada router.

Ilustración 17. Interfaces configuradas en cada router



3. Configurar VLANs, Puertos troncales, puertos de acceso, encapsulamiento, Inter-VLAN Routing y Seguridad en los Switches acorde a la topología de red establecida.

Para S1

enable
config t

```
vlan 30
name Administracion
vlan 40
name Mercadeo
vlan 200
name Mantenimiento
exit
int vlan 200
```

```
interface vlan 200
ip address 192.168.99.2 255.255.255.0
no shutdown
exit
ip default-gateway 192.168.99.1
interface f0/3
switchport mode trunk
```

```
switchport trunk native vlan 1
interface f0/24
switchport mode trunk
switchport trunk native vlan 1
```

```
interface range f0/2, f0/4-23, g0/1-2
switch mode access
interface f0/1
switch mode access
switch access vlan 30
interface range f0/2, f0/4-23, g0/1-2
shutdown
```

Para S3

```
vlan 30
name Administracion
vlan 40
name Mercadeo
vlan 200
name Mantenimiento
exit
int vlan 200
```

```
ip address 192.168.99.3 255.255.255.0
no shutdown
exit
ip default-gateway 192.168.99.1
exit
```

Para R1

```
Enable
Config t
int g0/1.30
encapsulation dot1Q 30
ip address 192.168.30.1 255.255.255.0
int g0/1.40
ip address 192.168.40.1 255.255.255.0
int g0/1.30
encapsulation dot1Q 30
ip address 192.168.30.1 255.255.255.0
int g0/1.40
ip address 192.168.40.1 255.255.255.0
```

4. En el Switch 3 deshabilitar DNS lookup

```
enable
config t
no ip domain-lookup
```

5. Asignar direcciones IP a los Switches acorde a los lineamientos.

Para S1

```
enable
config t
interface vlan 99
ip address 192.168.99.2 255.255.255.0
no shutdown
exit
```

Para S3

```
enable
config t
interface vlan 99
ip address 192.168.99.3 255.255.255.0
exit
ip default-gateway 192.168.99.1
```

6. Desactivar todas las interfaces que no sean utilizadas en el esquema de red.

Para S1

```
enable
config t
interface range f0/2, f0/4-23, g0/1-2
```

shutdown

Para S3

```
enable
config t
interface range f0/2, f0/4-23, g0/1-2
shutdown
```

7. Implement DHCP and NAT for IPv4

Para R3

```
enable
config t
interface loopback 4
ip address 192.168.4.1 255.255.255.0
no shutdown
exit
```

```
interface loopback 5
ip address 192.168.5.1 255.255.255.0
no shutdown
exit
```

```
interface loopback 6
ip address 192.168.6.1 255.255.255.0
no shutdown
exit
```

8. Configurar R1 como servidor DHCP para las VLANs 30 y 40.

```
enable
config t
ip dhcp excluded-address 172.16.30.0
ip dhcp pool
```

9. Reservar las primeras 30 direcciones IP de las VLAN 30 y 40 para configuraciones estáticas.

Tabla 2. Reservas de direcciones IP

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.
-----------------------------------	--

Para R1

```
enable
config t
ip dhcp excluded-address 192.168.30.1 192.168.30.30
ip dhcp excluded-address 192.168.40.1 192.168.40.30
```

```
ip dhcp pool ADMINISTRACION
dns-server 10.10.10.11
default-router 192.168.30.1
network 192.168.30.1 255.255.255.0
```

```
ip dhcp pool MERCADEO
dns-server 10.10.10.11
default-router 192.168.40.1
network 192.168.30.1 255.255.255.0
```

10. Configurar NAT en R2 para permitir que los hosts puedan salir a internet

```
config t
ip http server (no es soportado este comando)
ip nat inside source static 10.10.10.10 209.165.200.229
interface g0/0
ip nat outside
interface g0/1
ip nat inside
```

