PRUEBA DE HABILIDADES PRÁCTICAS CCNA

Presentado por:

LICETH DEL CARMEN MORA CHIMÁ

COD. 57292617

Docente:

GIOVANNY ALBERTO BRACHO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD

Escuela De Ciencias Básicas, Tecnología E Ingeniería

Ingeniería de Sistemas

Diplomado De Profundización Cisco (Diseño E Implementación De Soluciones Integradas LAN / WAN)

Santa Marta, junio de 2018

TABLA DE CONTENIDO

Resumen 3
Abstract 4
Introducción 5
Objetivos 6
Prueba de habilidades prácticas 7-51
Conclusiones 52
Bibliografía 53

RESUMEN

El presente trabajo contiene la Configuración de red LAN WAN para una empresa que cuenta con sucursales en varias ciudades del país, se trata de un diseño que va desde parametrización de contraseñas de acceso, direccionamiento IP (estática - DHCP), hostname, puertos troncales, VLANS, protócolo de enrutamiento OSPFv2 y encapsulamiento, esto para las sedes en Bogotá, Medellín y Bucaramanga.

Se trató de detallar cada uno de los procesos de configuración, con el fin de dar una mayor información del desarrollo de los ejercicios.

ABSTRACT

The present work contains the WAN LAN configuration for a company that has branches in several cities of the country, it is a design that goes from parameterization of access passwords, IP addressing (static - DHCP), hostname, trunk ports, VLANS, OSPFv2 routing protocol and encapsulation, this for the offices in Bogotá, Medellín and Bucaramanga.

We tried to detail each of the configuration processes, in order to give more information on the development of the exercises.

INTRODUCCIÓN

La tecnología corre a pasos agigantados y es necesario que junto a ella lo hagan las personas que pretenden estar a la vanguardia, pero todo eso no sería posible si no existieran las redes, ellas son fundamentales a la hora de iniciar esa carrera de avances e innovación, puesto que son la autopista por la cual avanza el monstruo tecnológico, sin éstas, no habrían rutas, direcciones y por ende comunicación. Por lo cual, los estudiantes y profesionales en Sistemas, Telecomunicaciones y tecnología en general, deben conocer los conceptos, definiciones, manejar la minucia y poder configurar equipos de redes de datos y voz. Es por ello, que para muchos Ingenieros en formación el estudio de las redes se convierte en un punto de inicio en la creación de su perfil profesional, puesto que estando allí se encuentran con el universo en infraestructura y configuración de las redes, lo que suele ser tan atractivo al observar la funcionalidad y beneficios, que terminan convirtiéndose en especialistas y enamorados del tema.

En el presente trabajo se plasma la configuración de una red LAN/WAN para una empresa con varias sucursales en el país, en ella se implementó configuración de dispositivos: encapsulación de contraseñas, VLANS, protocolos, visualización de tablas de enrutamiento, lista resumida de interfaces, entre muchas otras que le permiten a las diferentes sedes comerciales practicar la comunicación con eficiencia y seguridad. Luego de cada proceso de configuración, se realizó la verificación de los dispositivos y por supuesto la revisión a nivel general de la red, lo que evidencia el perfecto intercambio de información que se puede realizar en ella.

OBJETIVOS

OBJETIVO GENERAL

Conocer e implementar una red LAN/WAN que permita la interconexión de dispositivos ubicados en varias ciudades del país.

OBJETIVOS ESPECÍFICOS

- ✓ Identificar y utilizar la topología de red señalada.
- ✓ Ubicar VLANs y troncales.
- ✓ Configurar dispositivos intermedios y finales.
- ✓ Utilizar comandos indicados para encapsulamiento.
- ✓ Implementar procesos de seguridad, como la encriptación.

PRUEBA DE HABILIDADES PRÁCTICAS CCNA

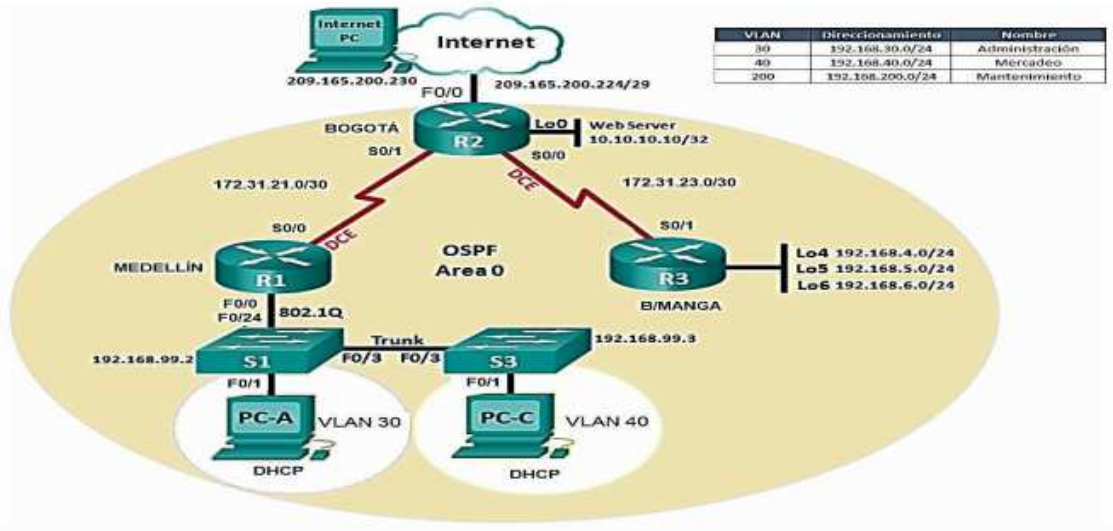
Descripción general de la prueba de habilidades

La evaluación denominada “Prueba de habilidades prácticas”, forma parte de las actividades evaluativas del Diplomado de Profundización CCNA, la cual busca identificar el grado de desarrollo de competencias y habilidades que fueron adquiridas a lo largo del diplomado y a través de la cual se pondrá a prueba los niveles de comprensión y solución de problemas relacionados con diversos aspectos de Networking. Para esta actividad, el estudiante dispone de cerca de dos semanas para realizar las tareas asignadas en cada uno de los escenarios propuestos, acompañado de los respectivos procesos de documentación de la solución, correspondientes al registro de la configuración de cada uno de los dispositivos, la descripción detallada del paso a paso de cada una de las etapas realizadas durante su desarrollo, el registro de los procesos de verificación de conectividad mediante el uso de comandos ping, traceroute, show ip route, entre otros. La prueba de habilidades podrá ser desarrollada en el Laboratorio SmartLab o mediante el uso de herramientas de Simulación (Puede ser Packet Tracer o GNS3). El estudiante es libre de escoger bajo qué mediación tecnológica resolverá cada escenario. No obstante, es importante mencionar que aquellos estudiantes que hagan uso del laboratorio SmartLab se les considerará un estímulo adicional a la hora de evaluar el informe, teniendo en cuenta que su trabajo fue realizado sobre equipos reales y con ello será la oportunidad poner a prueba las habilidades y competencias adquiridas durante el diplomado. Adicionalmente, es importante considerar, que esta actividad puede ser realizada en varias sesiones sobre este entorno, teniendo en cuenta que disponen de casi 15 días para su desarrollo.

