

PRUEBA DE HABILIDADES PRÁCTICAS

Presenta

ANA FRANCENE BAUTISTA LARGO

1051240470

Presentado a

GIOVANNI ALBERTO BRACHO

**UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
ESCUELA DE CIENCIAS BASICAS TECNOLOGIA E INGENIERIA
DIPLOMADO DE PROFUNDIZACIÓN CISCO (DISEÑO E IMPLEMENTACIÓN
DE SOLUCIONES INTEGRADAS LAN / WAN)**

2018

Introducción

La implantación de herramientas de simulación como *Packet Tracer* permite realizar diseños de topologías de red y/o configuración de dispositivos, ya que brinda la posibilidad de analizar cada proceso que se ejecuta de acuerdo a la capa del modelo OSI, puesto que se puede detectar y corregir errores potenciales dentro del sistema de comunicación en el cual se realizan las configuraciones básicas y necesarias que permiten interconectar entre sí cada uno de los dispositivos que forman parte del escenario. Por lo tanto se implementan los lineamientos establecidos para el direccionamiento IP, protocolos de enrutamiento y demás aspectos que forman parte de la topología de red.

Dentro del desarrollo del presente documento se realiza la simulación de un entorno de Redes de comunicaciones, creando topologías de Red mediante la selección de los dispositivos y su respectiva ubicación en el área de trabajo.

Dentro de los aspectos más importantes en el desarrollo de la topología propuesta se destaca la simulación de la implementación del Protocolo de Información de Encaminamiento RIP V2 (protocolo de puerta de enlace interna – Interior Gateway Protocol, IGP), Protocolo de Configuración Dinámica de Host (DHCP) que proporciona además de la puerta de enlace predeterminada y la máscara de subred, un host de protocolo Internet (IP) con su dirección IP automáticamente.

Así mismo, se realiza implementación de la conversión de direcciones de red o NAT, el principio de NAT consiste en utilizar una conexión de pasarela a Internet, que tenga al menos una interfaz de red conectada a la red interna y al menos una interfaz de red conectada a Internet (con una dirección IP enrutable) para poder conectar todos los equipos a la red.

De igual forma se simula el funcionamiento de las ACLs tanto extendidas como de tipo estándar. Sabemos que las primeras son más eficientes en cuanto al filtrado. Sin embargo tanto extendidas como estándar, las ACLs son mecanismos de clasificación de tráfico y direcciones.

Finalmente, aunque no menos importante, se realiza la configuración básica de los dispositivos presentes en el escenario; es decir, configuración del direccionamiento IP acorde con la topología de red, VLANs, puertos troncales y de acceso, encapsulamiento, seguridad, configuración de las listas de acceso e identificar los correctos procesos de comunicación y redireccionamiento de tráfico de datos entre terminales mediante el uso de comandos como PING y TRACEROUTE.

Objetivos

Objetivo General

Aplicar los conocimientos adquiridos sobre configuración de Redes utilizando herramientas de simulación.

