

## PRUEBA DE HABILIDADES PRACTICAS CCNA

Una empresa de tecnología que posee tres sucursales en distintas ciudades, requiere de un administrador de red, que deberá configurar el mejor escenario posible basado en redes cisco.

JORGE ENRIQUE RIAÑO CASTILLO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA  
ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERÍA  
INGENIERÍA ELECTRÓNICA  
ZIPAQUIRÁ  
2018

## PRUEBA DE HABILIDADES PRACTICAS CISCO

Una empresa de tecnología que posee tres sucursales en distintas ciudades, requiere de un administrador de red, que deberá configurar el mejor escenario posible basado en redes cisco.

JORGE ENRIQUE RIAÑO CASTILLO

Informe final del diplomado de cisco ofrecido como opción de grado por la universidad nacional abierta y a distancia UNAD

Director de curso: JUAN CARLOS VESGA

Tutor: EFRAIN ALEJANDRO PÉREZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA  
ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERÍA  
INGENIERÍA ELECTRÓNICA  
ZIPAQUIRÁ  
2018



## AGRADECIMIENTOS

En especial, un sincero gesto de agradecimientos a todas a que las personas que me apoyaron en este hermoso proceso, a mis tutores, a mis colegas y familiares que de una u otra manera me apoyaron en el proceso. Finalmente a la persona más especial y que siempre ha creído en mí, mi esposa Lina. Gracias por todo.

Finalmente, presentar un gran gesto de agradecimiento a la universidad nacional abierta y a distancia (UNAD) en general junto con todo su amplio equipo de trabajo, que sin su valioso modelo no sería posible que muchas personas pudiéramos optar por este tipo de formación. Sinceramente y profundamente agradecido con todo el apoyo y espacio de formación, espero continuar perteneciendo a esta gran familia y poder hacer parte del futuro de la misma.

## TABLA DE CONTENIDO

LISTAS DE TABLAS.....	7
RESUMEN.....	8
INTRODUCCIÓN.....	9
PLANTEAMIENTO DEL PROBLEMA.....	10
Topología de la red.....	10
DESARROLLO E IMPLEMENTACIÓN.....	13
1. CONFIGURACIÓN BÁSICA DE LOS DISPOSITIVOS Y DEL DIRECCIONAMIENTO IP.....	13
1.1. CONFIGURACIÓN BÁSICA Y DE SEGURIDAD EN LOS HOST .....	14
2. Configuración del direccionamiento IP.....	17
2.1. Configuración de IP Router 1: .....	18
2.2. Configuración de IP Router 2: .....	19
2.3. Configuración de IP Router 3: .....	20
3. Configuración de protocolo OSPF.....	21
3.1. Configuración del protocolo OSPF por dispositivo .....	21
3.2. Tablas de enrutamiento y routers conectados.....	24
3.3. Lista resumida por interface pos ospf con costo por interface.....	25
4. Configuración de VLAN, puestos troncales, puntos de acceso, encapsulado, entre otros. ....	27
Creación de la VLAN nativa, según la tabla de direccionamiento. ....	27
4.1. Creación de vlan 30, 40 y 200 .....	28
4.2. Routing entre vlan's.....	32
5. Deshabilitar en S3 DNS lookup.....	33
6. Asignar direcciones IP a los switches según lineamientos. ....	33
6.1. Configuración IP VLAN switch 1 .....	33
6.2. Configuración IP VLAN switch 2.....	33
7. Desactivación de las interfaces inutilizadas en el esquema de red.....	33

7.1. Router 1.....	33
7.2. Router 2.....	34
7.3. Router 3.....	35
7.4. Switch 1.....	35
7.5. Switch 3.....	36
8. Implementación de DHCP y NAT para IPv4 .....	37
8.1. Configuración de R1 como servidor DHCP para las VLAN's 30 y 40 ....	37
8.2. Reservación de las primeras 30 direcciones IP de las VLAN 30 y 40. ..	38
8.3. Configuración de NAT en R2 para habilitar la salida a internet de los host	38
8.4. Configuración de listas de restricción o permiso para el tráfico de R1 o R3 hacia R2.....	38
8.4.2. Listas de tipo extendido.....	39
9. Verificación de comunicación y direccionamiento de tráfico. ....	39
CONCLUSIONES .....	44
BIBLIOGRAFÍA.....	46

## LISTAS DE TABLAS

<i>Tabla 1: OSPFv2 área 0</i> .....	11
<i>Tabla 2: reserva de direcciones solicitada</i> .....	12
Tabla 3: Direccionamiento IP requerido.....	17
Tabla 4: Direccionamiento para las VLAN que se den crear. ....	27

## RESUMEN

Este documento contiene el desarrollo de la prueba de habilidades prácticas, propuesta como trabajo final del diplomado de redes de cisco (CCNA1 y CCNA2), en el cual se integran los conocimientos teórico-prácticos adquiridos en el transcurso del diplomado. Como objeto principal se encuentra el desarrollo de una serie de pasos, para solucionar un problema típico dentro de la administración de redes cisco.

En este problema se plantea una situación característica de la administración de redes, la cual requiere para su solución e implementación el uso de las temáticas previamente vistas en este diplomado, por lo tanto, el estudiante administrador de red, deberá iniciar con la comprensión de los requerimientos y diseñar una tipología en la herramienta de Packet Tracer, posteriormente debe establecer y configurar los dispositivos, router, switch y pc's, con el fin de dar solución a los requerimientos. Además debe configurar parámetros de seguridad, redes VLAN, seguridad, switching, routing, entre otros. Que permiten obtener como resultado la configuración, administración y control de una red básica, pero que integre de manera experimental y práctica los conceptos y técnicas adquiridos en el diplomado.

Finalmente este documento es la evidencia del proceso de aprendizaje que se llevó a cabo, así como se constituye como evidencia de la culminación de un proceso de formación y aprendizaje que requirió de esfuerzo y dedicación.

## INTRODUCCIÓN

La implementación de redes cisco, permite brindar soluciones tecnológicas, de comunicación, administración, control y seguridad de la información para empresas y negocios en cualquier ámbito de la sociedad actual tan globalizada. Con la realización de este trabajo, se ejemplifica a partir de los aprendizajes adquiridos en el diplomado de profundización cisco CCNA 1 y 2, el diseño e implementación de una red integrada Cisco para una empresa supuesta de tecnología que cuenta con tres sedes en distintas empresas y que requiere de comunicación, seguridad e internet, entre otros parámetros descritos más adelante en este trabajo.

Para el desarrollo adecuado de esta implementación, se plantea a partir del problema una serie de pasos, en donde se deberá establecer a partir de la topología, los requerimientos básicos de la red, respecto de los equipos físicos de la misma, posteriormente se establecen las necesidades de configuración e interconexión de los mismos cumpliendo con una topología estándar brindada en la guía de trabajo.

Concordando con esto, se deben establecer el direccionamiento IP de la red y sus dispositivos, para posteriormente configurar un protocolo e enrutamiento OSPFv2, con algunos criterios definidos en el problema. Continuando con el desarrollo se deberá configurar las VLANs, solicitadas en la misma guía, aplicar parámetros de seguridad básicos y estándar de las redes cisco, implementar DHCP y NAT junto con listas ACL de tipos estándar y extendidos según las necesidades observadas por el administrador de la red. De esta manera se determina y se encamina la metodología pensada a emplear en el desarrollo de la red.

Por último el trabajo está limitado a ser un elemento práctico que integra brevemente la aplicación de los conceptos aprendidos en el desarrollo del diplomado y se constituye como un procedentico teórico practico de cómo se configura de manera básica una red con los requerimientos descritos en el planteamiento del problema.

## PLANTEAMIENTO DEL PROBLEMA

Para el adecuado desarrollo del curso y finalización del mismo, diplomado cisco CCNA1 y 2, se propone el desarrollo de manera individual, en el cual el estudiante pueda llevar a buen término los siguientes aspectos solicitados.

Descripción del escenario para la prueba de habilidades.

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 la red.