Finalmente, el informe deberá cumplir con las normas ICONTEC para la presentación de trabajos escritos, teniendo en cuenta que este documento deberá ser entregado al final del curso en el Repositorio Institucional, acorde con los

lineamientos institucionales para grado. Proceso que les será socializado al finalizar el curso. Es muy importante mencionar que esta actividad es de carácter INDIVIDUAL. El informe deberá estar acompañado de las respectivas evidencias de configuración de los dispositivos, las cuales generarán veracidad al trabajo realizado. El informe deberá ser entregado en el espacio creado para tal fin en el Campus Virtual de la UNAD. 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



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

Ilustración 1 Topología de red a implementar

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

   - ✓ Configuración del router 1 (Medellín) La imagen siguiente muestra los comandos utilizados para establecer la configuración del router Medellín:

```
enable
conf term
no ip domain-lookup
hostname Medellin
interface s0/0/0
description conexion con Bogota
ip address 172.31.21.1 255.255.255.252
clock rate 128000
no shutdown
exit
!
ip route 0.0.0.0 0.0.0.0 s0/0/0
exit
!
copy running-config startup-config
```

   - ✓ Configuración del router 2 (Bogotá) A continuación se muestran los comandos necesarios para la configuración inicial del router Bogotá:

```
enable
conf term
no ip domain-lookup
hostname Bogota
##En el siguiente comando se presenta un error,
##por ello se procedde a configurar un servidor web
##real en la topologia.
ip http server

interface s0/0/0
description conexion con Bucaramanga
ip address 172.31.23.1 255.255.255.252
clock rate 128000
no shutdown
exit
!
interface s0/0/1
description conexion con Medellin
ip address 172.31.21.2 255.255.255.252
no shutdown
exit
!
interface f0/0
description conexion a ISP
ip address 209.165.200.225 255.255.255.248
no shutdown
exit
!
interface f0/1
description conexion con servidor web
ip address 10.10.10.1 255.255.255.0
no shutdown
exit
!
ip route 0.0.0.0 0.0.0.0 f0/0
exit
!
copy running-config startup-config
```

Packet Tracer no soporta la ejecución de comandos para la habilitación de servicio web en routers, por ello se procede a configurar un servidor real en la topología. Las siguientes líneas muestran la configuración de la interfaz en el router:

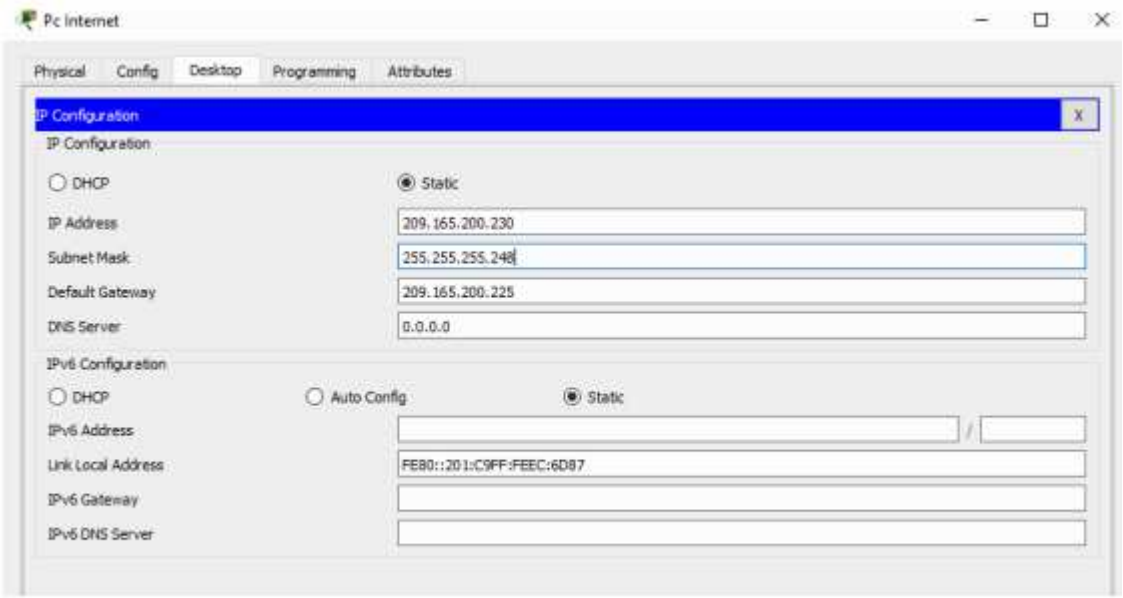
```
interface f0/1
description conexion con servidor web
ip address 10.10.10.1 255.255.255.0
no shutdown
exit
```

- ✓ Configuración del router 3 (B/manga). Las siguientes líneas de comando muestran al detalle la configuración establecida en el router B/manga:

```
enable
conf term
no ip domain-lookup
hostname Bucaramanga
interface s0/0/1
description conexion con Bogota
ip address 172.31.23.2 255.255.255.252
no shutdown
exit
!
interface loopback 4
ip address 192.168.4.1 255.255.255.0
no shutdown
exit
!
interface loopback 5
ip address 192.168.5.1 255.255.255.0
no shutdown
exit
!
```

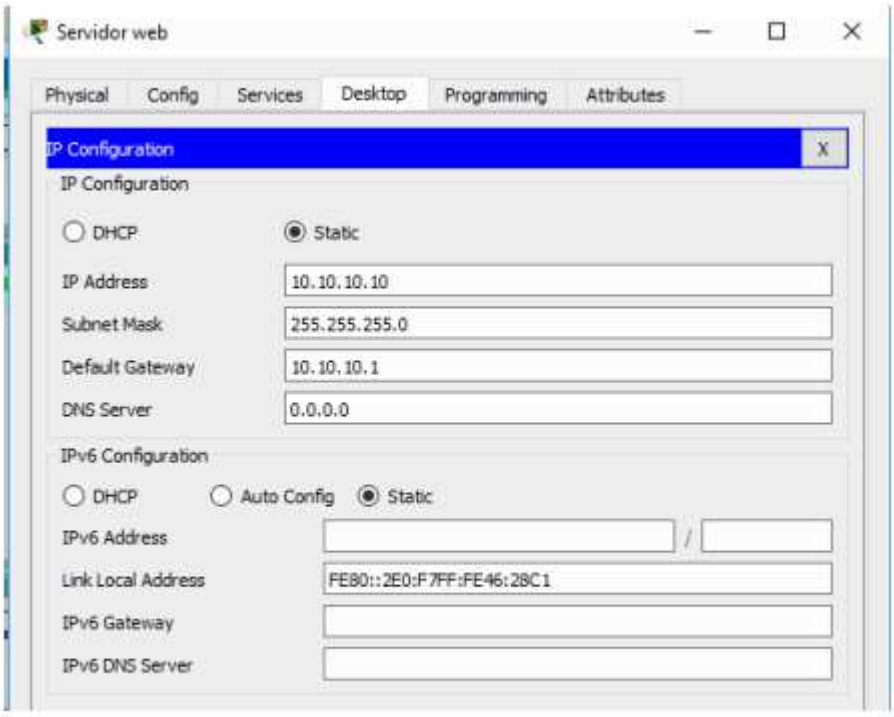
```
interface loopback 6
ip address 192.168.6.1 255.255.255.0
no shutdown
exit
!
ip route 0.0.0.0 0.0.0.0 s0/0/1
exit
!
copy running-config startup-config
```

- ✓ Configuración del Pc Internet. La configuración del Pc Internet se detalla a continuación:



El Pc Internet usa la dirección IP 209.165.200.225 como gateway predeterminado, la cual se estableció en la interfaz f0/0 del router Bogotá.

