



Solución de Estudio de Caso Bajo el Uso de Tecnología CISCO

Presentado por

Marelis Carmona Burgos

Código: 33102531

Grupo: 203092_28

Universidad Nacional Abierta Y A Distancia UNAD

Ingeniería de Telecomunicaciones

Cartagena - Bolívar

Diciembre de 2018



Solución de Estudio de Caso Bajo el Uso de Tecnología CISCO

Presentado por

Marelis Carmona Burgos

Código: 33102531

Grupo: 203092_28

Presentado a

Diego Édison Ramírez

Universidad Nacional Abierta Y A Distancia UNAD

Ingeniería de Telecomunicaciones

Cartagena - Bolívar

Diciembre de 2018

AGRADECIMIENTOS

Primeramente, doy gracias a Dios, por todas sus bendiciones, por guiarme durante todo este tiempo, y permitirme haber llegado hasta este momento tan importante de mi formación profesional.

Igualmente quiero agradecer al director y tutor del diplomado de profundización Cisco (diseño e implementación de soluciones integradas LAN/WAN), quienes compartieron sus conocimientos, me asesoraron y acompañaron durante el desarrollo de este logrando el crecimiento como persona, estudiante y en un futuro como profesional en Ingeniería de Telecomunicaciones.

Finalmente, expreso mis agradecimientos a la Universidad Nacional Abierta y a Distancia (UNAD), en especial al CCAV Cartagena y a todas las personas que con la enseñanza de sus valiosos conocimientos han aportado de una u otra forma en la consecución de este logro, que me permitirá crecer día a día como profesional.

RESUMEN

A través de este trabajo se ponen en práctica los conocimientos y competencias adquiridas durante el desarrollo del diplomado de profundización CISCO (diseño e implementación de soluciones integradas LAN/WAN).

Curso en el que se estudió introducción a las redes y principios básicos de routing y switching como parte del programa de Cisco Networking, conceptos que sirven de guía para resolver los posibles problemas que se puedan presentar en la cotidianidad profesional.

Entre los conceptos desarrollados durante el curso que han sido puestos en práctica en el desarrollo de este trabajo se puede mencionar la creación de redes Ethernet simple mediante routers y switches. El uso de comandos de la interfaz de línea de comandos (CLI) de Cisco para realizar configuraciones básicas de routers y switches.

Configurar las operaciones básicas en una red de routing y switching pequeña y resolver los problemas relacionados.

Configuración y la resolución de problemas de VLAN y del routing entre VLAN, configuración dinámica de host (DHCP) y del sistema de nombres de dominio (DNS) para IPv4 e IPv6.

TABLA DE CONTENIDO

INTRODUCCION.....	10
1. OBJETIVOS.....	11
1.1 OBJETIVO GENERAL.....	11
1.2 OBJETIVOS ESPECÍFICOS	11
Descripción de escenarios propuestos para la prueba de habilidades	12
2. Escenario 1	12
2.2 Configurar los parámetros de los dispositivos	12
2.3 Los puertos de red que no se utilizan se deben deshabilitar.	15
2.4 La información de dirección IP R1, R2 y R3 debe cumplir con la tabla 1.....	17
2.5 Laptop20, Laptop21, PC20, PC21, Laptop30, Laptop31, PC30 y PC31 deben obtener información IPv4 del servidor DHCP.....	17
2.6 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.	18
2.7 R1 debe tener una ruta estática predeterminada al ISP que se configuró y que incluye esa ruta en el dominio RIPv2.....	19
2.8 R2 es un servidor de DHCP para los dispositivos conectados al puerto FastEthernet0/0.....	20
2.9 R2 debe, además de enrutamiento a otras partes de la red, ruta entre las VLAN 100 y 200.....	20
2.10 El Servidor0 es sólo un servidor IPv6 y solo debe ser accesibles para los dispositivos en R3 (ping).....	21
2.11 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.....	21
2.12 La interfaz FastEthernet 0/0 del R3 también deben tener direcciones IPv4 e IPv6 configuradas (dual- stack).	22

2.13 R1, R2 y R3 deben saber sobre las rutas de cada uno y la ruta predeterminada desde R1.	22
2.14 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.....	23
3. Escenario 2.....	25
3.1 Configuración básica de dispositivos	27
3.2 Configurar el direccionamiento IP acorde con la topología de red para cada uno de los dispositivos que forman parte del escenario.	27
3.2. Configurar el protocolo de enrutamiento OSPFv2 bajo los siguientes criterios:	29
3.3 Configurar VLANs, Puertos troncales, puertos de acceso, encapsulamiento, Inter-VLAN Routing y Seguridad en los Switches acorde a la topología de red establecida. .	31
3.4 Asignar direcciones IP a los Switches acorde a los lineamientos	34
3.5 Desactivar todas las interfaces que no sean utilizadas en el esquema de red.	35
3.6 Implement DHCP and NAT for IPv4	35
3.7 Configurar R1 como servidor DHCP para las VLANs 30 y 40	36
3.8 Reservar las primeras 30 direcciones IP de las VLAN 30 y 40 para configuraciones estáticas.....	36
3.10 Configurar al menos dos listas de acceso de tipo estándar a su criterio para restringir o permitir tráfico desde R1 o R3 hacia R2.....	38
3.11 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.....	38
3.12 Verificar procesos de comunicación y redireccionamiento de tráfico en los routers mediante el uso de Ping y Traceroute.	39
4. CONCLUSIONES	40
5. REFERENCIAS BIBLIOGRAFICAS	41
.....	41

LISTA DE IMÁGENES

IMAGEN 1 Topología de la red	12
IMAGEN 2 Asignación de puertos VLAN	14
IMAGEN 3 Verificación show vlan	14
IMAGEN 4 Verificación de interfaces asignadas.....	15
IMAGEN 5 Puertos sin usar deshabilitados	16
IMAGEN 6 Interfaz en S2	16
IMAGEN 7 Configuración de direcciones IP	17
IMAGEN 8 Configuración DHCP IPv4	17
IMAGEN 9 NAT con sobrecarga en IPv4.....	18
IMAGEN 10 Ruta estática y dominio RIPv2.....	19
IMAGEN 11 DHCP Server	20
IMAGEN 12 Enrutamiento entre vlan 100 y 200	20
IMAGEN 13 Prueba de conectividad	21
IMAGEN 14 DHCPv6.....	21
IMAGEN 15 IPv4 e IPv6 dual-stack	22
IMAGEN 16 Adicionar Rip	23
IMAGEN 17 Verificación conectividad desde PC-PT30.....	23
IMAGEN 18 Verificación conectividad desde Laptop-31.....	24
IMAGEN 19 Verificación conectividad desde PC-PT31	24
IMAGEN 20 Topología Escenario 2	25
IMAGEN 21 Tarjeta serial	26
IMAGEN 22 Internet-PC	27
IMAGEN 23 Configuración dirección IP	28
IMAGEN 24 Configuración direccionamiento Web Server	29

IMAGEN 25 Verificación OPSF vecinos en R3.....	30
IMAGEN 26 Verificación de Protocolos en R2.....	30
IMAGEN 27 Verificación de rutas OPSF en R1	31
IMAGEN 28 Configuración VLANs en S3	32
IMAGEN 29 Configuración de seguridad	33
IMAGEN 30 Verificación de conectividad	34
IMAGEN 31 Asignación de IP en S1.....	34
IMAGEN 32 Desactivación de puertos.....	35
IMAGEN 33 Reserva primeras 30 direcciones.....	37
IMAGEN 34 NAT en R2	37
IMAGEN 35 Listas de acceso	38
IMAGEN 36 Ping desde R1	39
IMAGEN 37 Verificación Listas de acceso.....	39

LISTA DE TABLAS

TABLA 1 Tabla de direccionamiento.....	13
TABLA 2 Protocolo OSPFv2.....	29
TABLA 3 Tabla de Direccionamiento VLANs.....	31
TABLA 4 Configuración de DHCP pool para VLAN	36

INTRODUCCION

La prueba de habilidades prácticas, es la actividad evaluativa final del diplomado de profundización CCNA, la cual busca identificar las competencias y habilidades adquiridas durante el desarrollo del diplomado usando la herramienta de simulación Cisco Packet Tracer en cada una de las actividades propuestas. Logrando con esto poner a prueba la comprensión de lo estudiado además de dar solución a problemas relacionados con diversos aspectos de Networking. Finalmente se dará solución a dos ejercicios propuestos a través de los cuales se pondrá en práctica algunos conceptos de networking tales como: inicialización de dispositivos de red, configuración básica de Routers, Servidores, Switches; seguridad en dispositivos de comunicación, aplicación de routing, Vlans, configuración OSPF, implementación DHCP, NAT, configuración y verificación de ACL.

1. OBJETIVOS

1.1 OBJETIVO GENERAL

Poner en práctica los conceptos estudiados durante el diplomado para identificar su comprensión y habilidades para solucionar problemas relacionados con diversos aspectos de Networking.

1.2 OBJETIVOS ESPECÍFICOS

Para lograr el objetivo general se han planteado los siguientes objetivos específicos:

- ✓ Armar una red y configurar los parámetros básicos de los dispositivos.
- ✓ 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.
- ✓ Verificar la conectividad de los dispositivos mediante el uso de comandos: ping, traceroute, y show ip route.

Descripción de escenarios propuestos para la prueba de habilidades

2. Escenario 1

2.1 Armar la red y realizar el cableado

Recursos necesarios

- 4 Routers (Cisco 1841) con 2 puertos FastEthernet, 2 puertos Seriales
- 2 Switches (Cisco 2960)
- 1 Servidor (Genérico PT)
- 4 PCs con sistema operativo Windows 7, con tarjeta de red
- 4 Laptops
- Cables Serial y Ethernet

Topología

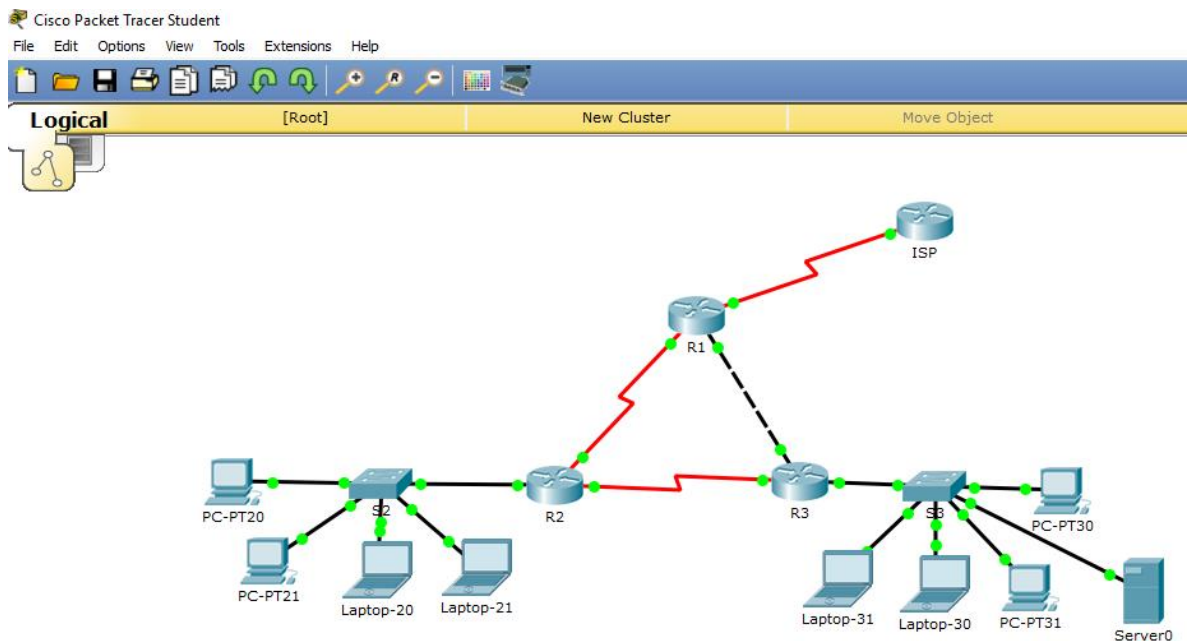


Imagen 1. Topología de la red

2.2 Configurar los parámetros de los dispositivos

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

El administrador	Interfaces	Dirección IP	Máscara de subred	Gateway predeterminado
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:db8:130::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 1. De Direccionamiento

```

S2
Physical Config CLI
IOS Command Line Interface

Press RETURN to get started.

S2>enable
S2#config t
Enter configuration commands, one per line. End with CNTL/Z.
S2 (config)#vlan 100
S2 (config-vlan)#name LAPTOPS
S2 (config-vlan)#exit
S2 (config)#vlan 200
S2 (config-vlan)#name DESTOPS
S2 (config-vlan)#exit
S2 (config)#end
S2#
%SYS-5-CONFIG_I: Configured from console by console
  
