

Prueba De Habilidades Prácticas CCNA

Diplomado De Profundización Cisco (Diseño E Implementación De Soluciones Integradas Lan / Wan)

Luis Mosos Ladino

Cod. 9.726.724

**Universidad Nacional Abierta Y A Distancia
Escuela De Ciencias Básicas Tecnología E Ingeniería
Programa Ingeniería De Sistemas
Diplomado De Profundización Cisco
Bogotá D.C.
Mayo de 2018**

Prueba De Habilidades Prácticas CCNA

Diplomado De Profundización Cisco (Diseño E Implementación De Soluciones Integradas Lan / Wan)

Luis Mosos Ladino

Cod. 9.726.724

**Trabajo escrito para optar por el título de:
Ingeniería De Sistemas**

Tutor

Ing. Efrain Alejandro Perez

Director de Diplomado

PhD. Juan Carlos Vesga Ferreira

**Universidad Nacional Abierta Y A Distancia
Escuela De Ciencias Básicas Tecnología E Ingeniería
Programa Ingeniería De Sistemas
Diplomado De Profundización Cisco
Bogotá D.C.
Mayo de 2018**

Dedicatoria

Mi trabajo final lo dedico con todo mi corazón a Dios por darme la capacidad intelectual y física de afrontar este proyecto de estudio, llenando mi vida de bendiciones y poniendo en mis manos todas las herramientas para culminar esta etapa de conocimiento.

A mi esposa y mis hijos por brindarme el espacio de sus vidas y entregar su energía emocional para impulsar mis sueños.

A mis padres y hermanos que han estado a mi lado concediéndome el apoyo necesario para no desfallecer y continuar adelante.

Y muy especialmente a todas las personas que han creído en mí...

Tabla De Contenido

Lista de Tablas	5
Lista de Figuras	6
Glosario	8
Resumen	10
Introducción	11
Objetivo General	12
Objetivos específicos	12
1. Descripción Del Escenario Propuesto Para La Prueba De Habilidades	13
1.2. Requerimientos para el desarrollo del escenario propuesto para la prueba de habilidades	14
2. Desarrollo Del Escenario Propuesto Para La Prueba De Habilidades Prácticas	16
2.1. Implementación de la topología de red en software Packet Tracer 6.1.1.0001	16
2.1.1. Tabla de direccionamiento	17
2.2. Configuración del direccionamiento IP acorde con la topología de red	18
2.3. Configuración de VLANs, Puertos troncales, puertos de acceso, encapsulamiento, Inter-VLAN Routing y Seguridad en los Switches acorde a la topología de red establecida	25
2.4. Configuración del protocolo de enrutamiento OSPFv2	28
2.5. Tablas de enrutamiento y routers conectados por OSPFv2	31
2.6. Lista resumida de interfaces por OSPF en en la cual se ilustra el costo de cada interface 34	
2.7. Lista de la información de OSPF Process ID, Router ID, Address summarizations, Routing Networks, and passive interfaces configured en cada router	39
2.8. Inhabilitación del DNS lookup en el swicht S1	42
2.9. Implementación de DHCP y NAT para IPv4	43
2.10. Configurar NAT en R2 para permitir que los hosts puedan salir a internet	44
2.11. Configuración de las listas de acceso estándar y dinámicas	45
2.12. Verificación de procesos de comunicación	46
Conclusiones	52
Referencias Bibliográficas	53

Lista de Tablas

Tabla 1. Cuadro de datos propuesto para la configuración del protocolo de enrutamiento OSPFv2.	14
Tabla 2. Cuadro de datos propuesto para la configuración de DHCP pool para VLAN 30 y VLAN 40.	15
Tabla 3. Tabla de direccionamiento implementado.....	17

Lista de Figuras

Figura 1. topología de red propuesta	13
Figura 2. Implementación de la topología de red propuesta sobre el software Packet Tracer 6.1.1.0001	17
Figura 3. Configuración dispositivo Internet PC	18
Figura 4. Configuración Router R1	19
Figura 5. Configuración Router R1	20
Figura 6. Configuración Router R3	21
Figura 7. Configuración Switch S1.	22
Figura 8. Configuración Switch S2.	23
Figura 9. Configuración Web Server.	24
Figura 10. Configuración de VLANs, Puertos troncales y puertos de acceso en el Switch S1.	25
Figura 11. Configuración de VLANs, Puertos troncales y puertos de acceso en el Switch S2.	26
Figura 12. Configuración del encapsulamiento y asignación de las direcciones IP en el Router R1.....	27
Figura 13. Configuración del protocolo de enrutamiento OSPFv2 en el Router R1.	28
Figura 14. Configuración del protocolo de enrutamiento OSPFv2 en el Router R2	29
Figura 15. Configuración del protocolo de enrutamiento OSPFv2 en el Router R3.	30
Figura 16. Tabla de enrutamiento y configuración de OSPFv2 en el Router R1.	31
Figura 17. Tabla de enrutamiento y configuración de OSPFv2 en el Router R2.	32
Figura 18. Tabla de enrutamiento y configuración de OSPFv2 en el Router R3.	33
Figura 19. Lista de interface de OSPFv2 en el Router R1.	34
Figura 20. Continuación de lista de interface de OSPFv2 en el Router R1.....	35
Figura 21. Lista de interface de OSPFv2 en el Router R2.	36
Figura 22. Continuación de lista de interface de OSPFv2 en el Router R2.....	37
Figura 23. Lista de interface de OSPFv2 en el Router R3.	38
Figura 24. Lista de información de los parámetros y configuración en el Router R1	39
Figura 25. Lista de información de los parámetros y configuración en el Router R2.....	40
Figura 26. Lista de información de los parámetros y configuración en el Router R3.....	41
Figura 27. Inhabilitación del DNS lookup en el Switch S1.....	42
Figura 28. Implementación de DHCP y NAT para IPv4 por medio de la configuración del Router R1.....	43
Figura 29. Configuración de la NAT en el Router R2.....	44
Figura 30. Configuración de las listas de acceso estándar y dinámicas el Router R2.	45
Figura 31. Configuración de la DHCP en la PC-A.....	46
Figura 32. Configuración de la DHCP en la PC-C.	47
Figura 33. Ejecución del comando Ping entre PC-A y PC-C	48
Figura 34. Verificación acceso web desde Internet PC a Web Server.....	49

Figura 35. Verificación de conectividad con el comando tracert entre PC-A y Web Server.	50
Figura 36. Verificación de conectividad con el comando traceroute entre R1 y Web Server, PC-A, PC-C e Internet PC.	51

Glosario

Conectividad: es la capacidad de un dispositivo de conectarse con otro dispositivo de una forma autónoma.

Dirección IP: es un direccionamiento utilizado para identificar un dispositivo en la red.

DNS: (sistema de nombres de dominio) es la nomenclatura utilizada para asociar información de dominio y la dirección IP de cada uno de los dispositivos que conforman o acceden a una red.

DHCP: (Protocolo de configuración dinámica de host) de tipo cliente/servidor en el que un servidor cuenta con un listado de direcciones IP dinámicas y las asigna a los clientes en el momento en el que se encuentran disponibles.

Encapsulamiento: es el proceso en el que los datos que se encuentran dispuestos para ser enviados a través de una red se ubican en paquetes con la capacidad de ser administrados y rastreados por el administrador de la red

NAT. protocolo con el cual se intercambian o transportan paquetes entre dos redes normalmente incompatibles.

OSPF: protocolo de enrutamiento desarrollado para redes IP, de tipo enlace-estado.

Ping: comando utilizado para realizar un diagnóstico de estado de comunicación entre dos o más equipos en el cual se puede determinar la velocidad, calidad y estado de red.

Protocolos de enrutamiento: conjunto de reglas que permiten determinar la mejor ruta para enviar paquetes de datos entre routers.

Puertos troncales: enlace punto a punto para enviar y recibir el tráfico entre routers o switches.

Topología física: disposición de cada uno de los dispositivos o hardware dentro de una red.

Topología lógica: es la forma que utilizan los hosts para comunicarse a través de una red.

VLAN: procedimiento para establecer redes lógicas de una forma independiente dentro de una misma red física.

Resumen

En el presente trabajo se desarrolló una práctica en la cual mediante el análisis de un escenario propuesto se realizó su descripción detallada, la implementación de su topología física, las configuraciones de cada uno de los dispositivos y la verificación de la conectividad de cada uno de ellos por medio de la simulación del escenario en el software Packet Tracer 6.1.1.0001.

Introducción

Por medio del presente trabajo, se abordarán las diferentes temáticas relacionadas con el proceso de aprendizaje realizado durante el desarrollo del Diplomado de Profundización CCNA, específicamente en la implementación de un escenario propuesto en el cual se realizará la configuración de cada uno de los dispositivos que comprende el diseño físico, la ejecución de los diferentes comandos de programación para la verificación de su conectividad.