- ✓ Configuración del Servidor web. La imagen siguiente muestra la configuración realizada en el Servidor web:



✓ Configuración del switch 1 (S1) A continuación se detalla la configuración inicial realizada en el S1:

```
enable
conf terminal
hostname S1
enable secret class
line con 0
pass cisco
login
line vty 0 4
pass cisco
login
exit
!
service password-encryption
banner motd =¡El acceso no autorizado esta prohibido!=
copy running-config startup-config
```

- ✓ Configuración del switch 3 (S3)

```
enable
conf terminal
hostname S3
no ip domain-lookup
enable secret class
line con 0
pass cisco
login
line vty 0 4
pass cisco
login
exit
!
service password-encryption
banner motd =¡El acceso no autorizado esta prohibido!=
copy running-config startup-config
```

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

OSPFv2 área 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

La configuración OSPF se estableció de la siguiente manera:

- ✓ Router Medellín. Los comandos de la configuración son los siguientes:

```
enable
conf term
!OSPF e id de router
router ospf 1
router-id 1.1.1.1
!Notificando redes conectadas directamente
network 172.31.21.0 0.0.0.3 area 0
network 192.168.30.0 0.0.0.255 area 0
network 192.168.40.0 0.0.0.255 area 0
network 192.168.200.0 0.0.0.255 area 0
!Estableciendo interfaces LAN como pasiva
passive-interface f0/0.30
passive-interface f0/0.40
passive-interface f0/0.200
exit
!Ancho de banda para interfaz s0/0/0
interface s0/0/0
bandwidth 128
!Costo de metrica
ip ospf cost 7500
end
copy running-config startup-config
```

- ✓ Router Bogotá. Los comandos de la configuración son los siguientes:

```
enable
conf term
!OSPF e id de router
router ospf 1
router-id 2.2.2.2
!Notificando redes conectadas directamente
network 172.31.21.0 0.0.0.3 area 0
network 172.31.23.0 0.0.0.3 area 0
network 10.10.10.0 0.0.0.255 area 0
!Estableciendo interfaces LAN como pasiva
passive-interface f0/1
exit
!Ancho de banda para interfaz seriales
interface s0/0/0
bandwidth 128
exit
interface s0/0/1
bandwidth 128
exit
!Costo de metrica para la serial s0/0/0
interface s0/0/0
ip ospf cost 7500
end
copy running-config startup-config
```

- ✓ Router Bucaramanga. Los comandos de la configuración son los siguientes:

```
enable
conf term
!OSPF e id de router
router ospf 1
router-id 3.3.3.3
!Notificando redes conectadas directamente
network 172.31.23.0 0.0.0.3 area 0
network 192.168.4.0 0.0.3.255 area 0
!Estableciendo interfaces LAN como pasiva
passive-interface lo4
passive-interface lo5
passive-interface lo6
exit
!Ancho de banda para interfaz serial s0/0/1
interface s0/0/1
bandwidth 128
end
copy running-config startup-config
```

Verificar información de OSPF

Visualizar tablas de enrutamiento y routers conectados por OSPFv2

Este proceso de verificación se realiza con la ejecución del comando show ip ospf neighbor. Este comando se ejecuta en cada uno de los router en modo de acceso privilegiado. A continuación se muestran los resultados para cada uno de los routers.

- ✓ Router Medellín

```
Medellin#show ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address
Interface
2.2.2.2           0   FULL/  -        00:00:36    172.31.21.2
Serial0/0/0
```

✓ Router Bogotá

```
Bogota#show ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address
Interface
3.3.3.3           0   FULL/  -        00:00:36    172.31.23.2
Serial0/0/0
1.1.1.1           0   FULL/  -        00:00:39    172.31.21.1
Serial0/0/1
```

✓ Router Bucaramanga

```
Bucaramanga#show ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address
Interface
2.2.2.2           0   FULL/  -        00:00:37    172.31.23.1
Serial0/0/1
```

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

El comando utilizado para esta labor es show ip ospf interface. Este comando se ejecuta en cada uno de los routers en modo de acceso privilegiado. Los resultados se muestran a continuación:

- ✓ Router Medellín

```
Medellin#show ip ospf interface

Serial0/0/0 is up, line protocol is up
  Internet address is 172.31.21.1/30, Area 0
  Process ID 1, Router ID 1.1.1.1, Network Type POINT-TO-POINT, Cost: 7500
  Transmit Delay is 1 sec, State POINT-TO-POINT, Priority 0
  No designated router on this network
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:05
  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)
FastEthernet0/0.30 is up, line protocol is up
  Internet address is 192.168.30.1/24, Area 0
  Process ID 1, Router ID 1.1.1.1, Network Type BROADCAST, Cost: 1
  Transmit Delay is 1 sec, State WAITING, Priority 1
  No designated router on this network
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
```

```
    No Hellos (Passive interface)
  Index 2/2, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 0, Adjacent neighbor count is 0
  Suppress hello for 0 neighbor(s)
FastEthernet0/0.40 is up, line protocol is up
  Internet address is 192.168.40.1/24, Area 0
  Process ID 1, Router ID 1.1.1.1, Network Type BROADCAST, Cost: 1
  Transmit Delay is 1 sec, State WAITING, Priority 1
  No designated router on this network
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    No Hellos (Passive interface)
  Index 3/3, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 0, Adjacent neighbor count is 0
  Suppress hello for 0 neighbor(s)
FastEthernet0/0.200 is up, line protocol is up
  Internet address is 192.168.200.1/24, Area 0
  Process ID 1, Router ID 1.1.1.1, Network Type BROADCAST, Cost: 1
  Transmit Delay is 1 sec, State WAITING, Priority 1

    No designated router on this network
    No backup designated router on this network
    Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
      No Hellos (Passive interface)
    Index 4/4, flood queue length 0
    Next 0x0(0)/0x0(0)
    Last flood scan length is 1, maximum is 1
    Last flood scan time is 0 msec, maximum is 0 msec
    Neighbor Count is 0, Adjacent neighbor count is 0
    Suppress hello for 0 neighbor(s)
  Medellin#
```