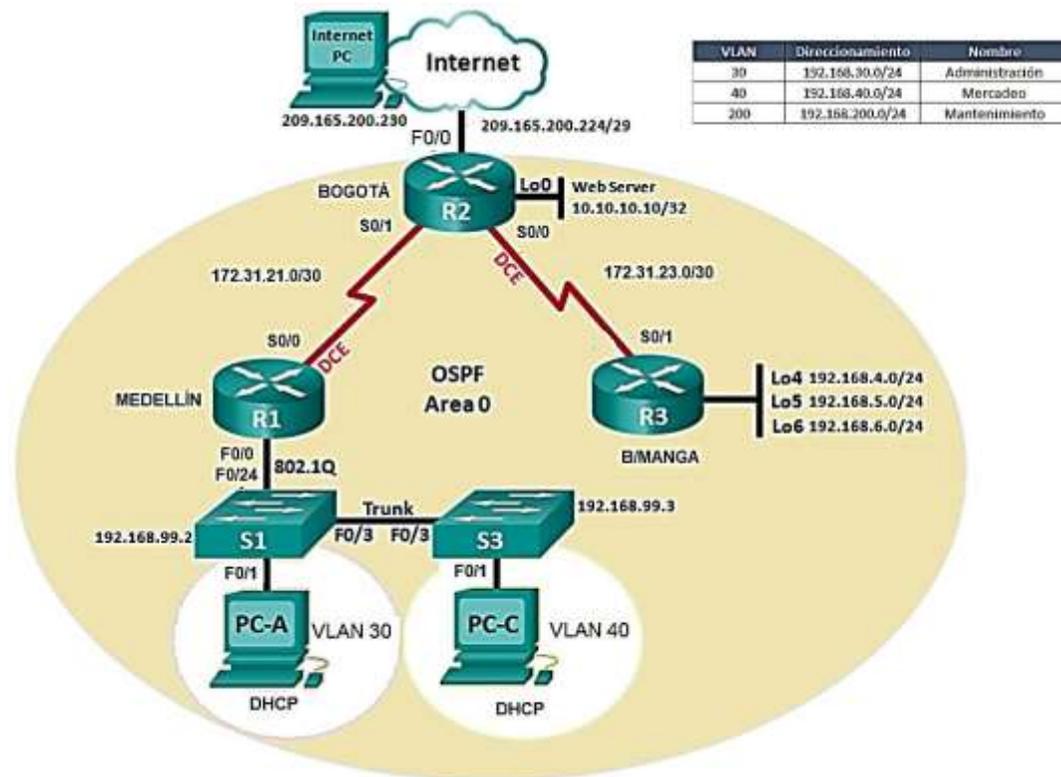


Figura 1: Diseño estándar propuesto para el desarrollo de habilidades prácticas.

Se solicita particularmente el desarrollo de los siguientes ítems:

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:

*Tabla 1: OSPFv2 área 0*

<b>Configuración Ítem o tarea</b>	<b>Especificación</b>
<b>Router ID R1</b>	1.1.1.1
<b>Router ID R2</b>	2.2.2.2
<b>Router ID R3</b>	3.3.3.3
<b>Configurar todas las interfaces LAN como pasivas</b>	
<b>Establecer el ancho de banda para enlaces seriales en</b>	128 Kb/s
<b>Ajustar el costo en la métrica de S0/0 a</b>	7500

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. Implementar DHCP y NAT para 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.

*Tabla 2: reserva de direcciones solicitada*

<b>Configurar DHCP pool para VLAN 30</b>	<b>Name: ADMINISTRACIÓN</b> <b>DNS-Server: 10.10.10.11</b> <b>Domain-Name: ccna-unad.com</b> <b>Establecer default Gateway.</b>
<b>Configurar DHCP pool para VLAN 40</b>	Name: MERCADEO DNS-Server: 10.10.10.11 Domain-Name: ccna-unad.com Establecer default Gateway.

10. Configurar NAT en R2 para permitir que los host 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 re-direccionamiento de tráfico en los routers mediante el uso de Ping y Traceroute.

## DESARROLLO E IMPLEMENTACIÓN

Con base en las solicitudes establecidas en la descripción y planteamiento del problema, es necesario establecer en primera instancia algunos elementos teóricos respecto de la topología y diseño preliminar de la red que espera implementar y administrar con base en los conocimientos adquiridos durante el desarrollo del curso diplomado en redes de CISCO. Por tanto en este momento se hace uso de la herramienta virtual de cisco, Packet Tracer. En el cual se establece la siguiente topología.

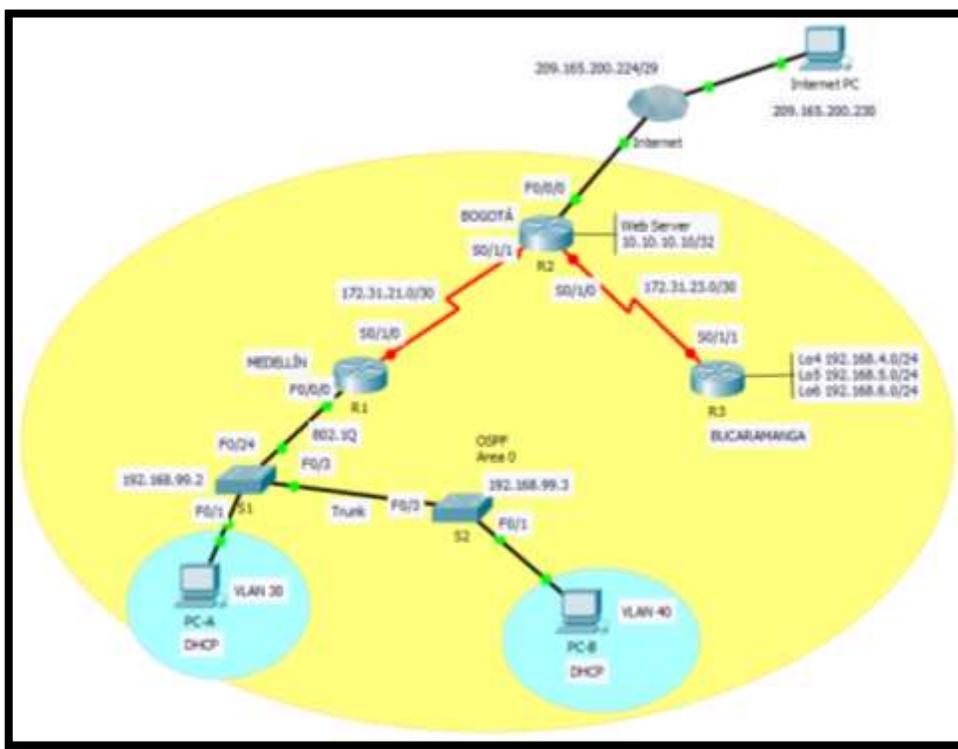


Figura 2. Topología requerida para el ejercicio (Desarrollada en Packet Tracer E. Riaño).

### 1. CONFIGURACIÓN BÁSICA DE LOS DISPOSITIVOS Y DEL DIRECCIONAMIENTO IP.

Se inicia la configuración básica de los dispositivos, es decir establecer el nombre del host, las contraseñas de seguridad y banner de seguridad entre otros aspectos.

Es importante aclarar que las contraseñas establecidas en el diseño no son seguras, por lo tanto estas se establecieron solo por cuestiones pedagógicas, sin embargo en la puesta en marcha de la red estas deberían ser remplazadas por contraseñas seguras y para mejor seguridad cada dispositivo debería contar con una contraseña diferente.

### 1.1. CONFIGURACIÓN BÁSICA Y DE SEGURIDAD EN LOS HOST

Se aplican los siguientes comandos para general la configuración de los host según el lenguaje de programación aplicado en los dispositivos cisco CLI

#### 1.1.1. Router 1:

```
Router>en
Router#config t

Router(config)#hostname R1

R1(config)#enable secret WMS43

R1(config)#banner motd &!!NO SE PERMITE EL INGRESO, SOLAMENTE
PERSONAL AUTORIZADO!!&

R1(config)#line console 0
R1(config-line)#exec-timeout 5 30
R1(config-line)#password WMS
R1(config-line)#login
R1(config-line)#logging synchronous
R1(config-line)#exit

R1(config)#line vty 0 4
R1(config-line)#exec-timeout 5 30
R1(config-line)#password WMF
R1(config-line)#login
R1(config-line)#logging synchronous
R1(config-line)#exit
R1(config)#service password-encryption
R1(config)#exit

R1#copy run start
Destination filename [startup-config]?
Building configuration...
[OK]
```

#### 1.1.2. Router 2:

```
Router>en
```

```
Router#config t

Router(config)#hostname R2

R2(config)#enable secret WMS43

R2(config)#banner motd &!!NO SE PERMITE EL INGRESO, SOLAMENTE
PERSONAL AUTORIZADO!!&

R2(config)#line console 0
R2(config-line)#exec-timeout 5 30
R2(config-line)#password WMS
R2(config-line)#login
R2(config-line)#logging synchronous
R2(config-line)#exit

R2(config)#line vty 0 4
R2(config-line)#exec-timeout 5 30
R2(config-line)#password WMS
R2(config-line)#login
R2(config-line)#logging synchronous
R2(config-line)#exit
R2(config)#service password-encryption
R2(config)#exit

R2#copy run start
Destination filename [startup-config]?
Building configuration...
[OK]
```

### 1.1.3. Router 3:

```
Router>en
Router#config t
Router(config)#hostname R3

R3(config)#enable secret WMS43

R3(config)#banner motd &!!NO SE PERMITE EL INGRESO, SOLAMENTE
PERSONAL AUTORIZADO!!&

R3(config)#line console 0
R3(config-line)#exec-timeout 5 30
R3(config-line)#password WMS
R3(config-line)#login
R3(config-line)#logging synchronous
```

```
R3(config-line)#exit

R3(config)#line vty 0 4
R3(config-line)#exec-timeout 5 30
R3(config-line)#password WMS
R3(config-line)#login
R3(config-line)#logging synchronous
R3(config-line)#exit
R3(config)#service password-encryption
R3(config)#exit
```

```
R3#copy run start
Destination filename [startup-config]?
Building configuration...
[OK]
```

