

**EVALUACIÓN – PRUEBA DE HABILIDADES PRÁCTICAS CCNA.
(DISEÑO E IMPLEMENTACIÓN DE SOLUCIONES INTEGRADAS LAN / WAN).**

JHONNY BOLAÑOS ZUÑIGA

**UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
PROGRAMA DE INGENIERÍA DE SISTEMAS
DIPLOMADO DE PROFUNDIZACIÓN CISCO
SANTIAGO DE CALI
2019**

**EVALUACIÓN – PRUEBA DE HABILIDADES PRÁCTICAS CCNA.
(DISEÑO E IMPLEMENTACIÓN DE SOLUCIONES INTEGRADAS LAN / WAN).**

JHONNY BOLAÑOS ZUÑIGA

Trabajo de diplomado para optar por el título de Ingeniero de Sistemas

**Director:
INGENIERO GIOVANNI ALBERTO BRACHO**

**UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
PROGRAMA DE INGENIERÍA DE SISTEMAS
DIPLOMADO DE PROFUNDIZACIÓN CISCO
SANTIAGO DE CALI
2019**

Nota de Aceptación:

Aprobado por el Comité de Grado en cumplimiento de los requisitos exigidos por la Universidad Nacional Abierta y a Distancia – UNAD, para optar al título de Ingeniero de Sistemas.

Presidente de Jurado

Jurado

Jurado

Santiago de Cali, 18 de diciembre de 2018

DEDICATORIA

A mis padres por haberme forjado como la persona que soy en la actualidad, muchos de mis logros se los debo a ustedes, incluyendo el presente. Gracias por formarme con reglas y valores, y por la gran motivación que constantemente y día tras día me dieron y por lo que sigo alcanzando mis anhelos.

AGRADECIMIENTOS

Gracias primeramente a Dios, por permitirme tener y disfrutar a mi familia, por darme la vida y lo justa que puede llegar a ser

Gracias a mi familia por apoyarme en cada decisión y proyecto, permitiéndome cumplir con excelencia el desarrollo de este estudio. No ha sido sencillo el camino hasta ahora, pero gracias a sus aportes, a su amor y apoyo, lo complicado de lograr esta meta se ha notado menos. Les agradezco y hago presente mi gran afecto a ustedes, mi hermosa familia.

Gracias a mis formadores docentes, personas de gran sabiduría quienes se han esforzado por ayudarme, por esas ganas de transmitirme sus conocimientos, por todo lo que ha hecho que culmine con éxito a obtener una afable titulación profesional.

CONTENIDO

	Pág.
INTRODUCCIÓN	10
1. ESCENARIO 1	11
1.1 CONFIGURAR EL DIRECCIONAMIENTO IP ACORDE CON LA TOPOLOGÍA DE RED PARA CADA UNO DE LOS DISPOSITIVOS QUE FORMAN PARTE DEL ESCENARIO	12
1.1.1 Configuración Direccionamiento Router R1	12
1.1.2 Configuración Direccionamiento Router R2	12
1.1.3 Configuración Direccionamiento Router R3	13
1.1.4 Configuración Direccionamiento Switch S1	13
1.1.5 Configuración Direccionamiento Switch S3	14
1.2 CONFIGURAR EL PROTOCOLO DE ENRUTAMIENTO OSPFV2	14
1.2.1 Configuración enrutamiento OSPFv2 Router R1	14
1.2.2 Configuración enrutamiento OSPFv2 Router R2	15
1.2.3 Configuración enrutamiento OSPFv2 Router R3	15
1.3 VERIFICAR INFORMACIÓN DE OSPF	16
1.3.1 Visualizar tablas de enrutamiento y routers conectados por OSPFv2	16
1.3.2 Visualizar lista resumida de interfaces por OSPF en donde se ilustre el costo de cada interface	16
1.3.3 Visualizar el OSPF Process ID, Router ID, Address summarizations, Routing Networks, and passive interfaces configuradas en cada router.	17
1.4 CONFIGURAR VLANS, PUERTOS TRONCALES, PUERTOS DE ACCESO, ENCAPSULAMIENTO, INTER-VLAN ROUTING Y SEGURIDAD EN LOS SWITCHES ACORDE A LA TOPOLOGÍA DE RED ESTABLECIDA.	19
1.4.1 Configuración Switch S1	19
1.4.2 Configuración Switch S3	19
1.5 EN EL SWITCH 3 DESHABILITAR DNS LOOKUP	20
1.6 ASIGNAR DIRECCIONES IP A LOS SWITCHES ACORDE A LOS LINEAMIENTOS.	20
1.6.1 Configuración Direccionamiento Switch S1	20
1.6.2 Configuración Direccionamiento Switch S3	20
1.7 DESACTIVAR TODAS LAS INTERFACES QUE NO SEAN UTILIZADAS EN EL ESQUEMA DE RED.	21
1.7.1 Desactivación puertos en Switch S1	21
1.7.2 Desactivación puertos en Switch S3	21
1.8 IMPLEMENT DHCP AND NAT FOR IPV4 Y CONFIGURARE R1 COMO SERVIDOR DHCP PARA LAS VLANS 30 Y 40.	21
1.9 RESERVAR LAS PRIMERAS 30 DIRECCIONES IP DE LAS VLAN 30 Y 40 PARA CONFIGURACIONES ESTÁTICAS.	22
1.9.1 Configurar NAT en R2 para permitir que los host puedan salir a internet	22

1.9.2 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.	23
1.9.3 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.	23
1.10 VERIFICAR PROCESOS DE COMUNICACIÓN Y REDIRECCIONAMIENTO DE TRÁFICO EN LOS ROUTERS MEDIANTE EL USO DE PING Y TRACEROUTE.	23
2 ESCENARIO 2	29
2.1 SW1 VLAN Y LAS ASIGNACIONES DE PUERTOS DE VLAN	31
2.1.1 Configuración SW2	31
2.1.2 Configuración SW3	31
2.2 DESHABILITAR PUERTOS DE RED NO UTILIZADOS.	31
2.2.1 Deshabilitar puertos SW2	32
2.2.2 Configuración puertos SW3	32
2.3 CONFIGURACIÓN DE ROUTER.	32
2.3.1 Configuración Router R1	32
2.3.2 Configuración Router R2	32
2.3.3 Configuración Router R3	32
2.3.4 Configuración Router ISP	33
2.4 CONFIGURACIÓN SERVIDOR DHCP IPV4.	33
2.4.1 Configuración DHCP Router R2	33
2.4.2 Configuración DHCP Router R3	34
2.5 CONFIGURACIÓN DE NAT CON SOBRECARGA.	34
2.6 CREACIÓN RUTA ESTÁTICA.	35
2.7 CONFIGURACIÓN ROUTER COMO SERVIDOR DHCP.	35
2.8 ENRUTAMIENTO DE VLAN.	36
2.9 RESTRICCIÓN ACCESO A SERVIDOR.	36
2.10 CONFIGURACIÓN DUAL STACK EN NIC.	37
2.11 CONFIGURACIÓN DUAL STACK EN INTERFAZ.	38
2.12 CONFIGURACIÓN RIP VERSIÓN 2.	38
2.12.1 Configuración Router R1, R2 y R3	39
2.13 ENRUTAMIENTO ENTRE ROUTER.	39
2.13.1 Configuración Router R1	39
2.13.2 Configuración Router R2	39
2.13.3 Configuración Router R3	39
2.14 VERIFICACIÓN DE CONECTIVIDAD.	39
3. CONCLUSIONES	43
BIBLIOGRAFIA	44

LISTA DE ILUSTRACIONES

	Pág.
Ilustración 1. Esquema Inicial Escenario 2	11
Ilustración 2. Verificación OSPF	16
Ilustración 3. Interfaces por OSPF	16
Ilustración 4. Protocolos Router R1	17
Ilustración 5. Protocolos Router R1	18
Ilustración 6. Protocolos Router R3	18
Ilustración 7Lista acceso Router R2	23
Ilustración 8. Ping de Router 1 a PC-Internet	24
Ilustración 9. Conexión de Router R1 a Router R2 y R3	24
Ilustración 10. Ping Internet PC	25
Ilustración 11. Ping PC-A a PC-B	25
Ilustración 12. Tracert del PC-A a Internet PC	26
Ilustración 13. Comando Tracert y Ping desde PC-A a Router R3	26
Ilustración 14. Prueba conectividad a Servidor Web desde PC-C	27
Ilustración 15. Comando Tracert y Ping desde la PC-C a Internet PC	27
Ilustración 16. Comando tracert desde el Router R1 a Internet PC, Web Server y PC-C	28
Ilustración 17. Comando Ping desde los PC vlan 100 y 200 al ISP	34
Ilustración 18. Comando Ping desde los PC vlan 1 al ISP	35
Ilustración 19. Comando ping desde la red del router R3 hacia el Server0	36
Ilustración 20. Comando ping desde la red del Router R2 hacia el server0 (Sin conexión)	37
Ilustración 21. Validación de Dual-stack en red del router R3	38
Ilustración 22. Comando ping desde la red del router R2 hacia el ISP	40
Ilustración 23. Conectividad Router R1, R2 y R3 hacia el ISP	40
Ilustración 24. Comando ping desde la red del router R3 hacia el ISP	41
Ilustración 25. Comando ping desde la red del Router R3 hacia el Server0	41
Ilustración 26.Comando ping entre la red del router R3	42
Ilustración 27. Comando ping entre host de la red de los router R2 y R3	42

LISTA DE TABLAS

	Pág.
Tabla 1. Enrutamiento	12
Tabla 2. Criterios protocolo de enrutamiento OSPFV2 área 0	14
Tabla 3. Direccionamiento	29
Tabla 4. Asignación de VLAN y de puertos	30
Tabla 5. Enlaces troncales	30

INTRODUCCIÓN

Este trabajo es el resultado de todo el manejo que se tiene sobre redes las redes, con el fin que los estudiantes obtengan el conocimiento y las aptitudes que pueden aplicarse al área de Tics de nivel inicial y también para certificaciones CCNA logrando con esto optimar el acceso a los equipos y aprender a configurar esencialmente los aspectos físicos (hardware) y lógicos (software) de una Red, obteniendo el conocimiento previamente adquiridos.