```

Copy Paste

Imagen 2. Asignación de puertos VLAN

Verificar con show vlan para saber si están creadas las vlans.

```

S2
Physical Config CLI
IOS Command Line Interface

S2#show vlan

VLAN Name                Status    Ports
-----
1    default                active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                           Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                           Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                           Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                           Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                           Fa0/21, Fa0/22, Fa0/23, Fa0/24
100  LAPTOPS                active
200  DESTOPS                active
1002 fddi-default         act/unsup
1003 token-ring-default  act/unsup
1004 fddinet-default     act/unsup
1005 trnet-default       act/unsup

VLAN Type  SAID      MTU    Parent RingNo BridgeNo  Stp    BrdgMode Trans1 Trans2
-----
1    enet  100001   1500   -    -    -    -    -    0    0
100  enet  100100   1500   -    -    -    -    -    0    0
200  enet  100200   1500   -    -    -    -    -    0    0
1002 fddi  101002   1500   -    -    -    -    -    0    0
1003 tr   101003   1500   -    -    -    -    -    0    0
1004 fdnet 101004   1500   -    -    -    ieee -    0    0
1005 trnet 101005   1500   -    -    -    ibm  -    0    0

Remote SPAN VLANs
-----
  
```

Copy Paste

Imagen 3. Verificación show vlan

Guardamos los cambios con wr

Asignamos las interfaces

Verificamos que estén asignadas las interfaces

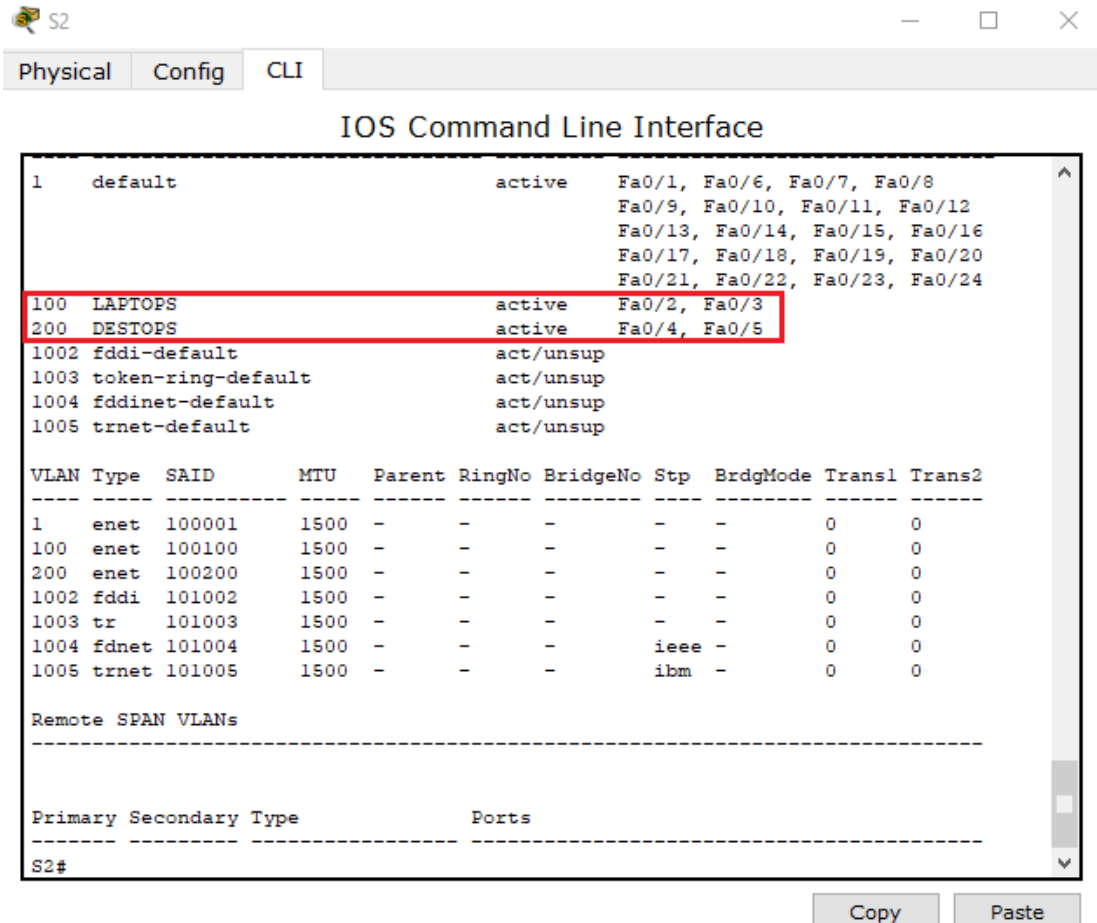


Imagen 4. Verificación de interfaces asignadas

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

Se deshabilitan los puertos en S2 y S3

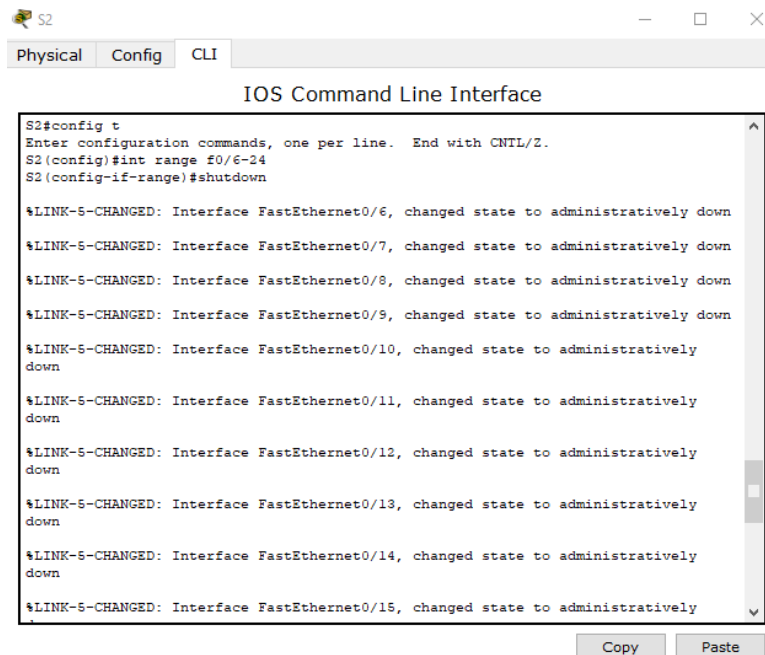


Imagen 5. Puertos sin usar deshabilitados

Se determina la interfaz troncal en el S2 y S3 utilizando el comando switchport mode trunk.

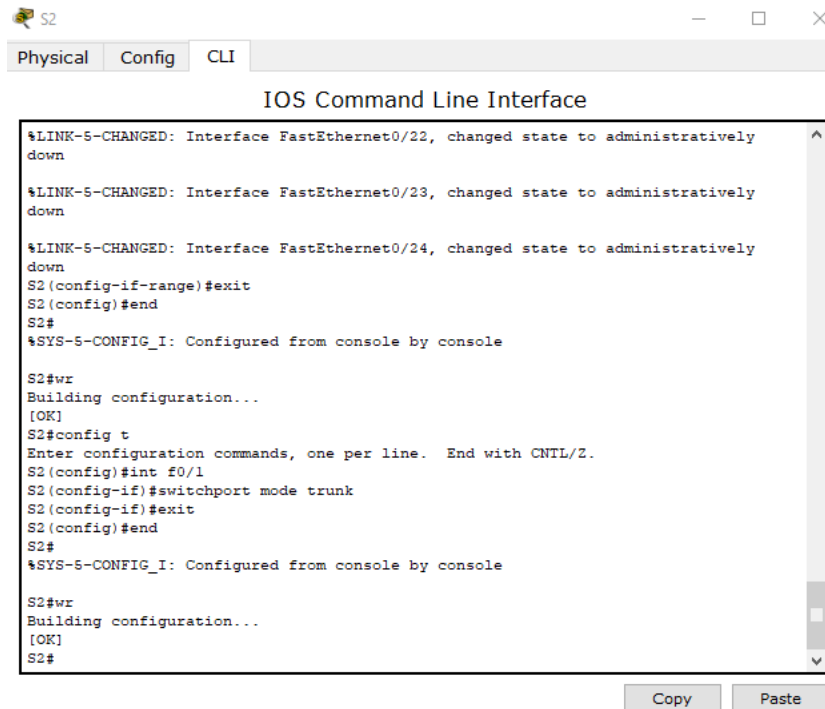
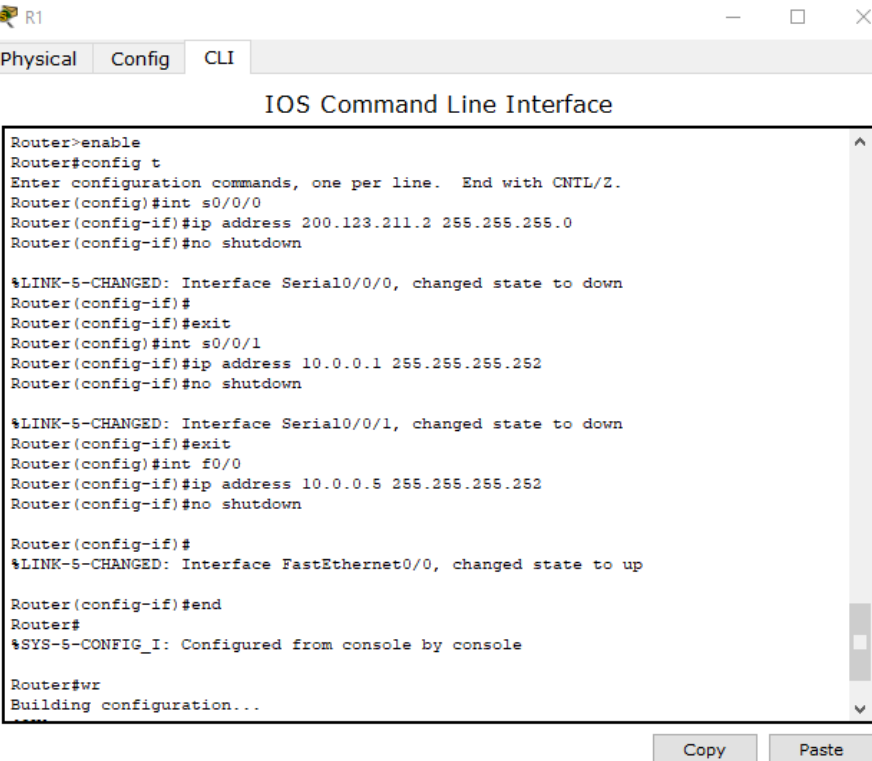


Imagen 6. Interfaz en S2

2.4 La información de dirección IP R1, R2 y R3 debe cumplir con la tabla 1. Se debe configurar las interfaces de los routers a través del comando ip address



```
Router>enable
Router#config t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#int s0/0/0
Router(config-if)#ip address 200.123.211.2 255.255.255.0
Router(config-if)#no shutdown

%LINK-5-CHANGED: Interface Serial0/0/0, changed state to down
Router(config-if)#
Router(config-if)#exit
Router(config)#int s0/0/1
Router(config-if)#ip address 10.0.0.1 255.255.255.252
Router(config-if)#no shutdown

%LINK-5-CHANGED: Interface Serial0/0/1, changed state to down
Router(config-if)#exit
Router(config)#int f0/0
Router(config-if)#ip address 10.0.0.5 255.255.255.252
Router(config-if)#no shutdown

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

Router(config-if)#end
Router#
%SYS-5-CONFIG_I: Configured from console by console

Router#wr
Building configuration...
```

Imagen 7. Configuración de direcciones IP

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

Configuramos DHCP en cada dispositivo desde desktop, accedemos a IP Configuración y activamos DHCP.