✓ Router Bogotá

```
Bogota#show ip ospf interface

Serial0/0/1 is up, line protocol is up
  Internet address is 172.31.21.2/30, Area 0
  Process ID 1, Router ID 2.2.2.2, Network Type POINT-TO-POINT, Cost: 781
  Transmit Delay is 1 sec, State POINT-TO-POINT, Priority 0
  No designated router on this network
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:04
  Index 1/1, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1 , Adjacent neighbor count is 1
    Adjacent with neighbor 1.1.1.1
  Suppress hello for 0 neighbor(s)
Serial0/0/0 is up, line protocol is up
  Internet address is 172.31.23.1/30, Area 0
  Process ID 1, Router ID 2.2.2.2, Network Type POINT-TO-POINT, Cost: 7500
  Transmit Delay is 1 sec, State POINT-TO-POINT, Priority 0
  No designated router on this network
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:04
  Index 2/2, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1 , Adjacent neighbor count is 1
    Adjacent with neighbor 3.3.3.3
  Suppress hello for 0 neighbor(s)
FastEthernet0/1 is up, line protocol is up
  Internet address is 10.10.10.1/24, Area 0
  Process ID 1, Router ID 2.2.2.2, Network Type BROADCAST, Cost: 1
  Transmit Delay is 1 sec, State WAITING, Priority 1
  No designated router on this network

  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    No Hellos (Passive interface)
  Index 3/3, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 0, Adjacent neighbor count is 0
  Suppress hello for 0 neighbor(s)
Bogota#
```

- ✓ Router Bucaramanga

```
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: 781
  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)
Loopback4 is up, line protocol is up
  Internet address is 192.168.4.1/24, Area 0
  Process ID 1, Router ID 3.3.3.3, Network Type LOOPBACK, Cost: 1
  Loopback interface is treated as a stub Host
Loopback5 is up, line protocol is up
  Internet address is 192.168.5.1/24, Area 0
  Process ID 1, Router ID 3.3.3.3, Network Type LOOPBACK, Cost: 1
  Loopback interface is treated as a stub Host
Loopback6 is up, line protocol is up
  Internet address is 192.168.6.1/24, Area 0
  Process ID 1, Router ID 3.3.3.3, Network Type LOOPBACK, Cost: 1
  Loopback interface is treated as a stub Host
Bucaramanga#
```

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

Para visualizar las características anteriores se ejecuta el comando show ip protocols en modo de acceso privilegiado. El comando se ejecuta en cada router y los resultados se muestran a continuación:

- ✓ Router Medellín

```
Medellin#show ip protocols

Routing Protocol is "ospf 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 1.1.1.1
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    172.31.21.0 0.0.0.3 area 0
    192.168.30.0 0.0.0.255 area 0
    192.168.40.0 0.0.0.255 area 0
    192.168.200.0 0.0.0.255 area 0
  Passive Interface(s):
    FastEthernet0/0.30
    FastEthernet0/0.40
    FastEthernet0/0.200
  Routing Information Sources:
    Gateway         Distance      Last Update
    1.1.1.1              110      00:02:45
    2.2.2.2              110      00:29:22
    3.3.3.3              110      00:21:25
  Distance: (default is 110)

Medellin#
```

- ✓ Router Bogotá

```
Bogota#show ip protocols

Routing Protocol is "ospf 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 2.2.2.2
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    172.31.21.0 0.0.0.3 area 0
    172.31.23.0 0.0.0.3 area 0
    10.10.10.0 0.0.0.255 area 0
  Passive Interface(s):
    FastEthernet0/1
  Routing Information Sources:
    Gateway         Distance      Last Update
    1.1.1.1              110      00:03:32
    2.2.2.2              110      00:00:07
    3.3.3.3              110      00:22:12
  Distance: (default is 110)

Bogota#
```

- ✓ Router Bucaramanga

```
Bucaramanga#show ip protocols

Routing Protocol is "ospf 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 3.3.3.3
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    172.31.23.0 0.0.0.3 area 0
    192.168.4.0 0.0.3.255 area 0
  Passive Interface(s):
    Loopback4
    Loopback5
    Loopback6
  Routing Information Sources:
    Gateway         Distance      Last Update
    1.1.1.1              110      00:05:13
    2.2.2.2              110      00:01:49
    3.3.3.3              110      00:23:53
  Distance: (default is 110)

Bucaramanga#
```

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

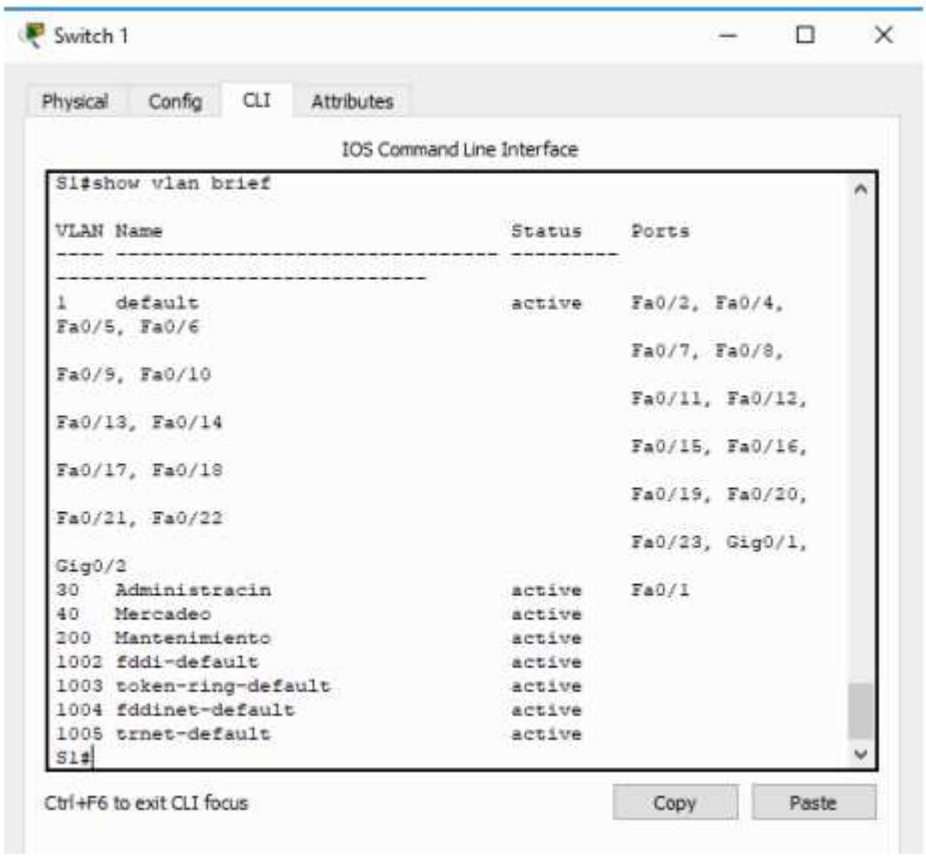
En la topología de red expuesta el direccionamiento ip de la vlan 200 (tabla) no coincide con las direcciones ip especificadas en los switches 1 y 3. La red de la vlan 200, que es la de Mantenimiento, es la 192.168.200.0 mientras la que se muestra para la configuración en los switches es la 192.168.99.0 (192.168.99.2 y 192.168.99.3), siendo estas diferentes al no coincidir con el tercer octeto. Acorde a lo anterior se procederá a configurar las direcciones ip de los switches teniendo en cuenta la red de la vlan de Mantenimiento.

✓ Configuración S1.