Para ser parte de la asociación que diseña, construye y sueña la tecnología de Redes, es determinar la conexión a todos en todo lugar, que cambia la representación en la que trabajamos, existimos, brincamos y aprendemos; la cual muestra varios caminos. Uno de los más importantes es el que se demuestra en el trabajando desde la Red por medio del packet tracer a través del Programa Cisco Networking Academy, respaldado por el líder mundial en Networking: Cisco Systems.

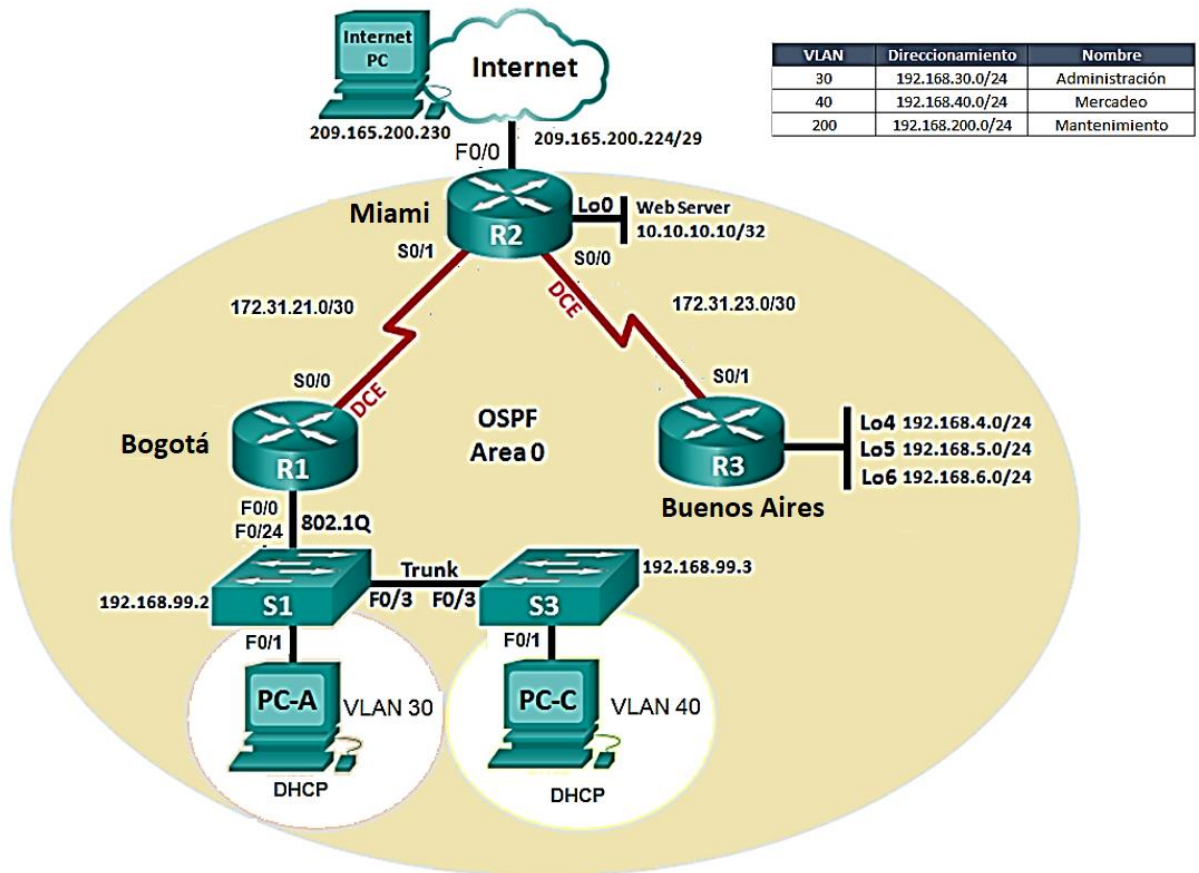
Avalada y reconocida en todo el mundo, la Certificación CCNA (Cisco Certified Network Associate), es la principal carta de presentación que un experto en Redes puede tener para iniciar su camino profesional dentro del mundo TI.

CCNA es la diplomado CCNA Routing & Switching que concluye con la adquisición de competencias y conocimientos para rendir el examen de Certificación Internacional CCNA (Cisco Certified Network Associate).

1. ESCENARIO 1

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.

Ilustración 1. Esquema Inicial Escenario 2



1.1 CONFIGURAR EL DIRECCIONAMIENTO IP ACORDE CON LA TOPOLOGÍA DE RED PARA CADA UNO DE LOS DISPOSITIVOS QUE FORMAN PARTE DEL ESCENARIO

Tabla 1. Enrutamiento

	DIRECCION IPv4	MASCARA	GATEWAY IPv4
Servidor Internet	209.165.200.230	255.255.255.248	209.165.200.255
R1 a R2 s0/0/0 a s0/0/1	172.31.21.1	255.255.255.252	
R2 a R1 s0/0/1 a s0/0/0	172.31.21.2	255.255.255.252	
R2 a R3 s0/0/0 a s0/0/1	172.31.23.1	255.255.255.252	
R3 a R2 s0/0/1 a s0/0/0	172.31.23.2	255.255.255.252	
R2 a PC Internet f0/0	209.165.200.225	255.255.255.248	
R2 Servidor Web Lo0	10.10.10.1	255.255.255.255	
Lo4 R3	192.168.4.1	255.255.255.0	
Lo5 R3	192.168.5.1	255.255.255.0	
Lo6 R3	192.168.6.1	255.255.255.0	
SW1	192.168.99.2	255.255.255.0	
SW3 VLAN	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	

1.1.1 Configuración Direccionamiento Router R1

```

ena
config t
no ip domain-lookup
hostname R1
int s0/0/0
ip address 172.31.21.1 255.255.255.252
clock rate 128000
no shutdown
ip route 0.0.0.0 0.0.0.0 s0/0/0

```

1.1.2 Configuración Direccionamiento Router R2

```

ena
config t
no ip domain-lookup
hostname R2
int s0/0/1

```

```
ip address 172.31.21.2 255.255.255.252
no shutdown
clock rate 128000
int s0/0/0
ip address 172.31.23.1 255.255.255.252
clock rate 128000
no shutdown
int f0/0
description ISP conexion
ip address 209.165.200.225 255.255.255.248
no shutdown
int f0/1
ip add 10.10.10.1 255.255.255.0
no shutdown
exit
ip route 0.0.0.0 0.0.0.0 f0/0
```

1.1.3 Configuración Direcccionamiento Router R3

```
ena
config t
no ip domain-lookup
hostname R3
int s0/0/1
ip address 172.31.23.2 255.255.255.252
no shutdown
clock rate 128000
int lo4
ip address 192.168.4.1 255.255.255.0
no shutdown
int lo5
ip address 192.168.5.1 255.255.255.0
no shutdown
int lo6
ip address 192.168.6.1 255.255.255.0
no shutdown
ip route 0.0.0.0 0.0.0.0 s0/0/1
```

1.1.4 Configuración Direcccionamiento Switch S1

```
ena
config t
hostname S1
interface vlan 1
```

```

ip address 192.168.99.2 255.255.255.0
no shutdown
exit
ip default-gateway 192.168.99.1

```

1.1.5 Configuración Direccionamiento Switch S3

```

ena
config t
hostname S3
interface vlan 1
ip address 192.168.99.3 255.255.255.0
no shutdown
exit
ip default-gateway 192.168.99.1

```

1.2 CONFIGURAR EL PROTOCOLO DE ENRUTAMIENTO OSPFV2

Bajo los siguientes criterios:

Tabla 2. Criterios protocolo de enrutamiento 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

1.2.1 Configuración enrutamiento OSPFv2 Router R1

```

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 0.0.0.255 area 0
network 192.168.40.0 0.0.0.255 area 0
passive-interface f0/0.30
passive-interface f0/0.40
auto-cost reference-bandwidth 9500

```

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

12.2 Configuración enrutamiento OSPFv2 Router R2

```
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
network 209.165.200.224 0.0.0.31 area 0
passive-interface f0/0
auto-cost reference-bandwidth 9500
exit
int s0/0/0
bandwidth 256
int s0/0/1
bandwidth 256
ip ospf cost 9500
exit
```

1.2.3 Configuración enrutamiento OSPFv2 Router R3

```
router ospf 1
router-id 8.8.8.8
network 172.31.23.0 0.0.0.3 area 0
network 192.168.4.0 0.0.3.255 area 0
passive-interface lo4
passive-interface lo5
passive-interface lo6
auto-cost reference-bandwidth 9500
exit
int s0/0/0
bandwidth 256
int s0/0/1
bandwidth 256
ip ospf cost 9500
exit
```

1.3 VERIFICAR INFORMACIÓN DE OSPF

1.3.1 Visualizar tablas de enrutamiento y routers conectados por OSPFv2

Ilustración 2. Verificación OSPF

```
R2#show ip ospf neighbor

Neighbor ID      Pri   State           Dead Time   Address
Interface
8.8.8.8          0    FULL/ -         00:00:30   172.31.23.2
Serial0/0/0
1.1.1.1          0    FULL/ -         00:00:30   172.31.21.1
Serial0/0/1
R2#
```