Lo anterior con base en la utilización de recursos y herramientas que se trabajaron en función de los protocolos y soporte de las comunicaciones por medio de las redes de datos, generando soluciones a problemas de conectividad. De igual manera se implementarán los diferentes niveles de seguridad aplicados a al escenario con el fin de mantener la integridad de la red y sus dispositivos frente a cualquier tipo amenaza.

La implementación de este escenario se realizará por medio de la simulación en el software packet tracer 6.1.1.0001. el cual nos permite experimentar con la topología física y analizar el comportamiento de toda la red del escenario propuesto.

Objetivo General

Dar solución al escenario propuesto como trabajo final del diplomado de profundización CCNA, desarrollando cada uno de los conocimientos adquiridos sobre la implementación y diseño de la topología física y lógica de una red.

Objetivos específicos

- Analizar la arquitectura propuesta con el fin de implementar su simulación por medio del software Packet Tracer 6.1.1.0001.
- Realizar la Configuración e interconectar entre sí cada uno de los dispositivos que forman parte del escenario propuesto de acuerdo con los protocolos establecidos para el diseño de una topología de red.
- Documentar y registrar cada uno de los procedimientos realizados para la configuración de los dispositivos y realizar la verificación de la conectividad entre cada uno de ellos.

1. Descripción Del Escenario Propuesto Para La Prueba De Habilidades

1.1. Escenario: Una empresa de Tecnología posee tres sucursales distribuidas en las ciudades de Bogotá, Medellín y Bucaramanga, 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 de red

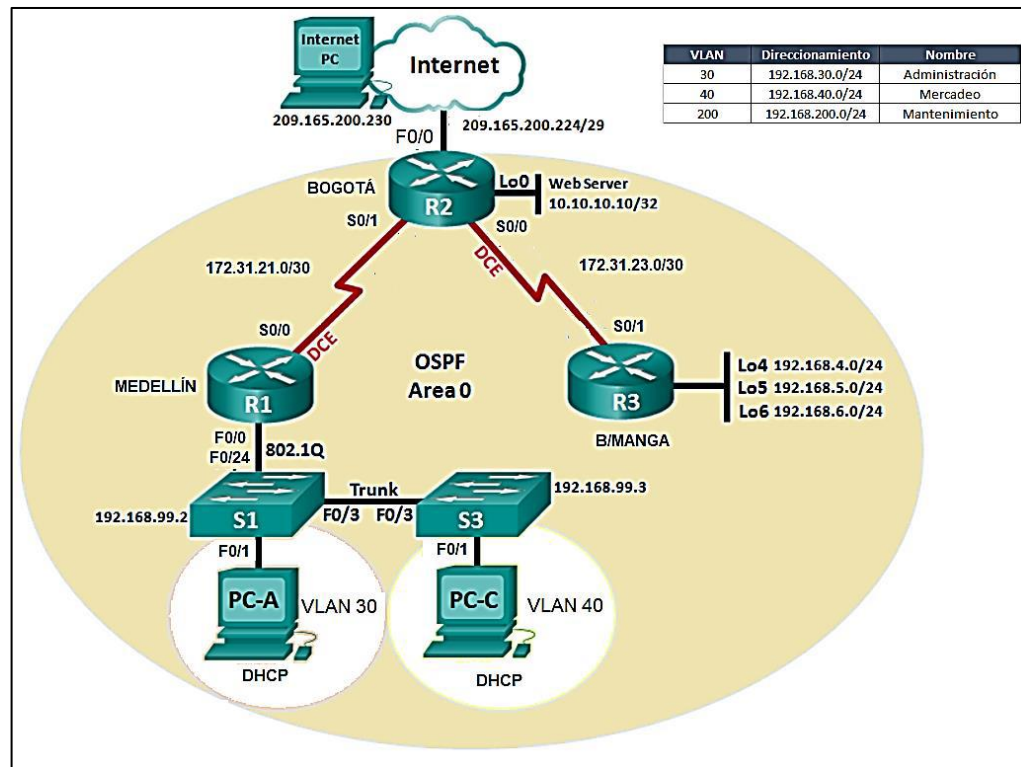


Figura 1. topología de red propuesta

1.2. Requerimientos para el desarrollo del escenario propuesto para la prueba de habilidades

1. Configurar el direccionamiento IP acorde con la topología de red para cada uno de los dispositivos que forman parte del escenario.
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	2.2.2.2
Router ID R3	3.3.3.3
Configurar todas las interfaces LAN como pasivas	
Establecer el ancho de banda para enlaces seriales en	128 Kb/s
Ajustar el costo en la métrica de S0/0 a	7500

Tabla 1. Cuadro de datos propuesto para la configuración del protocolo de enrutamiento OSPFv2.

Verificar información de OSPF

- Visualizar tablas de enrutamiento y routers conectados por OSPFv2
 - Visualizar lista resumida de interfaces por OSPF en donde se ilustre el costo de cada interface
 - Visualizar el OSPF Process ID, Router ID, Address summarizations, Routing Networks, and passive 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.
 4. En el Switch 3 deshabilitar DNS lookup
 5. Asignar direcciones IP a los Switches acorde a los lineamientos.

6. Desactivar todas las interfaces que no sean utilizadas en el esquema de red.
7. Implement DHCP and NAT for IPv4
8. Configurar R1 como servidor DHCP para las VLANs 30 y 40.
9. Reservar las primeras 30 direcciones IP de las VLAN 30 y 40 para configuraciones estáticas.

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 2. Cuadro de datos propuesto para la configuración de DHCP pool para VLAN 30 y VLAN 40.

10. Configurar NAT en R2 para permitir que los hosts puedan salir a internet
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.
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.
13. Verificar procesos de comunicación y redireccionamiento de tráfico en los routers mediante el uso de Ping y Traceroute.

2. Desarrollo Del Escenario Propuesto Para La Prueba De Habilidades Prácticas

Teniendo en cuenta la Descripción del escenario propuesto para la prueba de habilidades y utilizando el conocimiento obtenido durante el desarrollo del diplomado de profundización CCNA en cuanto a la solución de problemas relacionados con diversos aspectos de Networking, se realizará la siguiente implementación y configuración de la arquitectura planteada.

2.1. Implementación de la topología de red en software Packet Tracer

6.1.1.0001

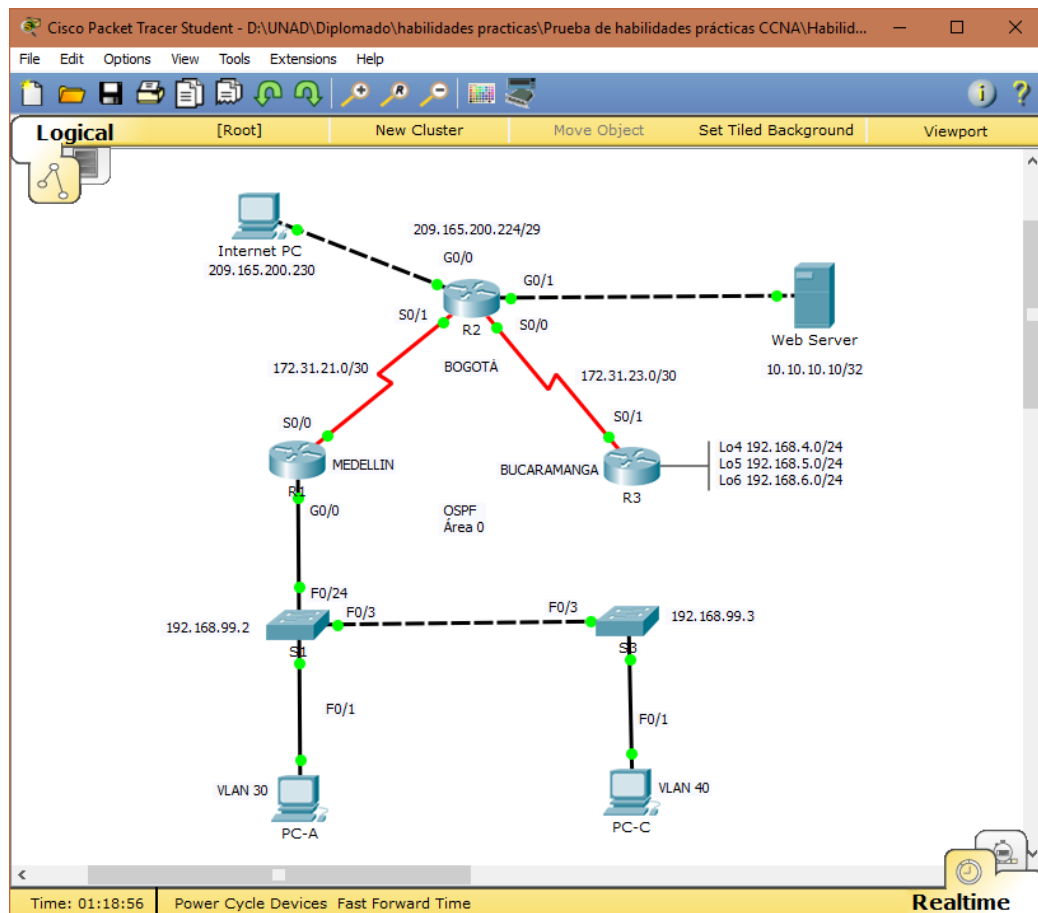


Figura 2. Implementación de la topología de red propuesta sobre el software Packet Tracer 6.1.1.0001