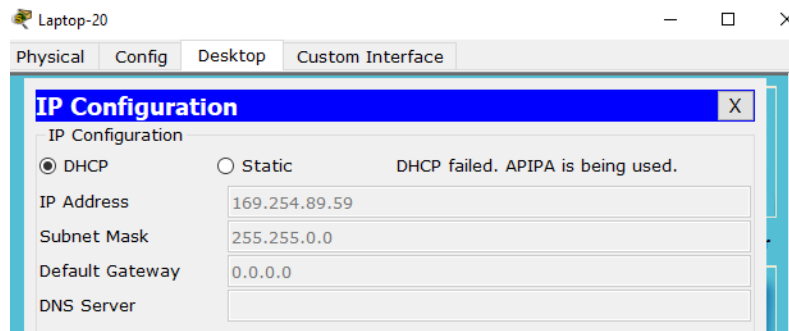


Imagen 8. Configuración DHCP IPv4

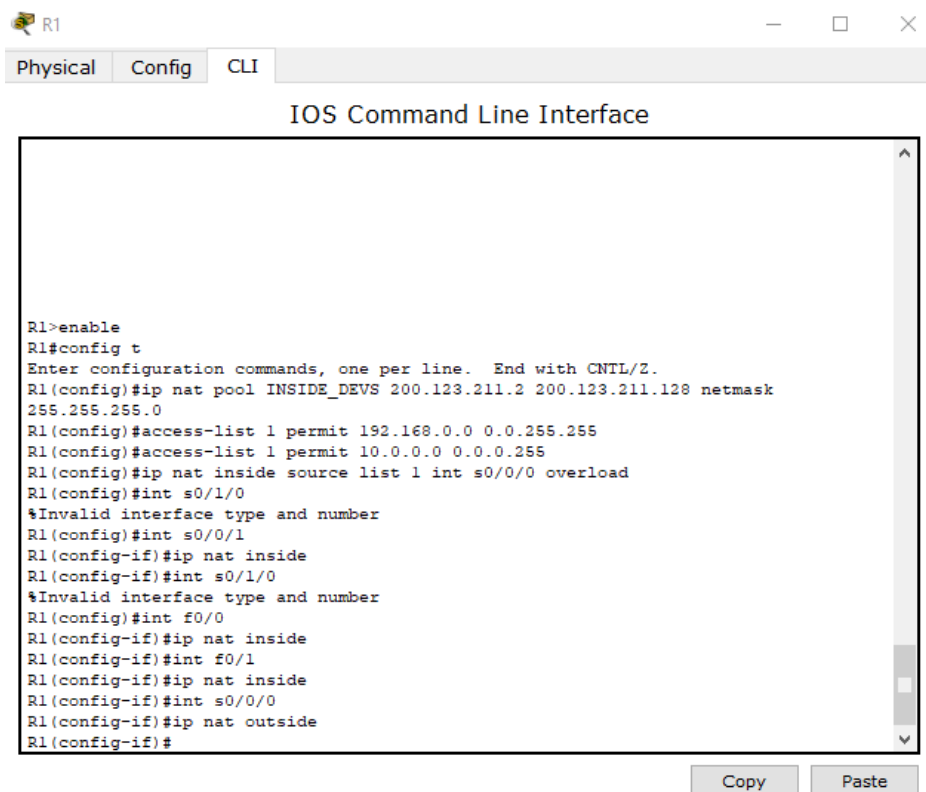
2.6 R1 debe realizar una NAT con sobrecarga sobre una dirección IPv4 pública. Asegúrese de que todos los terminales pueden comunicarse con Internet pública (haga ping a la dirección ISP) y la lista de acceso estándar se llama INSIDE-DEVS.

Se define la dirección IP pública a través del comando Gateway (config)# ip nat pool.

Se definen las listas de control de acceso que coincida con las direcciones IP privadas de LAN, utilizando el comando Gateway (config)# access-list 1 permit.

Definir la NAT desde la lista de origen interna hasta el conjunto externo con el comando Gateway(config)# ip nat inside source list 1 pool public_access overload.

Se emiten los comandos ip nat inside e ip nat outside para especificar las interfaces.



```
R1>enable
R1#config t
Enter configuration commands, one per line. End with CNTL/Z.
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 0.0.0.255
R1(config)#ip nat inside source list 1 int s0/0/0 overload
R1(config)#int s0/1/0
%Invalid interface type and number
R1(config)#int s0/0/1
R1(config-if)#ip nat inside
R1(config-if)#int s0/1/0
%Invalid interface type and number
R1(config)#int f0/0
R1(config-if)#ip nat inside
R1(config-if)#int f0/1
R1(config-if)#ip nat inside
R1(config-if)#int s0/0/0
R1(config-if)#ip nat outside
R1(config-if)#
```

Imagen 9. NAT con sobrecarga en IPv4

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

Se utiliza el comando ip nat inside source static tcp para configurar la ruta estática.

Se utiliza (config)#router rip para configurar los Rip versión 2.

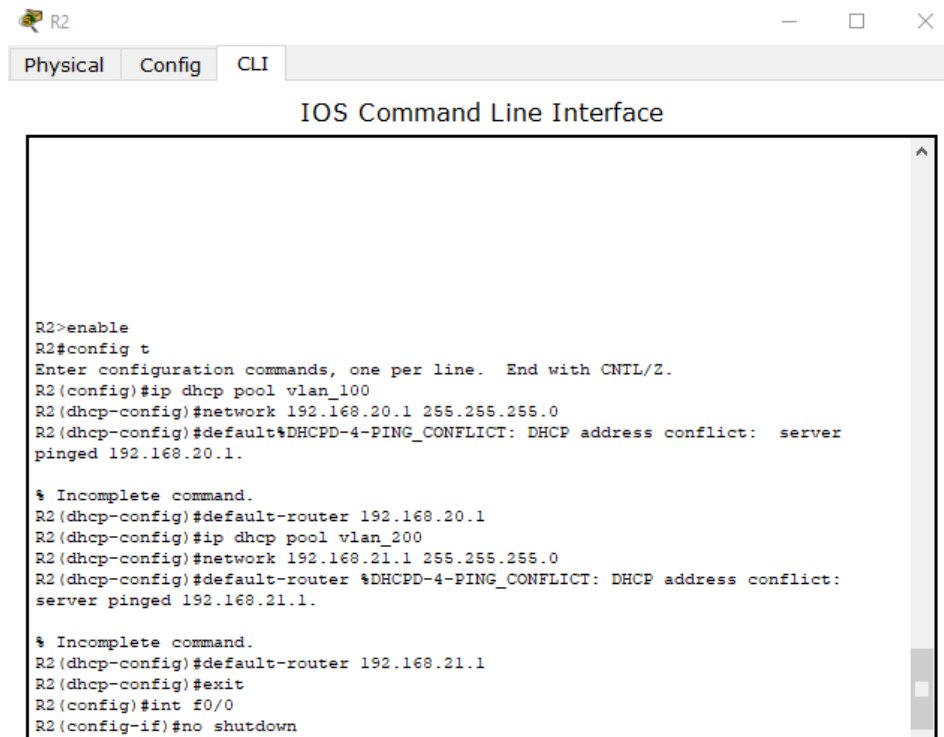
```
R1 (config)#ip nat inside source static tcp 192.168.30.6 80 200.123.211.1 80
^
% Invalid input detected at '^' marker.

R1(config)#int s0/0/1
R1(config-if)#ip nat inside
R1(config-if)#int f0/0
R1(config-if)#ip nat inside
R1(config-if)#int f0/1
R1(config-if)#ip nat inside
R1(config-if)#int s0/0/0
R1(config-if)#ip nat outside
R1(config-if)#exit
R1(config)#ip nat inside source static tcp 192.168.30.6 80 200.123.211.1 80
R1(config)#router rip
R1(config-router)#version 2
R1(config-router)#network 10.0.0.4
R1(config-router)#network 10.0.0.0
R1(config-router)#default-information originate
R1(config-router)#do show ip route connected
C 10.0.0.0/30 is directly connected, Serial0/0/1
C 200.123.211.0/24 is directly connected, Serial0/0/0
R1(config-router)#end
R1#
%SYS-5-CONFIG_I: Configured from console by console

R1#wr
Building configuration...
[OK]
R1#
```

Imagen 10. Ruta estática y dominio RIPv2

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



```
R2
Physical Config CLI
IOS Command Line Interface

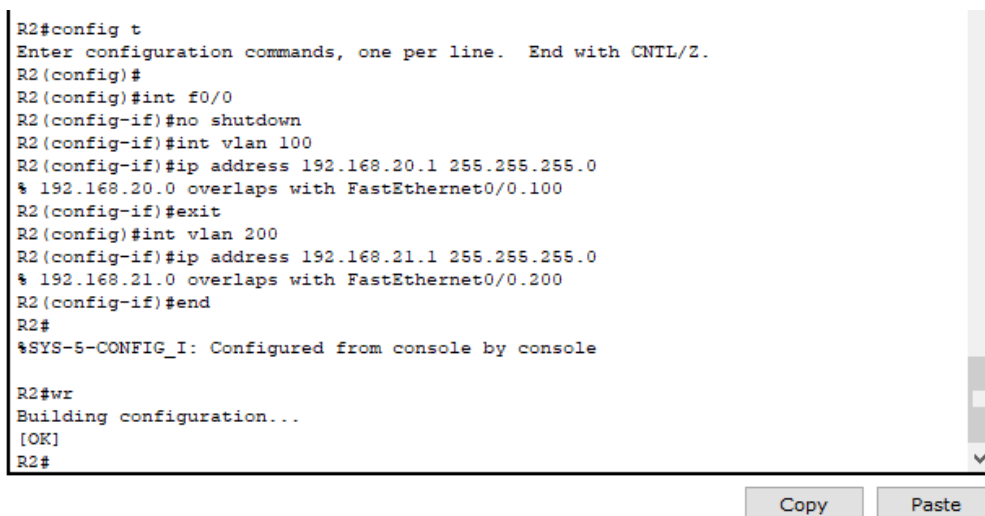
R2>enable
R2#config t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#ip dhcp pool vlan_100
R2(dhcp-config)#network 192.168.20.1 255.255.255.0
R2(dhcp-config)#default%DHCPD-4-PING_CONFLICT: DHCP address conflict: server
pinged 192.168.20.1.

% Incomplete command.
R2(dhcp-config)#default-router 192.168.20.1
R2(dhcp-config)#ip dhcp pool vlan_200
R2(dhcp-config)#network 192.168.21.1 255.255.255.0
R2(dhcp-config)#default-router %DHCPD-4-PING_CONFLICT: DHCP address conflict:
server pinged 192.168.21.1.

% Incomplete command.
R2(dhcp-config)#default-router 192.168.21.1
R2(dhcp-config)#exit
R2(config)#int f0/0
R2(config-if)#no shutdown
```

Imagen 11. DHCP Server

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



```
R2#config t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#
R2(config)#int f0/0
R2(config-if)#no shutdown
R2(config-if)#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)#end
R2#
%SYS-5-CONFIG_I: Configured from console by console

R2#wr
Building configuration...
[OK]
R2#
```

Copy Paste

Imagen 12. Enrutamiento entre VLAN 100 y 200

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

Se hace ping a los diferentes dispositivos.