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

Ilustración 3. Interfaces por OSPF

```
R2#show ip ospf interface

FastEthernet0/1 is up, line protocol is up
 Internet address is 10.10.10.1/24, Area 0
 Process ID 1, Router ID 209.165.200.225, Network Type BROADCAST, Cost: 1
 Transmit Delay is 1 sec, State DR, Priority 1
 Designated Router (ID) 209.165.200.225, Interface address 10.10.10.1
 No backup designated router on this network
 Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
   Hello due in 00:00:00
 Index 1/1, flood queue length 0
 Next 0x0(0)/0x0(0)
 Last flood scan length is 1, maximum is 1
 Last flood scan time is 0 msec, maximum is 0 msec
 Neighbor Count is 0, Adjacent neighbor count is 0
 Suppress hello for 0 neighbor(s)
Serial0/0/1 is up, line protocol is up
 Internet address is 172.31.21.2/30, Area 0
 Process ID 1, Router ID 209.165.200.225, Network Type POINT-TO-POINT, Cost: 9500
 Transmit Delay is 1 sec, State POINT-TO-POINT, Priority 0
 No designated router on this network
 No backup designated router on this network
 Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
```



```

Hello due in 00:00:09
Index 2/2, flood queue length 0
Next 0x0(0)/0x0(0)
Last flood scan length is 1, maximum is 1
Last flood scan time is 0 msec, maximum is 0 msec
Neighbor Count is 1 , Adjacent neighbor count is 1
  Adjacent with neighbor 1.1.1.1
  Suppress hello for 0 neighbor(s)
Serial0/0/0 is up, line protocol is up
Internet address is 172.31.23.1/30, Area 0
Process ID 1, Router ID 209.165.200.225, Network Type POINT-TO-POINT, Cost: 6152
Transmit Delay is 1 sec, State POINT-TO-POINT, Priority 0
No designated router on this network
No backup designated router on this network
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
  Hello due in 00:00:00
Index 3/3, flood queue length 0
Next 0x0(0)/0x0(0)
Last flood scan length is 1, maximum is 1
Last flood scan time is 0 msec, maximum is 0 msec
Neighbor Count is 1 , Adjacent neighbor count is 1
  Adjacent with neighbor 8.8.8.8
  Suppress hello for 0 neighbor(s)

```

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

Ilustración 4. Protocolos Router R1

```

R1#show ip protocol

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
  Passive Interface(s):
    FastEthernet0/0.30
    FastEthernet0/0.40
  Routing Information Sources:
    Gateway         Distance      Last Update
    1.1.1.1          110          00:07:31
    8.8.8.8          110          00:07:41
    209.165.200.225 110          00:07:31
  Distance: (default is 110)

```

Ilustración 5. Protocolos Router R1

```
R2#sh 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 209.165.200.225
  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):
    FastEthernet0/0
  Routing Information Sources:
    Gateway         Distance      Last Update
    1.1.1.1          110          00:06:13
    8.8.8.8          110          00:06:23
    209.165.200.225 110          00:06:12
  Distance: (default is 110)
```

Ilustración 6. Protocolos Router R3

```
R3#sh 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          00:07:02
    8.8.8.8          110          00:07:11
    209.165.200.225 110          00:07:01
  Distance: (default is 110)
```

1.4 CONFIGURAR VLANS, PUERTOS TRONCALES, PUERTOS DE ACCESO, ENCAPSULAMIENTO, INTER-VLAN ROUTING Y SEGURIDAD EN LOS SWITCHES ACORDE A LA TOPOLOGÍA DE RED ESTABLECIDA.

1.4.1 Configuración Switch S1

```
enable secret cisco
line console 0
pass cisco
line vty 0 4
pass cisco
login
exit
service password-encryption
exit
```

```
config t
vlan 30
name ADMINISTRACION
vlan 40
name MERCADEO
```

```
int f0/3
switchport mode trunk
switchport trunk native vlan 1
int f0/24
switchport mode trunk
switchport trunk native vlan 1
interface range fa0/1-2, fa0/4-23
switchport mode access
int f0/1
switchport mode access
switchport access vlan 30
int range fa0/2, fa0/4-23
shutdown
```

1.4.2 Configuración Switch S3

```
enable secret cisco
line console 0
pass cisco
line vty 0 4
pass cisco
login
```

```
exit
service password-encryption
exit
```

```
config t
vlan 30
name ADMINISTRACION
vlan 40
name MERCADEO
```

```
int f0/3
switchport mode trunk
switchport trunk native vlan 1
interface range fa0/1
switchport mode access
sw access vlan 40
```

1.5 EN EL SWITCH 3 DESHABILITAR DNS LOOKUP

```
Config t
no ip domain-lookup
```

1.6 ASIGNAR DIRECCIONES IP A LOS SWITCHES ACORDE A LOS LINEAMIENTOS.

1.6.1 Configuración Direccionamiento Switch S1

```
interface vlan 1
ip address 192.168.99.2 255.255.255.0
no shutdown
exit
ip default-gateway 192.168.99.1
```

1.6.2 Configuración Direccionamiento Switch S3

```
interface vlan 1
ip address 192.168.99.3 255.255.255.0
no shutdown
exit
ip default-gateway 192.168.99.1
```

1.7 DESACTIVAR TODAS LAS INTERFACES QUE NO SEAN UTILIZADAS EN EL ESQUEMA DE RED.

1.7.1 Desactivación puertos en Switch S1

```
int f0/1
int range fa0/2, fa0/4-23
shutdown
```

1.7.2 Desactivación puertos en Switch S3

```
int f0/1
int range fa0/2, fa0/4-24
shutdown
```

1.8 IMPLEMENT DHCP AND NAT FOR IPV4 Y CONFIGURARE R1 COMO SERVIDOR DHCP PARA LAS VLANS 30 Y 40.

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.

```
int f0/0.30
description VLAN ADMIN
encapsulation dot1q 30
ip address 192.168.30.1 255.255.255.0
exit
```

```
int f0/0.40
description VLAN MERCA
encapsulation dot1q 40
ip address 192.168.40.1 255.255.255.0
exit
```

```
ip dhcp pool vlan30
```

```
dns-server 10.10.10.11
default-router 192.168.30.1
network 192.168.30.0 255.255.255.0
ip domain-name ccna-unad.com
```

```
ip dhcp pool vlan40
dns-server 10.10.10.11
default-router 192.168.40.1
network 192.168.40.0 255.255.255.0
ip domain-name ccna-unad.com
```

1.9 RESERVAR LAS PRIMERAS 30 DIRECCIONES IP DE LAS VLAN 30 Y 40 PARA CONFIGURACIONES ESTÁTICAS.

```
ip dhcp excluded-address 192.168.30.2 192.168.30.31
ip dhcp excluded-address 192.168.40.2 192.168.40.31
```

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

```
int s0/0/1
ip nat inside
int f0/1
ip nat inside
int s0/0/0
ip nat inside
int f0/0
ip nat outside
ip nat pool INTERNET 209.165.200.225 209.165.200.225 netmask
255.255.255.224
access-list 01 permit 192.168.0.0 0.0.255.255
access-list 02 permit 172.31.0.0 0.0.255.255
access-list 03 permit 10.10.10.0 0.0.0.255

ip nat inside source list 01 pool INTERNET overload
ip nat inside source list 02 pool INTERNET overload
ip nat inside source list 03 pool INTERNET overload
```

1.9.2 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.

```
access-list 10 permit 172.31.21.0 0.0.0.3
access-list 10 permit 172.31.23.0 0.0.0.3
access-list 10 deny any
line vty
line vty 0 4
login
transport input telnet
access-class 10 in
```

1.9.3 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.

```
access-list 11 permit tcp 172.31.23.0 0.0.0.3 any eq 80
access-list 11 permit tcp 172.31.23.0 0.0.0.3 any eq 443
access-list 12 permit tcp 172.31.21.0 0.0.0.3 any eq 80
access-list 12 permit tcp 172.31.21.0 0.0.0.3 any eq 443
int s0/0/1
ip access-group 12 in
int s0/0/0
ip access-group 11 in
```

1.10 VERIFICAR PROCESOS DE COMUNICACIÓN Y REDIRECCIONAMIENTO DE TRÁFICO EN LOS ROUTERS MEDIANTE EL USO DE PING Y TRACEROUTE.

Ilustración 7 Lista acceso Router R2

```
R2#sh 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
Extended IP access list 101
 10 permit tcp any host 209.165.200.229 eq www
 20 permit icmp any any echo-reply
```

Ilustración 8. Ping de Router 1 a PC-Internet

```
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 80 percent (4/5), round-trip min/avg/max = 1/6/23
ms
```

Ilustración 9. Conexión de Router R1 a Router R2 y R3

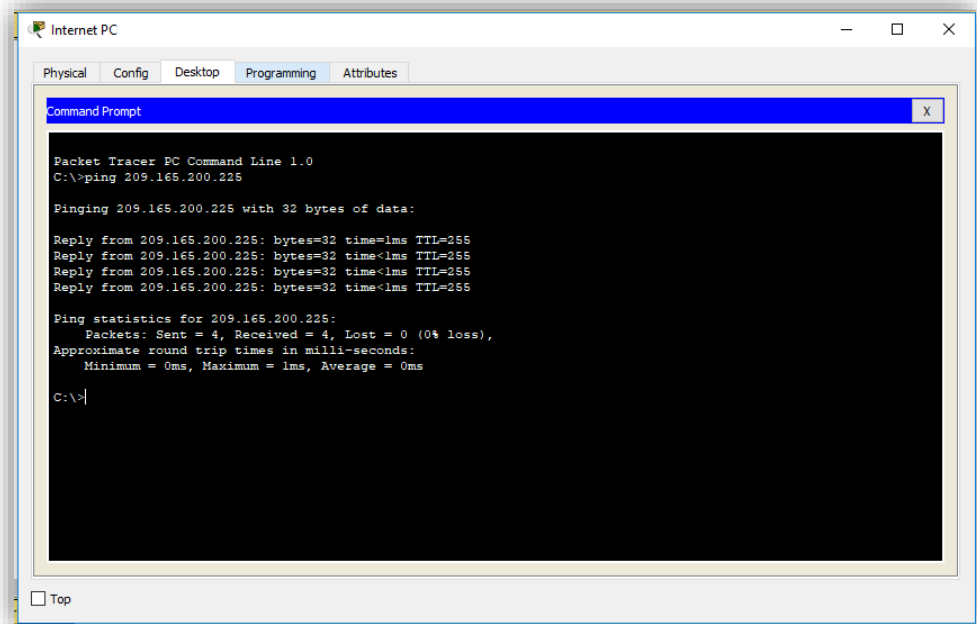
```
R1#ping 172.31.21.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.31.21.2, timeout is 2
seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max =
1/3/11 ms

R1#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 =
1/4/13 ms
```