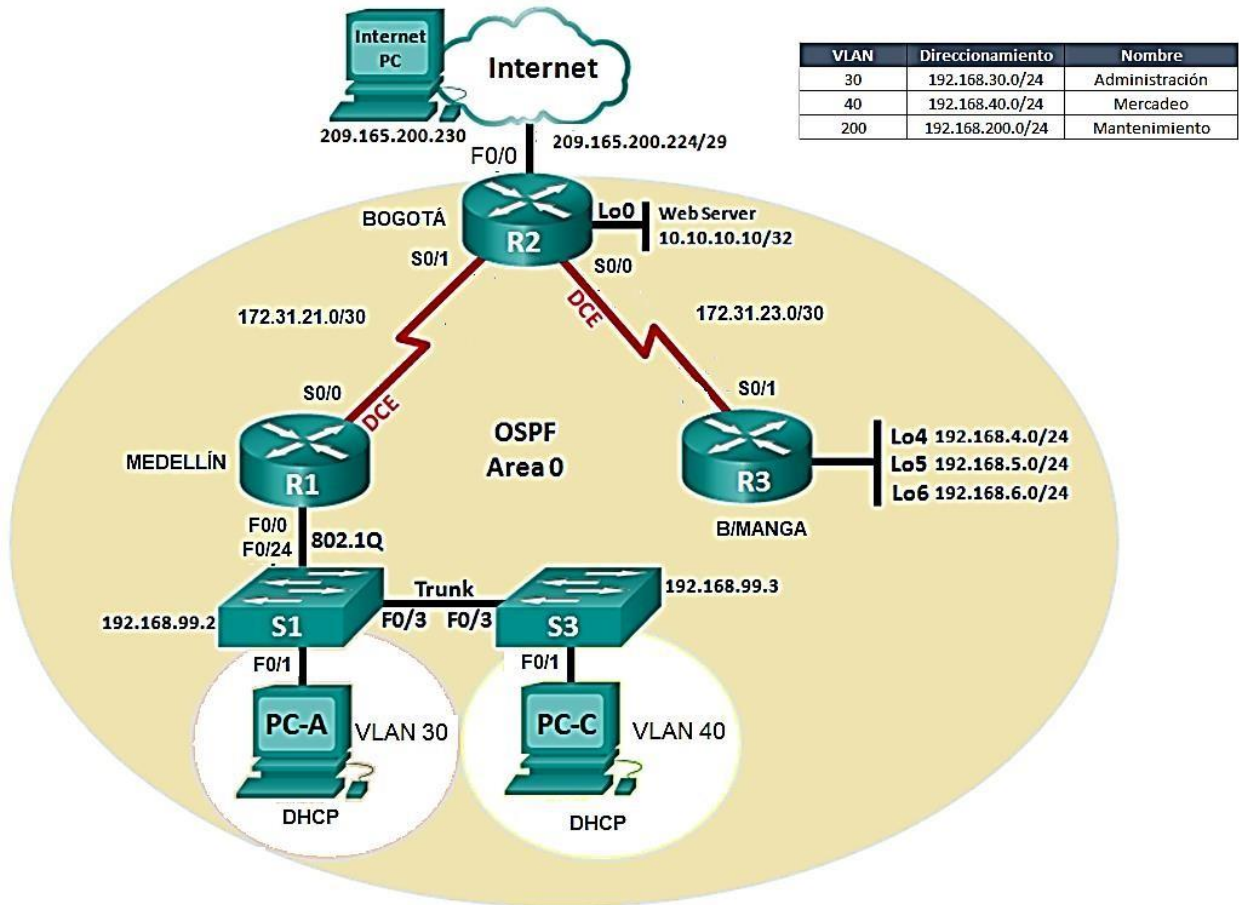
Objetivos Específicos

- Configurar el protocolo de enrutamiento OSPFv2.
- Realizar la configuración de los ajustes de los dispositivos.
- Asignar direcciones IPV4.
- Establecer la configuración y direccionamiento de las interfaces de Routers y Switches.
- Limitar el acceso a los dispositivos mediante configuración ACL.
- Configurar VLAN y enlaces troncales.

Descripción del escenario propuesto 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 red



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

En primer lugar inicializamos los dispositivos (Routers, switches, PCs)

La configuración se realiza haciendo uso de los comandos:

```
enable  
configure terminal  
no ip domain-lookup  
hostname
```

Lo que se pretende es ingresar por el modo privilegiado (enable) y asignar nombre a los dispositivos (hostname).