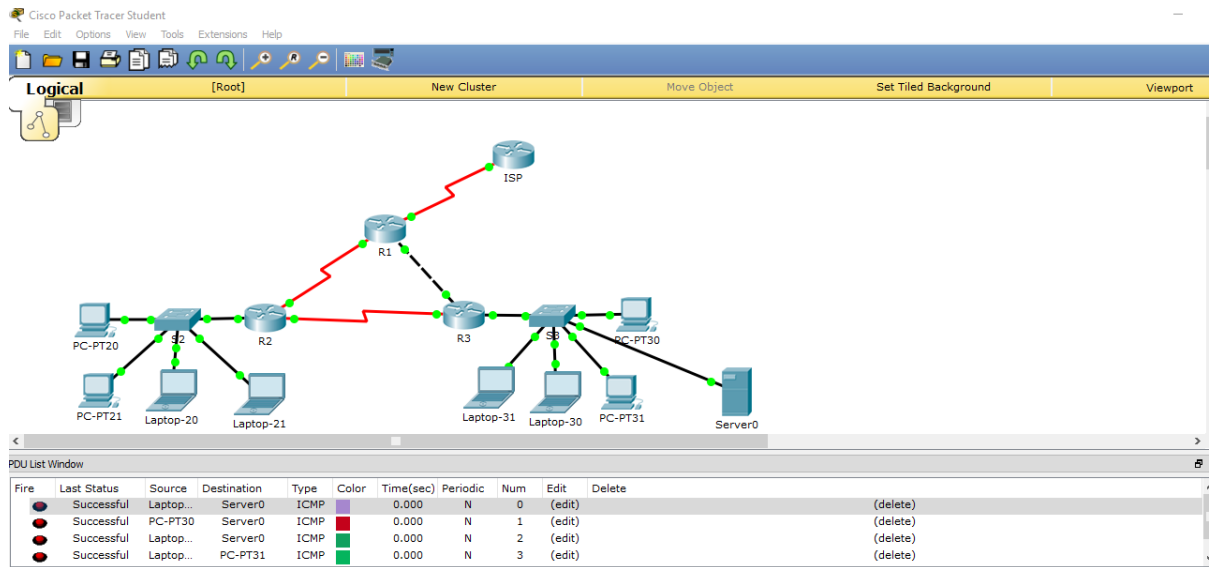


Imagen 13. Prueba de conectividad

2.11 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.

Se configuran desde desktop los DHCPv6

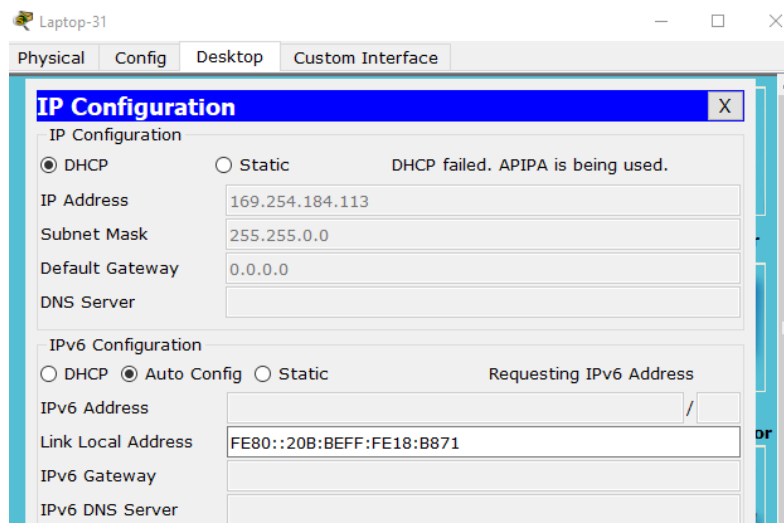
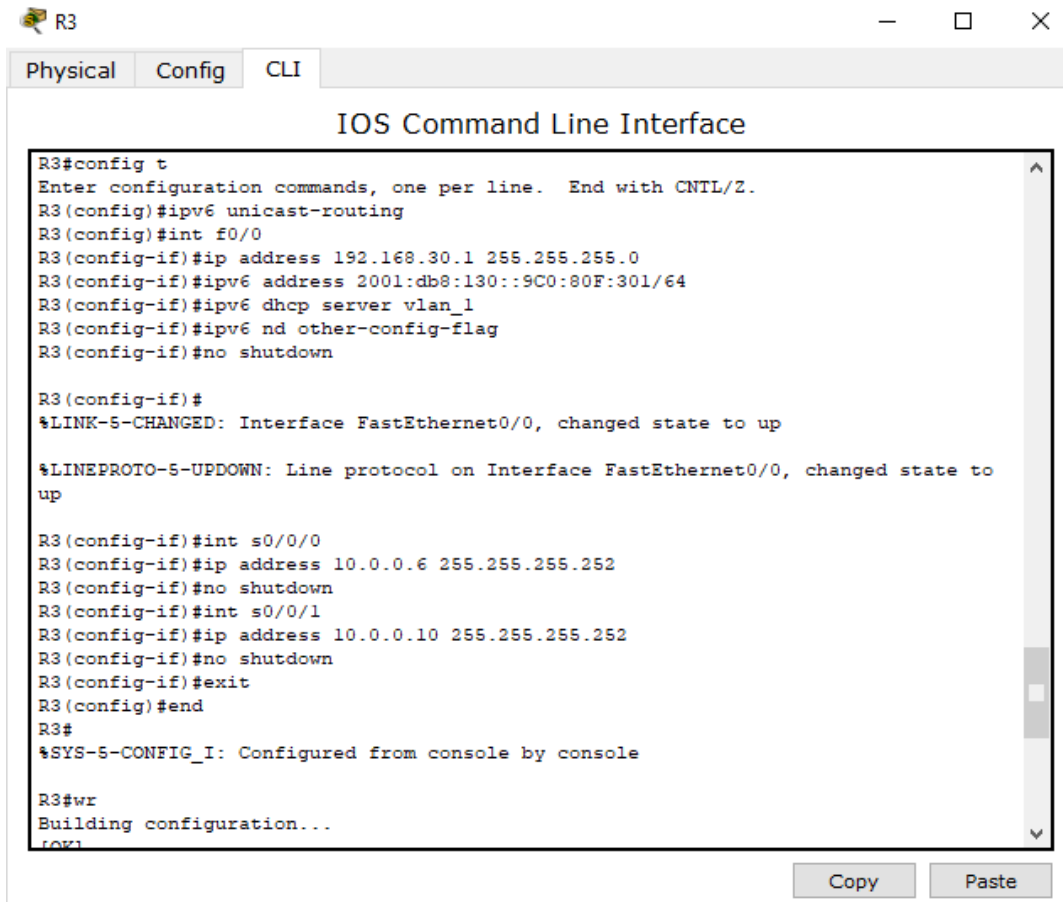


Imagen 14. DHCPv6

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

Se procede de la siguiente forma:



```
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)#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)#ipv6 dhcp server vlan_1
R3(config-if)#ipv6 nd other-config-flag
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)#int s0/0/0
R3(config-if)#ip address 10.0.0.6 255.255.255.252
R3(config-if)#no shutdown
R3(config-if)#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)#exit
R3(config)#end
R3#
%SYS-5-CONFIG_I: Configured from console by console

R3#wr
Building configuration...
[OK]
```

Imagen 15. IPv4 e IPv6 dual-stack

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

Se crea la ruta accediendo a R1 configuración, Rip, escribir la dirección Ip 200.123.211.0 y por ultimo presionar clic en el botón adicionar (Add).

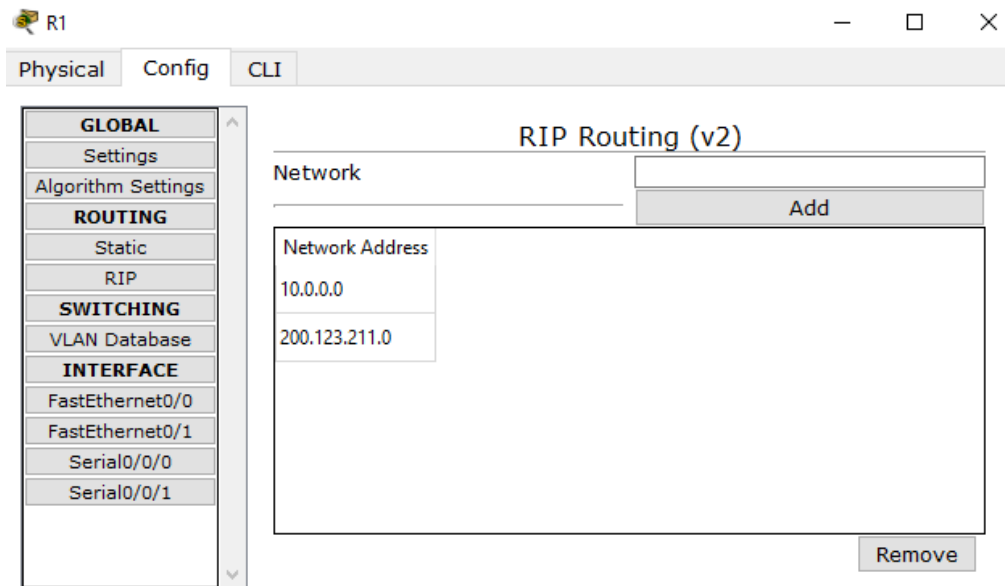


Imagen 16. Adicionar Rip

2.14 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.