Ilustración 10. Ping Internet PC



The screenshot shows a window titled "Internet PC" with tabs for Physical, Config, Desktop, Programming, and Attributes. A Command Prompt window is open, displaying the output of a ping command to 209.165.200.225. The output shows four successful replies with 0% loss and 0ms round trip times.

```
Packet Tracer PC Command Line 1.0
C:\>ping 209.165.200.225

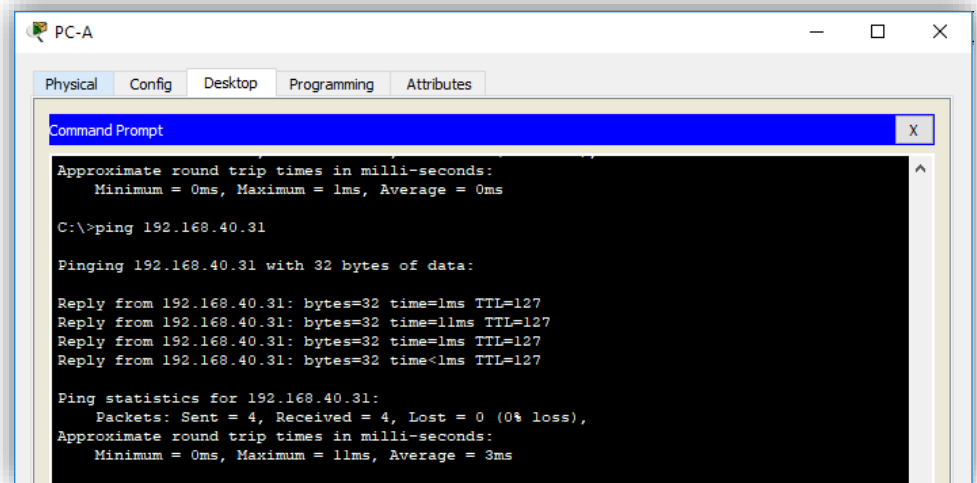
Pinging 209.165.200.225 with 32 bytes of data:

Reply from 209.165.200.225: bytes=32 time=1ms TTL=355
Reply from 209.165.200.225: bytes=32 time<1ms TTL=355
Reply from 209.165.200.225: bytes=32 time<1ms TTL=355
Reply from 209.165.200.225: bytes=32 time<1ms TTL=355

Ping statistics for 209.165.200.225:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>
```

Ilustración 11. Ping PC-A a PC-B



The screenshot shows a window titled "PC-A" with tabs for Physical, Config, Desktop, Programming, and Attributes. A Command Prompt window is open, displaying the output of a ping command to 192.168.40.31. The output shows four successful replies with 0% loss and 1ms round trip times.

```
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

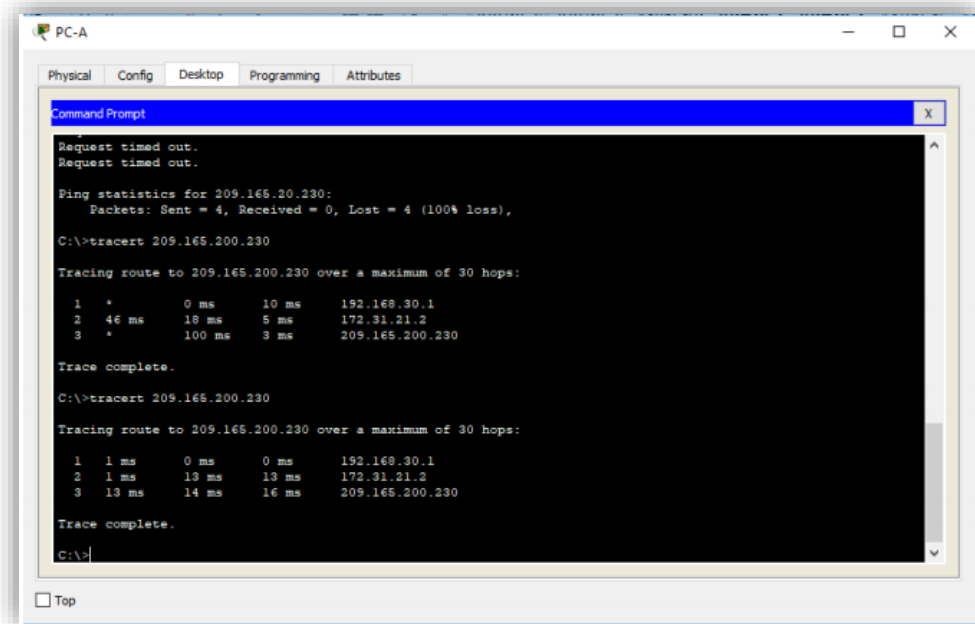
C:\>ping 192.168.40.31

Pinging 192.168.40.31 with 32 bytes of data:

Reply from 192.168.40.31: bytes=32 time=1ms TTL=127
Reply from 192.168.40.31: bytes=32 time=11ms TTL=127
Reply from 192.168.40.31: bytes=32 time=1ms TTL=127
Reply from 192.168.40.31: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.40.31:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 11ms, Average = 3ms
```

Ilustración 12. Tracert del PC-A a Internet PC



```
PC-A
Physical Config Desktop Programming Attributes
Command Prompt
Request timed out.
Request timed out.

Ping statistics for 209.165.20.230:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>tracert 209.165.200.230

Tracing route to 209.165.200.230 over a maximum of 30 hops:

  0  *         0 ms    10 ms   192.168.30.1
  1  46 ms    18 ms    5 ms   172.31.21.2
  2  *         100 ms   3 ms   209.165.200.230

Trace complete.

C:\>tracert 209.165.200.230

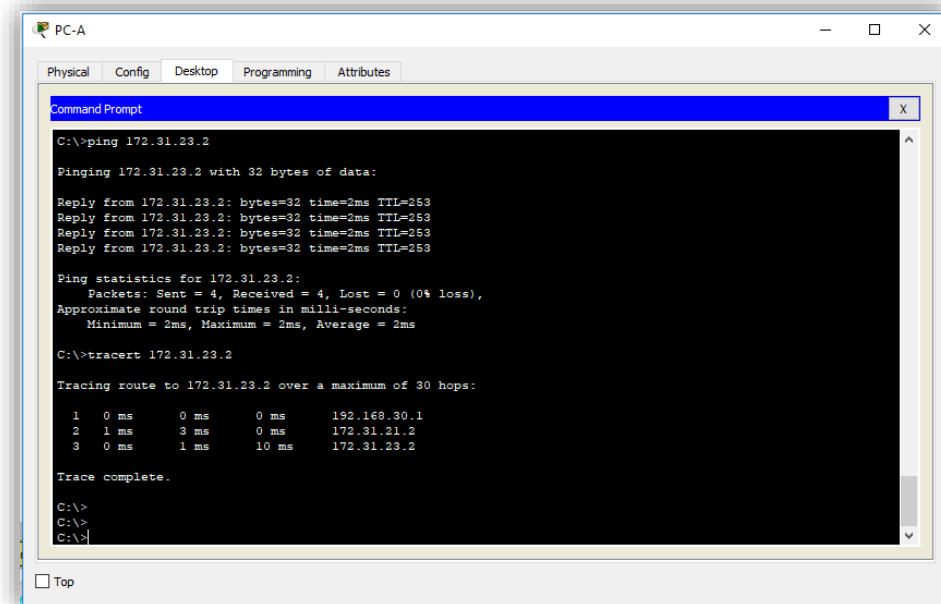
Tracing route to 209.165.200.230 over a maximum of 30 hops:

  0  1 ms     0 ms     0 ms   192.168.30.1
  1  1 ms    13 ms   13 ms   172.31.21.2
  2  13 ms  14 ms   16 ms   209.165.200.230

Trace complete.

C:\>
```

Ilustración 13. Comando Tracert y Ping desde PC-A a Router R3



```
PC-A
Physical Config Desktop Programming Attributes
Command Prompt
C:\>ping 172.31.23.2

Pinging 172.31.23.2 with 32 bytes of data:

Reply from 172.31.23.2: bytes=32 time=2ms TTL=253
Reply from 172.31.23.2: bytes=32 time=2ms TTL=253
Reply from 172.31.23.2: bytes=32 time=2ms TTL=253
Reply from 172.31.23.2: bytes=32 time=2ms TTL=253

Ping statistics for 172.31.23.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 2ms, Average = 2ms

C:\>tracert 172.31.23.2

Tracing route to 172.31.23.2 over a maximum of 30 hops:

  0  0 ms     0 ms     0 ms   192.168.30.1
  1  1 ms     3 ms     0 ms   172.31.21.2
  2  0 ms     1 ms    10 ms   172.31.23.2

Trace complete.

C:\>
C:\>
C:\>
```