2.1.1. Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred
R1	G0/0	192.168.1.1	255.255.255.0
	S0/0/0 (DCE)	172.31.21.1	255.255.255.252
R2	G0/0 (Lo0)	209.165.200.225	255.255.255.248
	G0/1	10.10.10.1	255.255.255.0
	S0/0/0	172.31.23.1	255.255.255.252
	S0/0/1 (DCE)	172.31.21.2	255.255.255.252
R3	S0/0/1	172.31.23.2	255.255.255.252
	Lo4	192.168.4.1	255.255.255.0
	Lo5	192.168.5.1	255.255.255.0
	Lo6	192.168.6.1	255.255.255.0
PC-A	NIC	192.168.30.31	255.255.255.0
Internet PC	NIC	209.165.200.230	255.255.255.248
PC-C	NIC	192.168.40.31	255.255.255.0
Web Server	Fa0	10.10.10.10	255.255.255.0

Tabla 3. Tabla de direccionamiento implementado

La configuración de acceso seguro a la línea de consola y acceso seguro al modo privilegiado se realiza por medio de la **contraseña: cisco**, y para la configuración de una contraseña encriptada para proporcionar un acceso seguro al modo privilegiado se realiza por medio de la **contraseña: ospf**.

2.2. Configuración del direccionamiento IP acorde con la topología de red.

Se realiza la configuración de cada uno de los dispositivos consistente en la asignación de direcciones IP de acuerdo a los datos establecidos en el escenario propuesto, y a la tabla de direccionamiento (tabla 3).

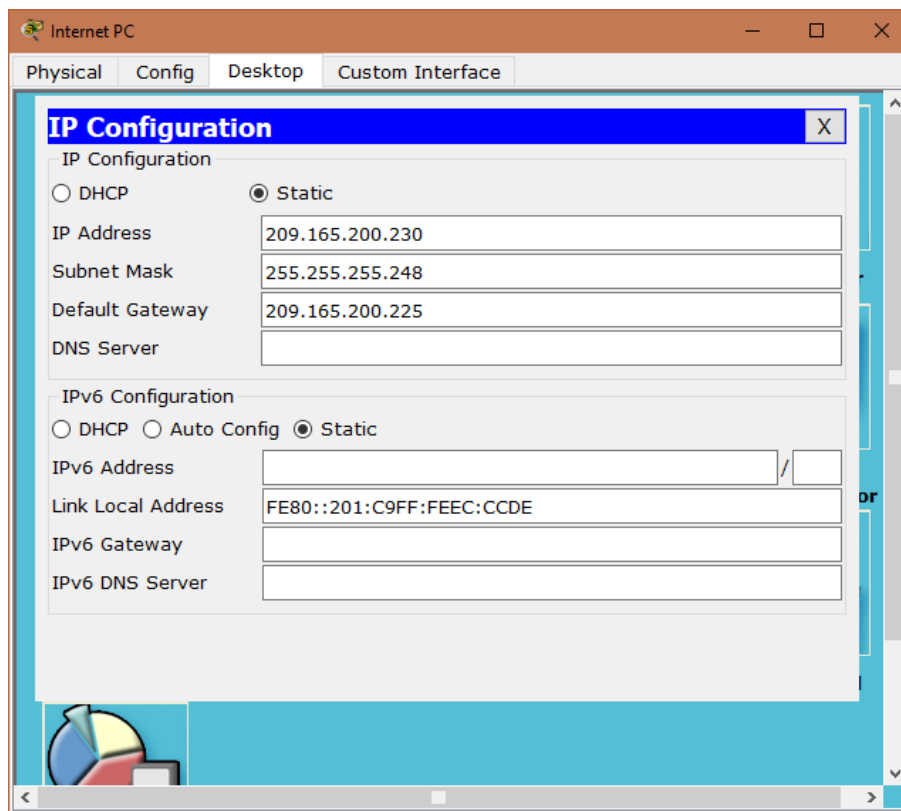


Figura 3. Configuración dispositivo Internet PC

```
Router>enable
Router#config t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname R1
R1(config)#enable secret ospf
R1(config)#line console 0
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#line vty 0 4
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#service password-encryption
R1(config)#banner ^ El acceso no autorizado se encuentra PROHIBIDO!$
^
% Invalid input detected at '^' marker.
R1(config)#banner ^El acceso no autorizado se encuentra PROHIBIDO!$
^
% Invalid input detected at '^' marker.
R1(config)#banner motd ^El acceso no autorizado se encuentra PROHIBIDO!$
R1(config)#int s0/0/0
R1(config-if)#description conexion a R2
R1(config-if)#ip address 172.31.21.1 255.255.255.252
R1(config-if)#clock rate 128000
R1(config-if)#no shutdown

%LINK-5-CHANGED: Interface Serial0/0/0, changed state to down
R1(config-if)#exit
R1(config)#ip route 0.0.0.0 0.0.0.0 s0/0/0
%Default route without gateway, if not a point-to-point interface, may impact
performance
R1(config)#
```

Figura 4. Configuración Router R1.

```
R2
Physical Config CLI
IOS Command Line Interface

Router>enable
Router#config t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname R2
R2(config)#enable secret ospf
R2(config)#line console 0
R2(config-line)#password cisco
R2(config-line)#login
R2(config-line)#line vty 0 4
R2(config-line)#password cisco
R2(config-line)#login
R2(config-line)#service password-encryption
R2(config)#banner motd $El acceso no autorizado se encuentra PROHIBIDO!$
R2(config)#int s0/0/1
R2(config-if)#description conexion a R1
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

R2(config-if)#
%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 conexion a R3
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)#int g0/0
R2(config-if)#description conexion a Internet PC
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 GigabitEthernet0/0, changed state to up

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

R2(config-if)#int g0/1
R2(config-if)#ip address 10.10.10.1 255.255.255.0
R2(config-if)#no shutdown

R2(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to up

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

Copy Paste
```

Figura 5. Configuración Router R1.

```

R3
Physical Config CLI
IOS Command Line Interface

Router#config t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname R3
R3(config)#enable secret ospf
R3(config)#line console 0
R3(config-line)#password cisco
R3(config-line)#login
R3(config-line)#line vty 0 4
R3(config-line)#password cisco
R3(config-line)#login
R3(config-line)#service password-encryption
R3(config)#banner motd %El acceso no autorizado se encuentra PROHIBIDO!%
R3(config)#int s0/0/1
R3(config-if)#description conexion a R2
R3(config-if)#ip address 172.31.23.1 255.255.255.252
R3(config-if)#no shutdown

R3(config-if)#
%LINK-5-CHANGED: Interface Serial10/0/1, changed state to up

R3(config-if)#int lo4
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial10/0/1, changed state to up

R3(config-if)#
%LINK-5-CHANGED: Interface Loopback4, changed state to up

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

R3(config-if)#ip address 192.168.4.1 255.255.255.0
R3(config-if)#no shutdown
R3(config-if)#int lo5

R3(config-if)#
%LINK-5-CHANGED: Interface Loopback5, changed state to up

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

R3(config-if)#ip address 192.168.5.1 255.255.255.0
R3(config-if)#no shutdown
R3(config-if)#int lo6

R3(config-if)#
%LINK-5-CHANGED: Interface Loopback6, changed state to up

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

R3(config-if)#ip address 192.168.6.1 255.255.255.0
R3(config-if)#exit
R3(config)#ip route 0.0.0.0 0.0.0.0 s0/0/1
%Default route without gateway, if not a point-to-point interface, may impact
performance
R3(config)#
Copy Paste

```

Figura 6. Configuración Router R3.

```
Switch S1
Physical Config CLI
IOS Command Line Interface
Compiled wed 12-Oct-08 22:08 by pt_team
Press RETURN to get started!

%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up
%LINK-5-CHANGED: Interface FastEthernet0/3, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to up

Switch>enable
Switch#config t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname S1
S1(config)#enable secret ospf
S1(config)#line console 0
S1(config-line)#password cisco
S1(config-line)#login
S1(config-line)#line vty 0 4
S1(config-line)#password cisco
S1(config-line)#login
S1(config-line)#service password-encryption
S1(config)#banner motd #El acceso no autorizado se encuentra PROHIBIDO!#
S1(config)#
```

Figura 7. Configuración Switch S1.

```
Switch>enable
Switch#config t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname S3
S3(config)#enable secret ospf
S3(config)#line console 0
S3(config-line)#password cisco
S3(config-line)#login
S3(config-line)#line vty 0 4
S3(config-line)#password cisco
S3(config-line)#login
S3(config-line)#service password-encryption
S3(config)#banner motd #El acceso no autorizado se encuentra PROHIBIDO!#
S3(config)#
```

Figura 8. Configuración Switch S2.