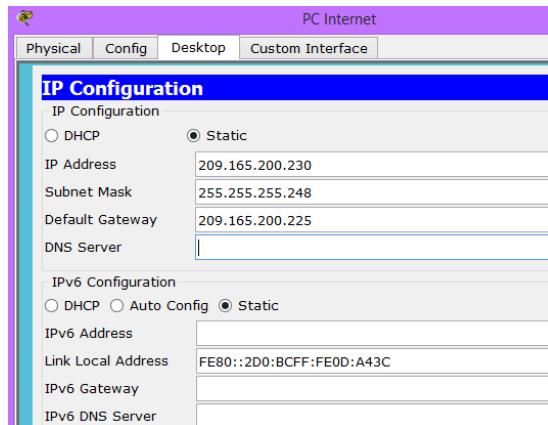


Ilustración 1. PC Internet

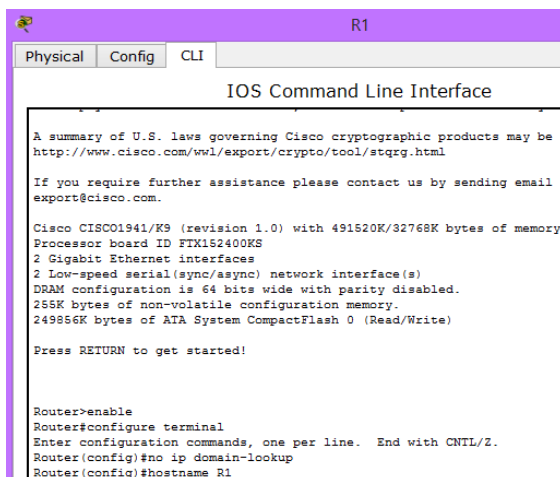


Ilustración 2. Router 1

```
R2
Physical Config CLI
IOS Command Line Interface
third-party authority to import, export, distribute or use encryption.
Importers, exporters, distributors and users are responsible for
compliance with U.S. and local country laws. By using this product you
agree to comply with applicable laws and regulations. If you are unabl
to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be f
http://www.cisco.com/wvl/export/crypto/tool/stqrg.html

If you require further assistance please contact us by sending email t
export@cisco.com.

Cisco CISC01941/K9 (revision 1.0) with 491520K/32768K bytes of memory.
Processor board ID FTX152400KS
2 Gigabit Ethernet interfaces
2 Low-speed serial(sync/async) network interface(s)
DRAM configuration is 64 bits wide with parity disabled.
255K bytes of non-volatile configuration memory.
249856K bytes of ATA System CompactFlash 0 (Read/Write)

Press RETURN to get started!

Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#no ip domain-lookup
Router(config)#hostname R2
R2(config)#
```

Ilustración 3. Router 2

```
R3
Physical Config CLI
IOS Command Line Interface
third-party authority to import, export, distribute or use encrypt
Importers, exporters, distributors and users are responsible for
compliance with U.S. and local country laws. By using this produc
agree to comply with applicable laws and regulations. If you are
to comply with U.S. and local laws, return this product immediate

A summary of U.S. laws governing Cisco cryptographic products may
http://www.cisco.com/wvl/export/crypto/tool/stqrg.html

If you require further assistance please contact us by sending em
export@cisco.com.

Cisco CISC01941/K9 (revision 1.0) with 491520K/32768K bytes of me
Processor board ID FTX152400KS
2 Gigabit Ethernet interfaces
2 Low-speed serial(sync/async) network interface(s)
DRAM configuration is 64 bits wide with parity disabled.
255K bytes of non-volatile configuration memory.
249856K bytes of ATA System CompactFlash 0 (Read/Write)

Press RETURN to get started!

Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#no ip domain-lookup
Router(config)#hostname R3
R3(config)#
```

Ilustración 4. Router 3

```

S1
Physical Config CLI
IOS Command Line Interface

Switch  Ports  Model          SW Version      SW I
-----  -
*      1      26      WS-C2960-24TT  12.2            C2960

Cisco IOS Software, C2960 Software (C2960-LANBASE-M), Version 1:
SOFTWARE (fc1)
Copyright (c) 1986-2005 by Cisco Systems, Inc.
Compiled Wed 12-Oct-05 22:05 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,
up
%LINK-5-CHANGED: Interface FastEthernet0/3, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3,
up

Switch>enable
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#no ip domain-lookup
Switch(config)#hostname S1
S1(config)#

```

Ilustración 5. Switch 1

```

S3
Physical Config CLI
IOS Command Line Interface

Switch  Ports  Model          SW Version      SW I
-----  -
*      1      26      WS-C2960-24TT  12.2            C:

Cisco IOS Software, C2960 Software (C2960-LANBASE-M), Version
SOFTWARE (fc1)
Copyright (c) 1986-2005 by Cisco Systems, Inc.
Compiled Wed 12-Oct-05 22:05 by pt_team

Press RETURN to get started!

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

Switch>enable
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#no ip domain-lookup
Switch(config)#hostname S3
S3(config)#

```

Ilustración 6. Switch 3

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

OSPFv2 area 0

Configuration Item or Task	Specification
Router ID R1	1.1.1.1
Router ID R2	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

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.

```

R1
-----
Physical Config CLI
IOS Command Line Interface
R1#en
R1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
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)#exit
R1(config)#int s0/0/0
R1(config-if)#bandwidth 128
R1(config-if)#ip ospf cost 7500
R1(config-if)#