VLANs. En modo de configuración global se ejecutaron los siguientes comandos:

```
config term
vlan 30
name Administración
vlan 40
name Mercadeo
vlan 200
name Mantenimiento
exit
```

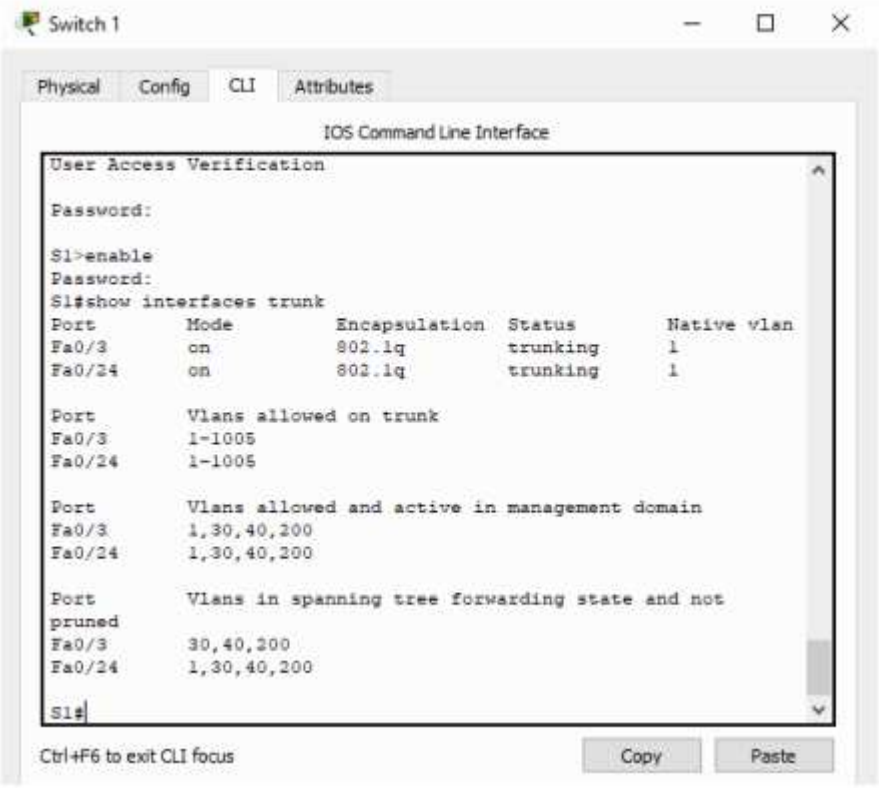
A continuación se muestra la verificación (se usa en comando show vlan brief):



Puertos troncales y encapsulación. Se configuraron las interfaces f0/3 y f0/24 como troncal y ambos puertos fueron asignados a la vlan nativa 1. Los comandos (en modo de configuración global) se muestran a continuación:

```
interf f0/3
switchport mode trunk
switchport trunk native vlan 1
exit
!
interf f0/24
switchport mode trunk
switchport trunk native vlan 1
exit
```

Se ejecuta el comando show interfaces trunk en modo de configuración global para verificar los puertos troncales. El comando muestra lo siguiente:

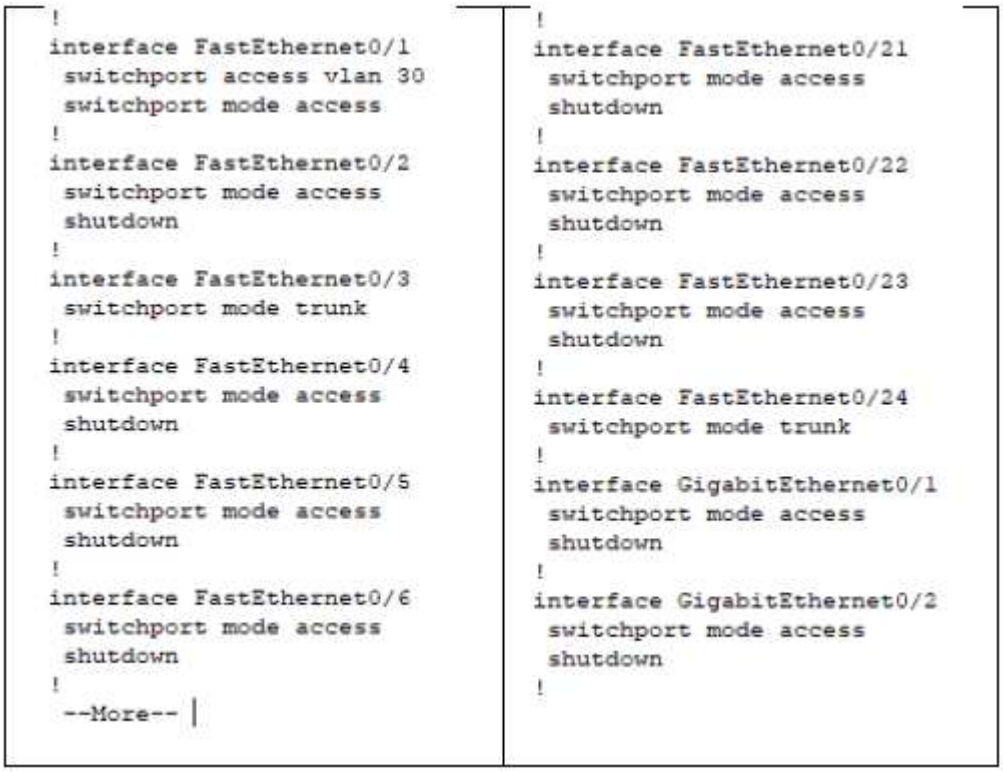


Como se puede observar en la imagen anterior, las interfaces f0/3 y f0/24 se encuentran en modo troncal y están asociadas a la VLAN 1.

Configuración de puertos de acceso. Los siguientes comandos muestran la configuración de puertos en modo acceso.

```
interf range fa0/1-2, fa0/4-23, g0/1-2
switchport mode access
exit
!
interf f0/1
switchport mode access
switchport access vlan 30
exit
```

El resultado (resumen) de la ejecución de los comandos anteriores se muestra a continuación:



```
!
interface FastEthernet0/1
 switchport access vlan 30
 switchport mode access
!
interface FastEthernet0/2
 switchport mode access
 shutdown
!
interface FastEthernet0/3
 switchport mode trunk
!
interface FastEthernet0/4
 switchport mode access
 shutdown
!
interface FastEthernet0/5
 switchport mode access
 shutdown
!
interface FastEthernet0/6
 switchport mode access
 shutdown
!
 --More--
```

```
!
interface FastEthernet0/21
 switchport mode access
 shutdown
!
interface FastEthernet0/22
 switchport mode access
 shutdown
!
interface FastEthernet0/23
 switchport mode access
 shutdown
!
interface FastEthernet0/24
 switchport mode trunk
!
interface GigabitEthernet0/1
 switchport mode access
 shutdown
!
interface GigabitEthernet0/2
 switchport mode access
 shutdown
!
```

Configuración de seguridad. La seguridad en el switch fue establecida cuando se realizó la configuración inicial de este. Los comandos ejecutados fueron los siguientes:

```
enable secret class
line con 0
pass cisco
login
line vty 0 4
pass cisco
login
exit
!
service password-encryption
banner motd =¡El acceso no autorizado esta prohibido!=
copy running-config startup-config
```