#### 1.1.4. Switch 1:

```
Switch>en
Switch#config t
Switch(config)#hostname S1
S1(config)#enable secret WMS43
S1(config)#banner motd &!!NO SE PERMITE EL INGRESO, SOLAMENTE
PERSONAL AUTORIZADO!!&
```

```
S1(config)#line console 0
S1(config-line)#exec-timeout 5 30
S1(config-line)#password WMS
S1(config-line)#login
S1(config-line)#logging synchronous
S1(config-line)#exit
```

```
S1(config)#line vty 0 15
S1(config-line)#exec-timeout 5 30
S1(config-line)#password WMS
S1(config-line)#login
S1(config-line)#logging synchronous
S1(config-line)#exit
S1(config)#service password-encryption
S1(config)#exit
```

```
S1#copy run start
Destination filename [startup-config]?
Building configuration...
[OK]
```

### 1.1.5. Switch 3:

```
Switch>en
Switch#config t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname S1
S3(config)#enable secret WMS43
S3(config)#banner motd &!!NO SE PERMITE EL INGRESO, SOLAMENTE
PERSONAL AUTORIZADO!!&
S3(config)#line console 0
S3(config-line)#exec-timeout 5 30
S3(config-line)#password WMS
S3(config-line)#login
S3(config-line)#logging synchronous
S3(config-line)#exit
S3(config)#line vty 0 15
S3(config-line)#exec-timeout 5 30
S3(config-line)#password WMS
S3(config-line)#login
S3(config-line)#logging synchronous
S3(config-line)#exit
S3(config)#service password-encryption
S3(config)#exit

S1#copy run start
Destination filename [startup-config]?
Building configuration...
[OK]
```

## 2. Configuración del direccionamiento IP.

En este momento y a partir del diseño presentado o propuesto en el planteamiento del problema, se dispone a obtener y configurar las direcciones IP necesarias en los host, con el fin de dar cumplimiento a esta etapa en el diseño de la red.

*Tabla 3: Direccionamiento IP requerido.*

Dispositivo	interfaz	Dirección IP	Mascara de subred	Gateway Predeterminado
<b>Internet</b>	Ethernet	209.165.200.225	255.255.255.248	N/A
<b>R1</b>	S0/0/0	172.31.21.2	255.255.255.252	N/A
	G0/0	192.168.99.1	255.255.255.0	N/A
<b>R2</b>	S0/0/0	172.31.23.1	255.255.255.252	N/A
	S0/0/1	172.31.21.1	255.255.255.252	N/A
	Web Server	10.10.10.10	255.255.255.255	N/A

	G0/0	209.165.200.226	255.255.255.248	N/A
<b>R3</b>	S0/0/1	172.31.23.2	255.255.255.252	N/A
	Lo4	192.168.4.0	255.255.255.0	N/A
	Lo5	192.168.5.0	255.255.255.0	N/A
	Lo6	192.168.6.0	255.255.255.0	N/A
<b>S1</b>	VLAN 1	192.168.99.2	255.255.255.0	192.168.99.1
	VLAN30	192.168.30.2	255.255.255.0	192.168.99.1
	VLAN40	192.168.40.2	255.255.255.0	192.168.99.1
	VLAN200	192.168.200.2	255.255.255.0	192.168.99.1
<b>S3</b>	VLAN 1	192.168.99.3	255.255.255.0	192.168.99.1
	VLAN30	192.168.30.3	255.255.255.0	192.168.99.1
	VLAN40	192.168.40.3	255.255.255.0	192.168.99.1
	VLAN200	192.168.200.3	255.255.255.0	192.168.99.1
<b>PC-A</b>	NIC	DHCP		
<b>PC-B</b>	NIC	DHCP		
<b>Internet PC</b>	NIC	209.165.200.230	255.255.255.248	

A partir de esta tabla es posible iniciar con las configuraciones particulares en casa dispositivo o host de la red, mediante los siguientes comandos en CLI. Es importante resaltar que para configurar la terminal de internet (nube), se utilizó un switch con la VLAN 1 predeterminada, con la ip 209.165.200.226/29, de la misma forma se incluye en la configuración del protocolo OSPF de R2.

## 2.1. Configuración de IP Router 1:

```
R1#Config t
R1(config)#interface S0/0/0
R1(config-if)#ip address 172.31.21.2 255.255.255.252
R1(config-if)#description Link a R2
R1(config-if)#no shutdown

R1(config)#interface G0/0
R1(config)#ip address 192.168.99.1 255.255.255.0
R1(config-if)#description Link a S1
R1(config-if)#no shutdown
R1(config-if)#end
```

```
Building configuration...
[OK]
R1#Config t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#interface S0/0/0
R1(config-if)#ip address 172.31.21.2 255.255.255.252
R1(config-if)#description Link a R2
R1(config-if)#clock rat 128000
R1(config-if)#no shutdown

%LINK-5-CHANGED: Interface Serial0/0/0, changed state to down
R1(config-if)#interface G0/0
R1(config-if)#ip address 192.168.99.1 255.255.255.0
R1(config-if)#description Link a 802.1Q
R1(config-if)#no shutdown

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

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

R1(config-if)#end
R1#
%SYS-5-CONFIG_I: Configured from console by console

R1#
```

## 2.2. Configuración de IP Router 2:

```
R2#config t
R2(config)#interface s0/0/1
R2(config-if)#ip address 172.31.21.1 255.255.255.252
R2(config-if)#description Link a R1
R2(config-if)#no shutdown

R2(config)#interface s0/0/0
R2(config-if)#ip address 172.31.23.1 255.255.255.252
R2(config-if)#description link a R3
R2(config-if)#no shutdown

R2(config)#interface G0/0
R2(config-if)#ip address 209.165.200.225 255.255.255.248
R2(config-if)#description link a Internet
R2(config-if)#no shutdown

R2(config)#interface loopback0
R2(config-if)#ip address 10.10.10.10 255.255.255.255
R2(config-if)#description link a Web Server
R2(config-if)#no shutdown

R2(config-if)#end
```

```
changed state to up

R2#config t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#interface s0/0/1
R2(config-if)#ip address 172.31.21.2 255.255.255.252
R2(config-if)#description Link a R1
R2(config-if)#no shutdown
R2(config-if)#interface s0/0/0
R2(config-if)#ip address 172.31.23.1 255.255.255.252
R2(config-if)#clock rate 128000
R2(config-if)#description link a R3
R2(config-if)#no shutdown
R2(config-if)#interface G0/0
R2(config-if)#ip address 209.165.200.226 255.255.255.248
R2(config-if)#description link a Internet
R2(config-if)#no shutdown
R2(config-if)#interface loopback0
R2(config-if)#ip address 10.10.10.10 255.255.255.255
R2(config-if)#description link a Web Server
R2(config-if)#no shutdown
R2(config-if)#end
R2#
%SYS-5-CONFIG_I: Configured from console by console

R2#
```

### 2.3. Configuración de IP Router 3:

```
R3#config t
R3(config)#interface s0/0/1
R3(config-if)#ip address 172.31.23.2 255.255.255.252
R3(config-if)#description Link a R3
R3(config-if)#no shutdown

R3(config)#interface loopback4
R3(config-if)#ip address 192.168.4.1 255.255.255.0
R3(config-if)#description Link a Lo4
R3(config-if)#no shutdown

R3(config)#interface loopback5
R3(config-if)#ip address 192.168.5.1 255.255.255.0
R3(config-if)#description Link a Lo5
R3(config-if)#no shutdown

R3(config)#interface loopback6
R3(config-if)#ip address 192.168.6.1 255.255.255.0
R3(config-if)#description Link a Lo6
R3(config-if)#no shutdown

R3(config-if)#end
```

```

%SYS-5-CONFIG_I: Configured from console by console

R3#config t
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#interface s0/0/1
R3(config-if)#ip address 172.31.23.2 255.255.255.252
R3(config-if)#description Link a R3
R3(config-if)#no shutdown
R3(config-if)#interface loopback4
R3(config-if)#ip address 192.168.4.1 255.255.255.0
R3(config-if)#description Link a Lo4
R3(config-if)#no shutdown
R3(config-if)#interface loopback5
R3(config-if)#ip address 192.168.5.1 255.255.255.0
R3(config-if)#description Link a Lo5
R3(config-if)#no shutdown
R3(config-if)#interface loopback6
R3(config-if)#ip address 192.168.6.1 255.255.255.0
R3(config-if)#description Link a Lo6
R3(config-if)#no shutdown
R3(config-if)#end
R3#copy run start
%SYS-5-CONFIG_I: Configured from console by console

R3#copy run start
Destination filename [startup-config]?
Building configuration...
[OK]

```

### 3. Configuración de protocolo OSPF.

En una segunda instancia se solicita establecer y configurar el protocolo OSPF, para tal fin se dispone de los siguientes comandos de configuración. También es importante resaltar que se tiene en cuenta los parámetros descritos y estipulados en la tabla 1.