```

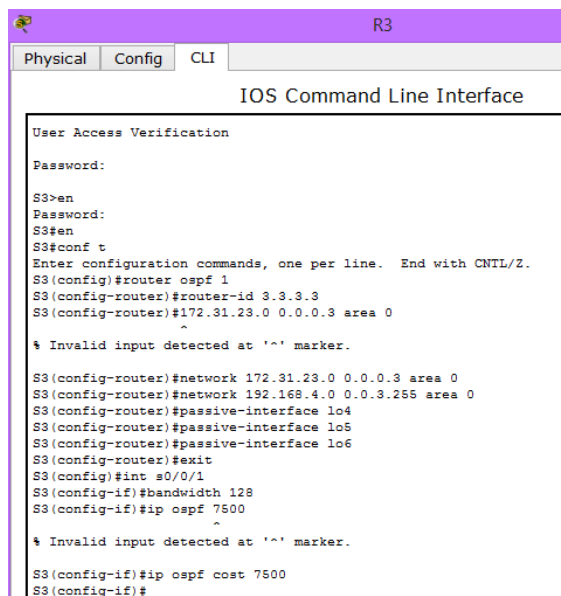
Ilustración 7. OSPF en Router 1

```

R2
-----
Physical Config CLI
IOS Command Line Interface
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, ct
Acceso no autorizado
User Access Verification
Password:
R2>en
Password:
R2#en
R2#conf 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 172.31.23.0 0.0.0.3 area 0
R2(config-router)# network 172.31.23.0 0.0.0.3 area 0
R2(config-router)# network 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)#pass
% Incomplete command.
R2(config-router)#passive-interface g0/1
R2(config-router)#int s0/0/0
R2(config-if)#bandwidth 128
R2(config-if)#int s0/0/1
R2(config-if)#bandwidth 128
R2(config-if)#int s0/0/0
R2(config-if)#ip ospf cost 7500
R2(config-if)#

```

Ilustración 8. OSPF en Router 2



```
R3
Physical Config CLI
IOS Command Line Interface

User Access Verification
Password:
S3>en
Password:
S3#en
S3#conf t
Enter configuration commands, one per line. End with CNTL/Z.
S3(config)#router ospf 1
S3(config-router)#router-id 3.3.3.3
S3(config-router)#172.31.23.0 0.0.0.3 area 0
^
% Invalid input detected at '^' marker.

S3(config-router)#network 172.31.23.0 0.0.0.3 area 0
S3(config-router)#network 192.168.4.0 0.0.3.255 area 0
S3(config-router)#passive-interface lo4
S3(config-router)#passive-interface lo5
S3(config-router)#passive-interface lo6
S3(config-router)#exit
S3(config)#int s0/0/1
S3(config-if)#bandwidth 128
S3(config-if)#ip ospf 7500
^
% Invalid input detected at '^' marker.

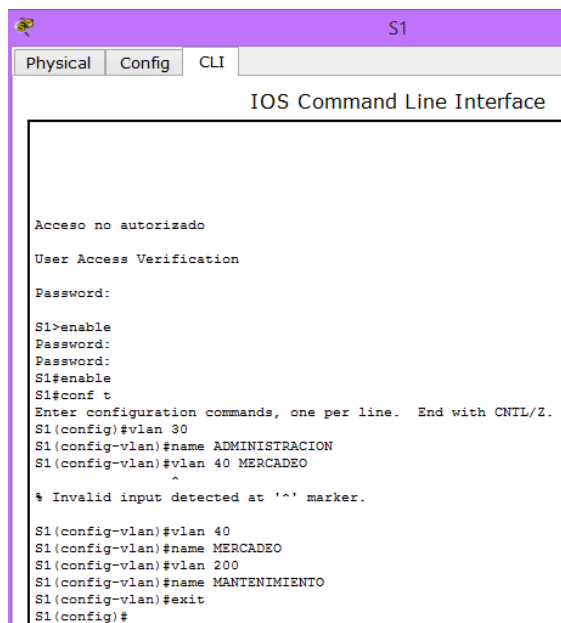
S3(config-if)#ip ospf cost 7500
S3(config-if)#
```