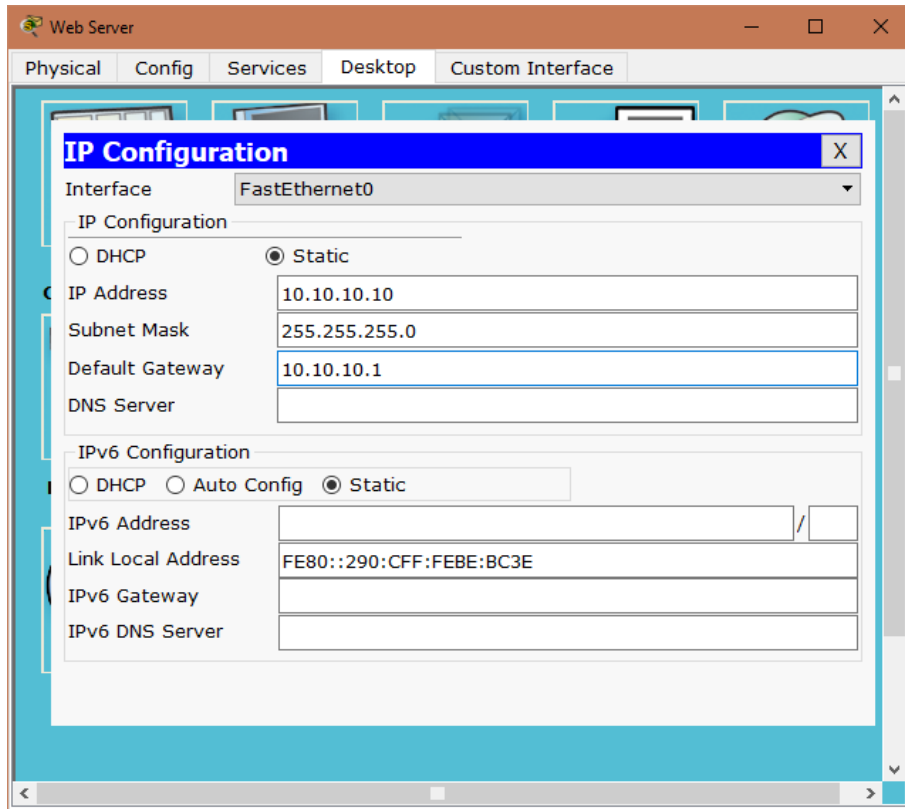
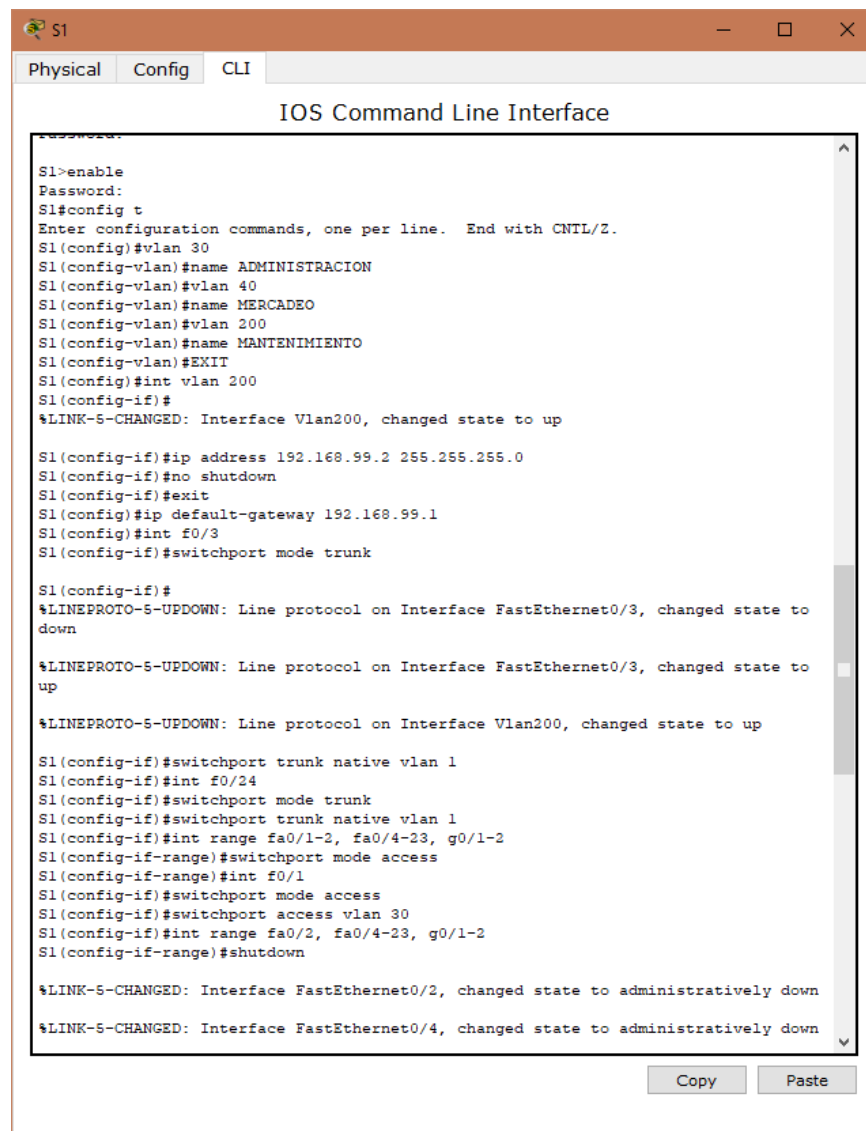


Figura 9. Configuración Web Server.

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

Se configuran las VLANs de acuerdo con los datos suministrados en el escenario propuesto, se asigna la dirección IP al administrador de la VLANs para lo cual después de analizar la topología se asigno a L VLANs 200.



```

S1>enable
Password:
S1#config t
Enter configuration commands, one per line. End with CNTRL/Z.
S1(config)#vlan 30
S1(config-vlan)#name ADMINISTRACION
S1(config-vlan)#vlan 40
S1(config-vlan)#name MERCADEO
S1(config-vlan)#vlan 200
S1(config-vlan)#name MANTENIMIENTO
S1(config-vlan)#EXIT
S1(config)#int vlan 200
S1(config-if)#
%LINK-5-CHANGED: Interface Vlan200, changed state to up

S1(config-if)#ip address 192.168.99.2 255.255.255.0
S1(config-if)#no shutdown
S1(config-if)#exit
S1(config)#ip default-gateway 192.168.99.1
S1(config)#int f0/3
S1(config-if)#switchport mode trunk

S1(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to
down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to
up

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

S1(config-if)#switchport trunk native vlan 1
S1(config-if)#int f0/24
S1(config-if)#switchport mode trunk
S1(config-if)#switchport trunk native vlan 1
S1(config-if)#int range fa0/1-2, fa0/4-23, g0/1-2
S1(config-if-range)#switchport mode access
S1(config-if-range)#int f0/1
S1(config-if)#switchport mode access
S1(config-if)#switchport access vlan 30
S1(config-if)#int range fa0/2, fa0/4-23, g0/1-2
S1(config-if-range)#shutdown

%LINK-5-CHANGED: Interface FastEthernet0/2, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/4, changed state to administratively down
  
```

Figura 10. Configuración de VLANs, Puertos troncales y puertos de acceso en el Switch S1.

```
S3>enable
Password:
S3#config t
Enter configuration commands, one per line. End with CNTL/Z.
S3(config)#vlan 30
S3(config-vlan)#name ADMINISTRACION
S3(config-vlan)#vlan 40
S3(config-vlan)#name MERCADEO
S3(config-vlan)#vlan 200
S3(config-vlan)#name MANTENIMIENTO
S3(config-vlan)#EXIT
S3(config)#int vlan 200
S3(config-if)#
%LINK-5-CHANGED: Interface Vlan200, changed state to up

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

S3(config-if)#ip address 192.168.99.3 255.255.255.0
S3(config-if)#no shutdown
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 fa0/1-2, fa0/4-24, g0/1-2
S3(config-if-range)#switchport mode access
S3(config-if-range)#int f0/1
S3(config-if)#switchport mode access
S3(config-if)#switchport access vlan 40
S3(config-if)#int range fa0/2, fa0/4-24, g0/1-2
S3(config-if-range)#shutdown

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

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

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

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

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

Figura 11. Configuración de VLANs, Puertos troncales y puertos de acceso en el Switch S2.