La siguiente imagen muestra el resultado de la configuración de seguridad.

```
S1#show running-config
Building configuration...

Current configuration : 2314 bytes
!
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname S1
!
enable secret 5 $1$mERr$9cTjUIEqNGurQiFU.ZeCi1
!

banner motd ^CEl acceso no autorizado esta prohibido!




^C
!
!
!
line con 0
 password 7 0822455D0A16
 login
!
line vty 0 4
 password 7 0822455D0A16
 login
line vty 5 15
```

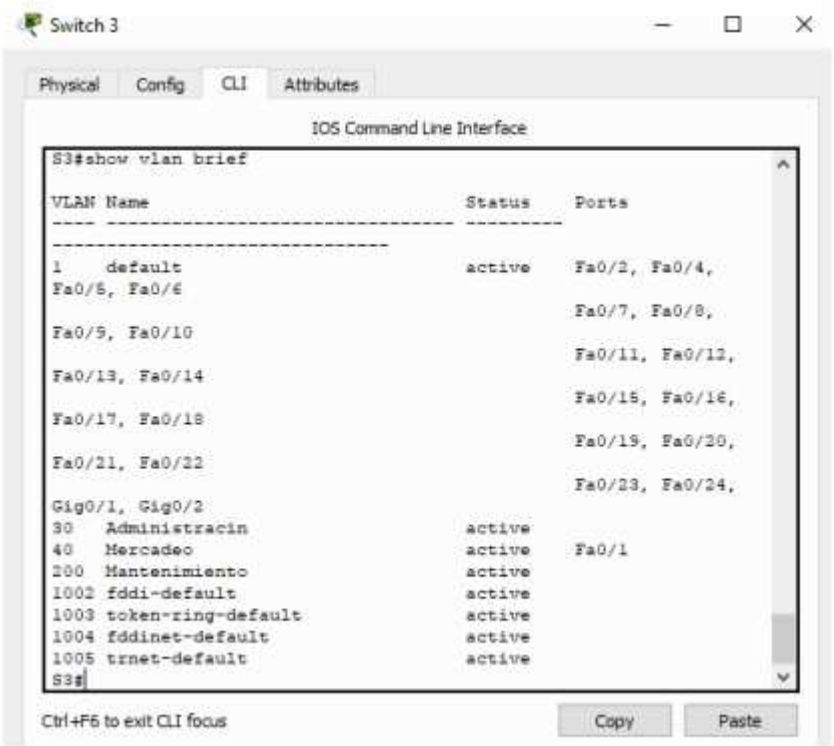
```
 login
!
!
!
end
```

✓ Configuración switch 3 (S3).

VLANs. En modo de configuración global se ejecutaron los siguientes comandos:

```
config term
vlan 30
name Administración
vlan 40
name Mercadeo
vlan 200
name Mantenimiento
exit
```

A continuación se muestra la verificación (se usa en comando show vlan brief):



Puertos troncales y encapsulación. Solo se configuró la interfaz f0/3 como troncal. Los comandos (en modo de configuración global) se muestran a continuación:

```
interf f0/3
switchport mode trunk
switchport trunk native vlan 1
exit
```

Se ejecuta el comando show interfaces trunk en modo de configuración global para verificar los puertos troncales. El comando muestra lo siguiente:

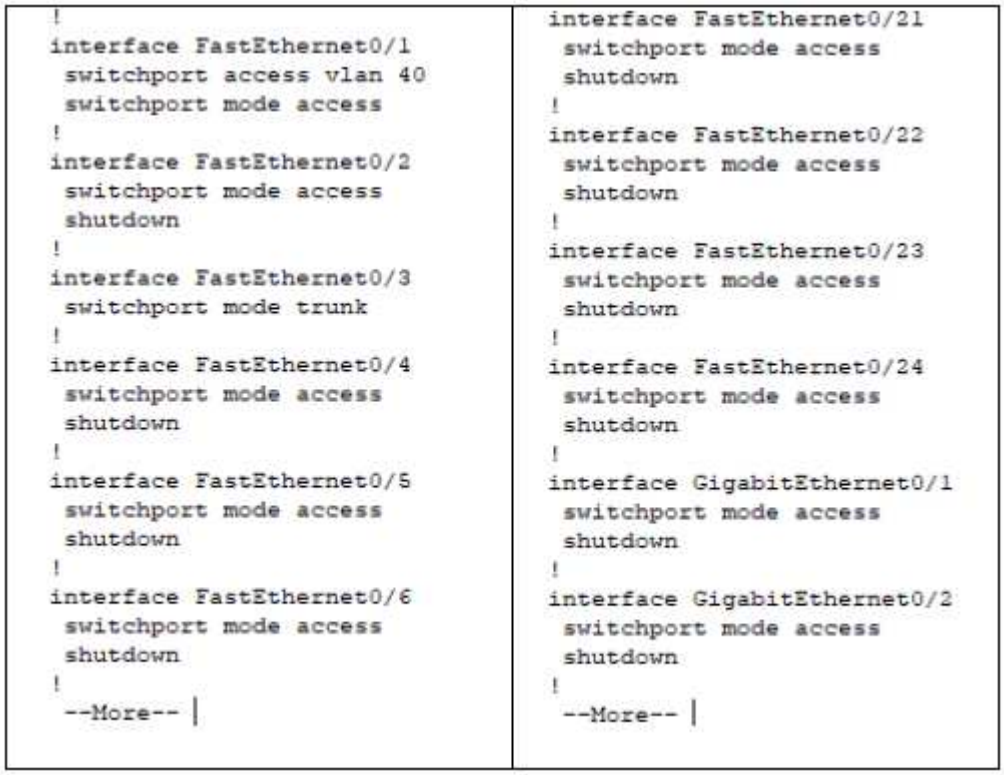
```
S3#show interf trunk
Port        Mode         Encapsulation  Status        Native vlan
Fa0/3       on           802.1q         trunking      1

Port        Vlans allowed on trunk
Fa0/3       1-1005

Port        Vlans allowed and active in management domain
Fa0/3       1,30,40,200

Port        Vlans in spanning tree forwarding state and not
pruned
Fa0/3       1,30,40,200
```

Como se puede observar en la imagen anterior, el puerto f0/3 se encuentra en modo troncal y está asociado a la vlan nativa 1.

Configuración de puertos de acceso. Los siguientes comandos muestran la configuración de puertos en modo acceso.

```
interf range fa0/1-2, fa0/4-24, g0/1-2
switchport mode access
exit
!
interf f0/1
switchport mode access
switchport access vlan 40
exit
```

El resultado (resumen) de la ejecución de los comandos anteriores se muestra a continuación (se utiliza el comando show running-config en modo privilegiado):



```
!
interface FastEthernet0/1
 switchport access vlan 40
 switchport mode access
!
interface FastEthernet0/2
 switchport mode access
 shutdown
!
interface FastEthernet0/3
 switchport mode trunk
!
interface FastEthernet0/4
 switchport mode access
 shutdown
!
interface FastEthernet0/5
 switchport mode access
 shutdown
!
interface FastEthernet0/6
 switchport mode access
 shutdown
!
 --More--
```

```
interface FastEthernet0/21
 switchport mode access
 shutdown
!
interface FastEthernet0/22
 switchport mode access
 shutdown
!
interface FastEthernet0/23
 switchport mode access
 shutdown
!
interface FastEthernet0/24
 switchport mode access
 shutdown
!
interface GigabitEthernet0/1
 switchport mode access
 shutdown
!
interface GigabitEthernet0/2
 switchport mode access
 shutdown
!
 --More--
```

La imagen anterior muestra el modo de acceso de las interfaces y su estado. Todas las interfaces del S3 están en modo de acceso menos la interfaz f0/3.