Ilustración 14. Prueba conectividad a Servidor Web desde PC-C

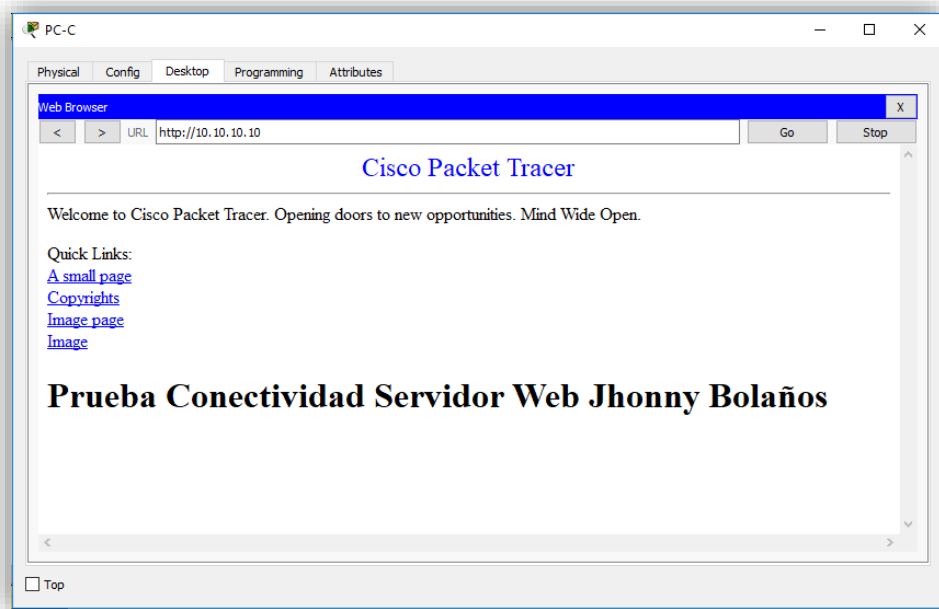


Ilustración 15. Comando Tracert y Ping desde la PC-C a Internet PC

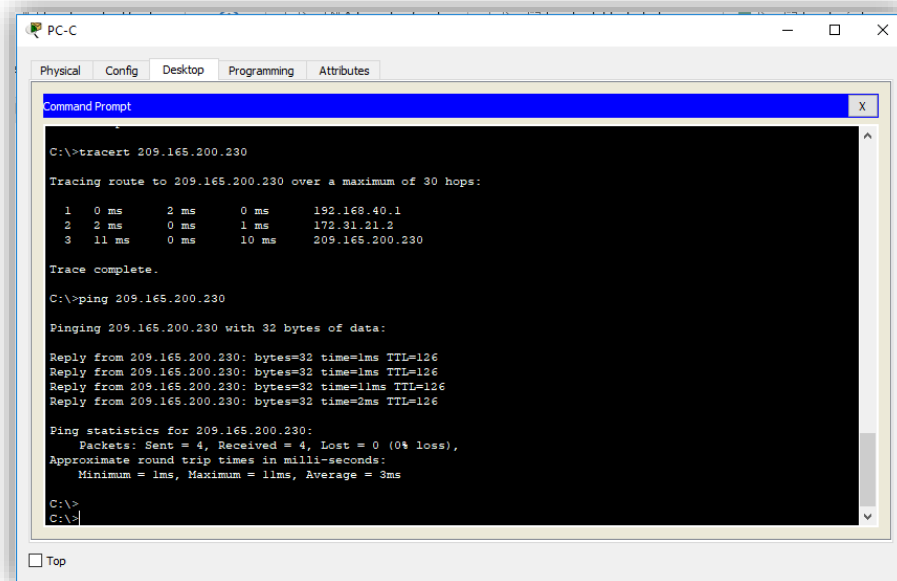
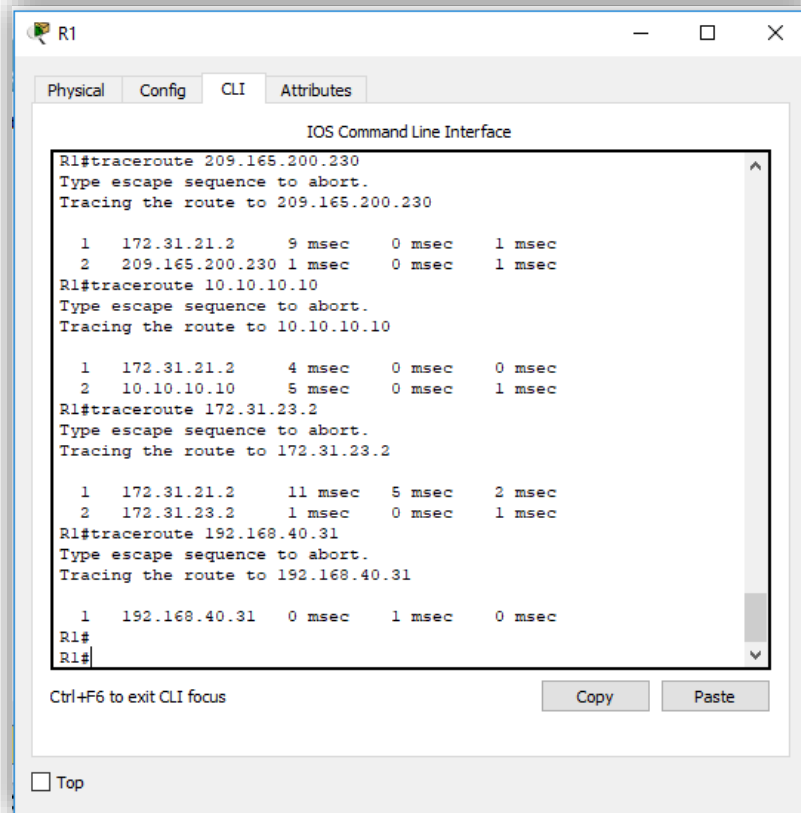


Ilustración 16. Comando tracert desde el Router R1 a Internet PC, Web Server y PC-C



2. ESCENARIO 2

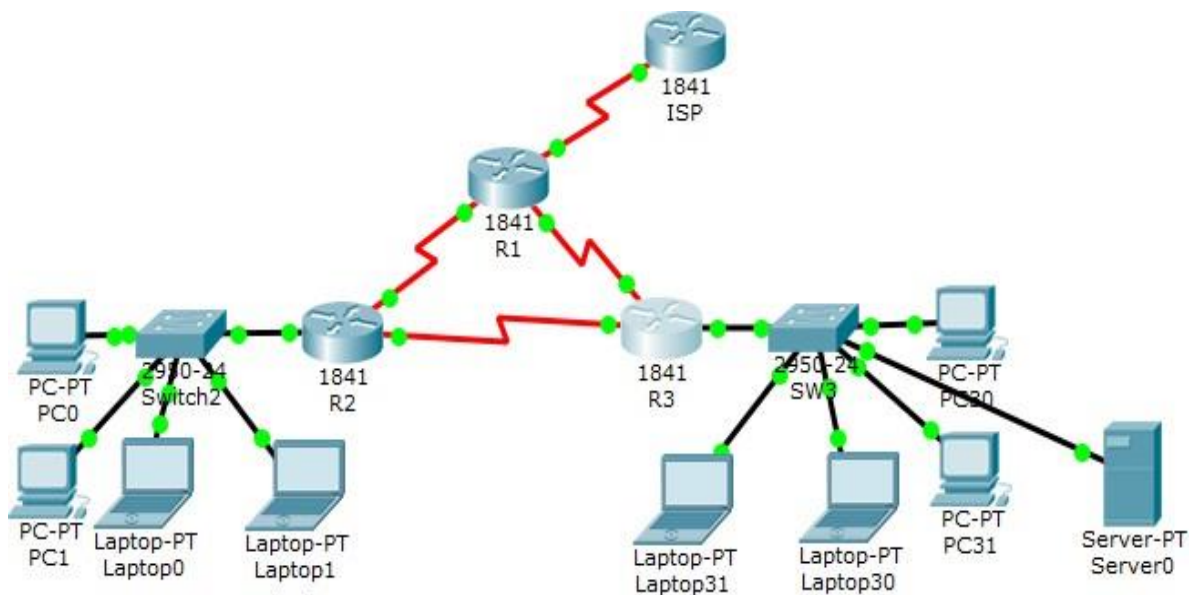


Tabla 3. Direcccionamiento

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

Continuación Tabla 3

El administrador	Interfaces	Dirección IP	Máscara de subred	Gateway predeterminado
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 4. Asignación de VLAN y de puertos

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

Tabla 5. Enlaces troncales

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

Situación

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.