```
R1#config t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#int g0/0.30
R1(config-subif)#description Administracion LAN
R1(config-subif)#encapsulation dot1q 30
R1(config-subif)#ip address 192.168.30.1 255.255.255.0
R1(config-subif)#int g0/0.40
R1(config-subif)#description Mercadeo LAN
R1(config-subif)#encapsulation dot1q 40
R1(config-subif)#ip address 192.168.40.1 255.255.255.0
R1(config-subif)#int g0/0.200
R1(config-subif)#description Mantenimiento LAN
R1(config-subif)#encapsulation dot1q 200
R1(config-subif)#ip address 192.168.200.1 255.255.255.0
R1(config-subif)#int g0/0
R1(config-if)#no shutdown

R1(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up

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

%LINK-5-CHANGED: Interface GigabitEthernet0/0.30, changed state to up

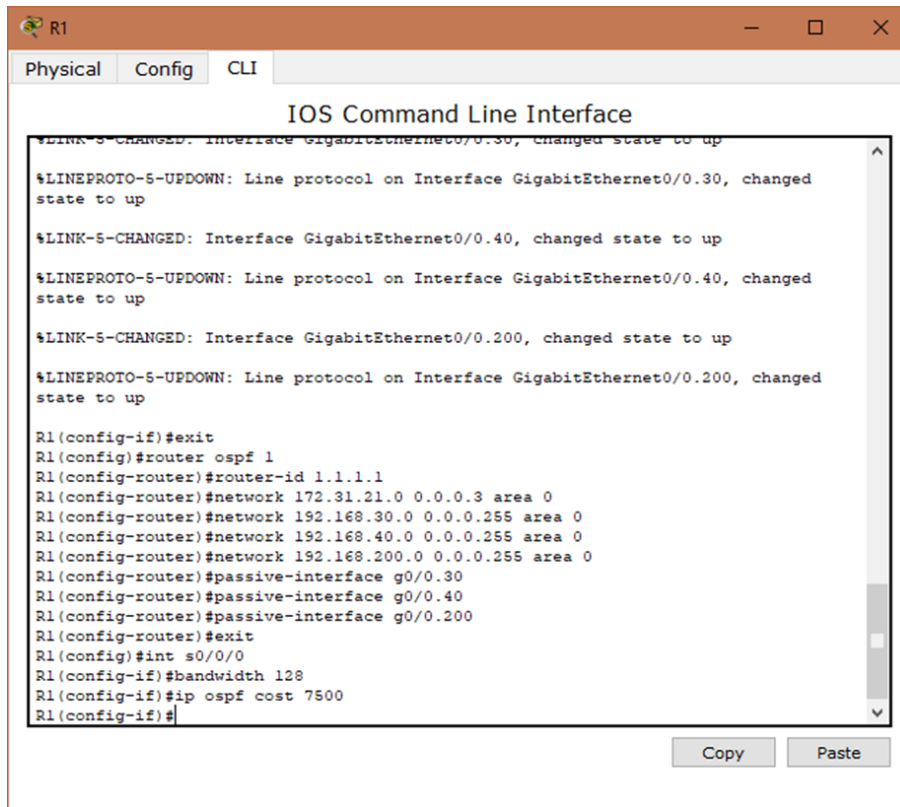
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0.30, changed
state to up

%LINK-5-CHANGED: Interface GigabitEthernet0/0.40, changed state to up
```

Figura 12. Configuración del encapsulamiento y asignación de las direcciones IP en el Router R1.

2.4. Configuración del protocolo de enrutamiento OSPFv2

Se realiza la configuración de todos los routers utilizando el protocolo de enrutamiento OSPF v2 para realizar la programación de las redes con el ID de área 0 para cada uno de ellos. A continuación, se ilustra la implementación de esta configuración.



```

R1
-----
Physical  Config  CLI
-----
IOS Command Line Interface

%LINK-5-CHANGED: Interface GigabitEthernet0/0.30, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0.30, changed
state to up
%LINK-5-CHANGED: Interface GigabitEthernet0/0.40, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0.40, changed
state to up
%LINK-5-CHANGED: Interface GigabitEthernet0/0.200, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0.200, changed
state to up

R1(config-if)#exit
R1(config)#router ospf 1
R1(config-router)#router-id 1.1.1.1
R1(config-router)#network 172.31.21.0 0.0.0.3 area 0
R1(config-router)#network 192.168.30.0 0.0.0.255 area 0
R1(config-router)#network 192.168.40.0 0.0.0.255 area 0
R1(config-router)#network 192.168.200.0 0.0.0.255 area 0
R1(config-router)#passive-interface g0/0.30
R1(config-router)#passive-interface g0/0.40
R1(config-router)#passive-interface g0/0.200
R1(config-router)#exit
R1(config)#int s0/0/0
R1(config-if)#bandwidth 128
R1(config-if)#ip ospf cost 7500
R1(config-if)#
  
```

Figura 13. Configuración del protocolo de enrutamiento OSPFv2 en el Router R1.

```
R2
Physical Config CLI
IOS Command Line Interface

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1, changed state to up
El acceso no autorizado se encuentra PROHIBIDO!

User Access Verification

Password:

R2>en
Password:
R2#config t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#router ospf 1
R2(config-router)#router-id 2.2.2.2
R2(config-router)#network 172.31.21.0 0.0.0.3 area 0
R2(config-router)#network 172.31.21.0 0.0.0.3 area 0
00:20:33: %OSPF-5-ADJCHG: Process 1, Nbr 1.1.1.1 on Serial0/0/1 from LOADING to FULL, Loading Done
R2(config-router)#network 172.31.23.0 0.0.0.3 area 0
R2(config-router)#network 10.10.10.0 0.0.0.255 area 0
R2(config-router)#passive-interface g0/1
R2(config-router)#int s0/0/1
R2(config-if)#bandwidth 128
R2(config-if)#ip ospf cost 7500
R2(config-if)#int s0/0/0
R2(config-if)#bandwidth 128
R2(config-if)#ip ospf cost 7500
R2(config-if)#
```

Figura 14. Configuración del protocolo de enrutamiento OSPFv2 en el Router R2

```
R3
Physical Config CLI
IOS Command Line Interface
R3(Config)#router ospf 1
R3(config-router)#router-id 3.3.3.3
R3(config-router)#network 172.31.23.0 0.0.0.3 area 0
R3(config-router)#network 172.31.23.0 0.0.0.3 area 0
00:27:45: %OSPF-5-ADJCHG: Process 1, Nbr 2.2.2.2 on Serial0/0/1 from LOADING to FULL, Loading Done
R3(config-router)#network 192.168.4.0 0.3.255 area 0
^
% Invalid input detected at '^' marker.
R3(config-router)#network 192.168.4.0 0.0.3.255 area 0
R3(config-router)#passive-interface lo4
R3(config-router)#passive-interface lo5
R3(config-router)#passive-interface lo6
R3(config-router)#exit
R3(config)#int s0/0/1
R3(config-if)#bandwidth 128
R3(config-if)#ip ospf cost 7500
R3(config-if)#exit
R3(config)#exit
R3#
%SYS-5-CONFIG_I: Configured from console by console
R3#show ip ospf neighbor

Neighbor ID      Pri   State           Dead Time   Address        Interface
2.2.2.2          0    FULL/ -         00:00:33   172.31.23.1   Serial0/0/1
R3#
```

Figura 15. Configuración del protocolo de enrutamiento OSPFv2 en el Router R3.

2.5. Tablas de enrutamiento y routers conectados por OSPFv2

Se ejecuta el comando **show ip ospf neighbor** con el cual tendremos acceso a las tablas de enrutamiento y configuración de Router conectados por OSPFv2

```
El acceso no autorizado se encuentra PROHIBIDO!  
User Access Verification  
Password:  
R1>en  
Password:  
R1#show ip neighbord  
^  
% Invalid input detected at '^' marker.  
R1#show ip neighbor  
^  
% Invalid input detected at '^' marker.  
R1#show ip ospf neighbor  


| Neighbor ID | Pri | State  | Dead Time | Address     | Interface   |
|-------------|-----|--------|-----------|-------------|-------------|
| 2.2.2.2     | 0   | FULL/- | 00:00:31  | 172.31.21.2 | Serial0/0/0 |

  
R1#
```

Figura 16. Tabla de enrutamiento y configuración de OSPFv2 en el Router R1.

```
Press RETURN to get started.

El acceso no autorizado se encuentra PROHIBIDO!