11. Configurar al menos dos listas de acceso de tipo estándar a su criterio en para restringir o permitir tráfico desde R1 o R3 hacia R2.

```
enable
config t
access-list 1 permit 169.254.211.2 255.255.0.0
interface serial 0/0/0

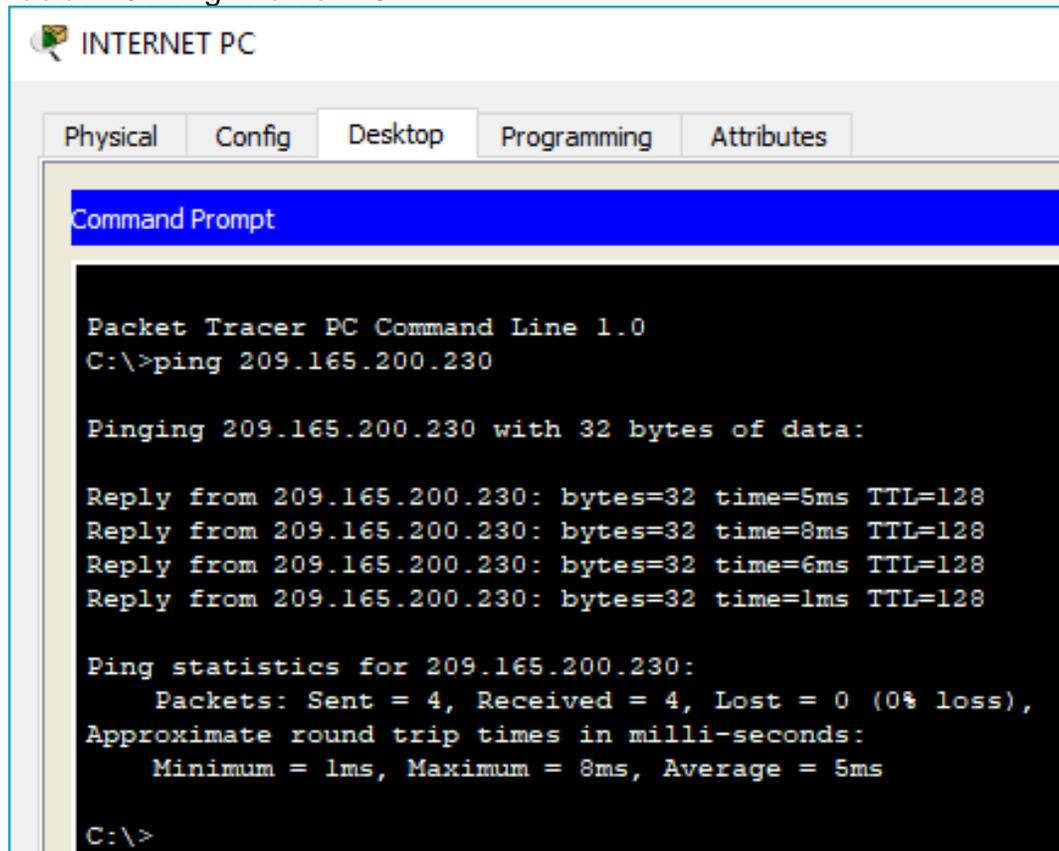
access-list 1 permit 169.254.220.39 255.255.0.0
interface serial 0/0/0
```

12. Configurar al menos dos listas de acceso de tipo extendido o nombradas a su criterio en para restringir o permitir tráfico desde R1 o R3 hacia R2.

```
enable
config t
access-list 101 permit icmp any any echo-reply
interface g0/0
ip access-group 101 in
ip access-group 101 out
```

13. Verificar procesos de comunicación y redireccionamiento de tráfico en los routers mediante el uso de Ping y Traceroute.