Ilustración 9. OSPF en Router 3

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

En la configuración de las VLAN hacemos uso de los comandos:

vlan
name

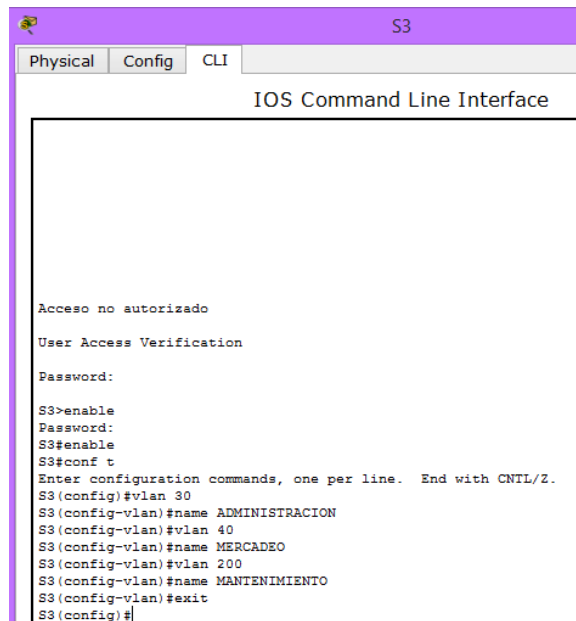


```
S1
Physical Config CLI
IOS Command Line Interface

Acceso no autorizado
User Access Verification
Password:
S1>enable
Password:
S1#enable
S1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
S1(config)#vlan 30
S1(config-vlan)#name ADMINISTRACION
S1(config-vlan)#vlan 40 MERCADEO
^
% Invalid input detected at '^' marker.

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)#
```

Ilustración 10. VLAN (Switch 1)



```

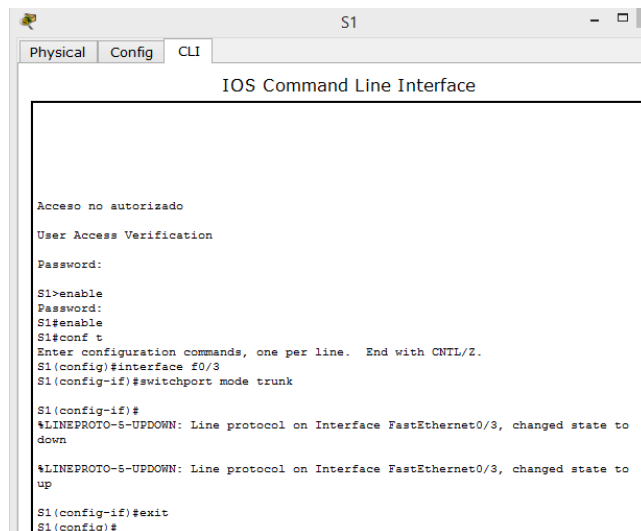
S3
Physical Config CLI
IOS Command Line Interface

Acceso no autorizado
User Access Verification
Password:
S3>enable
Password:
S3#enable
S3#conf 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)#

```

Ilustración 11. VLAN (Switch 3)

En el caso de los puertos troncales utilizamos los comandos:
switchport mode trunk



```

S1
Physical Config CLI
IOS Command Line Interface

Acceso no autorizado
User Access Verification
Password:
S1>enable
Password:
S1#enable
S1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
S1(config)#interface 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
S1(config-if)#exit
S1(config)#

```

Ilustración 12. Puerto Troncal Switch 1

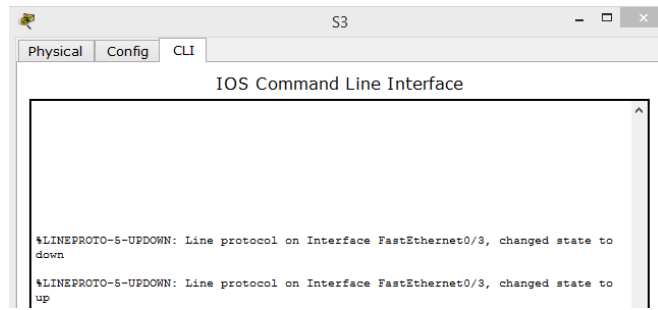


Ilustración 13. . Puerto Troncal Switch 3

A continuación se configura Inter-VLAN Routing y Seguridad en los Switches:

```
no ip domain-lookup
hostname S1
enable secret class
line console 0
password cisco
login
line vty 0 4
password cisco
login
service password-encryption
banner motd %Acceso no autorizado%
```