#### 3.1. Configuración del protocolo OSPF por dispositivo

##### 3.1.1. Configuración del protocolo OSPF en R1.

```

R1(config)#ROUTER OSPF 10
R1(config-router)#router-id 1.1.1.1
R1(config-router)#network 192.168.99.0 0.0.0.255 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)#network 172.31.21.0 0.0.0.3 area 0
R1(config-router)#passive-int g0/0.1
R1(config-router)#passive-int g0/0.30
R1(config-router)#passive-int g0/0.40
R1(config-router)#passive-int g0/0.200
R1(config-router)#end

R1(config)#int s0/0/0
R1(config-if)#bandwidth 128000
R1(config-if)#ip ospf cost 7500
R1(config-if)#end

```

```
R1#CONFIG T
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#
R1(config)#ROUTER OSPF 10
R1(config-router)#router-id 1.1.1.1
R1(config-router)#network 192.168.99.0 0.0.0.255 area 0
R1(config-router)#network 172.31.21.0 0.0.0.3 area 0
R1(config-router)#passive-int g0/0
R1(config-router)#end
R1#
%SYS-5-CONFIG_I: Configured from console by console

R1#
02:07:24: %OSPF-5-ADJCHG: Process 10, Nbr 2.2.2.2 on Serial0/0/0
from LOADING to FULL, Loading Done
```

### 3.1.2. Configuración del protocolo OSPF en R2.

```
R2(config)#router ospf 10
R2(config-router)#router-id 2.2.2.2
R2(config-router)#network 209.165.200.224 0.0.0.7 area 0
R2(config-router)#network 172.31.21.0 0.0.0.3 area 0
R2(config-router)#network 172.31.23.0 0.0.0.3 area 0
R2(config-router)#network 10.10.10.10 0.0.0.0 area 0
R2(config-router)#passive-int g0/0
R2(config-router)#passive-int loopback0
R2(config-router)#end
```

```
R2(config)#int s0/0/1
R2(config-if)#bandwidth 128000
R2(config-if)#ip ospf cost 7500
R2(config-if)#end
```

```
R2(config)#int s0/0/0
R2(config-if)#bandwidth 128000
R2(config-if)#ip ospf cost 7500
R2(config-if)#end
```

```

R2#config t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#router ospf 10
R2(config-router)#router-id 2.2.2.2
R2(config-router)#network 209.165.200.224 0.0.0.7 area 0
R2(config-router)#network 172.31.21.0 0.0.0.3 area 0
R2(config-router)#network 172.31.23.0 0.0.0.3 area 0
R2(config-router)#network 10.10.10.10 0.0.0.0 area 0
R2(config-router)#passive-int g0/0
R2(config-router)#passive-int loopback0
R2(config-router)#end
R2#
%SYS-5-CONFIG_I: Configured from console by console

R2#
02:07:24: %OSPF-5-ADJCHG: Process 10, Nbr 1.1.1.1 on Serial0/0/1
from LOADING to FULL, Loading Done

R2#
02:08:37: %OSPF-5-ADJCHG: Process 10, Nbr 3.3.3.3 on Serial0/0/0
from LOADING to FULL, Loading Done

```

### 3.1.3. Configuración del protocolo OSPF en R3.

```

R3(config)#router ospf 10
R2(config-router)#router-id 3.3.3.3
R3(config-router)#network 192.168.4.0 0.0.0.255 area 0
R3(config-router)#network 192.168.5.0 0.0.0.255 area 0
R3(config-router)#network 192.168.6.0 0.0.0.255 area 0
R3(config-router)#network 172.31.23.0 0.0.0.3 area 0
R3(config-router)#passive-int loopback4
R3(config-router)#passive-int loopback5
R3(config-router)#passive-int loopback6
R3(config-router)#end

R3(config)#int s0/0/1
R3(config-if)#bandwidth 128000
R3(config-if)#ip ospf cost 7500
R3(config-if)#end

```

```

R3#config t
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#router ospf 1
R3(config-router)#router-id 3.3.3.3
R3(config-router)#network 192.168.4.0 0.0.0.255 area 0
R3(config-router)#network 192.168.5.0 0.0.0.255 area 0
R3(config-router)#network 192.168.6.0 0.0.0.255 area 0
R3(config-router)#network 172.31.23.0 0.0.0.3 area 0
R3(config-router)#passive-int loopback4
R3(config-router)#passive-int loopback5
R3(config-router)#passive-int loopback6
R3(config-router)#end
R3#
%SYS-5-CONFIG_I: Configured from console by console

R3#
02:08:37: %OSPF-5-ADJCHG: Process 1, Nbr 2.2.2.2 on Serial0/0/1
from LOADING to FULL, Loading Done

```

Ahora podemos verificar en cada uno de los router los vecinos ospf en donde se muestran cada una de las adyacencias:

### 3.2. Tablas de enrutamiento y routers conectados.

Para poder observar los vecinos ospf y la información de routing, es posible usar los comandos **show ip ospf neighbor** para observar los vecinos, y el comando **show IP route**, para ver la tabla de routing, obteniendo el siguiente resultado:

En R1:

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#SHOW IP ROUTE
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route

Gateway of last resort is not set

10.0.0.0/32 is subnetted, 1 subnets
O 10.10.10.10/32 [110/65] via 172.31.21.2, 00:06:45, Serial0/0/0
172.31.0.0/16 is variably subnetted, 3 subnets, 2 masks
C 172.31.21.0/30 is directly connected, Serial0/0/0
L 172.31.21.2/32 is directly connected, Serial0/0/0
O 172.31.23.0/30 [110/128] via 172.31.21.2, 00:06:45, Serial0/0/0
192.168.99.0/24 is variably subnetted, 2 subnets, 2 masks
C 192.168.99.0/24 is directly connected, GigabitEthernet0/0
L 192.168.99.1/32 is directly connected, GigabitEthernet0/0
209.165.200.0/29 is subnetted, 1 subnets
O 209.165.200.224/29 [110/65] via 172.31.21.2, 00:06:45, Serial0/0/0

```

En R2:

Neighbor ID	Pri	State	Dead Time	Address	Interface
1.1.1.1	0	FULL/ -	00:00:38	172.31.21.2	Serial0/0/1
3.3.3.3	0	FULL/ -	00:00:38	172.31.23.2	Serial0/0/0

```

R2#SHOW IP ROUTE
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS
inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

    10.0.0.0/32 is subnetted, 1 subnets
C       10.10.10.10/32 is directly connected, Loopback0
       172.31.0.0/16 is variably subnetted, 4 subnets, 2 masks
C       172.31.21.0/30 is directly connected, Serial0/0/1
L       172.31.21.2/32 is directly connected, Serial0/0/1
C       172.31.23.0/30 is directly connected, Serial0/0/0
L       172.31.23.1/32 is directly connected, Serial0/0/0
O       192.168.99.0/24 [110/65] via 172.31.21.2, 00:07:48, Serial0/0/1
       209.165.200.0/24 is variably subnetted, 2 subnets, 2 masks
C       209.165.200.224/29 is directly connected, GigabitEthernet0/0
L       209.165.200.226/32 is directly connected, GigabitEthernet0/0

```

En R3:

Neighbor ID	Pri	State	Dead Time	Address	Interface
2.2.2.2	0	FULL/ -	00:00:38	172.31.23.1	Serial0/0/1

```

R3#SHOW IP ROUTE
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS
inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

    10.0.0.0/32 is subnetted, 1 subnets
O       10.10.10.10/32 [110/65] via 172.31.23.1, 00:07:52, Serial0/0/1
       172.31.0.0/16 is variably subnetted, 3 subnets, 2 masks
O       172.31.21.0/30 [110/128] via 172.31.23.1, 00:07:52, Serial0/0/1
C       172.31.23.0/30 is directly connected, Serial0/0/1
L       172.31.23.2/32 is directly connected, Serial0/0/1
O       192.168.99.0/24 [110/129] via 172.31.23.1, 00:07:52, Serial0/0/1
       209.165.200.0/29 is subnetted, 1 subnets
O       209.165.200.224/29 [110/65] via 172.31.23.1, 00:07:52,
Serial0/0/1

```

### 3.3. Lista resumida por interface pos ospf con costo por interface.

Mediante el comando **show ip interface brief**, es posible obtener una lista que muestra mediante una lista las distintas interfaces, el PID, el área la dirección IP el costo el estado, sin embargo no es posible usarlo en el Packet Tracer. A continuación se presentan los resultados del comando show IP ospf interface s-/- para cada uno de los routers y cada una de sus interfaces:

```
R1#show ip ospf interface s0/0/0
```

```
Serial0/0/0 is up, line protocol is up
Internet address is 172.31.21.2/30, Area 0
Process ID 10, 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 00:00:01
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 2.2.2.2
Suppress hello for 0 neighbor(s)
```

```
R2#show ip ospf interface s0/0/0
```

```
R2#SHOW IP OSPF INTERFACE S0/0/0

Serial0/0/0 is up, line protocol is up
Internet address is 172.31.23.1/30, Area 0
Process ID 10, 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 00:00:05
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 3.3.3.3
Suppress hello for 0 neighbor(s)
```

```
R2#show ip ospf interface s0/0/1
```

```
R2#SHOW IP OSPF INTERFACE S0/0/1

Serial0/0/1 is up, line protocol is up
Internet address is 172.31.21.2/30, Area 0
Process ID 10, 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 00:00:01
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)
```

```
R3#show ip ospf interface s0/0/1
```

```

R3#SHOW IP OSPF INTERFACE S0/0/1

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 00:00:08
 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)

```

4. Configuración de VLAN, puestos troncales, puntos de acceso, encapsulado, entre otros.

Como ya es claro, las VLAN se diseñan para segmentar las redes conmutadas. En este caso el método también se conoce como “routing entre VLAN con router-on-a-stick”. Particularmente para dar solución a esta solicitud, se inicia a partir de la tabla propuesta en la definición del problema.

*Tabla 4: Direccionamiento para las VLAN que se den crear.*

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

Creación de la VLAN nativa, según la tabla de direccionamiento.

Se activan las VLAN nativas en los dos switches S1 y S3, mediante los siguientes comandos:

```

S1(config)#config t
S1(config)#interface vlan 1
S1(config-if)#ip address 192.168.99.2 255.255.255.0
S1(config-if)#no shutdown
S1(config-if)#end

```

```

S3#config t
S3(config)#interface vlan 1
S3(config-if)#ip address 192.168.99.3 255.255.255.0
S3(config-if)#no shutdown
S3(config-if)#end

```

Se debe configurar el Gateway predeterminado en los dos switches mediante:

```
S1(config)#ip default-gateway 192.168.99.1
```

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

#### 4.1. Creación de vlan 30, 40 y 200

A continuación se presentan los comandos necesarios para el establecimiento de las VLANs configuradas en los dispositivos que se desprenden del router uno, el cual hará el routing para estas velan, descrito y configurado más adelante.

##### 4.1.1. Switch 1:

```
S1(config)#vlan 30
S1(config-vlan)# name Administracion
S1(config-vlan)# exit
S1(config)#interface vlan 30
S1(config-if)#ip address 192.168.30.2 255.255.255.0
S1(config-if)#no shutdown
S1(config)#vlan 40
S1(config-vlan)# name Mercadeo
S1(config-vlan)# exit
S1(config)#interface vlan 40
S1(config-if)#ip address 192.168.40.2 255.255.255.0
S1(config-if)#no shutdown
S1(config)#vlan 200
S1(config-vlan)# name Mantenimiento
S1(config-vlan)# exit
S1(config)#interface vlan 200
S1(config-if)#ip address 192.168.200.2 255.255.255.0
S1(config-if)#no shutdown
```

VLAN Name	Status	Ports
1 default	active	Fa0/1, Fa0/2, Fa0/3, Fa0/4 Fa0/5, Fa0/6, Fa0/7, Fa0/8 Fa0/9, Fa0/10, Fa0/11, Fa0/12 Fa0/13, Fa0/14, Fa0/15, Fa0/16 Fa0/17, Fa0/18, Fa0/19, Fa0/20 Fa0/21, Fa0/22, Fa0/23, Fa0/24 Gig0/1, Gig0/2
30 Administracion	active	
40 Mantenidos	active	
200 Mantenimiento	active	
1002 cddi-default	act/unsup	
1003 cckae-ring-default	act/unsup	
1004 fdinet-default	act/unsup	
1005 rxnet-default	act/unsup	

VLAN	Type	SAID	MTU	Parent	RingNo	BridgeNo	Stp	BridgeMode	Trans1	Trans2
1	enet	100001	1500	-	-	-	-	-	0	0
30	enet	100030	1500	-	-	-	-	-	0	0
40	enet	100040	1500	-	-	-	-	-	0	0
200	enet	100200	1500	-	-	-	-	-	0	0
1002	fdnl	101002	1500	-	-	-	-	-	0	0
1003	rs	101003	1500	-	-	-	-	-	0	0
1004	fdnet	101004	1500	-	-	-	ieee	-	0	0
1005	rxnet	101005	1500	-	-	-	ibm	-	0	0

Se asignan los respectivos puertos, primero se configura el puerto f0/1, el cual solo debe estar como puerto de acceso, y debe pertenecer a la VLAN 30.

```
S1(config)#interface f0/1
S1(config-if)#switchport mode access
S1(config-if)#switchport Access vlan 30
S1(config-if)#exit
```

Enseguida se debe configurar tanto el puerto f0/3 y f0/24 como enlaces troncales.

```
S1(config)#interface f0/3
S1(config-if)#switchport mode trunk
S1(config-if)#interface f0/24
S1(config-if)#switchport mode trunk
S1(config-if)#exit
```

También se trasladan todos los demás puertos del switch, es decir lo que están temporalmente inutilizados del VLAN de mantenimiento a la VLAN 200 para mejorar la seguridad de acceso en el switch mover puertos

```
S1(config)#interface range g0/1-2
S1(config-if)#switchport Access vlan 200
S1(config)#exit
S1(config)#interface f0/2
S1(config-if)#switchport Access vlan 200
S1(config-if)#exit
S1(config)#interface range f0/4-23
S1(config-if)#switchport Access vlan 200
S1(config-if)#exit
```

VLAN Name	Status	Ports
1 default	active	
30 Administracion	active	Fa0/1
40 Mercadeo	active	
88 VLAN0088	active	Fa0/2, Fa0/4, Fa0/5, Fa0/6 Fa0/7, Fa0/8, Fa0/9, Fa0/10 Fa0/11, Fa0/12, Fa0/13, Fa0/14 Fa0/15, Fa0/16, Fa0/17, Fa0/18 Fa0/19, Fa0/20, Fa0/21, Fa0/22 Fa0/23, Gig0/1, Gig0/2
200 Mantenimiento	active	
1002 fddi-default	act/unsup	
1003 token-ring-default	act/unsup	
1004 fddinet-default	act/unsup	
1005 rsmnet-default	act/unsup	

VLAN	Type	SAID	MTU	Parent	RingNo	BridgeNo	Stp	BridgeMode	Trans1	Trans2
1	enat	100001	1500	-	-	-	-	-	0	0
30	enat	100030	1500	-	-	-	-	-	0	0
40	enat	100040	1500	-	-	-	-	-	0	0
88	enat	100088	1500	-	-	-	-	-	0	0

Se realiza de manera similar con el switch 3

#### 4.1.2. Switch 3

```

S3(config)#vlan 30
S3(config-vlan)# name Administracion
S3(config-vlan)# exit
S3(config)#interface vlan 30
S3(config-if)#ip address 192.168.30.3 255.255.255.0
S3(config-if)#no shutdown
S3(config)#vlan 40
S3(config-vlan)# name Mercadeo
S3(config-vlan)# exit
S3(config)#interface vlan 40
S3(config-if)#ip address 192.168.40.3 255.255.255.0
S3(config-if)#no shutdown
S3(config)#vlan 200
S3(config-vlan)# name Mantenimiento
S3(config-vlan)# exit
S3(config)#interface vlan 200
S3(config-if)#ip address 192.168.200.3 255.255.255.0
S3(config-if)#no shutdown

```

```

S1(config-l1)#end
S1#
%SYS-5-CONFIG_I: Configured from console by console

S1#show vlan

VLAN Name                Status    Ports
-----
1    default                active    Fa0/1
30   Administracion          active    Fa0/1
40   Mercadeo                active    Fa0/2, Fa0/4, Fa0/5, Fa0/6
200  Mantenimiento           active    Fa0/7, Fa0/8, Fa0/9, Fa0/10
                                           Fa0/11, Fa0/12, Fa0/13, Fa0/14
                                           Fa0/15, Fa0/16, Fa0/17, Fa0/18
                                           Fa0/19, Fa0/20, Fa0/21, Fa0/22
                                           Fa0/23, Gig0/1, Gig0/2

1002 fddi-default          act/unsup
1003 token-ring-default   act/unsup
1004 fddinet-default      act/unsup
1005 trnet-default        act/unsup

VLAN Type  SAID      MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
-----
1    enet    100001   1500  -     -     -     -     -     0     0
30   enet    100030   1500  -     -     -     -     -     0     0
40   enet    100040   1500  -     -     -     -     -     0     0
--More--

```

Se asignan los respectivos puertos, primero se configura el puerto f0/1, el cual solo debe estar como puerto de acceso, y debe pertenecer a la VLAN 40.

```

S3(config)#interface f0/1
S3(config-if)#switchport mode access
S3(config-if)#switchport Access vlan 40
S3(config-if)#exit

```

Enseguida se debe configurar el puerto f0/3 como enlace troncales.

```

S3(config)#interface f0/3
S3(config-if)#switchport mode trunk
S3(config-if)#exit

```

También se trasladan todos los demás puertos del switch, es decir lo que están temporalmente inutilizados del VLAN default a la VLAN 10 para mejorar la seguridad de acceso en el switch

```

S3(config)#interface range g0/1-2
S3(config-if)#switchport Access vlan 200
S3(config-if)#exit
S3(config)#interface f0/2
S3(config-if)#switchport Access vlan 200
S3(config-if)#exit
S3(config)#interface range f0/4-24
S3(config-if)#switchport Access vlan 200
S3(config-if)#exit

```

```

S3(config)#end
S3#
%SYS-5-CONFIG_I: Configured from console by console

S3#show vlan

VLAN Name                Status    Ports
-----
1    default                active
30   Administracion          active
40   Mercadeo                active    Fa0/1
200  Mantenimiento           active    Fa0/2, Fa0/4, Fa0/5, Fa0/6
                                           Fa0/7, Fa0/8, Fa0/9, Fa0/10
                                           Fa0/11, Fa0/12, Fa0/13, Fa0/14
                                           Fa0/15, Fa0/16, Fa0/17, Fa0/18
                                           Fa0/19, Fa0/20, Fa0/21, Fa0/22
                                           Fa0/23, Fa0/24, Gig0/1, Gig0/2

1002 fddi-default          act/unsup
1003 token-ring-default   act/unsup
1004 fddinet-default       act/unsup
1005 trnet-default        act/unsup

VLAN Type  SAID      MTU   Parent RingNo BridgeNo  Stp  BrdgMode Trans1 Trans2
-----
1    enet  100001   1500  -     -     -       -   -         0      0
30   enet  100030   1500  -     -     -       -   -         0      0
40   enet  100040   1500  -     -     -       -   -         0      0
--More--

```

#### 4.2. Routing entre vlan's

Se configura el R1 para enrutar a varias VLAN mediante la creación de subinterfaces para cada VLAN. Este método de routing entre VLAN se denomina "router-on-a-stick".