User Access Verification

Password:

R2>en
Password:
R2#show ip ospf neighbor

Neighbor ID    Pri  State           Dead Time   Address      Interface
1.1.1.1        0    FULL/ -         00:00:31   172.31.21.1  Serial0/0/1
3.3.3.3        0    FULL/ -         00:00:33   172.31.23.2  Serial0/0/0
R2#
```

Figura 17. Tabla de enrutamiento y configuración de OSPFv2 en el Router R2.

R3

Physical Config CLI

IOS Command Line Interface

```

%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

00:00:10: %OSPF-5-ADJCHG: Process 1, Nbr 2.2.2.2 on Serial0/0/1 from LOADING to FULL, Loading Done

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

00:10:50: %OSPF-5-ADJCHG: Process 1, Nbr 2.2.2.2 on Serial0/0/1 from FULL to DOWN, Neighbor Down: Interface down or detached

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

00:11:00: %OSPF-5-ADJCHG: Process 1, Nbr 2.2.2.2 on Serial0/0/1 from LOADING to FULL, Loading Done
El acceso no autorizado se encuentra PROHIBIDO!

User Access Verification

Password:

R3>en
Password:
R3#show ip ospf neighbor

Neighbor ID    Pri   State           Dead Time   Address        Interface
2.2.2.2        0     FULL/ -         00:00:31   172.31.23.1   Serial0/0/1
R3#
    
```

Copy Paste

Figura 18. Tabla de enrutamiento y configuración de OSPFv2 en el Router R3.

2.6. Lista resumida de interfaces por OSPF en en la cual se ilustra el costo de cada interface

Se ejecuta el comando **show ip ospf interface** con el cual tendremos acceso a las listas de interfaces por OSPF.

```

R1#show ip ospf interface
Serial0/0/0 is up, line protocol is up
 Internet address is 172.31.21.1/30, Area 0
 Process ID 1, Router ID 1.1.1.1, Network Type POINT-TO-POINT, Cost: 7500
 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 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 1 , Adjacent neighbor count is 1
   Adjacent with neighbor 2.2.2.2
 Suppress hello for 0 neighbor(s)
GigabitEthernet0/0.30 is up, line protocol is up
 Internet address is 192.168.30.1/24, Area 0
 Process ID 1, Router ID 1.1.1.1, Network Type BROADCAST, Cost: 1
 Transmit Delay is 1 sec, State WAITING, Priority 1
 No designated router on this network
 No backup designated router on this network
 Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
   No Hellos (Passive interface)
 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 0, Adjacent neighbor count is 0
 Suppress hello for 0 neighbor(s)
  
```

Figura 19. Lista de interface de OSPFv2 en el Router R1.

```
R1
Physical Config CLI
IOS Command Line Interface

GigabitEthernet0/0.40 is up, line protocol is up
Internet address is 192.168.40.1/24, Area 0
Process ID 1, Router ID 1.1.1.1, Network Type BROADCAST, Cost: 1
Transmit Delay is 1 sec, State WAITING, Priority 1
No designated router on this network
No backup designated router on this network
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
  No Hellos (Passive interface)
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 0, Adjacent neighbor count is 0
Suppress hello for 0 neighbor(s)
GigabitEthernet0/0.200 is up, line protocol is up
Internet address is 192.168.200.1/24, Area 0
Process ID 1, Router ID 1.1.1.1, Network Type BROADCAST, Cost: 1
Transmit Delay is 1 sec, State WAITING, Priority 1
No designated router on this network
No backup designated router on this network
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
  No Hellos (Passive interface)
Index 4/4, 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)
R1#
R1#
R1#
```

Figura 20. Continuación de lista de interface de OSPFv2 en el Router R1.

```
R2
Physical Config CLI
IOS Command Line Interface
Password:
R2#show ip ospf interface

Serial0/0/1 is up, line protocol is up
Internet address is 172.31.21.2/30, Area 0
Process ID 1, Router ID 2.2.2.2, Network Type POINT-TO-POINT, Cost: 7500
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 00:00:04
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 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 2.2.2.2, Network Type POINT-TO-POINT, Cost: 7500
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 00:00:06
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 3.3.3.3
Suppress hello for 0 neighbor(s)
```

Figura 21. Lista de interface de OSPFv2 en el Router R2.

```
Supress hello for 0 neighbor(s)
GigabitEthernet0/1 is up, line protocol is up
Internet address is 10.10.10.1/24, Area 0
Process ID 1, Router ID 2.2.2.2, Network Type BROADCAST, Cost: 1
Transmit Delay is 1 sec, State WAITING, Priority 1
No designated router on this network
No backup designated router on this network
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
  No Hellos (Passive interface)
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 0, Adjacent neighbor count is 0
Supress hello for 0 neighbor(s)
R2#
R2#
R2#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1, changed state to down
00:50:59: %OSPF-5-ADJCHG: Process 1, Nbr 1.1.1.1 on Serial0/0/1 from FULL to DOWN,
Neighbor Down: Interface down or detached
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to down
```

Figura 22. Continuación de lista de interface de OSPFv2 en el Router R2.

```

R3
Physical Config CLI
IOS Command Line Interface
Password:
R3#show ip ospf interface

Loopback4 is up, line protocol is up
Internet address is 192.168.4.1/24, Area 0
Process ID 1, Router ID 3.3.3.3, Network Type LOOPBACK, Cost: 1
Loopback interface is treated as a stub Host
Loopback5 is up, line protocol is up
Internet address is 192.168.5.1/24, Area 0
Process ID 1, Router ID 3.3.3.3, Network Type LOOPBACK, Cost: 1
Loopback interface is treated as a stub Host
Loopback6 is up, line protocol is up
Internet address is 192.168.6.1/24, Area 0
Process ID 1, Router ID 3.3.3.3, Network Type LOOPBACK, Cost: 1
Loopback interface is treated as a stub Host
Serial0/0/1 is up, line protocol is up
Internet address is 172.31.23.2/30, Area 0
Process ID 1, Router ID 3.3.3.3, Network Type POINT-TO-POINT, Cost: 7500
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 00:00:07
Index 4/4, 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 2.2.2.2
Suppress hello for 0 neighbor(s)
R3#
Copy Paste

```

Figura 23. Lista de interface de OSPFv2 en el Router R3.

2.7. Lista de la información de OSPF Process ID, Router ID, Address summarizations, Routing Networks, and passive interfaces configured en cada router.

Se ejecuta el comando **show ip protocols** con el cual tendremos acceso a la información de los parámetros y configuración del estado actual de cualquier proceso activo configurado en los routers.

```

R1#
R1#
R1#
R1#
R1#show ip protocols

Routing Protocol is "ospf 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 1.1.1.1
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    172.31.21.0 0.0.0.3 area 0
    192.168.30.0 0.0.0.255 area 0
    192.168.40.0 0.0.0.255 area 0
    192.168.200.0 0.0.0.255 area 0
  Passive Interface(s):
    GigabitEthernet0/0.30
    GigabitEthernet0/0.40
    GigabitEthernet0/0.200
  Routing Information Sources:
    Gateway         Distance      Last Update
    1.1.1.1           110          00:20:13
    2.2.2.2           110          00:13:04
    3.3.3.3           110          00:08:09
  Distance: (default is 110)

R1#
  
```

Figura 24. Lista de información de los parámetros y configuración en el Router R1

```

R2>en
Password:
R2#show ip ospf neighbor

Neighbor ID      Pri   State           Dead Time   Address        Interface
1.1.1.1          0     FULL/ -         00:00:31   172.31.21.1   Serial0/0/1
3.3.3.3          0     FULL/ -         00:00:33   172.31.23.2   Serial0/0/0
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 2.2.2.2
  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):
    GigabitEthernet0/1
  Routing Information Sources:
    Gateway         Distance      Last Update
    1.1.1.1          110          00:18:33
    2.2.2.2          110          00:11:25
    3.3.3.3          110          00:06:30
  Distance: (default is 110)

R2#
  
```

Figura 25. Lista de información de los parámetros y configuración en el Router R2.