2.1 SW1 VLAN Y LAS ASIGNACIONES DE PUERTOS DE VLAN

2.1.1 Configuración SW2

```
ena
config t
hostname SW1

vlan 100
name LAPTOPS
vlan 200
name DESKTOP

int range f0/2-3
switchport mode access
switchport access vlan 100
no shu

int range f0/4-5
switchport mode access
switchport access vlan 200
no shu

interface f0/1
switchport mode trunk
```

2.1.2 Configuración SW3

```
ena
config t
hostname SW3

int range f0/2-7
switchport mode access
switchport access vlan 1
no shu
```

2.2 DESHABILITAR PUERTOS DE RED NO UTILIZADOS.

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

2.2.1 Deshabilitar puertos SW2

```
int range f0/6-24  
shut
```

2.2.2 Configuración puertos SW3

```
int range f0/7-24  
shut
```

2.3 CONFIGURACIÓN DE ROUTER.

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

2.3.1 Configuración Router R1

```
ena  
config t  
hostname R1  
int s0/0/0  
ip add 200.123.211.2 255.255.255.0  
no shut  
int s0/1/0  
ip address 10.0.0.1 255.255.255.252  
no shut  
int s0/1/1  
ip address 10.0.0.5 255.255.255.252  
no shut
```

2.3.2 Configuración Router R2

```
ena  
config t  
hostname R2  
int s0/0/0  
ip add 10.0.0.2 255.255.255.252  
no shut  
int s0/0/1  
ip add 10.0.0.9 255.255.255.252  
no shut
```

2.3.3 Configuración Router R3

```
ena  
config t
```



```
hostname R3
int s0/0/0
ip add 10.0.0.6 255.255.255.252
no shut
int s0/0/1
ip add 10.0.0.10 255.255.255.252
no shut
```

2.3.4 Configuración Router ISP

```
ena
config t
hostname ISP
int s0/0/0
ip add 200.123.211.1 255.255.255.0
no shut
```

2.4 CONFIGURACIÓN SERVIDOR DHCP IPV4.

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

2.4.1 Configuración DHCP Router R2

```
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
```

```
int f0/0.100
encap dot1q 100
ip add 192.168.20.1 255.255.255.0
no shut
```

```
int f0/0.200
encap dot1q 200
ip add 192.168.21.1 255.255.255.0
no shut
```

```
int f0/0
no shut
```

2.4.2 Configuración DHCP Router R3

```
ip dhcp pool vlan1
network 192.168.30.1 255.255.255.0
default-router 192.168.30.1
```

2.5 CONFIGURACIÓN DE NAT CON SOBRECARGA.

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.

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

Ilustración 17. Comando Ping desde los PC vlan 100 y 200 al ISP

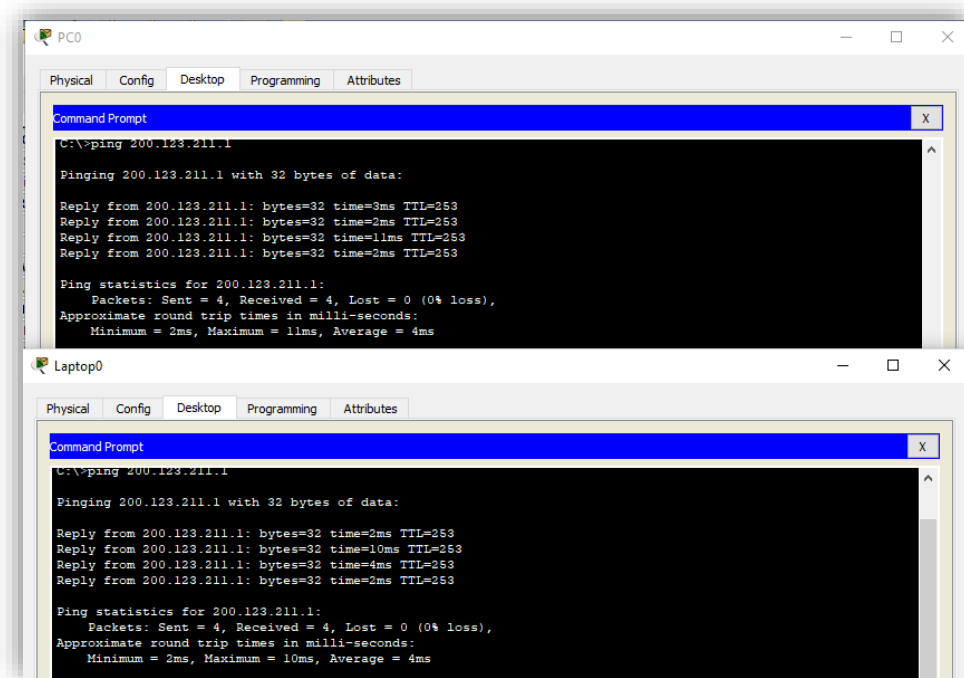
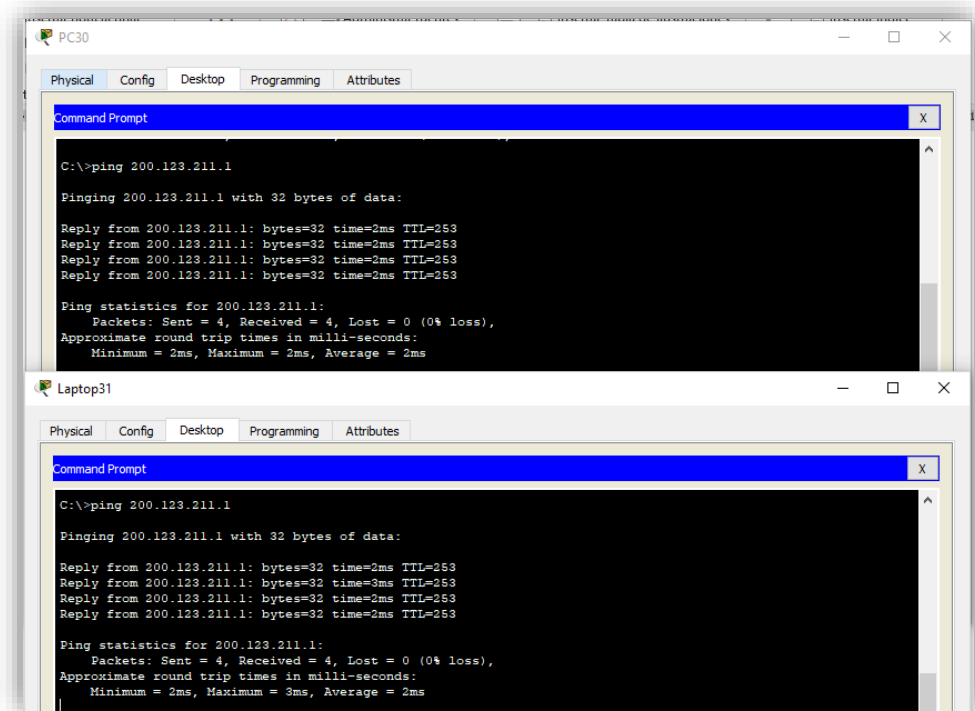


Ilustración 18. Comando Ping desde los PC vlan 1 al ISP



2.6 CREACIÓN RUTA ESTÁTICA.

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

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

2.7 CONFIGURACIÓN ROUTER COMO SERVIDOR DHCP.

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

```
ip dhcp excluded-address 10.0.0.2 10.0.0.9  
ip dhcp pool INSIDE-DEVS
```

```
network 192.168.20.1 255.255.255.0
network 192.168.21.1 255.255.255.0
default-router 192.168.1.1
dns-server 0.0.0.0
```

2.8 ENRUTAMIENTO DE VLAN.

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

```
interface vlan 100
ip address 192.168.20.1 255.255.255.0
interface vlan 200
ip address 192.168.21.1 255.255.255.0
```

2.9 RESTRICCIÓN ACCESO A SERVIDOR.

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

Ilustración 19. Comando ping desde la red del router R3 hacia el Server0

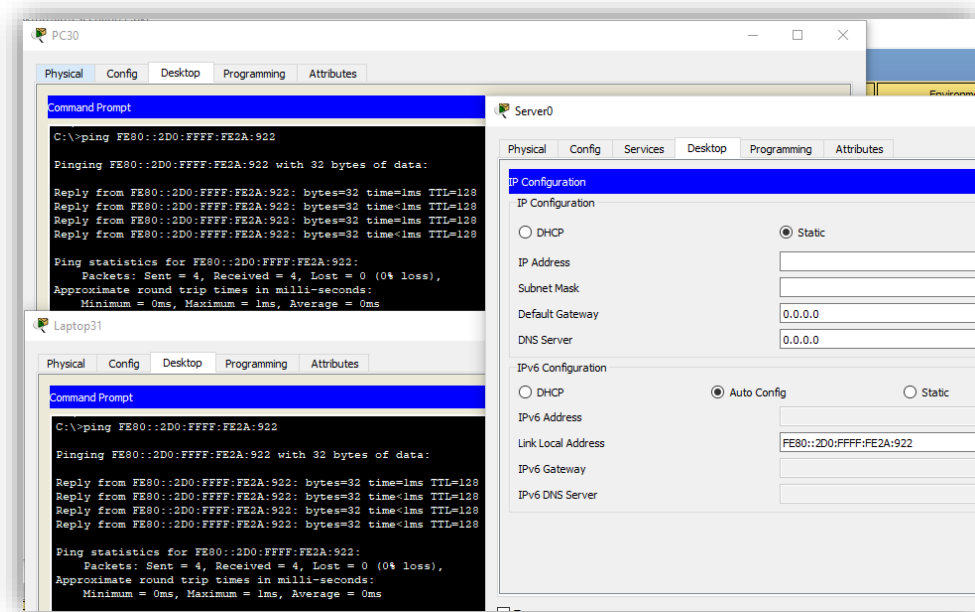
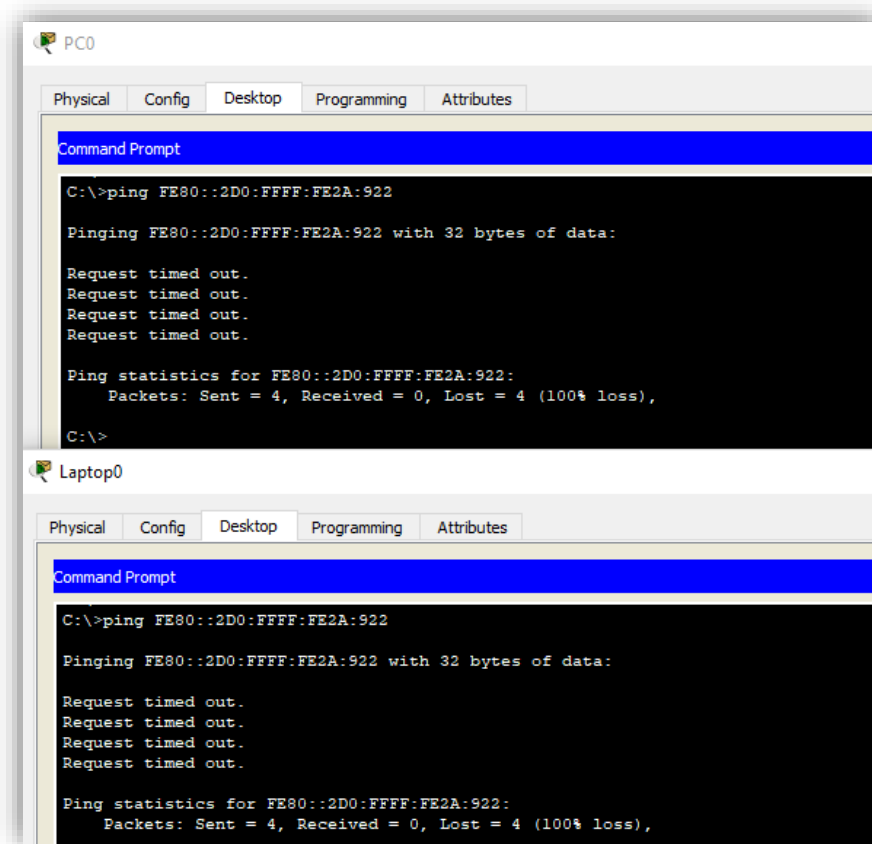