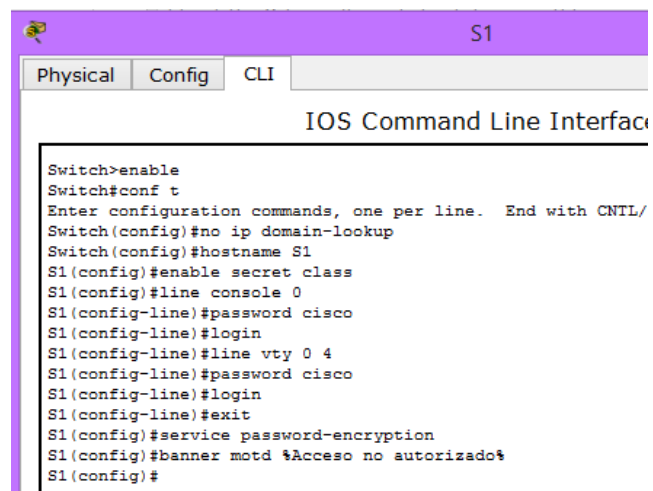


Ilustración 14. Switch 1

```

Switch>enable
Switch#conf t
Enter configuration commands, one per line. End
Switch(config)#no ip domain-lookup
Switch(config)#hostname S3
S3(config)#enable secret class
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)#exit
S3(config)#service password-encryption
S3(config)#banner motd %Acceso no autorizado%
S3(config)#

```

Ilustración 15. Switch 3

4. En el Switch 3 deshabilitar DNS lookup

```

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1, chang
Acceso no autorizado

User Access Verification

Password:

R3>en
R3#enable
R3#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#no ip domain-lookup
R3(config)#host S3
S3(config)#enable secret class
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)#exit
S3(config)#service password-encryption
^
% Invalid input detected at '^' marker.
S3(config)#service password-encryption
S3(config)#banner motd %Acceso no autorizado%
S3(config)#

```

Ilustración 16. DNS Lookup

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

Se asigna la dirección IP al Switch 1 (192.168.99.2)
ip address
no shutdown

```
S1
Physical Config CLI
IOS Command Line Inter
Password:
S1#en
S1#conf t
Enter configuration commands, one per line. End with C
S1(config)#interface vlan 30
S1(config-if)#
%LINK-5-CHANGED: Interface Vlan30, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan30,
S1(config-if)#ip address 192.168.99.2 255.255.255.0
S1(config-if)#no shutdown
S1(config-if)#exit
S1(config)#exit
S1#
%SYS-5-CONFIG_I: Configured from console by console
S1#show ip interface vlan 30
Vlan30 is up, line protocol is up
Internet address is 192.168.99.2/24
```

Ilustración 17. IP Switch 1

Se asigna la IP al Switch 3 (192.168.99.3)

```
S3
Physical Config CLI
IOS Command Line Interf
S3#en
S3#conf t
Enter configuration commands, one per line. End with CN
S3(config)#interface vlan 40
S3(config-if)#
%LINK-5-CHANGED: Interface Vlan40, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan40,
S3(config-if)#ip address 192.168.99.3 255.255.255.0
S3(config-if)#no shutdown
S3(config-if)#exit
S3(config)#exit
S3#
%SYS-5-CONFIG_I: Configured from console by console
S3#show ip interface vlan 40
Vlan40 is up, line protocol is up
Internet address is 192.168.99.3/24
Broadcast address is 255.255.255.255
```

Ilustración 18. IP Switch 3

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

Para ello ingresamos al Switch 3, donde ingresamos el comando int range :

```

S3
Physical Config CLI
IOS Command Line Interface
* Inverse input detected at marker
S3(config-vlan)#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
S3(config-if)#ip address 192.168.99.3 255.255.255.0
* 192.168.99.0 overlaps with Vlan40
S3(config-if)#exit
S3(config)#ip default-gateway 192.168.99.1
S3(config)#int fa0/3
S3(config-if)#switchport mode trunk
S3(config-if)#switchport trunk native vlan 1
S3(config-if)#int range fa0/1-2, fa0/4-17, fa0/19-24, g1/1-2
S3(config)#