```
Loopback4 is up, line protocol is up
Internet address is 192.168.6.1/24
Vlan1 is administratively down, line protocol is down
R3#
R3#
R3#
R3#
R3#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 3.3.3.3
  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          00:18:05
    2.2.2.2          110          00:10:57
    3.3.3.3          110          00:06:02
  Distance: (default is 110)

R3#
```

Figura 26. Lista de información de los parámetros y configuración en el Router R3.

2.8. Inhabilitación del DNS lookup en el swicht S1

Para deshabilitar el DNS lookup, es necesario ejecutar el comando **no ip domain-lookup**.

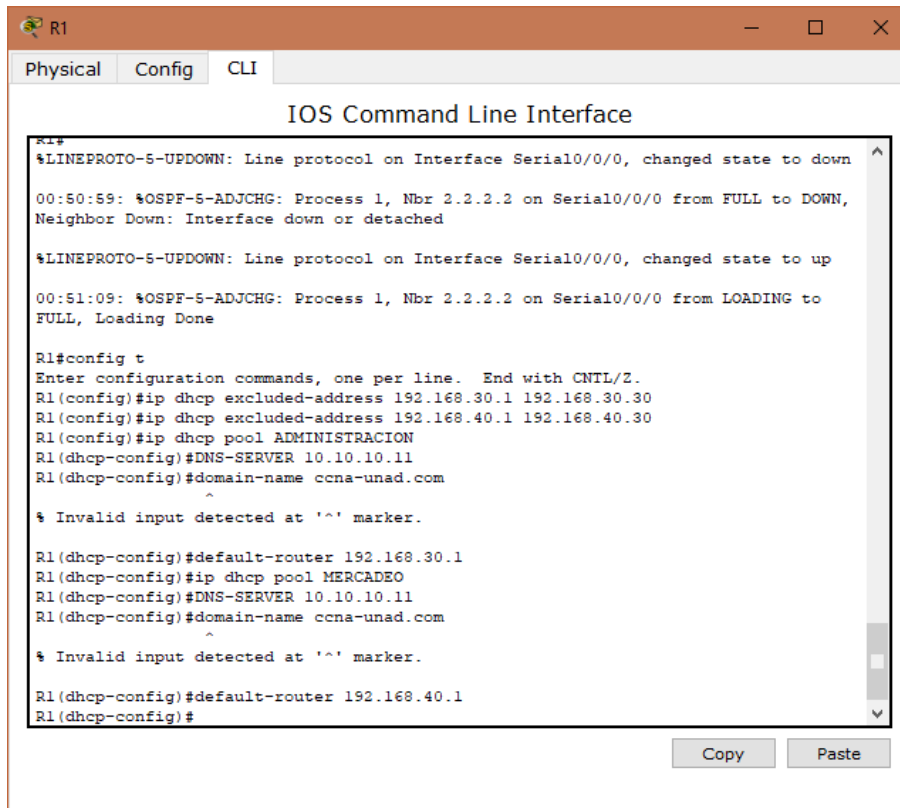
```
Switch>enable
Switch#config t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname S3
S3(config)#enable secret ospf
S3(config)#line console 0
S3(config-line)#password cisco
S3(config-line)#login
S3(config-line)#line vty 0 4
S3(config-line)#password cisco
S3(config-line)#login
S3(config-line)#service password-encryption
S3(config)#banner motd #El acceso no autorizado se encuentra PROHIBIDO!#
S3(config)#exit
S3#
%SYS-5-CONFIG_I: Configured from console by console

S3#config t
Enter configuration commands, one per line. End with CNTL/Z.
S3(config)#no ip domain-lookup
S3(config)#
```

Figura 27. Inhabilitación del DNS lookup en el Switch S1.

2.9. Implementación de DHCP y NAT para IPv4

Se realiza la Implementación de DHCP y NAT para IPv4 por medio de la configuración del Router R1 como servidor DHCP para las VLANs 30 y 40 y posteriormente se realiza la reserva de las primeras 30 direcciones IP de las VLANs para configuraciones estáticas.



```

R1#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to down
00:50:59: %OSPF-5-ADJCHG: Process 1, Nbr 2.2.2.2 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
00:51:09: %OSPF-5-ADJCHG: Process 1, Nbr 2.2.2.2 on Serial0/0/0 from LOADING to FULL, Loading Done

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)#domain-name ccna-unad.com
^
% Invalid input detected at '^' marker.
R1(dhcp-config)#default-router 192.168.30.1
R1(dhcp-config)#ip dhcp pool MERCADEO
R1(dhcp-config)#DNS-SERVER 10.10.10.11
R1(dhcp-config)#domain-name ccna-unad.com
^
% Invalid input detected at '^' marker.
R1(dhcp-config)#default-router 192.168.40.1
R1(dhcp-config)#
  
```

Figura 28. Implementación de DHCP y NAT para IPv4 por medio de la configuración del Router R1.

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

Se realiza la configuración de la Nat R2 para habilitar la conexión entre las redes.

```
R2
Physical Config CLI
IOS Command Line Interface
Press RETURN to get started!
El acceso no autorizado se encuentra PROHIBIDO!
User Access Verification
Password:
R2>en
Password:
R2#config t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#user webuser privilege 15 secret cisco12345
R2(config)#ip http server
^
% Invalid input detected at '^' marker.
R2(config)#ip nat inside source static 10.10.10.10 209.165.200.229
R2(config)#int g0/0
R2(config-if)#ip nat outside
R2(config-if)#int g0/1
R2(config-if)#ip nat inside
R2(config-if)#exit
```

Figura 29. Configuración de la NAT en el Router R2.

2.11. Configuración de las listas de acceso estándar y dinámicas.

Se realiza la configuración de dos listas de acceso de tipo estándar y dos listas de acceso de tipo extendido para restringir o permitir tráfico desde R1 o R3 hacia R2.

```

R2 (Config)#exit
R2#
%SYS-5-CONFIG_I: Configured from console by console

R2#config t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#ip nat pool INTERNET 209.165.200.225 209.165.200.228 netmask
R2(config)#exit
R2#
%SYS-5-CONFIG_I: Configured from console by console

R2#config t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#ip nat pool INTERNET 209.165.200.225 209.165.200.228 netmask
R2(config)#access-list 101 permit icmp host 172.31.21.0 host 209.165.200.225
R2(config)#access-list 102 permit icmp host 172.31.23.0 host 209.165.200.225
R2(config)#end
R2#
%SYS-5-CONFIG_I: Configured from console by console

R2#show access-list
Standard IP access list 1
 10 permit 192.168.30.0 0.0.0.255
Standard IP access list 2
 10 permit 192.168.4.0 0.0.0.255
Extended IP access list 101
 10 permit icmp host 172.31.21.0 host 209.165.200.225
Extended IP access list 102
 10 permit icmp host 172.31.23.0 host 209.165.200.225
R2#
    
```

Figura 30. Configuración de las listas de acceso estándar y dinámicas el Router R2.

2.12. Verificación de procesos de comunicación.

Se realiza la verificación de procesos de comunicación y de los procesos de redireccionamiento de tráfico en los dispositivos que comprenden el escenario propuesto mediante el uso de Ping y Traceroute.

Verificación la configuración de la IP con DHCP en la PC-A:

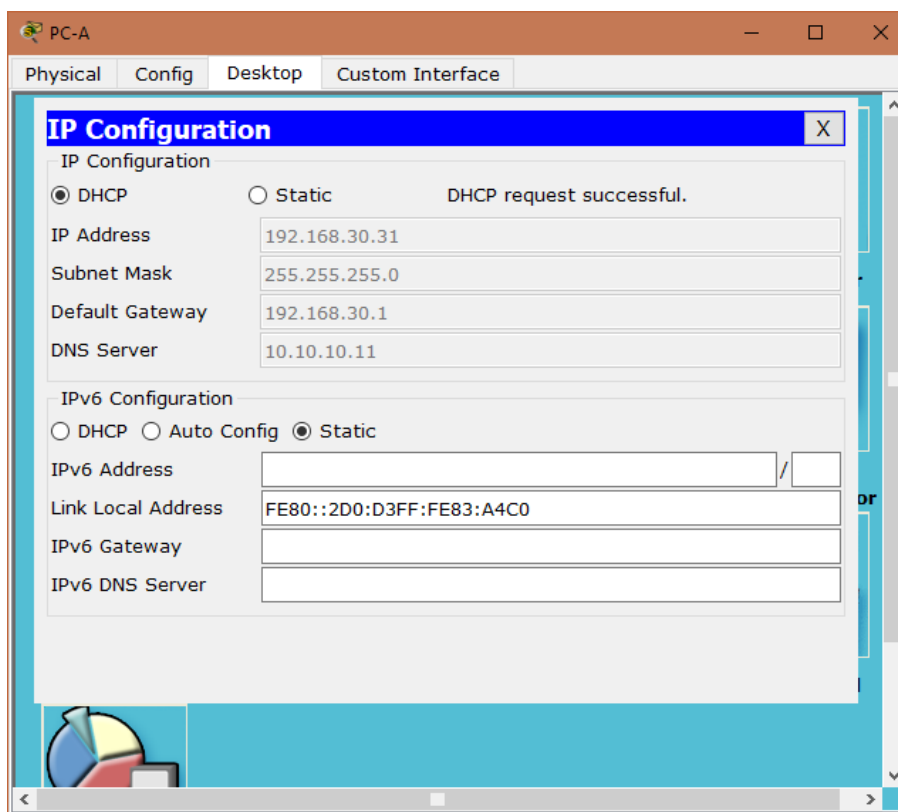


Figura 31. Configuración de la DHCP en la PC-A.

Verificación la configuración de la IP con DHCP en la PC-C:

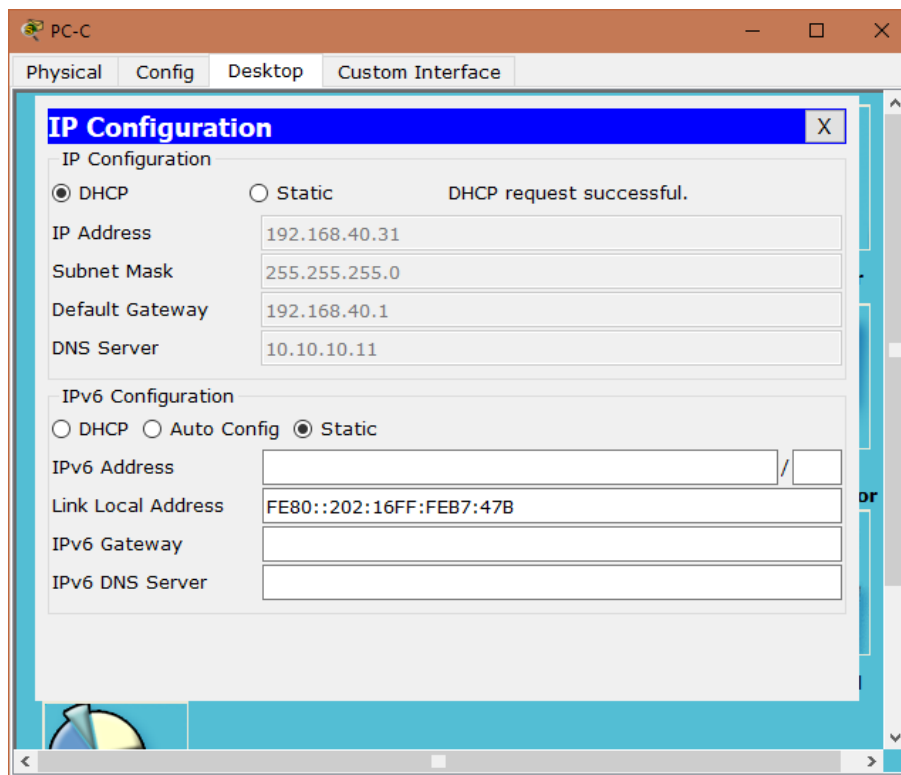


Figura 32. Configuración de la DHCP en la PC-C.

Verificación de conectividad por medio del comando ping entre PC-A y PC-C