Configuración de seguridad. La seguridad en el switch fue establecida cuando se realizó la configuración inicial de este. Los comandos ejecutados fueron los siguientes:

```
enable secret class
line con 0
pass cisco
login
line vty 0 4
pass cisco
login
exit
!
service password-encryption
banner motd =¡El acceso no autorizado esta prohibido!=
copy running-config startup-config
```

La siguiente imagen muestra el resultado de la configuración de seguridad.

```
S3#show running-config
Building configuration...

Current configuration : 2338 bytes
!
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname S3
!
enable secret 5 $1$mERr$9cTjUIEqNGurQiFU.ZeCi1
!


banner motd ^CEl acceso no autorizado esta prohibido!^C
!
!
!
line con 0
 password 7 0822455D0A16
 login
!
line vty 0 4
 password 7 0822455D0A16
 login
line vty 5 15
```

- ✓ Configuración inter-Vlan routing

La configuración se realiza en el router para establecer la comunicación entre las VLANs. Se configuran las direcciones ip en las subinterfaces de la interfaz f0/0 y se les asigna su encapsulamiento. Los comandos para la configuración son los siguientes:

```
enable
config terminal
interface f0/0.30
description LAN Administración
encapsulation dot1q 30
ip address 192.168.30.1 255.255.255.0
exit
!
interface f0/0.40
description LAN Mercadeo
encapsulation dot1q 40
ip address 192.168.40.1 255.255.255.0
exit
!
interface f0/0.200
description LAN Mantenimiento
encapsulation dot1q 200
ip address 192.168.200.1 255.255.255.0
exit
!
interface f0/0
no shutdown
exit
copy running-config startup-config
```

Se utilizan las primeras direcciones ip disponibles de cada una de las redes VLAN en las subinterfaces de la f0/0. La siguiente imagen muestra resumen del resultado de la configuración:

```
Medellin#show ip interface brief
Interface              IP-Address      OK? Method Status
Protocol
FastEthernet0/0        unassigned      YES unset  up
up
FastEthernet0/0.30     192.168.30.1    YES manual up
up
FastEthernet0/0.40     192.168.40.1    YES manual up
up
FastEthernet0/0.200    192.168.200.1   YES manual up
up
```

4. En el Switch 3 deshabilitar DNS lookup.

En la configuración inicial del switch 3 se deshabilitó dicha opción. Los comandos son los siguientes:

```
enable
conf terminal
no ip domain-lookup
```

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

A ambos switches se les fue asignado el direccionamiento ip teniendo en cuenta la dirección de red 192.168.200.0/24. Los comandos se muestran a continuación:

S1

```
interf vlan 200
ip address 192.168.200.2 255.255.255.0
no shutdown
exit
!
ip default-gateway 192.168.200.1
```

Se verifica la configuración con el comando show running-config. A continuación se muestra el resultado de interés.

```
interface Vlan200
 mac-address 0030.f23b.e702
 ip address 192.168.200.3 255.255.255.0
!
ip default-gateway 192.168.200.1
!
```

S3

```
interf vlan 200
ip address 192.168.200.3 255.255.255.0
no shutdown
exit
!
ip default-gateway 192.168.200.1
```

Se verifica la configuración con el comando show running-config. A continuación se muestra el resultado de interés.

```
interface Vlan200
 mac-address 0009.7c39.2402
 ip address 192.168.200.2 255.255.255.0
!
ip default-gateway 192.168.200.1
!
```

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

Las interfaces de los switches que no se están utilizando fueron desactivadas en el ítem tres. Los comandos (inicialmente en modo de configuración global) empleados fueron los siguientes:

S3

```
interf range f0/2, f0/4-24, g0/1-2
shutdown
end
```

7. Implementar DHCP and NAT para IPv4 (Este es el título, las labores son los puntos del 8 - 13)

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

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

Configurar DHCP pool para VLAN 30	Name: ADMINISTRACION DNS-Server: 10.10.10.11 Domain-Name: ccna-unad.com Establecer default gateway.
Configurar DHCP pool para VLAN 40	Name: MERCADEO DNS-Server: 10.10.10.11 Domain-Name: ccna-unad.com Establecer default gateway.

Se configuró el R1 como servidor DHCP para las VLANs 30 y 40 y también se crearon los pools con los siguientes comandos:

```
enable
conf term
!Habilitando servicio dhcp (por lo general está
!habilitado)
service dhcp
!Reservando las primeras 30 direcciones vlan 30
ip dhcp excluded-address 192.168.30.1 192.168.30.30
!Reservando las primeras 30 direcciones vlan 40
ip dhcp excluded-address 192.168.40.1 192.168.40.30
!Creando pool dhcp para la vlan 30
ip dhcp pool ADMINISTRACION
dns-server 10.10.10.11
domain-name ccna-unad.com
default-router 192.168.30.1
network 192.168.30.0 255.255.255.0
exit
ip dhcp pool MERCADEO
dns-server 10.10.10.11
domain-name ccna-unad.com
default-router 192.168.40.1
network 192.168.40.0 255.255.255.0
end
copy running-config startup-config
```

A continuación se muestran la configuración de parámetros de direccionamiento ip de los host PC-A y PC-C, donde se obtienen mediante DHCP:

PC-A

PC-C

Como se puede observar los dos PCs tienen configurados sus parámetros de configuración IP por DHCP.

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

La configuración de NAT en R2 se estableció de acuerdo a los siguientes comandos:

```
!!NAT en R2
enable
conf term
!Creando NAT-POOL
ip nat pool NAT-POOL1 209.165.200.225 209.165.200.229 netmask 255.255.255.248
access-list 1 permit 192.168.30.0 0.0.0.255
access-list 1 permit 192.168.40.0 0.0.0.255
ip nat inside source list 1 pool NAT-POOL1
interf s0/0/1
ip nat inside
exit
interf f0/0
ip nat outside
end
```

Se tomó en cuenta la red 209.165.200.224/29 para el pool de direcciones públicas, mientras que se creó la ACL 1 (con dos configuraciones) para permitir la salida a internet de las VLAN 30 y 40

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.