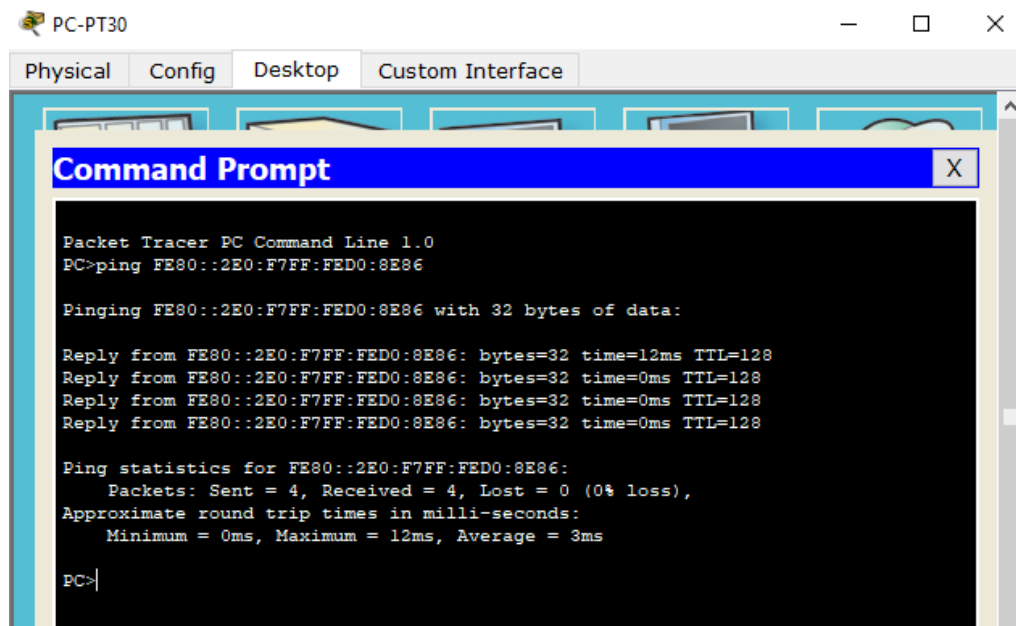


Imagen 17. Verificación conectividad desde PC-PT30

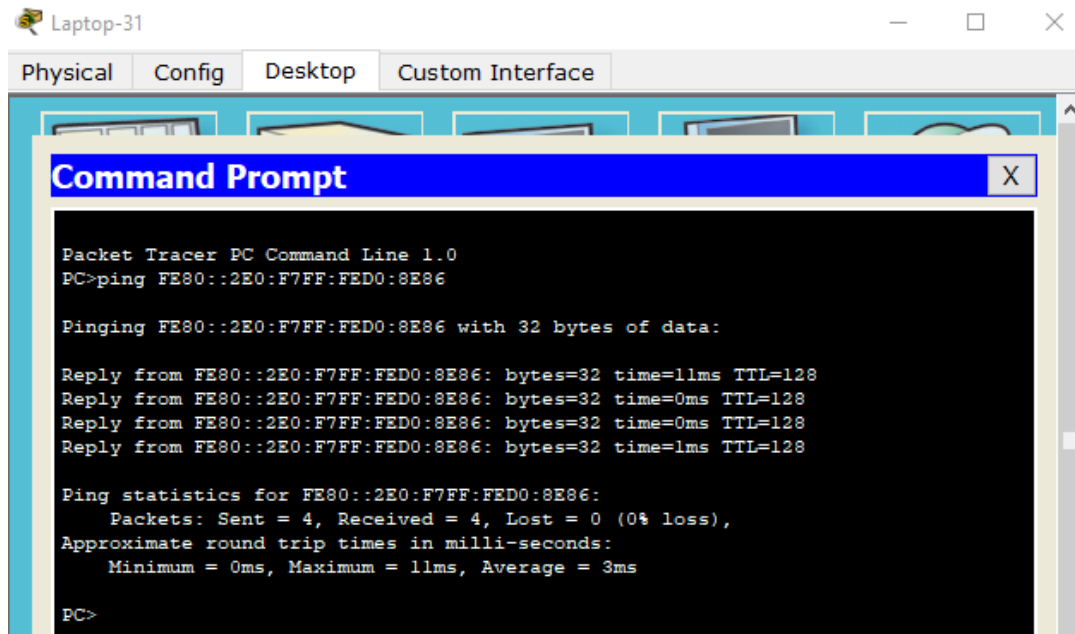


Imagen 18. Verificación conectividad desde Laptop-31

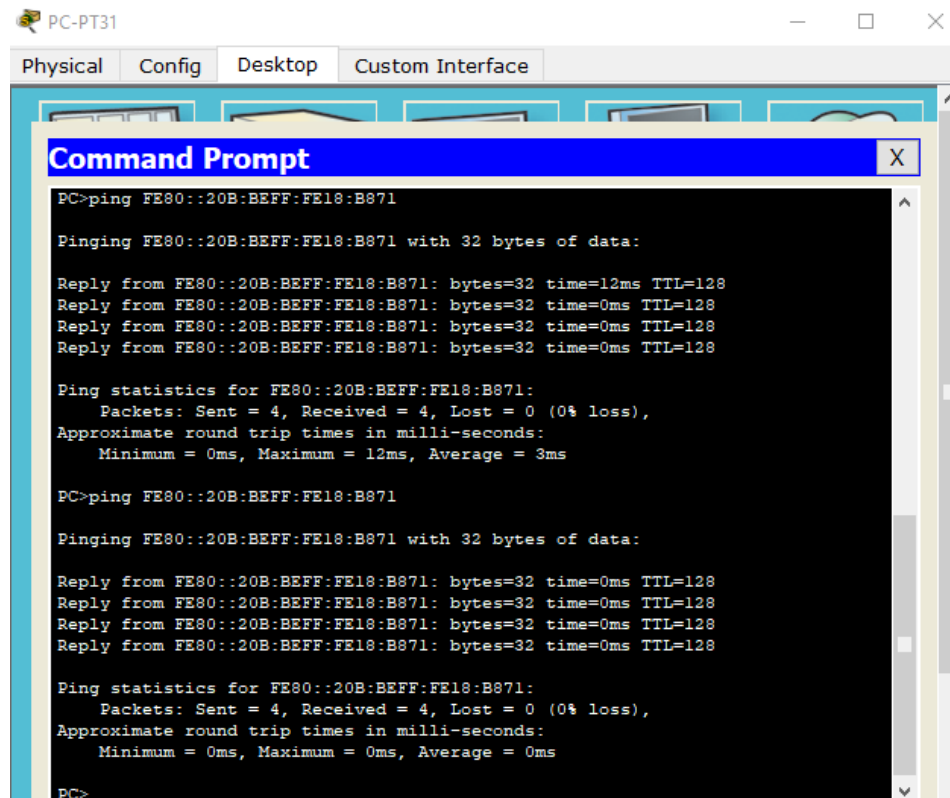


Imagen 19. Verificación conectividad desde PC-PT31

3. Escenario 2

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

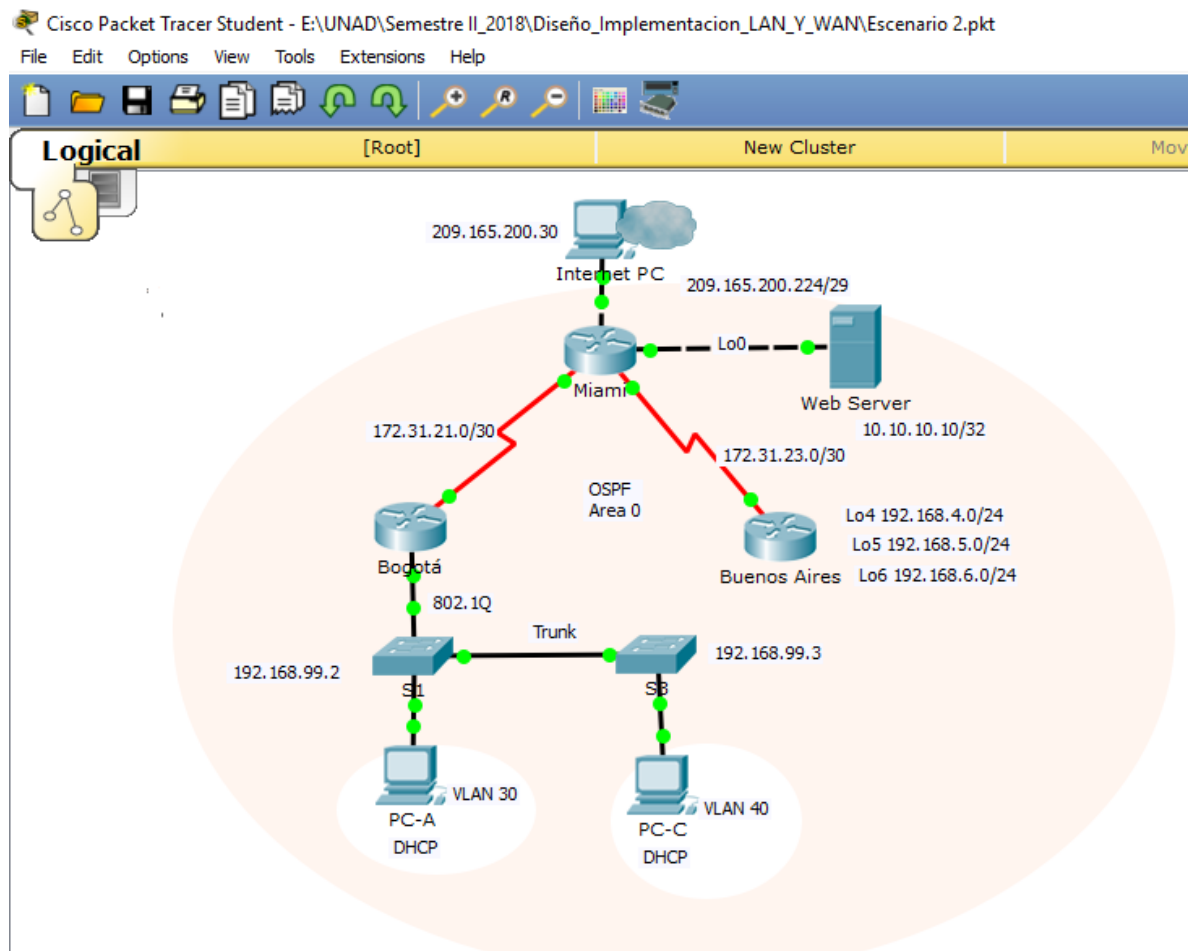


Imagen 20. Topología Escenario 2

Recursos necesarios

- 3 Routers (Cisco 1841) con 2 puertos FastEthernet, 2 puertos Seriales
- 2 Switches (Cisco 2960)
- 1 Servidor (Genérico PT)
- 3 PCs con sistema operativo Windows 7, con tarjeta de red
- Cables Serial y Ethernet

Para el caso de los Routers se deberá agregar la tarjeta de comunicación Serial.

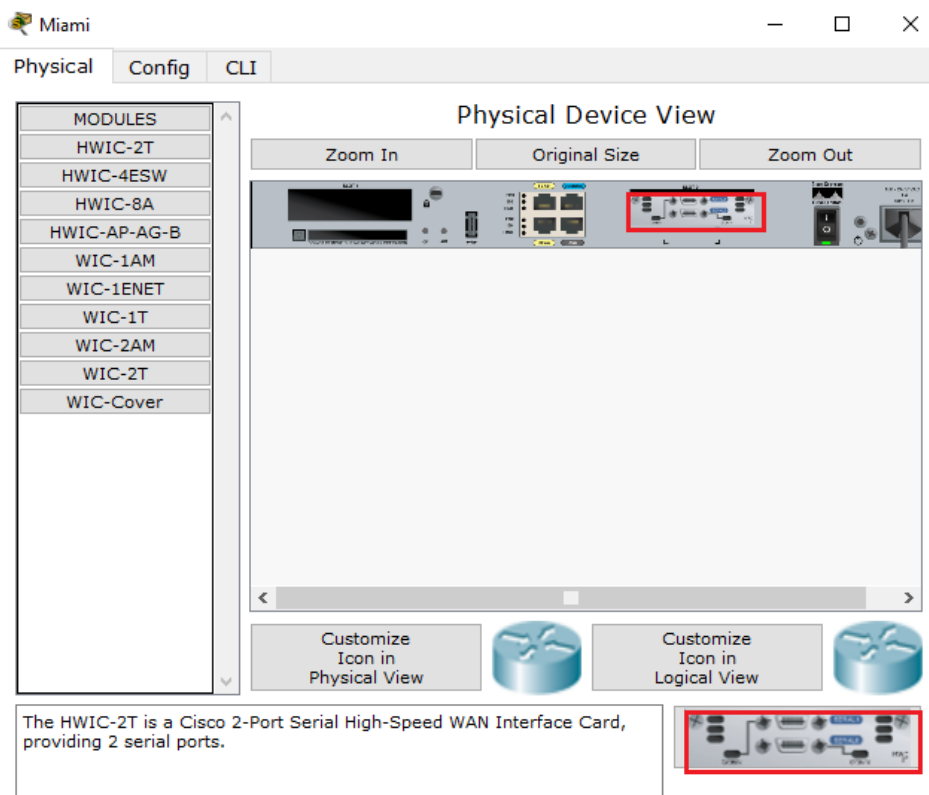


Imagen 21. Tarjeta serial

Configuración de un PC para ubicarlo como “Internet-PC” en la topología

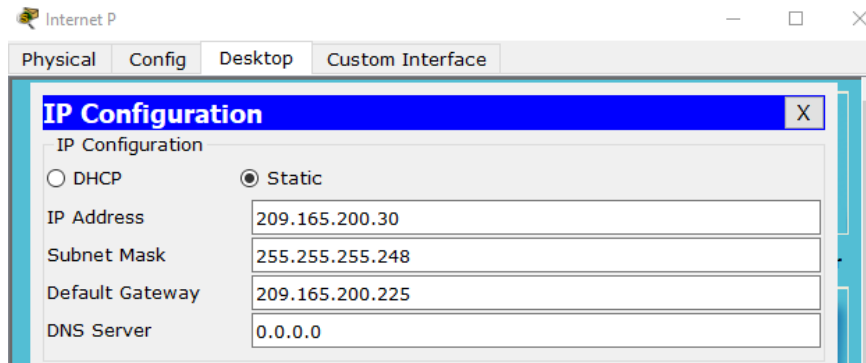


Imagen 22. Internet – PC

3.1 Configuración básica de dispositivos

- “Bogotá” nombrarlo: R1 con el comando hostname
- “Miami” nombrarlo: R2 con el comando hostname
- “Buenos Aires” nombrarlo: R3 con el comando hostname
- S1: nombrarlo “S1” con el comando hostname
- S3: nombrarlo “S3” con el comando hostname
- Exec Password: class con el comando enable secret class
- Console Access Password: cisco
- Telnet Access Password: cisco
- Encriptar contraseñas con el comando service password-encryption
- MOTD banner: Prohibido personal no autorizado
- A cada Switch deshabilitar DNS lookup

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

Configurar en “Bogotá” la conexión hacia “Miami”.