```
PC-A
Physical Config Desktop Custom Interface

Command Prompt
PC>ping 192.168.40.31

Pinging 192.168.40.31 with 32 bytes of data:

Request timed out.
Reply from 192.168.40.31: bytes=32 time=1ms TTL=127
Reply from 192.168.40.31: bytes=32 time=0ms TTL=127
Reply from 192.168.40.31: bytes=32 time=0ms TTL=127

Ping statistics for 192.168.40.31:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

PC>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=0ms 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

PC>
```

Figura 33. Ejecución del comando Ping entre PC-A y PC-C

Verificación acceso web desde el dispositivo Internet PC al dispositivo de Web Server.

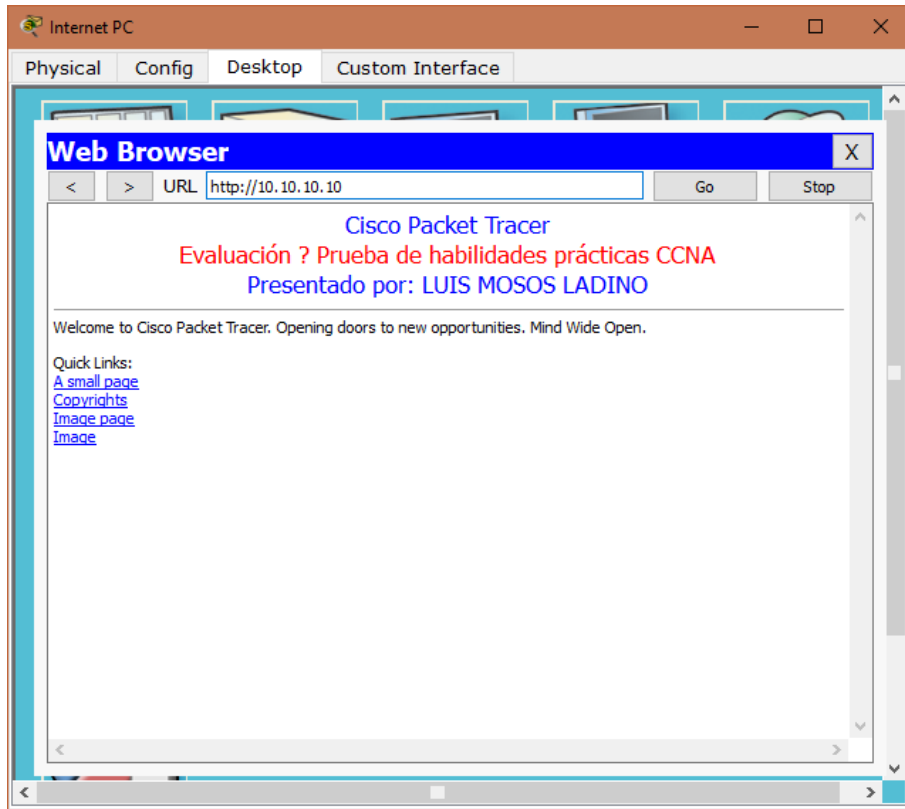


Figura 34. Verificación acceso web desde Internet PC a Web Server

Verificación de conectividad de extremo a extremo con el comando `tracert` entre PCA y web server.

```
PC-C
Physical Config Desktop Custom Interface
Command Prompt
15 * * * * Request timed out.
16 * * * * Request timed out.
17 * * * * Request timed out.
18 * * * * Request timed out.
19 * * * * Request timed out.
20 * * * * Request timed out.
21 * * * * Request timed out.
22 * * * * Request timed out.
23 * * * * Request timed out.
24 * * * * Request timed out.
25 * * * * Request timed out.
26 * * * * Request timed out.
27 * * * * Request timed out.
28 * * * * Request timed out.
29 * * * * Request timed out.
30 * * * * Request timed out.

Trace complete.

PC>tracert 10.10.10.1

Tracing route to 10.10.10.1 over a maximum of 30 hops:

  1  0 ms    0 ms    0 ms    192.168.40.1
  2  1 ms    1 ms    2 ms    10.10.10.1

Trace complete.

PC>
```

Figura 35. Verificación de conectividad con el comando `tracert` entre PC-A y Web Server.

Verificación de conectividad con la ejecución del comando Traceroute.

```

R1
-----
Physical  Config  CLI
-----
IOS Command Line Interface

User Access Verification

Password:

R1>en
Password:
R1#traceroute 10.10.10.1
Type escape sequence to abort.
Tracing the route to 10.10.10.1

 0  172.31.21.2      3 msec    1 msec    3 msec
R1#traceroute 192.165.200.225
Type escape sequence to abort.
Tracing the route to 192.165.200.225

 0  172.31.21.2      14 msec   1 msec    0 msec
 1  *                *
 2  *                *
 3  *                *
 4
R1#traceroute 192.168.30.1
Type escape sequence to abort.
Tracing the route to 192.168.30.1

 0  192.168.30.1    0 msec    3 msec    3 msec
R1#traceroute 192.168.40.1
Type escape sequence to abort.
Tracing the route to 192.168.40.1

 0  192.168.40.1   11 msec   9 msec    3 msec
R1#
    
```

Figura 36. Verificación de conectividad con el comando traceroute entre R1 y Web Server, PC-A, PC-C e Internet PC.

Conclusiones

- Se dio solución practica del escenario propuesto teniendo como base fundamental cada uno de los conocimientos adquiridos durante el desarrollo del Diplomado de Profundización CCNA en cuanto a la implementación y diseño de la topología física y lógica de una red.
- Se analizo la arquitectura propuesta con el fin de implementarla sobre el software de simulación Packet Tracer 6.1.1.0001. el cual no dio las herramientas necesarias para la puesta en marcha de este laboratorio.
- Se aplicaron los conocimientos adquiridos para la la Configuración de protocolos que permiten interconectar cada uno de los dispositivos establecidos para el diseño de una topología de red.
- Por medio de este trabajo final se documentó cada uno de los procedimientos realizados en la implementación del escenario propuesto y se registró la verificación de conectividad entre los dispositivos de acuerdo con la finalidad de el laboratorio practico.

Referencias Bibliográficas

- 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>
- Lucas, M. (2009). Cisco Routers for the Desperate: Router and Switch Management, the Easy Way. San Francisco: No Starch Press. Recuperado de: <http://bibliotecavirtual.unad.edu.co:2048/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=e000xww&AN=440032&lang=es&site=ehost-live>
- 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). Conceptos de Routing. Principios de Enrutamiento y Conmutación. Recuperado de: <https://static-course-assets.s3.amazonaws.com/RSE50ES/module4/index.html#4.0.1.1>
- 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 Dinámico. Principios de Enrutamiento y Conmutación. Recuperado de: <https://static-course-assets.s3.amazonaws.com/RSE50ES/module7/index.html#7.0.1.1>
- 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). 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). 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>