Ilustración 18. Ping Internet PC



The screenshot shows a window titled "INTERNET PC" with tabs for Physical, Config, Desktop, Programming, and Attributes. The "Desktop" tab is active, displaying a "Command Prompt" window. The command prompt shows the execution of a ping command to the IP address 209.165.200.230. The output indicates that all four packets were received successfully with a 0% loss rate. The round trip times are: Minimum = 1ms, Maximum = 8ms, and Average = 5ms.

```
Packet Tracer PC Command Line 1.0
C:\>ping 209.165.200.230

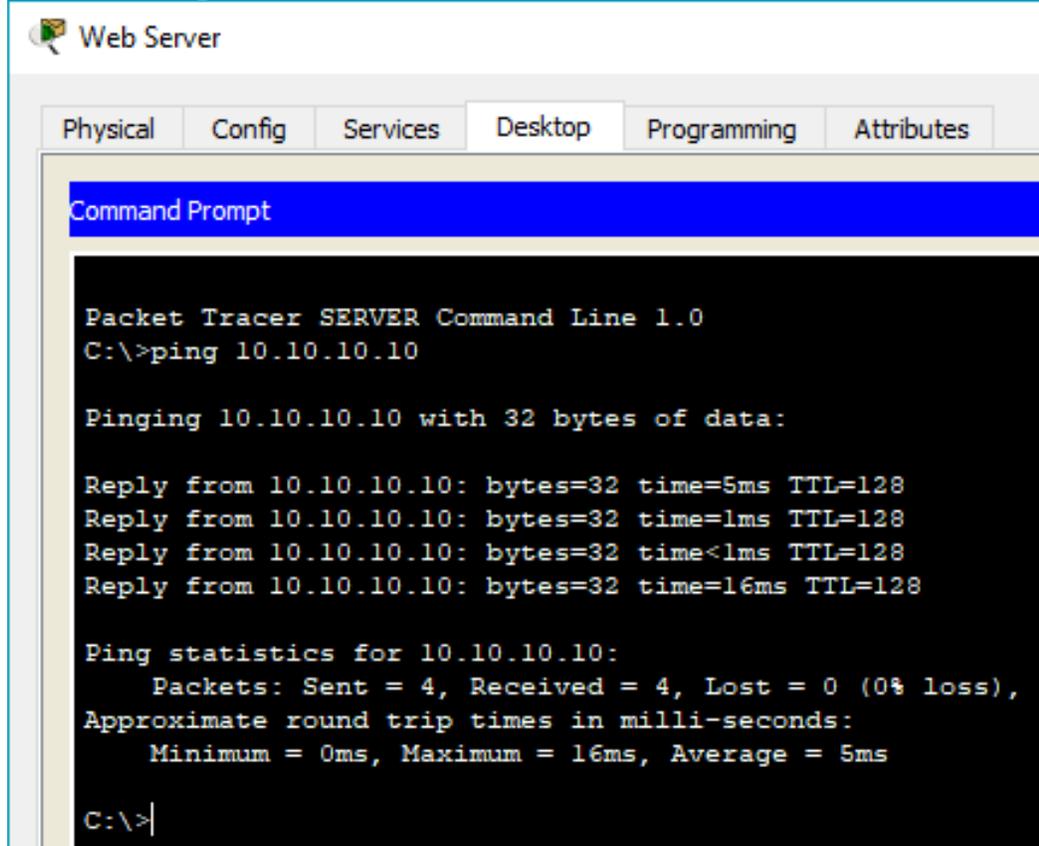
Pinging 209.165.200.230 with 32 bytes of data:

Reply from 209.165.200.230: bytes=32 time=5ms TTL=128
Reply from 209.165.200.230: bytes=32 time=8ms TTL=128
Reply from 209.165.200.230: bytes=32 time=6ms TTL=128
Reply from 209.165.200.230: bytes=32 time=1ms TTL=128

Ping statistics for 209.165.200.230:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 8ms, Average = 5ms

C:\>
```

Ilustración 19. Ping Web Server



The screenshot shows a window titled "Web Server" with a "Desktop" tab selected. Inside the desktop is a "Command Prompt" window. The text in the Command Prompt is as follows:

```
Packet Tracer SERVER Command Line 1.0
C:\>ping 10.10.10.10

Pinging 10.10.10.10 with 32 bytes of data:

Reply from 10.10.10.10: bytes=32 time=5ms TTL=128
Reply from 10.10.10.10: bytes=32 time=1ms TTL=128
Reply from 10.10.10.10: bytes=32 time<1ms TTL=128
Reply from 10.10.10.10: bytes=32 time=16ms TTL=128

Ping statistics for 10.10.10.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 16ms, Average = 5ms

C:\>
```

Conclusiones

- Se realiza la configuración correspondiente para el escenario 1 y cada uno de sus dispositivos, donde se logra diseñar una topología estable ya que se hizo uso de la tabla de direccionamiento entregada en la respectiva guía.
- Dentro del escenario 1 se realiza la configuración de la topología de manera exitosa basados en las VLAN y puertos asociados en la tabla.
- Para el escenario 1 se logra implementar el enmascaramiento mejor conocido como NAT de los dispositivos correspondientes.
- En el escenario 1 se realiza las diferentes configuraciones de routing y Vlan, las cuales incluyen direccionamiento IP entre troncales y subinterfaces.
- Dentro de los diferentes escenarios se comprende de una manera más clara cual es la funcionalidad concreta del protocolo DHCP, donde se evidencia que su prioridad operativa es el ahorro de tiempo de la gestión correspondiente entre las IP de la topología diseñada.
- Dentro del escenario 2 se realiza la habilitación del protocolo DHCP sobre un servidor que cuenta con una administración centralizada de cada una de las diferentes direcciones IP que se encuentran dentro de la topología establecida.