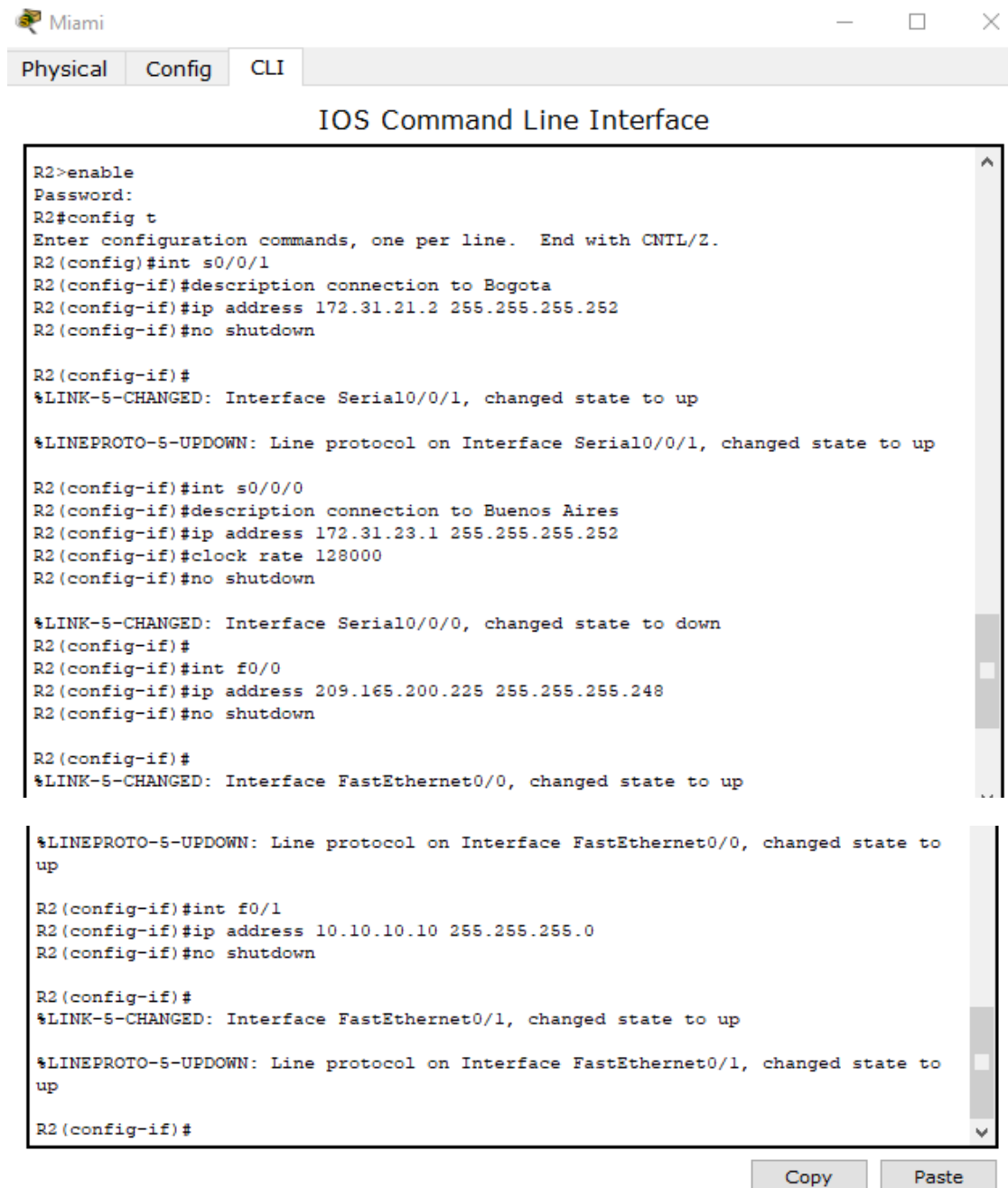
Configurar en “Miami” las siguientes interfaces:

Configurar conexión hacia Bogotá

Configurar conexión hacia Buenos Aires

Establecer conexión hacia PC-Internet

Establecer conexión hacia Web Server



```
R2>enable
Password:
R2#config t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#int s0/0/1
R2(config-if)#description connection to Bogota
R2(config-if)#ip address 172.31.21.2 255.255.255.252
R2(config-if)#no shutdown

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

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1, changed state to up

R2(config-if)#int s0/0/0
R2(config-if)#description connection to Buenos Aires
R2(config-if)#ip address 172.31.23.1 255.255.255.252
R2(config-if)#clock rate 128000
R2(config-if)#no shutdown

%LINK-5-CHANGED: Interface Serial0/0/0, changed state to down
R2(config-if)#
R2(config-if)#int f0/0
R2(config-if)#ip address 209.165.200.225 255.255.255.248
R2(config-if)#no shutdown

R2(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

R2(config-if)#int f0/1
R2(config-if)#ip address 10.10.10.10 255.255.255.0
R2(config-if)#no shutdown

R2(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to
up

R2(config-if)#
```

Copy Paste

Imagen 23. Configuración direccionamiento IP

Configurar en “Buenos Aires” los siguientes parámetros:

Configurar la conexión hacia “Miami”

Configurar loopbacks 4 – 5 – 6

Realizar la configuración del direccionamiento del Web Server

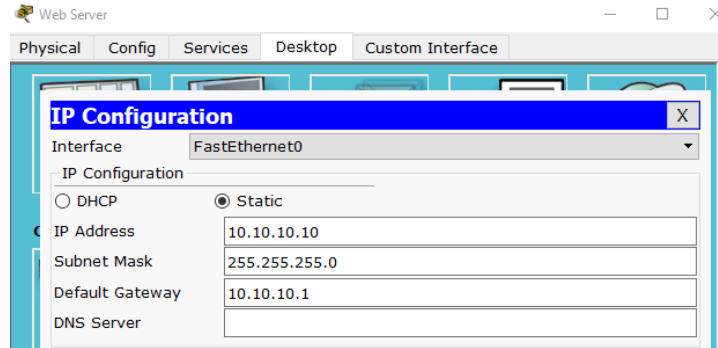


Imagen 24. Configuración direccionamiento Web Server

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

OSPFv2 area 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

Tabla 2 Protocolo OSPFv2

Para esto se debe utilizar el comando (config-router)#router-id y verificar los OPSF vecinos con el comando #show ip ospf neighbor.

```
R3#show ip ospf neighbor
```

Neighbor ID	Pri	State	Dead Time	Address	Interface
5.5.5.5	0	FULL/ -	00:00:33	172.31.23.1	Serial0/0/1

```
R3#
```

Copy Paste

Imagen 25. Verificación de OPSF vecinos en R3

Verificar la configuración del protocolo de enrutamiento utilizando el comando #show ip protocols.

```
password.  
R2>enable  
Password:  
R2#show running configuration  
^  
% Invalid input detected at '^' marker.  
R2#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  
Routing Information Sources:  
 Gateway Distance Last Update  
 1.1.1.1 110 00:27:10  
 5.5.5.5 110 00:13:19  
 8.8.8.8 110 00:09:48  
Distance: (default is 110)  
R2#
```

Copy Paste

Imagen 26. Verificación de Protocolos en R2

Verificamos las rutas dinámicas de OSPF configuradas en los routers utilizando el comando #show ip route ospf

```

Bogotá
Physical Config CLI
IOS Command Line Interface

Prohibido el acceso no autorizado

User Access Verification

Password:

R1>enable
Password:
R1#show ip route ospf
 10.0.0.0/24 is subnetted, 1 subnets
O   10.10.10.0 [110/9595] via 172.31.21.2, 00:26:28, Serial0/0/0
 172.31.0.0/30 is subnetted, 2 subnets
O   172.31.23.0 [110/15652] via 172.31.21.2, 00:26:28, Serial0/0/0
 192.168.4.0/32 is subnetted, 1 subnets
O   192.168.4.1 [110/15653] via 172.31.21.2, 00:16:35, Serial0/0/0
 192.168.5.0/32 is subnetted, 1 subnets
O   192.168.5.1 [110/15653] via 172.31.21.2, 00:16:25, Serial0/0/0
 192.168.6.0/32 is subnetted, 1 subnets
O   192.168.6.1 [110/15653] via 172.31.21.2, 00:16:25, Serial0/0/0
R1#
  
```

Imagen 27. Verificación de rutas OPSF en R1

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

Tener en cuenta la siguiente tabla de VLANs

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

Tabla 3. Tabla de Direccionamiento VLANs

Se debe hacer lo siguiente en los switches:

Crear las VLAN utilizando el comando (config)#vlan

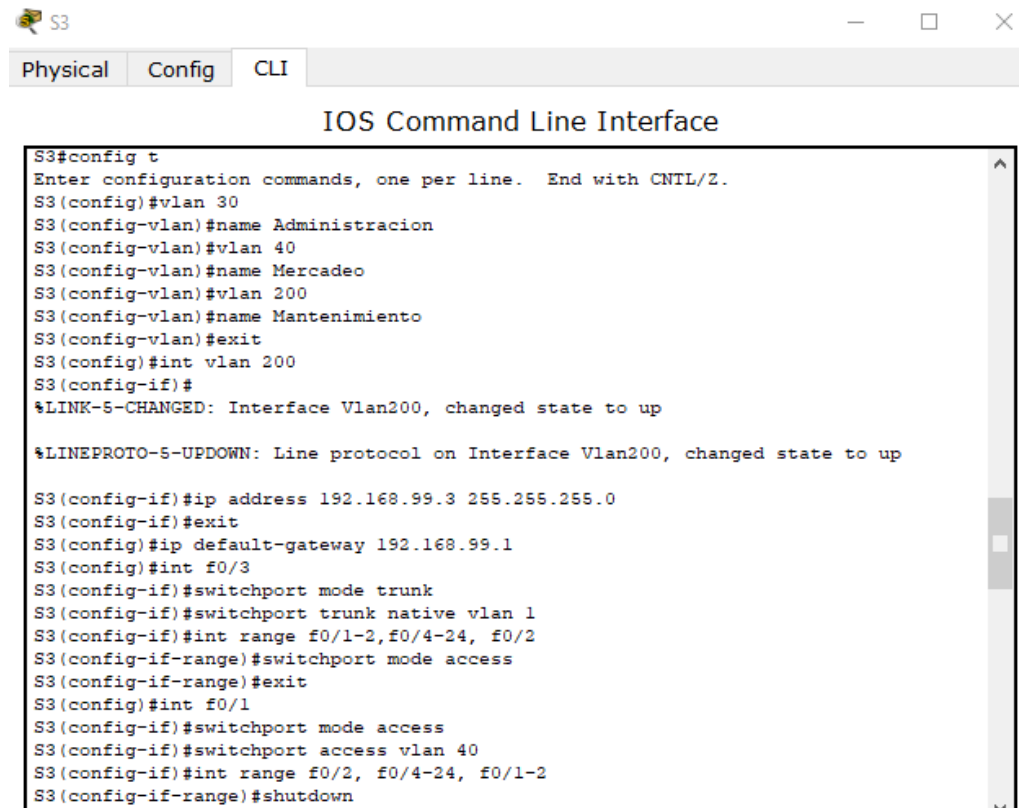
Configurar los puertos en modo troncal utilizando el comando (config-if)#switchport mode trunk

Configurar en los puertos f0/3 y f0/24 en modo troncal en la VLAN nativa utilizando el comando (config-if)#switchport trunk native vlan.