```

Ilustración 19. Interfaces no utilizadas

7. Implement DHCP and NAT for IPv4.

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

```

R1
Physical Config CLI
IOS Command Line Interface

R1 con0 is now available

Press RETURN to get started.

R1>enable
R1#configure terminal
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)#

```

Ilustración 20. Servidor DHCP

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

Para esta configuración ingresamos los comandos:

```

ip dhcp pool
network
dns-server
domain-name
default router

```

Configurar DHCP para VLAN 30	Name: ADMINISTRACION DNS-Server: 10.10.10.11 Domain-Name: ccna-unad.com Establecer default gateway
-------------------------------------	---

```
R1>enable
R1#configure terminal
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)#dhcp pool ADMINISTRACION
^
% Invalid input detected at '^' marker.
R1(config)#ip dhcp pool ADMINISTRACION
R1(dhcp-config)#network 192.168.30.0 255.255.255.0
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
^
% Invalid input detected at '^' marker.
R1(dhcp-config)#default-router 192.168.30.1
R1(dhcp-config)#
```

Ilustración 21. DHCP VLAN 30

Configurar DHCP para VLAN 40	Name: MERCADEO DNS-Server: 10.10.10.11 Domain-Name: ccna-unad.com Establecer default gateway
-------------------------------------	---

```
R1
Physical Config CLI
IOS Command Line Interface

Press RETURN to get started.

R1>enable
R1#configure terminal
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 MERCADEO
R1(dhcp-config)#network 192.168.40.0 255.255.255.0
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)#
```

Ilustración 22. DHCP VLAN 40

- 10. Configurar NAT en R2 para permitir que los host puedan salir a internet.
- 11. Configurar al menos dos listas de acceso de tipo extendido o nombradas a su criterio en para restringir o permitir tráfico desde R1 o R3 hacia R2.
- 12. Configurar al menos dos listas de acceso de tipo estándar a su criterio para restringir o permitir tráfico desde R1 o R3 hacia R2.

En este caso implementamos el comando permit host para autorizar a R1 enviar tráfico a R3:

ip access-list standar

```
R2
Physical Config CLI
IOS Command Line Interface

Password:

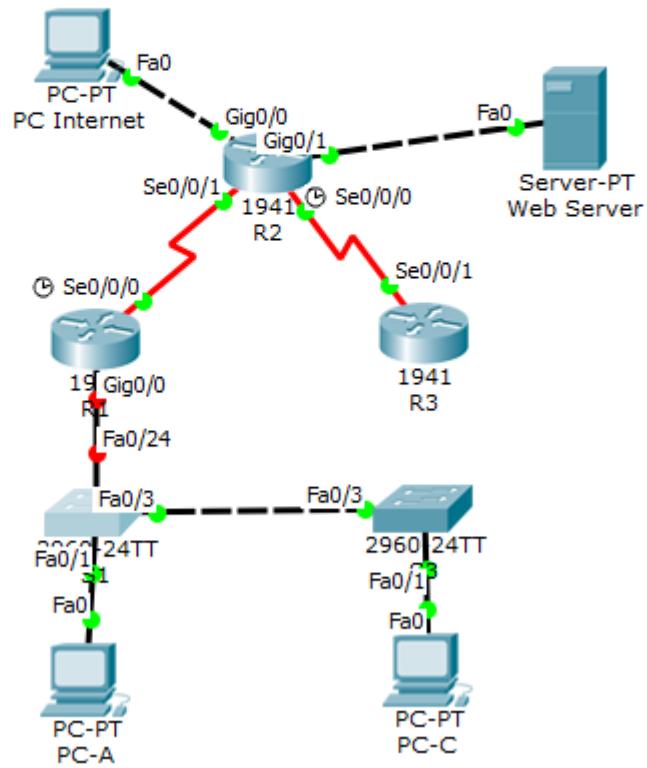
R2>en
Password:
R2(config)#ip access-list standard name
R2(config-std-nacl)#permit host 172.31.21.1
R2(config-std-nacl)#exit
R2(config)#
```

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

Cisco Packet Tracer Student

File Edit Options View Tools Extensions Help

Logical [Root] New Cluster Move Object



```
Router R1
Physical Config CLI
IOS Command Line Interface
router con0 is now available

Press RETURN to get started.

Router>en
Router#ping 172.31.21.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.31.21.2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/241/1186 ms

Router#
```

```
R2
Physical Config CLI
IOS Command Line Interface
R2 con0 is now available

Press RETURN to get started.

R2>en
R2#ping 172.31.23.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.31.23.2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/31/131 ms

R2#
```

Conclusiones

Tras realizar el procedimiento para la configuración de OSPF, se entiende que en primera medida se entra por el modo de configuración global (configure terminal) el cual activa el protocolo OSPF en el Router.