Glosario

LAN: Una LAN abarca computadoras y periféricos conectados a un servidor dentro de un área geográfica distinta, como una oficina o un establecimiento comercial. Las computadoras y otros dispositivos móviles utilizan una conexión LAN para compartir recursos como una impresora o un almacenamiento en red.

Wan: Es una red de computadoras que une varias redes locales, aunque sus miembros no estén todos en una misma ubicación física

NAT: Traducción de direcciones de red, también llamado enmascaramiento de IP o NAT, es un mecanismo utilizado por routers IP para intercambiar paquetes entre dos redes que asignan mutuamente direcciones incompatibles. Consiste en convertir, en tiempo real, las direcciones utilizadas en los paquetes transportados.

DHCP: Es un protocolo de red de tipo cliente/servidor mediante el cual un servidor DHCP asigna dinámicamente una dirección IP y otros parámetros de configuración de red a cada dispositivo.

RIPV: Es un protocolo de puerta de enlace interna o interior (Interior Gateway Protocol, IGP) utilizado por los routers o encaminadores para intercambiar información acerca de redes del Internet Protocol (IP) a las que se encuentran conectados.

Topología: En un anillo con un concentrador (unidad de acceso a múltiples estaciones, MAU) podemos decir que tenemos una topología en anillo, o de que se trata de un anillo con topología en estrella. La topología de red la determina únicamente la configuración de las conexiones entre nodos.

Ping: Es un comando o una herramienta de diagnóstico que permite hacer una verificación del estado de una determinada conexión de un host local con al menos un equipo remoto contemplado en una red de tipo TCP/IP. Sirve para determinar si una dirección IP específica o host es accesible desde la red o no

.IP: Es un número que identifica, de manera lógica y jerárquica, a una Interfaz en red (elemento de comunicación/conexión) de un dispositivo (computadora, tableta, portátil, smartphone) que utilice el protocolo IP o (Internet Protocol), que corresponde al nivel de red del modelo TCP/IP.

Dominio: en redes de computadoras, puede referirse a tres cosas: El conjunto de computadoras conectadas en una red informática que confían a uno de los equipos de dicha red, la administración de los usuarios y los privilegios que cada uno de los usuarios tiene en dicha red.

Enrutamiento: es el proceso de reenviar paquetes entre redes, siempre buscando la mejor ruta (la más corta). Para encontrar esa ruta óptima, se debe tener en cuenta la tabla de enrutamiento y algunos otros parámetros como la métrica, la distancia administrativa, el ancho de banda.

Referencias bibliográficas

- CISCO. (2014). VLANs. Principios de Enrutamiento y Conmutación. Recuperado de <https://static-course-assets.s3.amazonaws.com/RSE50ES/module3/index.html#3.0.1.1>
- CISCO. (2014). Enrutamiento entre VLANs. Principios de Enrutamiento y Conmutación. Recuperado de <https://static-course-assets.s3.amazonaws.com/RSE50ES/module5/index.html#5.0.1.1>
- UNAD (2014). Configuración de Switches y Routers [OVA]. Recuperado de <https://1drv.ms/u/s!AmIJYei-NT1lhgL9QChD1m9EuGqC>
- Odom, W. (2013). CISCO Press (Ed). CCNA ICND1 Official Exam Certification Guide. Recuperado de <http://ptgmedia.pearsoncmg.com/images/9781587205804/samplepages/9781587205804.pdf>
- Lammle, T. (2010). CISCO Press (Ed). Cisco Certified Network Associate Study Guide. Recuperado de <https://1drv.ms/b/s!AmIJYei-NT1lm3GQVfFFrjnEGFFU>
- CISCO. (2014). Asignación de direcciones IP. Fundamentos de Networking. Recuperado de <https://static-course-assets.s3.amazonaws.com/ITN50ES/module8/index.html#8.0.1.1>
- CISCO. (2014). OSPF de una sola área. Principios de Enrutamiento y Conmutación. Recuperado de <https://static-course-assets.s3.amazonaws.com/RSE50ES/module8/index.html#8.0.1.1>
- CISCO. (2014). DHCP. Principios de Enrutamiento y Conmutación. Recuperado de <https://static-course-assets.s3.amazonaws.com/RSE50ES/module10/index.html#10.0.1.1>