Configurar “mode access” los puertos restantes

Deshabilitar los puertos que no se usaran

Asignar las direcciones IP a las VLANs.



```
S3
Physical Config CLI
IOS Command Line Interface
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 Mercadeo
S3(config-vlan)#vlan 200
S3(config-vlan)#name Mantenimiento
S3(config-vlan)#exit
S3(config)#int vlan 200
S3(config-if)#
%LINK-S-CHANGED: Interface Vlan200, changed state to up

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

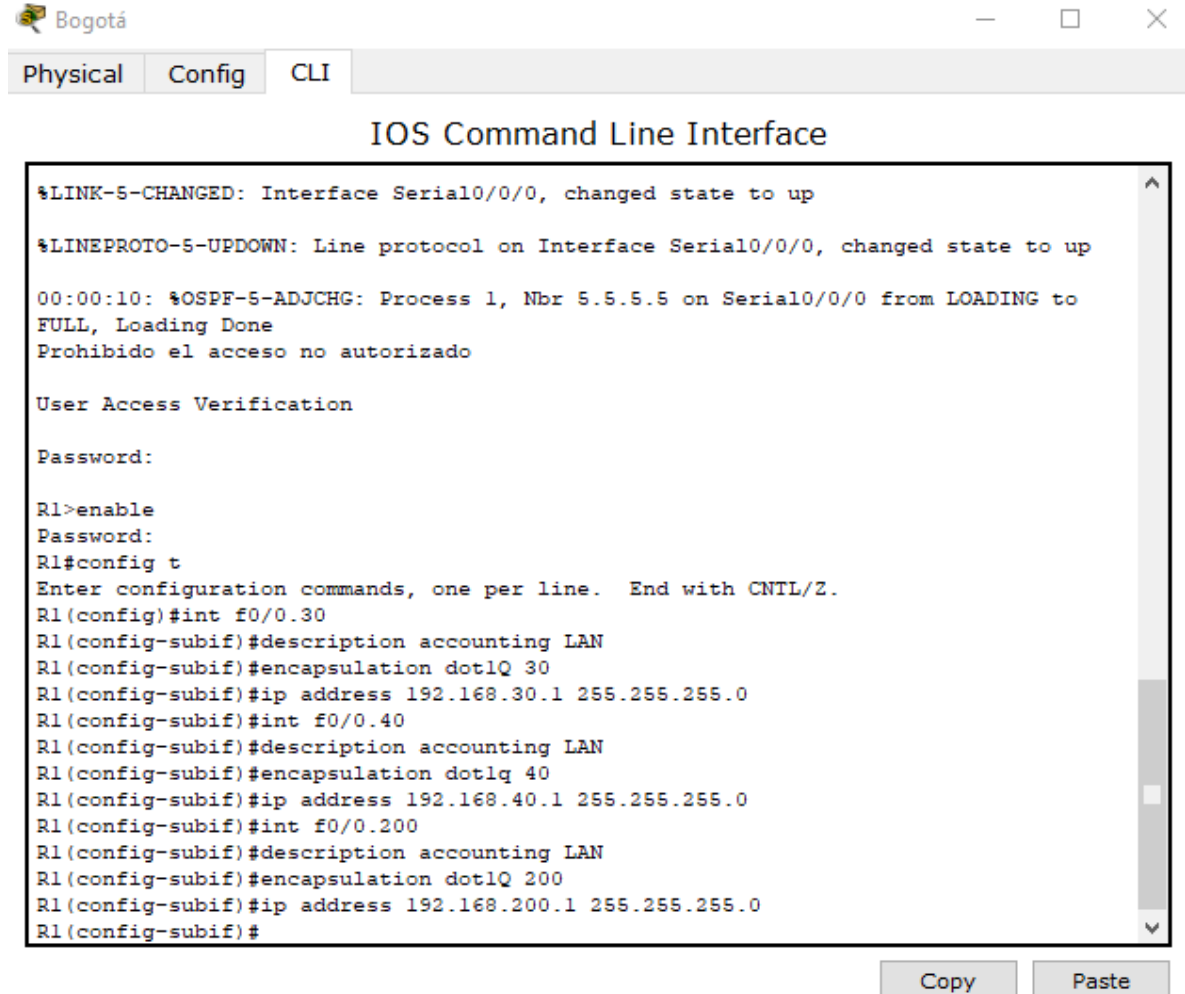
S3(config-if)#ip address 192.168.99.3 255.255.255.0
S3(config-if)#exit
S3(config)#ip default-gateway 192.168.99.1
S3(config)#int f0/3
S3(config-if)#switchport mode trunk
S3(config-if)#switchport trunk native vlan 1
S3(config-if)#int range f0/1-2,f0/4-24, f0/2
S3(config-if-range)#switchport mode access
S3(config-if-range)#exit
S3(config)#int f0/1
S3(config-if)#switchport mode access
S3(config-if)#switchport access vlan 40
S3(config-if)#int range f0/2, f0/4-24, f0/1-2
S3(config-if-range)#shutdown
```

Imagen 28. Configuración VLANs en S3

Configuración de seguridad Switch, VLANs, Inter-VLANs Routing

Configurar en Miami, lo siguiente:

- Configure 802.1Q subinterface .30 descripción de la conexión, asignar VLAN Administración, asignación de la primera dirección viable a esta interface.
- Configure 802.1Q subinterface .40 descripción de la conexión, asignar VLAN Mercadeo, asignación de la primera dirección viable a esta interface.
- Configure 802.1Q subinterface .200 descripción de la conexión, asignar VLAN Mantenimiento, asignación de la primera dirección viable a esta interface.
- Activar la conexión hacia S1.



```
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up
00:00:10: %OSPF-5-ADJCHG: Process 1, Nbr 5.5.5.5 on Serial0/0/0 from LOADING to FULL, Loading Done
Prohibido el acceso no autorizado

User Access Verification

Password:

R1>enable
Password:
R1#config t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#int f0/0.30
R1(config-subif)#description accounting LAN
R1(config-subif)#encapsulation dot1Q 30
R1(config-subif)#ip address 192.168.30.1 255.255.255.0
R1(config-subif)#int f0/0.40
R1(config-subif)#description accounting LAN
R1(config-subif)#encapsulation dot1q 40
R1(config-subif)#ip address 192.168.40.1 255.255.255.0
R1(config-subif)#int f0/0.200
R1(config-subif)#description accounting LAN
R1(config-subif)#encapsulation dot1Q 200
R1(config-subif)#ip address 192.168.200.1 255.255.255.0
R1(config-subif)#
```

Imagen 29. Configuración de seguridad

Verificación de conectividad

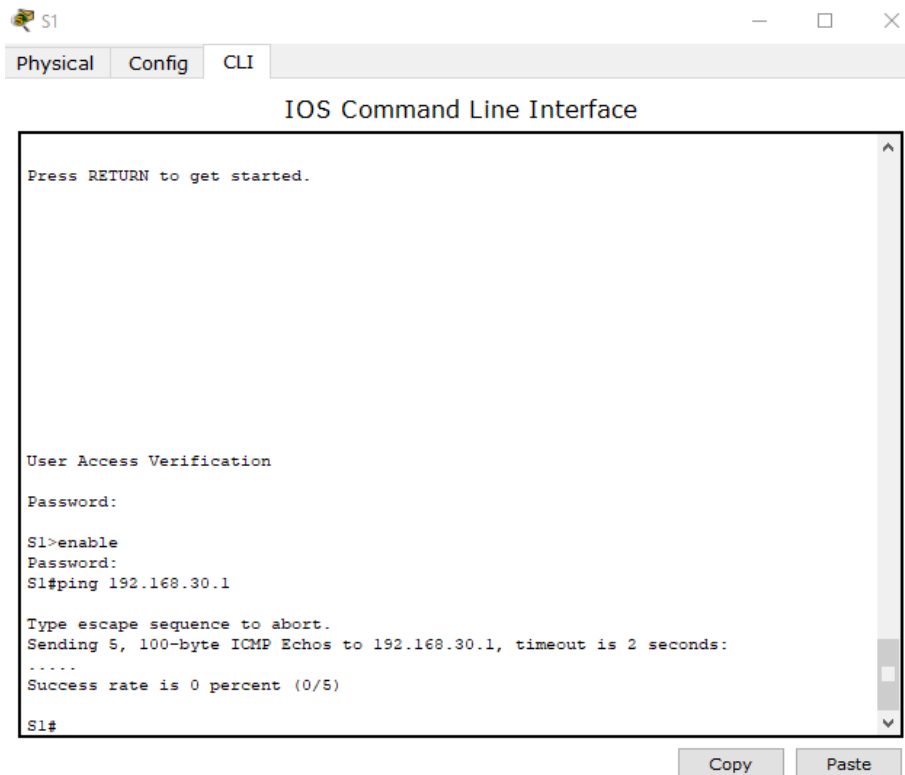


Imagen 30. Verificación de Conectividad

3.4 Asignar direcciones IP a los Switches acorde a los lineamientos

Para esto utilizamos el comando ip address

```
S1#config t
Enter configuration commands, one per line. End with CNTL/Z.
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
```

Imagen 31. Asignación de Ip en S1

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

Se emite el comando `int range` para especificar el rango de interfaces que serán desactivadas.

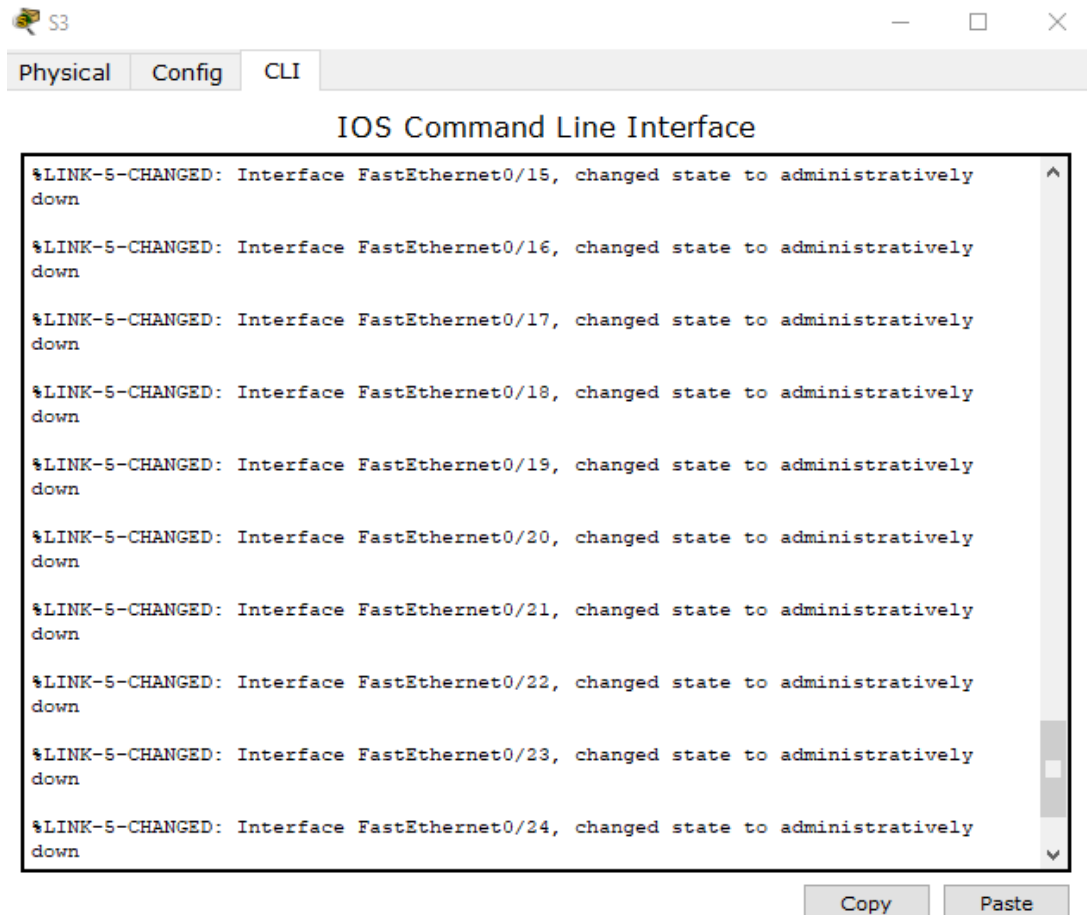


Imagen 32. Desactivación de puertos

3.6 Implement DHCP and NAT for IPv4

Se debe acceder al desktop de cada una de las PC y en Ip configuration activar DHCP.

Para configurar NAT se debe utilizar el comando `#ip nat inside source static`.

3.7 Configurar R1 como servidor DHCP para las VLANs 30 y 40

Para el desarrollo de este punto se debe tener en cuenta la siguiente tabla:

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.

Tabla 4. Configuración de DHCP pool para VLAN

Estando en R1 utilizar el comando `ip dhcp pool`, según las especificaciones de la tabla se indica el DNS del servidor, el router que se establecerá por defecto y la dirección IP de la red.