```

R1(config)#interface g0/0.1
R1(config-subif)#encapsulation dot1q 1
R1(config-subif)#ip address 192.168.99.1 255.255.255.0
R1(config-subif)#exit

```

```

R1(config)#interface g0/0.30
R1(config-subif)#encapsulation dot1q 30
R1(config-subif)#ip address 192.168.30.1 255.255.255.0
R1(config-subif)#exit

```

```

R1(config)#interface g0/0.40
R1(config-subif)#encapsulation dot1q 40
R1(config-subif)#ip address 192.168.40.1 255.255.255.0
R1(config-subif)#exit

```

```

R1(config)#interface g0/0.200
R1(config-subif)#encapsulation dot1q 40
R1(config-subif)#ip address 192.168.200.1 255.255.255.0
R1(config-subif)#exit
R1(config)#interface g0/0
R1(config)#no shutdown

```

### 5. Deshabilitar en S3 DNS lookup.

En el S3, se debe deshabilitar la búsqueda de DNS, esto se logra mediante el comando:

```
R3(config)#no ip domain-lookup
```

### 6. Asignar direcciones IP a los switches según lineamientos.

Según la topología que se presenta en el planteamiento del problema y acorde con los demás requerimientos, se establecen las direcciones IP de administración de los switches S1 y S2, de la siguiente manera:

#### 6.1. Configuración IP VLAN switch 1

```
S1#config t
S1(config)#interface vlan 1
S1(config-if)#ip address 192.168.99.2 255.255.255.0
S1(config-if)#no shutdown
S1(config-if)#end
```

#### 6.2. Configuración IP VLAN switch 2.

```
S2#config t
S2(config)#interface vlan 1
S2(config-if)#ip address 192.168.99.3 255.255.255.0
S2(config-if)#no shutdown
S2(config-if)#end
```

### 7. Desactivación de las interfaces inutilizadas en el esquema de red.

Por aspectos de seguridad básica en las redes de telecomunicaciones, en los distintos dispositivos, routers, y switches, es necesario deshabilitar los puestos o interfaces que no se están usando, por lo anterior, se deben seguir los siguientes pasos en cada uno de los hosts:

#### 7.1. Router 1.

Los comando son muy similares en todos los dispositivos, sin embargo las interfaces que se deben desactivas son distintas.

Ahora se procede a desconectar los puertos mediante:

```
R1(config)#interface g0/1
R1(config-if)#shutdown
```

Como respuesta se observa

```
R1 (config-if) #
%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state
to administratively down
```

De la misma forma se desactivan todos:

```
R1 (config-if) #interface s0/0/1
R1 (config-if) #shutdown
```

Como evidencia se usa el comando **show ip interface brief** y obtenemos la tabla:

```
R1#show ip interface brief
```

Interface	IP-Address	OK?	Method	Status	Protocol
GigabitEthernet0/0	192.168.99.1	YES	manual	up	up
GigabitEthernet0/0.10	192.168.10.1	YES	manual	up	up
GigabitEthernet0/0.30	192.168.30.1	YES	manual	up	up
GigabitEthernet0/0.40	192.168.40.1	YES	manual	up	up
GigabitEthernet0/0.200	192.168.200.1	YES	manual	up	up
GigabitEthernet0/1	unassigned	YES	unset	administratively down	down
Serial0/0/0	172.31.21.2	YES	manual	up	up
Serial0/0/1	unassigned	YES	unset	administratively down	down
Vlan1	unassigned	YES	unset	administratively down	down

## 7.2. Router 2.

De la misma manera que el router 1, se obtienen los siguientes comandos.

```
R2#show ip interface brief
```

Interface	IP-Address	OK?	Method	Status	Protocol
GigabitEthernet0/0	209.165.200.226	YES	manual	up	up
GigabitEthernet0/1	unassigned	YES	unset	up	down
Serial0/0/0	172.31.23.1	YES	manual	up	up
Serial0/0/1	172.31.21.2	YES	manual	up	up
Loopback0	10.10.10.10	YES	manual	up	up
Vlan1	unassigned	YES	unset	up	down

Se debe deshabilitar g0/1 y VLAN 1. Por tanto.

```
R2 (config) #interface g0/1
R2 (config-if) #shutdown
R2 (config) #interface vlan1
R2 (config-if) #shutdown
```

Se recibe como respuesta:

```
%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state
to administratively down
```

```
%LINK-5-CHANGED: Interface Vlan1, changed state to
administratively down
```

Y obtenemos la tabla.

```
R2#show ip interface brief
Interface          IP-Address      OK? Method Status      Protocol
GigabitEthernet0/0 209.165.200.226 YES manual up          up
GigabitEthernet0/1 unassigned      YES unset  administratively down down
Serial10/0/0       172.31.23.1    YES manual up          up
Serial10/0/1       172.31.21.2    YES manual up          up
Loopback0          10.10.10.10    YES manual up          up
Vlan1              unassigned      YES unset  administratively down down
```

### 7.3. Router 3.

```
R3(config)#interface g0/0
R3(config-if)#shutdown
R3(config)#interface g0/1
R3(config-if)#shutdown
R3(config)#interface s0/0/0
R3(config-if)#shutdown
R3(config)#interface vlan 1
R3(config-if)#shutdown
```

```
R3#show ip interface brief
Interface          IP-Address      OK? Method Status      Protocol
GigabitEthernet0/0 unassigned      YES unset  administratively down down
GigabitEthernet0/1 unassigned      YES unset  administratively down down
Serial10/0/0       unassigned      YES unset  administratively down down
Serial10/0/1       172.31.23.2    YES manual up          up
Loopback4          192.168.4.1    YES manual up          up
Loopback5          192.168.5.1    YES manual up          up
Loopback6          192.168.6.1    YES manual up          up
Vlan1              unassigned      YES unset  administratively down down
```

### 7.4. Switch 1.

```
S1#show ip interface brief
Interface          IP-Address      OK? Method Status      Protocol
FastEthernet0/1    unassigned      YES manual up          up
FastEthernet0/2    unassigned      YES manual down        down
FastEthernet0/3    unassigned      YES manual up          up
FastEthernet0/4    unassigned      YES manual down        down
FastEthernet0/5    unassigned      YES manual down        down
FastEthernet0/6    unassigned      YES manual down        down
FastEthernet0/7    unassigned      YES manual down        down
FastEthernet0/8    unassigned      YES manual down        down
FastEthernet0/9    unassigned      YES manual down        down
FastEthernet0/10   unassigned      YES manual down        down
FastEthernet0/11   unassigned      YES manual down        down
FastEthernet0/12   unassigned      YES manual down        down
FastEthernet0/13   unassigned      YES manual down        down
FastEthernet0/14   unassigned      YES manual down        down
FastEthernet0/15   unassigned      YES manual down        down
FastEthernet0/16   unassigned      YES manual down        down
FastEthernet0/17   unassigned      YES manual down        down
FastEthernet0/18   unassigned      YES manual down        down
FastEthernet0/19   unassigned      YES manual down        down
FastEthernet0/20   unassigned      YES manual down        down
FastEthernet0/21   unassigned      YES manual down        down
FastEthernet0/22   unassigned      YES manual down        down
FastEthernet0/23   unassigned      YES manual down        down
FastEthernet0/24   unassigned      YES manual up          up
GigabitEthernet0/1 unassigned      YES manual down        down
GigabitEthernet0/2 unassigned      YES manual down        down
Vlan1              unassigned      YES manual administratively down down
Vlan99             192.168.99.2   YES manual down        down
```

Deshabilitamos las interfaces con los comandos:

```

S1(config)#interface f0/2
S1(config-if)#shutdown
S1(config-if)#interface range f0/4-23
S1(config-if-range)#shutdown
S1(config-if-range)#interface range g0/1-2
S1(config-if-range)#shutdown

```

```

S1#show ip interface brief

```

Interface	IP-Address	OK?	Method	Status	Protocol
FastEthernet0/1	unassigned	YES	manual	up	up
FastEthernet0/2	unassigned	YES	manual	administratively down	down
FastEthernet0/3	unassigned	YES	manual	up	up
FastEthernet0/4	unassigned	YES	manual	administratively down	down
FastEthernet0/5	unassigned	YES	manual	administratively down	down
FastEthernet0/6	unassigned	YES	manual	administratively down	down
FastEthernet0/7	unassigned	YES	manual	administratively down	down
FastEthernet0/8	unassigned	YES	manual	administratively down	down
FastEthernet0/9	unassigned	YES	manual	administratively down	down
FastEthernet0/10	unassigned	YES	manual	administratively down	down
FastEthernet0/11	unassigned	YES	manual	administratively down	down
FastEthernet0/12	unassigned	YES	manual	administratively down	down
FastEthernet0/13	unassigned	YES	manual	administratively down	down
FastEthernet0/14	unassigned	YES	manual	administratively down	down
FastEthernet0/15	unassigned	YES	manual	administratively down	down
FastEthernet0/16	unassigned	YES	manual	administratively down	down
FastEthernet0/17	unassigned	YES	manual	administratively down	down
FastEthernet0/18	unassigned	YES	manual	administratively down	down
FastEthernet0/19	unassigned	YES	manual	administratively down	down
FastEthernet0/20	unassigned	YES	manual	administratively down	down
FastEthernet0/21	unassigned	YES	manual	administratively down	down
FastEthernet0/22	unassigned	YES	manual	administratively down	down
FastEthernet0/23	unassigned	YES	manual	administratively down	down
FastEthernet0/24	unassigned	YES	manual	up	up
GigabitEthernet0/1	unassigned	YES	manual	administratively down	down
GigabitEthernet0/2	unassigned	YES	manual	administratively down	down
Vlan1	unassigned	YES	manual	administratively down	down
Vlan99	192.168.99.2	YES	manual	down	down

### 7.5. Switch 3.

Comandos:

```

S3(config)#interface f0/2
S3(config-if)#shutdown
S3(config-if)#interface range f0/4-24
S3(config-if-range)#shutdown
S3(config-if-range)#interface range g0/1-2
S3(config-if-range)#shutdown

```

```

S3#show ip interface brief
Interface          IP-Address      OK? Method Status      Protocol
FastEthernet0/1    unassigned      YES manual up           up
FastEthernet0/2    unassigned      YES manual administratively down down
FastEthernet0/3    unassigned      YES manual up           up
FastEthernet0/4    unassigned      YES manual administratively down down
FastEthernet0/5    unassigned      YES manual administratively down down
FastEthernet0/6    unassigned      YES manual administratively down down
FastEthernet0/7    unassigned      YES manual administratively down down
FastEthernet0/8    unassigned      YES manual administratively down down
FastEthernet0/9    unassigned      YES manual administratively down down
FastEthernet0/10   unassigned      YES manual administratively down down
FastEthernet0/11   unassigned      YES manual administratively down down
FastEthernet0/12   unassigned      YES manual administratively down down
FastEthernet0/13   unassigned      YES manual administratively down down
FastEthernet0/14   unassigned      YES manual administratively down down
FastEthernet0/15   unassigned      YES manual administratively down down
FastEthernet0/16   unassigned      YES manual administratively down down
FastEthernet0/17   unassigned      YES manual administratively down down
FastEthernet0/18   unassigned      YES manual administratively down down
FastEthernet0/19   unassigned      YES manual administratively down down
FastEthernet0/20   unassigned      YES manual administratively down down
FastEthernet0/21   unassigned      YES manual administratively down down
FastEthernet0/22   unassigned      YES manual administratively down down
FastEthernet0/23   unassigned      YES manual administratively down down
FastEthernet0/24   unassigned      YES manual administratively down down
GigabitEthernet0/1 unassigned      YES manual administratively down down
GigabitEthernet0/2 unassigned      YES manual administratively down down
Vlan1              unassigned      YES manual administratively down down
Vlan99             192.168.99.3   YES manual down         down

```

## 8. Implementación de DHCP y NAT para IPv4

### 8.1. Configuración de R1 como servidor DHCP para las VLAN's 30 y 40

Para lograr esto, se debe utilizar el comando helper-address con la ip de la interface a la que llega al router 2, por tanto es s0/0/1 en R2 con ip 172.31.21.1, los comandos usados son:

```

R1#config t
R1(config)#ip dhcp pool ADMINISTRACIÓN
R1(dhcp-config)#network 192.168.99.0 255.255.255.0
R1(dhcp-config)#default-router 192.168.99.1
R1(dhcp-config)#dns-server 10.10.10.11
R1(dhcp-config)#domain-name ccna-unad.com
(nota: este comando no funciona en Packet Tracer "domain-
name")
R1(dhcp-config)#exit

```

```

R1#config t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#ip dhcp pool MERCADEO
R1(dhcp-config)#network 192.168.40.0 255.255.255.0
R1(dhcp-config)#default-router 192.168.99.1
R1(dhcp-config)#dns-server 10.10.10.11
R1(dhcp-config)#domain-name ccna-unad.com
R1(dhcp-config)#exit
R1(config)#

```

**8.2. Reservación de las primeras 30 direcciones IP de las VLAN 30 y 40.**  
Este procedimiento se realiza en el router 1, el cual funciona como el servidor de DHCP para estas VLAN 30 y 40. Los comandos necesarios para esta exclusión son;

```
R1#config t
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
```

### **8.3. Configuración de NAT en R2 para habilitar la salida a internet de los host**

Primero se configura la dirección del web server como una NAT estática, como la interfaz es Lo0 de simulación, es decir mediante el loopback, solamente contamos la dirección de entrada y se establece una de salida genérica.

```
R2>enable
R2#conf t
R2(config)#ip nat inside source static 10.10.10.10
64.100.50.1
```

Ahora se configura en R2 un grupo NAT que llamaremos RUT2POOL, donde se configuran algunas direcciones de 209.165.200.224/29, para esto se usan estas órdenes:

```
R2#config t
R2(config)#ip nat pool RUT2POOL 209.165.200.225
209.165.200.230 netmask 255.255.255.248
```

Enseguida se configuran las interfaces internas y externas.

```
R2(config)#int s0/0/1
R2(config-if)#ip nat outside
R2(config)#int s0/0/0
R2(config-if)#ip nat outside
R2(config-if)#exit
R2(config)#int Lo0
R2(config-if)#ip nat inside
R2(config)#int g0/0
R2(config-if)#ip nat inside
```

### **8.4. Configuración de listas de restricción o permiso para el tráfico de R1 o R3 hacia R2**

Para realizar la configuración de listas se establece la necesidad de la creación de dos listas tipo estándar y dos listas de tipo extendidas con su respectivo nombre,

con el fin de restringir o permitir el tráfico desde los routers R1 y R3, por lo tanto se realiza lo siguiente:

#### 8.4.1. Listas estándar.

Se introducen los siguientes comandos (NAT 1 de router 1):

```
R2(config)#ip access-list standard NAT1_D_R1
R2(config-std-nacl)#deny 192.168.30.0 0.0.0.255
R2(config-std-nacl)#permit 192.168.40.0 0.0.0.255
R2(config-std-nacl)#exit
```

(NAT 2 de router 3)

```
R2(config)#ip access-list standard NAT2_D_R3
R2(config-std-nacl)#permit 192.168.4.0 0.0.0.255
R2(config-std-nacl)#permit 192.168.5.0 0.0.0.255
R2(config-std-nacl)#deny 192.168.6.0 0.0.0.255
R2(config-std-nacl)#exit
```

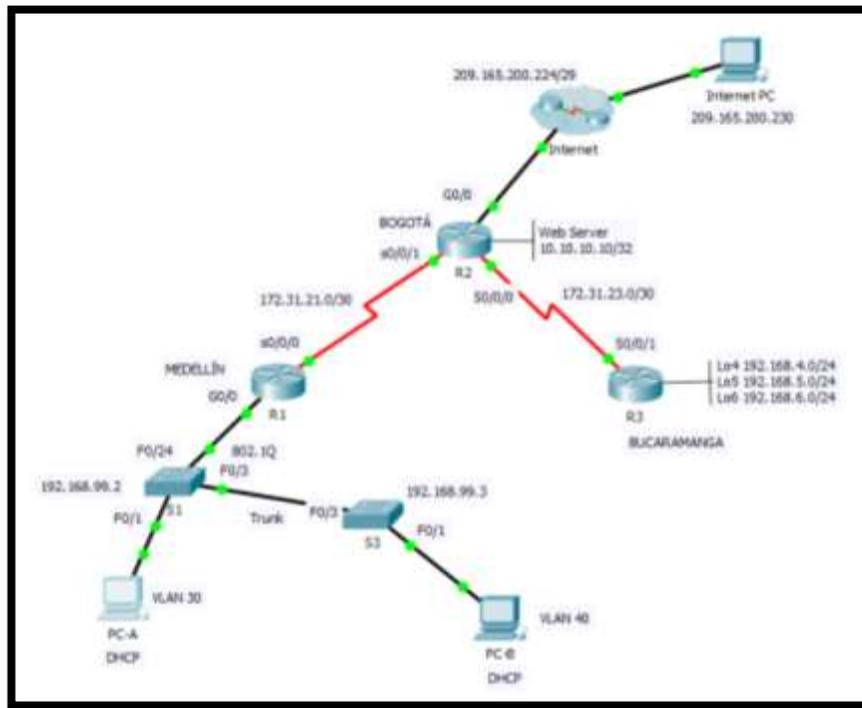
#### 8.4.2. Listas de tipo extendido.