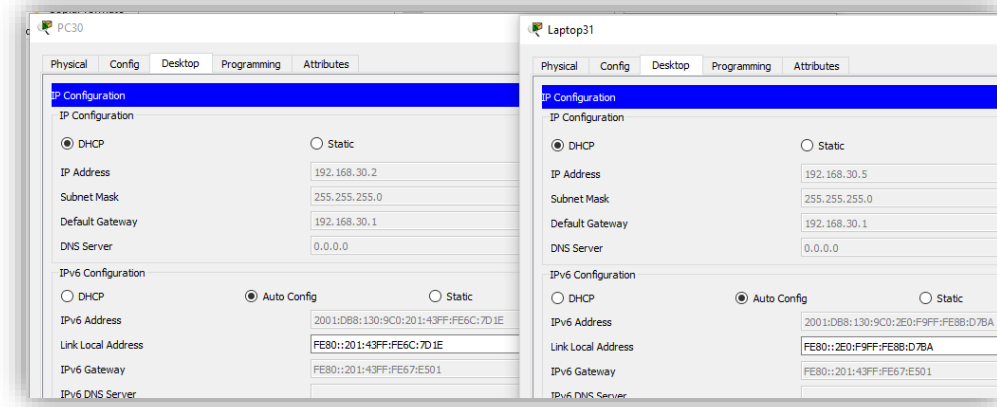
Ilustración 20. Comando ping desde la red del Router R2 hacia el server0 (Sin conexión)



2.10 CONFIGURACIÓN DUAL STACK EN NIC.

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.

Ilustración 21. Validación de Dual-stack en red del router R3



2.11 CONFIGURACIÓN DUAL STACK EN INTERFAZ.

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

```
ip dhcp pool vlan1
network 192.168.30.1 255.255.255.0
default-router 192.168.30.1
interface Fa0/0
ipv6 add 2001:db8:130::9C0:80F:301/64
no shut
ipv6 dhcp pool vlan1
dns-server 2001:DB8:130::
```

```
ipv6 unicast-routing
interface Fa0/0
ipv6 enable
ip add 192.168.30.1 255.255.255.0
ipv6 address 2001:db8:130:9C0:80F::301/64
no shut
```

2.12 CONFIGURACIÓN RIP VERSIÓN 2.

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

2.12.1 Configuración Router R1, R2 y R3

```
router rip  
version 2
```

2.13 ENRUTAMIENTO ENTRE ROUTER.

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

2.13.1 Configuración Router R1

```
network 10.0.0.4  
network 10.0.0.0  
default-information originate
```

2.13.2 Configuración Router R2

```
network 10.0.0.0  
network 10.0.0.8  
network 192.168.30.0  
network 192.168.20.0  
network 192.168.21.0
```

2.13.3 Configuración Router R3

```
network 192.168.0.0  
network 10.0.0.8  
network 10.0.0.4
```

2.14 VERIFICACIÓN DE CONECTIVIDAD.

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 22. Comando ping desde la red del router R2 hacia el ISP