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

Para reservar las direcciones ip de las VLAN se debe utilizar el comando `#ip dhcp excluded-address` tal como lo muestra la imagen

```
Prohibido el acceso no autorizado

User Access Verification

Password:

R1>enable
Password:
R1#config t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#ip dhcp excluded-address 192.168.30.1 192.168.30.30
R1(config)#ip dhcp excluded-address 192.168.40.1 192.168.40.30
R1(config)#ip dhcp pool ADMINISTRACION
R1(dhcp-config)#dns-server 10.10.10.11
R1(dhcp-config)#default-router 192.168.30.1
R1(dhcp-config)#network 192.168.30.0 255.255.255.0
R1(dhcp-config)#ip dhcp pool MERCADERO
R1(dhcp-config)#dns-server 10.10.10.11
R1(dhcp-config)#default-router 192.168.40.1
R1(dhcp-config)#network 192.168.40.0 255.255.255.0
R1(dhcp-config)#
```

Imagen 33. Reserva primeras 30 direcciones

3.9 Configurar NAT en R2 para permitir que los host puedan salir a internet

```
00:00:10: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up
00:00:10: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1, changed state to up
00:00:10: %OSPF-5-ADJCHG: Process 1, Nbr 0.0.0.0 on Serial0/0/0 from LOADING to FULL, Loading Done
00:00:10: %OSPF-5-ADJCHG: Process 1, Nbr 1.1.1.1 on Serial0/0/1 from LOADING to FULL, Loading Done
Prohibido el acceso no autorizado

User Access Verification

Password:

R2>enable
Password:
R2#config t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#int f0/0
R2(config-if)#ip nat outside
R2(config-if)#int f0/1
R2(config-if)#ip nat inside
R2(config-if)#exit
R2(config)#
```

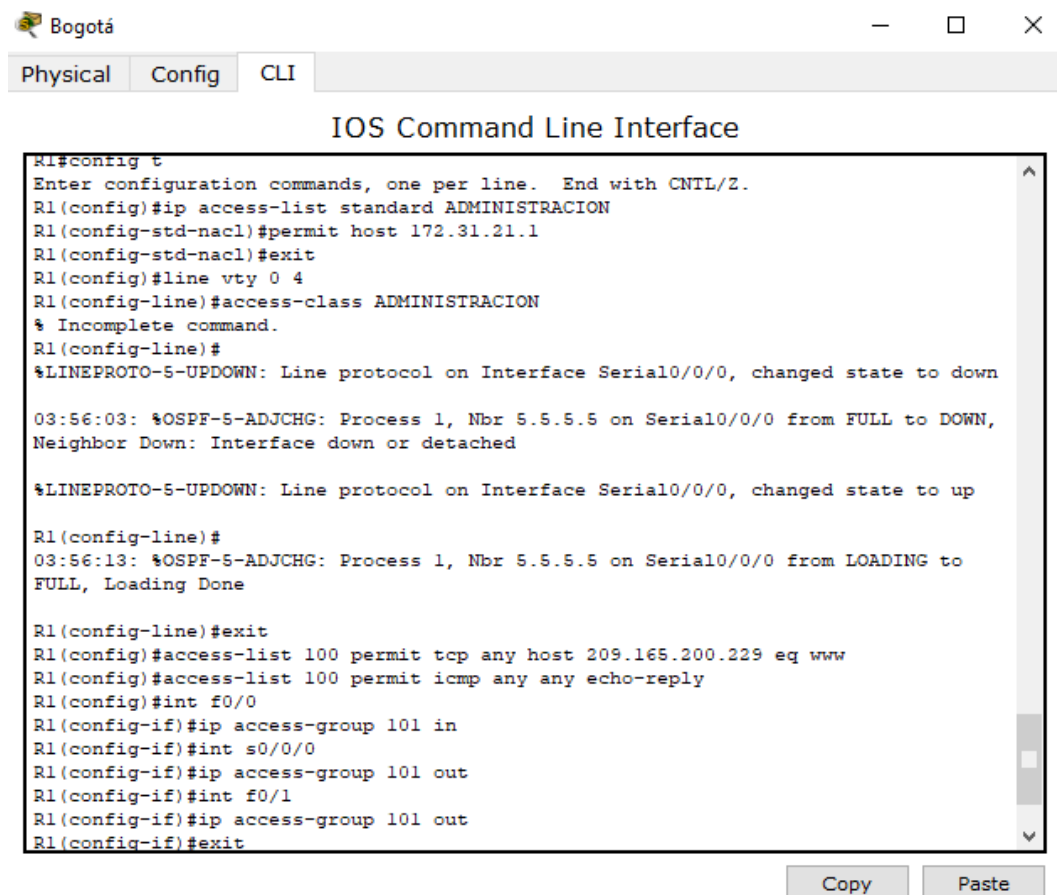
Imagen 34. NAT en R2

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

Se accede a R1 y se emite el comando #ip Access-list standard y se indica el host que será permitido utilizando el comando #permit host.

3.11 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.

Se accede a R1 y se emiten los comandos #access-list permit tcp any host, y #access-list permit icmp any any echo-reply. Igualmente se debe especificar la dirección IP del grupo de acceso con el comando #ip Access-group.



```
R1#config t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#ip access-list standard ADMINISTRACION
R1(config-std-nacl)#permit host 172.31.21.1
R1(config-std-nacl)#exit
R1(config)#line vty 0 4
R1(config-line)#access-class ADMINISTRACION
% Incomplete command.
R1(config-line)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to down

03:56:03: %OSPF-5-ADJCHG: Process 1, Nbr 5.5.5.5 on Serial0/0/0 from FULL to DOWN,
Neighbor Down: Interface down or detached

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

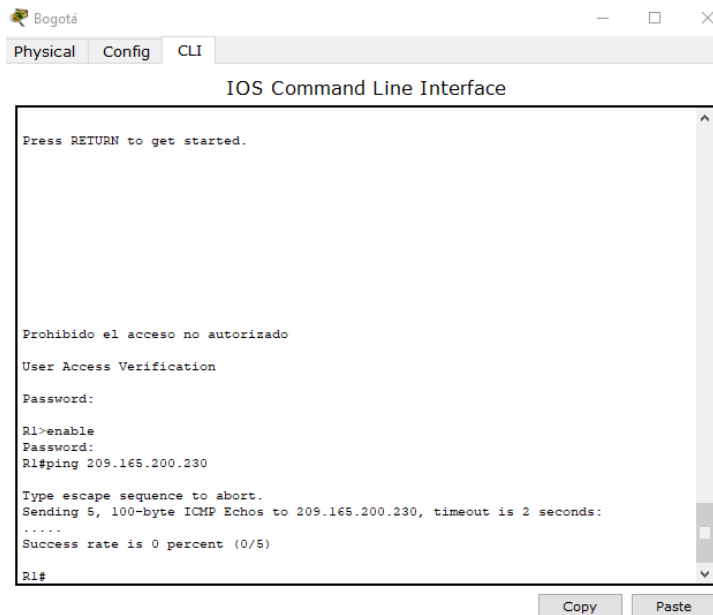
R1(config-line)#
03:56:13: %OSPF-5-ADJCHG: Process 1, Nbr 5.5.5.5 on Serial0/0/0 from LOADING to
FULL, Loading Done

R1(config-line)#exit
R1(config)#access-list 100 permit tcp any host 209.165.200.229 eq www
R1(config)#access-list 100 permit icmp any any echo-reply
R1(config)#int f0/0
R1(config-if)#ip access-group 101 in
R1(config-if)#int s0/0/0
R1(config-if)#ip access-group 101 out
R1(config-if)#int f0/1
R1(config-if)#ip access-group 101 out
R1(config-if)#exit
```

Imagen 35. Listas de acceso

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

Desde R1 se hace ping al Pc de Internet cuya dirección IP es 209.165.200.230



```
Bogotá
Physical Config CLI
IOS Command Line Interface
Press RETURN to get started.

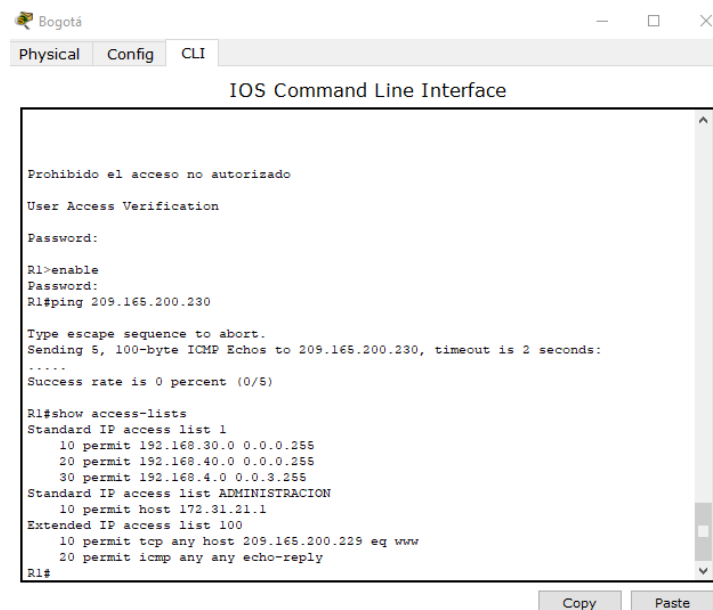
Prohibido el acceso no autorizado
User Access Verification
Password:
R1>enable
Password:
R1#ping 209.165.200.230

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 209.165.200.230, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)

R1#
```

Imagen 36. Ping desde R1

Igualmente se verifica la lista de acceso utilizando el comando #show Access-lists



```
Bogotá
Physical Config CLI
IOS Command Line Interface
Prohibido el acceso no autorizado
User Access Verification
Password:
R1>enable
Password:
R1#ping 209.165.200.230

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 209.165.200.230, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)

R1#show access-lists
Standard IP access list 1
 10 permit 192.168.30.0 0.0.0.255
 20 permit 192.168.40.0 0.0.0.255
 30 permit 192.168.4.0 0.0.3.255
Standard IP access list ADMINISTRACION
 10 permit host 172.31.21.1
Extended IP access list 100
 10 permit tcp any host 209.165.200.229 eq www
 20 permit icmp any any echo-reply

R1#
```

Imagen 37. Verificación Listas de acceso

4. CONCLUSIONES

Después de realizar este trabajo, podemos observar que se han puesto en práctica los conceptos y conocimientos adquiridos en el diplomado de Profundización CCNA, desde configuraciones básicas de los diferentes dispositivos, y armado de la red hasta la verificación de su funcionamiento.

Se logró comprender la configuración de seguridad de una red, Servidor de DHCP, NAT, RIPV2, configuración de direcciones IP, servidor IPv6, creación de VLAN, protocolo de enrutamiento OSPFv2, configuración de puertos troncales; listas de acceso estándar y extendido, y verificación de conectividad.

Se considera un trabajo enriquecedor teniendo en cuenta que son posibles casos que se pueden presentar en la cotidianidad como futuros profesionales de las telecomunicaciones, para lo cual debemos estar preparados para dar posible solución y apoyarnos en cada uno de estos conocimientos.

5. REFERENCIAS BIBLIOGRAFICAS

CISCO. (2014). Acceso a la red. Fundamentos de Networking. Recuperado de: <https://static-course-assets.s3.amazonaws.com/ITN50ES/module2/index.html#4.0.1.1>

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). Configuración y conceptos básicos de Switching. Principios de Enrutamiento y Conmutación. Recuperado de <https://static-course-assets.s3.amazonaws.com/RSE50ES/module2/index.html#2.0.1.1>

CISCO. (2014). Configuración de un sistema operativo de red. Fundamentos de Networking. Recuperado de <https://static-course-assets.s3.amazonaws.com/ITN50ES/module2/index.html#2.0.1.1>

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>

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>

CISCO. (2014). Enrutamiento Estático. Principios de Enrutamiento y Conmutación. Recuperado de <https://static-course-assets.s3.amazonaws.com/RSE50ES/module6/index.html#6.0.1.1>

CISCO. (2014). Listas de control de acceso. Principios de Enrutamiento y Conmutación. Recuperado de <https://static-course-assets.s3.amazonaws.com/RSE50ES/module9/index.html#9.0.1.1>

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>

UNAD (2014). PING y TRACER como estrategia en procesos de Networking [OVA]. Recuperado de <https://1drv.ms/u/s!AmIJYei-NT1lhgTCtKY-7F5KIRC3>

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). Protocolos y comunicaciones de red. Fundamentos de Networking. Recuperado de <https://static-course-assets.s3.amazonaws.com/ITN50ES/module2/index.html#3.0.1.1>

CISCO. (2014). Traducción de direcciones IP para IPv4. Principios de Enrutamiento y Conmutación. Recuperado de <https://static-course-assets.s3.amazonaws.com/RSE50ES/module11/index.html#11.0.1.1>