```
R2(config)#ip access-list extended NAT3_D_H40
R2(config-std-nacl)#deny TCP 192.168.40.31 0.0.0.255 any
```

```
R2(config)#ip Access-list extended NAT4_D_H30
R2(config-std-nacl)#permit UDP 192.168.30.31 0.0.0.255 any
```

### 9. Verificación de comunicación y direccionamiento de tráfico.

Finalizado el montaje y configuración de los parámetros requeridos y descritos en el planteamiento del problema, se dispone a demostrar las interconexiones entre la red y los caminos que deben seguir algunos paquetes y comunicación entre los routers que componen a la red



En primera instancia se comprueba la comunicación mediante el comando PING desde los host PC-A y PC-B con algunas interfaces dentro de los demás componentes de la red:

Desde PC-A hasta S1:

```
C:\>ping 192.168.40.2

Pinging 192.168.40.2 with 32 bytes of data:

Request timed out.
Reply from 192.168.40.2: bytes=32 time<1ms TTL=255
Reply from 192.168.40.2: bytes=32 time<1ms TTL=255
Reply from 192.168.40.2: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.40.2:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 192.168.99.2

Pinging 192.168.99.2 with 32 bytes of data:

Reply from 192.168.99.2: bytes=32 time=1ms TTL=255
Reply from 192.168.99.2: bytes=32 time<1ms TTL=255
Reply from 192.168.99.2: bytes=32 time=1ms TTL=255
Reply from 192.168.99.2: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.99.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

Desde PC-A hasta S2

```

C:\>ping 192.168.40.3

Pinging 192.168.40.3 with 32 bytes of data:

Request timed out.
Request timed out.
Reply from 192.168.40.3: bytes=32 time<1ms TTL=255
Reply from 192.168.40.3: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.40.3:
    Packets: Sent = 4, Received = 2, Lost = 2 (50% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 192.168.99.3

Pinging 192.168.99.3 with 32 bytes of data:

Request timed out.
Reply from 192.168.99.3: bytes=32 time<1ms TTL=255
Reply from 192.168.99.3: bytes=32 time<1ms TTL=255
Reply from 192.168.99.3: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.99.3:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

```

## Desde PC-A hasta Gateway predeterminado

```

C:\>ping 192.168.99.1

Pinging 192.168.99.1 with 32 bytes of data:

Reply from 192.168.99.1: bytes=32 time=1ms TTL=255
Reply from 192.168.99.1: bytes=32 time<1ms TTL=255
Reply from 192.168.99.1: bytes=32 time=1ms TTL=255
Reply from 192.168.99.1: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.99.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

```

## Desde PC-A hasta R2

```

C:\>ping 172.31.21.1

Pinging 172.31.21.1 with 32 bytes of data:

Reply from 172.31.21.1: bytes=32 time=2ms TTL=254
Reply from 172.31.21.1: bytes=32 time=1ms TTL=254
Reply from 172.31.21.1: bytes=32 time=1ms TTL=254
Reply from 172.31.21.1: bytes=32 time=2ms TTL=254

Ping statistics for 172.31.21.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 2ms, Average = 1ms

```

## Desde PC-A hasta Internet PC

```

C:\>ping 209.165.200.230

Pinging 209.165.200.230 with 32 bytes of data:

Reply from 209.165.200.230: bytes=32 time=2ms TTL=126
Reply from 209.165.200.230: bytes=32 time=1ms TTL=126
Reply from 209.165.200.230: bytes=32 time=2ms TTL=126
Reply from 209.165.200.230: bytes=32 time=10ms TTL=126

Ping statistics for 209.165.200.230:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 10ms, Average = 3ms

```

## Desde PC-A hasta Lo4, Lo5 y Lo6

```
C:\>ping 192.168.4.1

Pinging 192.168.4.1 with 32 bytes of data:

Reply from 192.168.4.1: bytes=32 time=2ms TTL=253

Ping statistics for 192.168.4.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 2ms, Average = 2ms

C:\>ping 192.168.5.1

Pinging 192.168.5.1 with 32 bytes of data:

Reply from 192.168.5.1: bytes=32 time=3ms TTL=253
Reply from 192.168.5.1: bytes=32 time=2ms TTL=253
Reply from 192.168.5.1: bytes=32 time=2ms TTL=253
Reply from 192.168.5.1: bytes=32 time=3ms TTL=253

Ping statistics for 192.168.5.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 3ms, Average = 2ms

C:\>ping 192.168.6.1

Pinging 192.168.6.1 with 32 bytes of data:

Reply from 192.168.6.1: bytes=32 time=3ms TTL=253
Reply from 192.168.6.1: bytes=32 time=2ms TTL=253
Reply from 192.168.6.1: bytes=32 time=3ms TTL=253
Reply from 192.168.6.1: bytes=32 time=2ms TTL=253

Ping statistics for 192.168.6.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 3ms, Average = 2ms
```

DE manera similar es posible comprobar y establecer la ruta que debe tomar la comunicación entre la PC-A hasta llegar a Internet PC, teniendo en cuenta los saltos entre los routers que los paquetes deben atravesar, mediante el comando Tracert en command line o Traceroute desde otro dispositivo:

```
C:\>tracert 209.165.200.230

Tracing route to 209.165.200.230 over a maximum of 30 hops:

  0  0 ms  0 ms  0 ms  192.168.30.1
  1  0 ms  1 ms  2 ms  172.31.21.1
  2  1 ms  0 ms  0 ms  209.165.200.230

Trace complete.
```

Es evidente que se realizan tres saltos para alcanzar el destino desde la PC-A hasta la Internet PC, estos son específicamente los Routers que se encuentran en su ruta más eficiente.

Mediante el comando Traceroute se comprueban los saltos desde S3 hasta la dirección de Web Server:

```
S3>traceroute 10.10.10.10
Type escape sequence to abort.
Tracing the route to 10.10.10.10

 1  192.168.99.1    1 msec    0 msec    0 msec
 2  172.31.21.1     6 msec    1 msec    1 msec
```

```
S3>traceroute 209.165.200.230
Type escape sequence to abort.
Tracing the route to 209.165.200.230

 1  192.168.99.1    1 msec    0 msec    1 msec
 2  172.31.21.1     0 msec    0 msec    2 msec
 3  209.165.200.230 10 msec   1 msec    1 msec
```

También es posible consultar las rutas y saltos que se requieren para alcanzar otros dispositivos dentro de la red. Así mismo es posible usar el comando **PING**, **TRACERT** en command line y **Traceroute** en los demás dispositivos dentro de la red y con programación cisco.

## CONCLUSIONES

A partir de los conceptos y destrezas aprendidas y practicadas en el desarrollo del diplomado de profundización de CISCO (Diseño e implementación de soluciones integradas LAN/WAN), se puede determinar que para una adecuada administración de la red, teniendo en cuenta la mayor cantidad de parámetros incluida la seguridad en las comunicaciones y la calidad QoS, es fundamental el correcto establecimiento de las direcciones IP, las cuales pueden hacerse mediante IPv4 o IPv6, que básicamente funcionan muy similar. A partir de esta etapa establecida correctamente y contando con un diseño de la topología, es más sencillo para el administrador de la red establecer el control y configuración de los demás parámetros.

Con la adecuada configuración y establecimiento del protocolo OSPFv2, es posible coordinar y controlar la manera en que los host dentro de la red se encuentran, de esta manera se puede establecer la importancia entre las rutas, la manera y los dispositivos que el tráfico deberá cruzar para poder hallar los host de destino mediante el protocolo TCP/IP muy utilizado en estas redes, específicamente en este ejercicios teórico-práctico. En este momento surge también la importancia de contar con elementos de configuración especiales dentro el protocolo OSPF, como son las interfaces configuradas de manera pasiva, el ancho de banda y el costo de la métrica, parámetros que permiten fortalecer la manera y eficiencia en que las redes manejan el tráfico según su protocolo establecido en OSPFv2.

La necesidad por establecer VLAN, que permitan no solo organizar y separar algunas terminales, según las dependencias con distintos requerimientos a la hora de generar tráfico en la red, sino que también mejorar la seguridad en el proceso e routing de una red o de una parte específica de la misma. Es un tipo de configuración muy importante para mejorar la calidad del servicio que se le brinda a la red. Por tanto el administrador debe tener muy claro todo el diseño de la red y la manera en que esta va a brindar tipos distintos de soluciones según las dependencias, el tráfico y el uso de la red para comunicaciones de la empresa en cuestión.

Otro aspecto de seguridad, es decir, que mejora la seguridad dentro de la administración de las redes, es la desactivación de interfaces inutilizadas y la agrupación de estas por VLAN en los dispositivos. De la misma forma otro aspecto que favorece la seguridad, así como mejorar el flujo de tráfico en la red, es la implementación de NAT y listas ACL en los routers, específicamente el uso de listas estándar se aplica para permitir o denegar el tráfico según las direcciones de la red, por su parte las listas de tipo extendido permiten realizar un filtrado más específico,

por tipo de paquetes o por puertos de acceso de la red. Es por esto que en el proceso de administración y configuración de la red, el conocimiento y manejo adecuado de las listas ACL y NAT, se constituyen como herramientas muy potentes a la hora de configurar y filtrar el tráfico en dispositivos frontera dentro de las redes LAN, como en el caso de esta práctica.

## BIBLIOGRAFÍA

CISCO. (2014). Documento de información pública de CISCO. En P. Tracer, *Representación de la Red*. CISCO Networking Academy.

CISCO. (2018). DIPLOMADO CCNA2.

CISCO Networking Academy. (2017). Packet Tracer. En Software. Copyright Cisco 2017: Version 7.1.0.0222.

Salmerón, L. J. (2014). QoS Clasificación y Marcado de tráfico. Obtenido de <https://sites.google.com/site/redesconvergentesjoseluis1203/unidad-ii-calidad-de-servicio-qos/4---clasificacion-y-marcado-de-trafico>