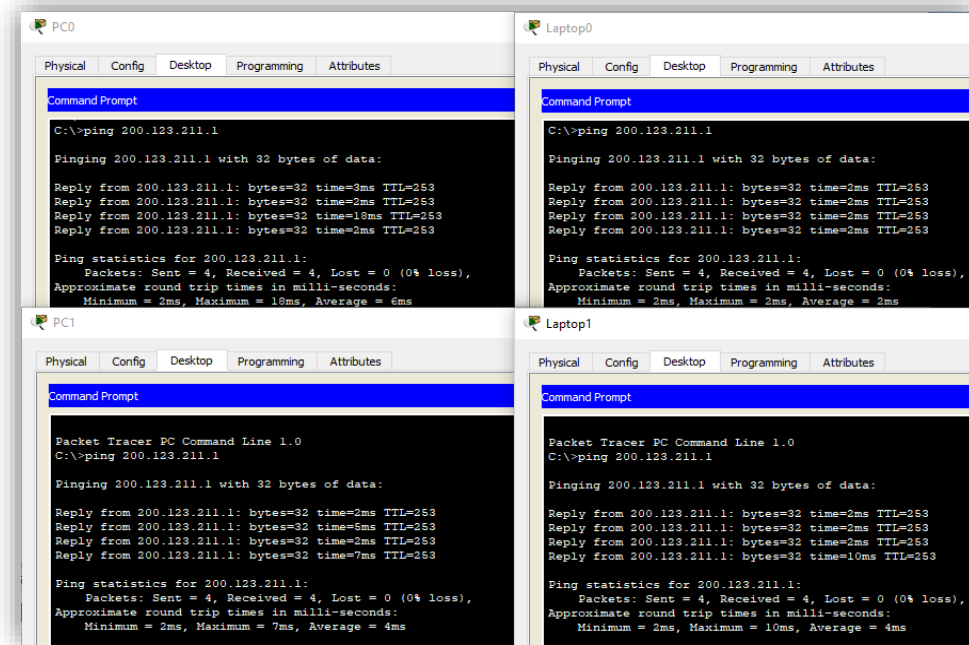


Ilustración 23. Conectividad Router R1, R2 y R3 hacia el ISP

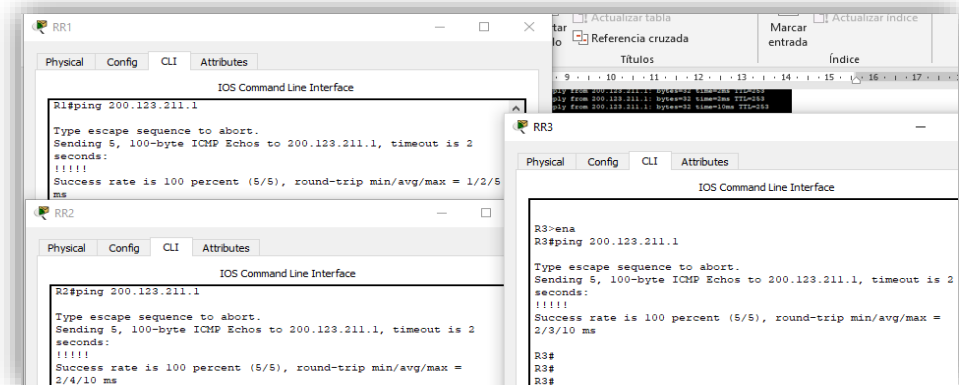


Ilustración 24. Comando ping desde la red del router R3 hacia el ISP

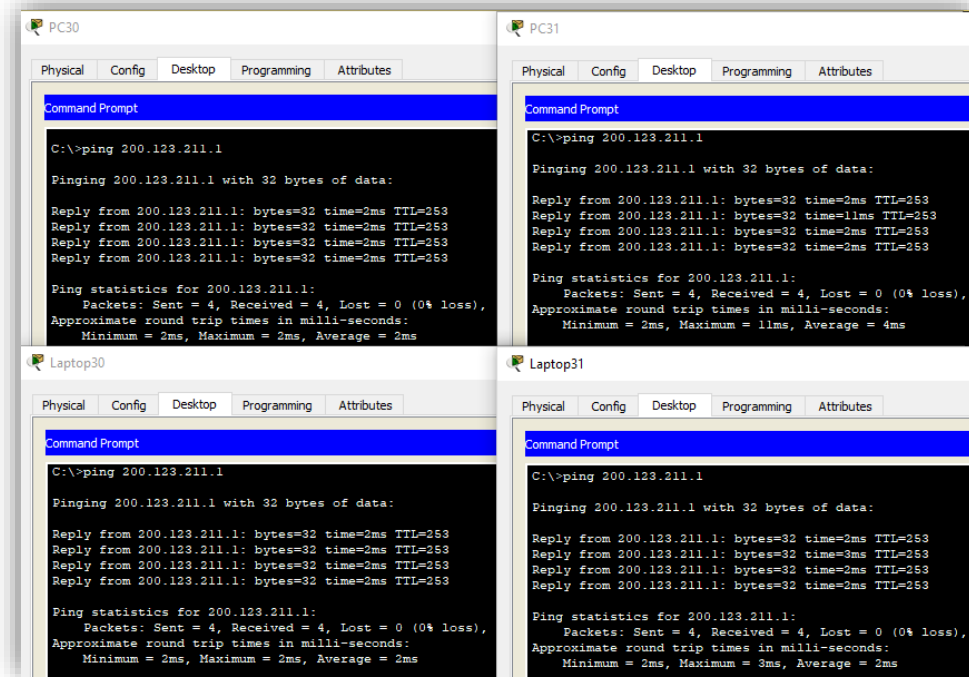


Ilustración 25. Comando ping desde la red del Router R3 hacia el Server0

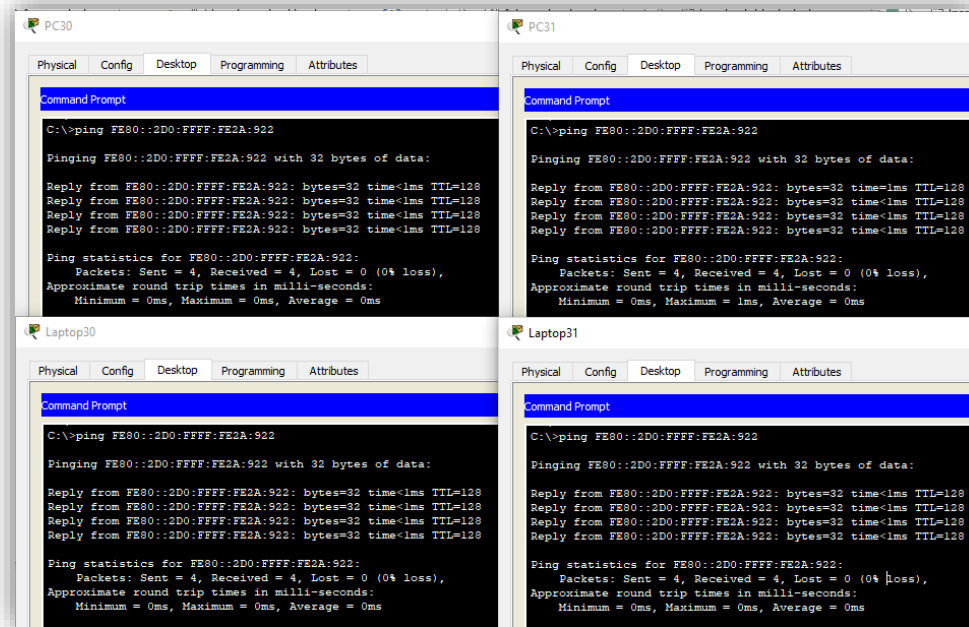


Ilustración 26. Comando ping entre la red del router R3

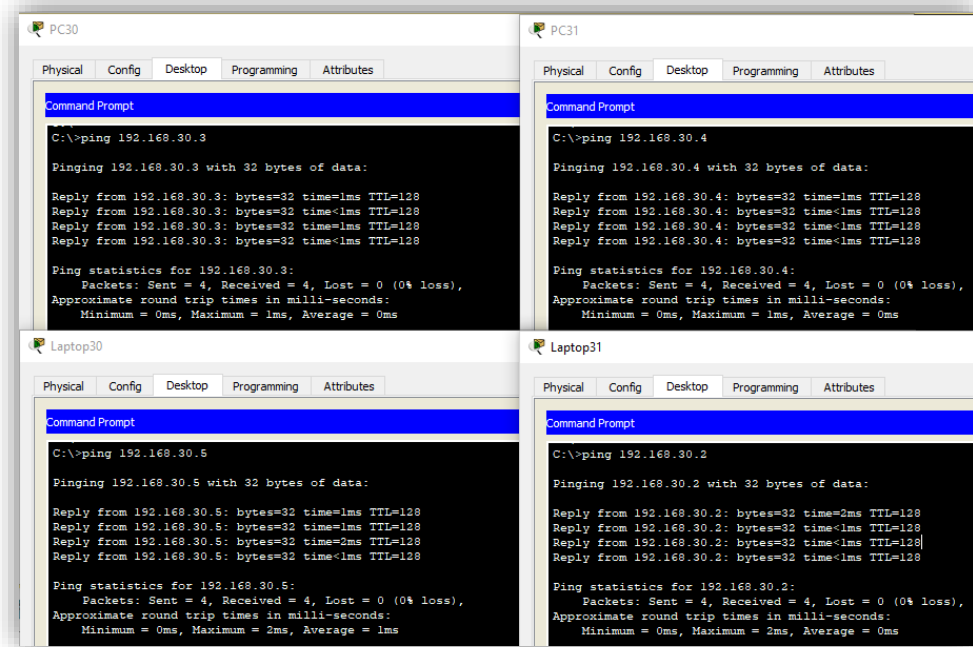
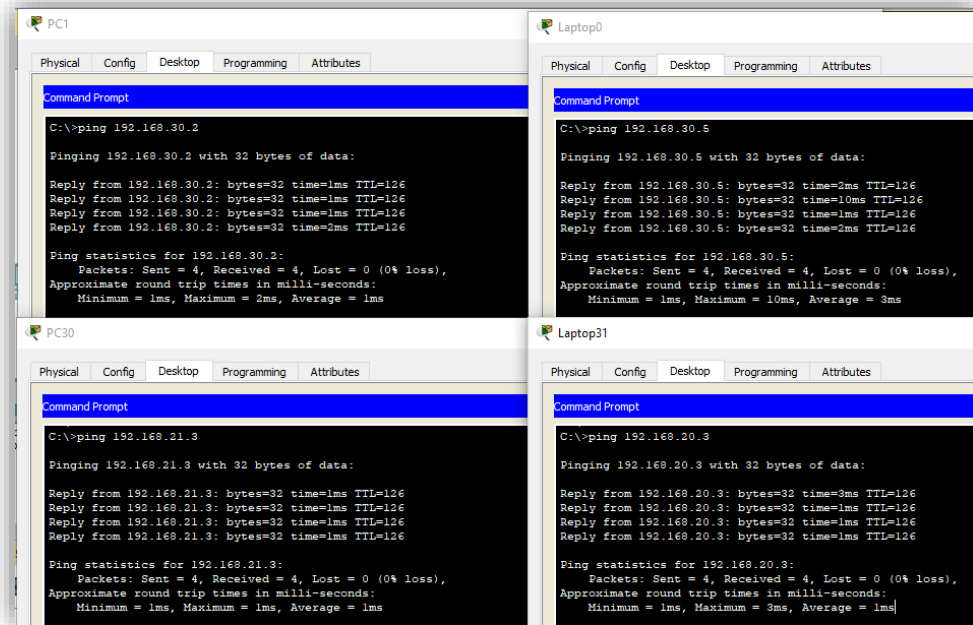


Ilustración 27. Comando ping entre host de la red de los router R2 y R3



3. CONCLUSIONES

Se realizó la configuración, la aplicación y la verificación de acuerdo a la implementación ACL para la red, así mismo se verificó que la implementación del acceso a la lista de control (ACL) se realizó correctamente de acuerdo a lo requerido.

Se configuraron los parámetros básicos de los dispositivos, armando una red con diferentes dispositivos implementando su configuración en dhcp4 y al igual para las VLAN, configurando también el routing IP.

Se estableció la configuración dhcp para ipv4 en un router cisco y se remarcó la importancia del uso del NAT en las redes internas, así como sacar un máximo aprovechamiento y las grandes cualidades que nos ofrece.

Comprendimos como las listas ACL IP pueden filtrar el tráfico de la red, y los tipos de ACL, así como también la configuración en los dispositivos Cisco.

Se trabajó con el protocolo OSPF el cual es muy parecido a RIP, con la diferencia que los paquetes son enviados por el camino más corto, ya que su configuración utiliza direcciones de los router más cercanos conociendo así el número de saltos entre router y router

Se reforzó el tema del DHCP el cual permite realizar la administración menos compleja de la red, evitando posibles conflictos y malas configuraciones en los hosts.

Fue necesario NAT para enmascarar la red interna y poder salir a través de una única dirección pública a internet, obteniendo con esto grandes ahorros en direcciones IPv4, Afortunadamente se ha resuelto el problema con IPv6.

Se fortaleció el uso de simulador packet tracer par estas actividades, así mismo se reforzó los temas vistos anteriormente

BIBLIOGRAFIA

Archivo. pkt de los escenarios 1 y 2 Disponible en internet:
https://drive.google.com/file/d/1YF3U2YmiyjwQtDZBuBnDu_TGhluN9PNR/view?usp=sharing

CISCO. Enrutamiento Dinámico. Principios de Enrutamiento y Conmutación. 2014. Disponible en internet: <https://static-course-assets.s3.amazonaws.com/RSE50ES/module7/index.html#7.0.1.1>

CISCO. DHCP. Principios de Enrutamiento y Conmutación. 2014. Disponible en internet: <https://static-course-assets.s3.amazonaws.com/RSE50ES/module10/index.html#10.0.1.1>

Odom, W. CISCO Press (Ed). CCNA ICND2 Official Exam Certification Guide. 2013. Disponible en internet: <http://een.iust.ac.ir/profs/Beheshti/Computer%20networking/Auxiliary%20materials/Cisco-ICND2.pdf>

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

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

CISCO. OSPF de una sola área. Principios de Enrutamiento y Conmutación. 2014. Disponible en internet: <https://static-course-assets.s3.amazonaws.com/RSE50ES/module8/index.html#8.0.1.1>

CISCO. Soluciones de Red. Fundamentos de Networking. 2014. Disponible en internet: <https://static-course-assets.s3.amazonaws.com/ITN50ES/module11/index.html#11.0.1.1>

LUCAS, Michael. Cisco Routers for the Desperate: Router and Switch Management, the Easy Way. 2 ed. San Francisco: No Starch Press, 2009. Disponible en internet: <https://1drv.ms/b/s!AmlJYei-NT1Im3L74BZ3bpMiXRx0>