Se comprenden los conceptos básicos de los protocolos de enrutamiento y su funcionamiento principal; el cual se ejecuta de manera simultánea en varios routers con el objetivo de completar y actualizar su tabla de enrutamiento recorriendo los menores caminos posibles para intercambiar información con otras redes.

Se distingue el protocolo RIP (Router Information Protocol) por ser uno de los más importantes en implementarse y servir de base para la evolución de los protocolos de enrutamiento dinámico.

Se implementó la configuración DHCP; haciendo uso del comando ip dhcp pool, el cual crea un conjunto de IPs con el nombre asignado y provoca que el Router entre en el modo de configuración DHCP.

Se comprendió el concepto de NAT estática, como el mecanismo usado por los Routers para intercambiar paquetes entre dos redes que tienen distintas direcciones.

De igual forma se adquirieron conocimientos acerca de NAT dinámica, donde el Router va a elegir qué direccionamiento agregarle al paquete para que pueda salir a internet, dicha elección la realiza dentro de una lista de direcciones disponibles.

Se verificó conexión entre distintos dispositivos, con el objetivo de comprobar si la misma era estable, para ello se implementó el comando ping.

Así mismo, se efectuaron verificaciones de diagnóstico en las conexiones, con el comando Traceroute, la diferencia encontrada es que al enviar una serie de paquetes nos muestra además la ruta que toma hasta llegar al destino, indicando además, los hosts por los que va pasando y el tiempo que toma en cada salto. En conjunto tanto ping como traceroute nos indican si tenemos una pérdida de paquetes y dónde exactamente se presentó la falla.

Bibliografía

Omarbetas. (2016). Protocolos DHCP, ICMP, NAT y ARP. Recuperado de <https://telematicos2.wordpress.com/2016/06/07/protocolos-dhcp-icmp-nat-y-arp/>

CISCO. (2014). Protocolos y comunicaciones de red. Fundamentos de Networking. Recuperado de <https://static-course-assets.s3.amazonaws.com/ITN50ES/module2/index.html#3.0.1.1>

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

CISCO. (2014). Ethernet. Fundamentos de Networking. Recuperado de: <https://static-course-assets.s3.amazonaws.com/ITN50ES/module2/index.html#5.0.1.1>

CISCO. (2014). Capa de red. Fundamentos de Networking. Recuperado de: <https://static-course-assets.s3.amazonaws.com/ITN50ES/module2/index.html#6.0.1.1>

CISCO. (2014). Capa de Transporte. Fundamentos de Networking. Recuperado de: <https://static-course-assets.s3.amazonaws.com/ITN50ES/module7/index.html#7.0.1.1>

CISCO. (2014). Asignación de direcciones IP. Fundamentos de Networking. Recuperado de: <https://static-course-assets.s3.amazonaws.com/ITN50ES/module8/index.html#8.0.1.1>

CISCO. (2014). SubNetting. Fundamentos de Networking. Recuperado de: <https://static-course-assets.s3.amazonaws.com/ITN50ES/module9/index.html#9.0.1.1>

CISCO. (2014). Capa de Aplicación. Fundamentos de Networking. Recuperado de: <https://static-course-assets.s3.amazonaws.com/ITN50ES/module10/index.html#10.0.1.1>

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

UNAD (2014). Configuración de Switches y Routers [OVA]. Recuperado de: <https://1drv.ms/u/s!AmlJYei-NT1lhgL9QChD1m9EuGqC>

Macfarlane, J. (2014). Network Routing Basics : Understanding IP Routing in Cisco Systems. Recuperado de: <http://bibliotecavirtual.unad.edu.co:2048/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=e000xww&AN=158227&lang=es&site=ehost-live>

CISCO. (2014). VLANs. Principios de Enrutamiento y Conmutación. Recuperado de: <https://static-course-assets.s3.amazonaws.com/RSE50ES/module3/index.html#3.0.1.1>

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

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