Los comandos para la configuración de la ACL estándar son los siguientes:

```
!!ACLs en R2
!!Creando lista de acceso estándar para solo permitir
!!acceso telnet/ssh desde el router 1 al router 2.
conf term
ip access-list standard Admin-Telnet
permit host 172.31.21.1
exit
line vty 0 4
access-class Admin-Telnet in
end
```

En la imagen anterior se muestra la restricción de acceso TELNET/SSH para cualquier red que no sea la 172.31.21.1 (que es la red del router Medellín). Se creó una ACL y se asignó a las líneas VTY. A continuación se muestra su resultado:

Acceso vía TELNET desde el router Medellín (Exitoso)

```
Medellin>enable
Medellin#telnet 172.31.21.2
Trying 172.31.21.2 ...Open

[Connection to 172.31.21.2 closed by foreign host]
Medellin#
```

Acceso vía TELNET desde el router B/manga (No exitoso)

```
Bucaramanga>
Bucaramanga>enable
Bucaramanga#telnet 172.31.21.2
Trying 172.31.21.2 ...
% Connection refused by remote host
Bucaramanga#
```

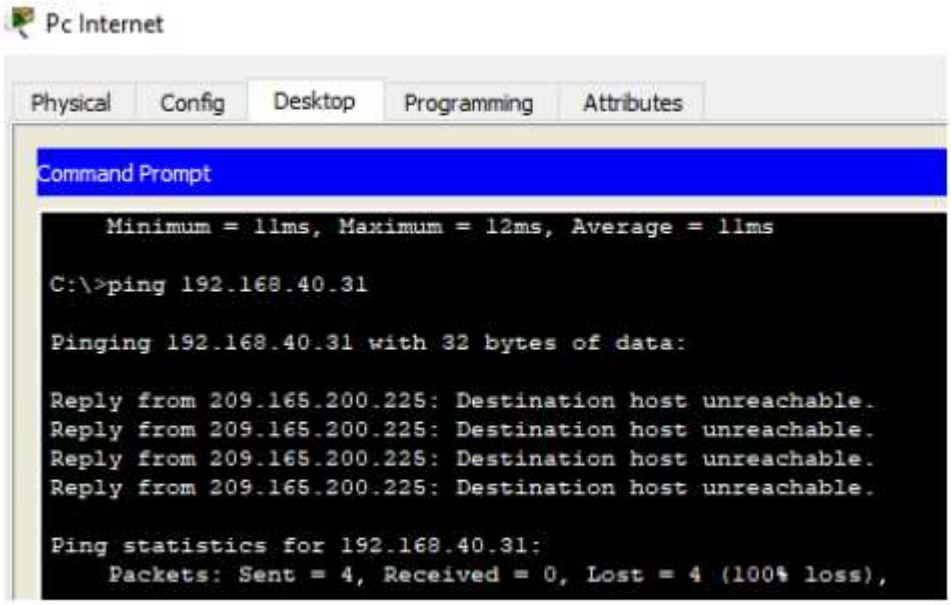
12. Configurar al menos dos listas de acceso de tipo extendido o nombradas a su criterio en para restringir o permitir tráfico desde R1 o R3 hacia R2.

Se configuró la ACL 101 en donde se restringe el proceso de ping (ICMP) desde la red externa (PC Internet) hacia la red interna, pero permitiendo lo contrario. A continuación se muestran los comandos ejecutados:

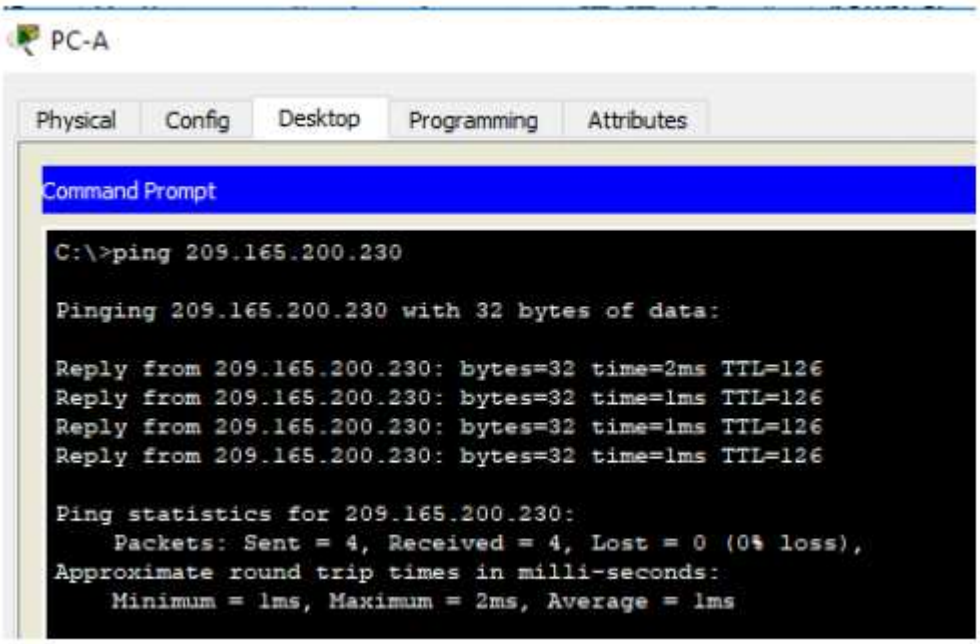
```
!!ACL extendida en R2
conf term
!!Previniendo ping desde la lan externa hacia la interna y
!!permintiendo lo inverso
access-list 101 permit icmp any any echo-reply
interf f0/0
ip access-group 101 in
interf f0/1
ip access-group 101 out
interf s0/0/1
ip access-group 101 out
interf s0/0/0
ip access-group 101 out
```

La anterior ACL se comprueba como se muestra a continuación:

- ✓ Ping desde el PC Internet hacia el PC-A (No exitoso)

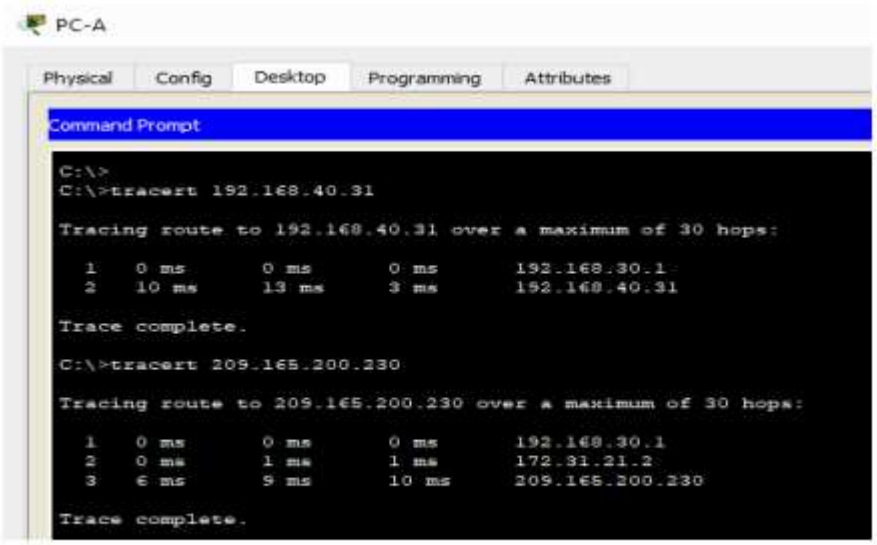


- ✓ Ping desde el PC-A hacia el PC Internet (Exitoso)

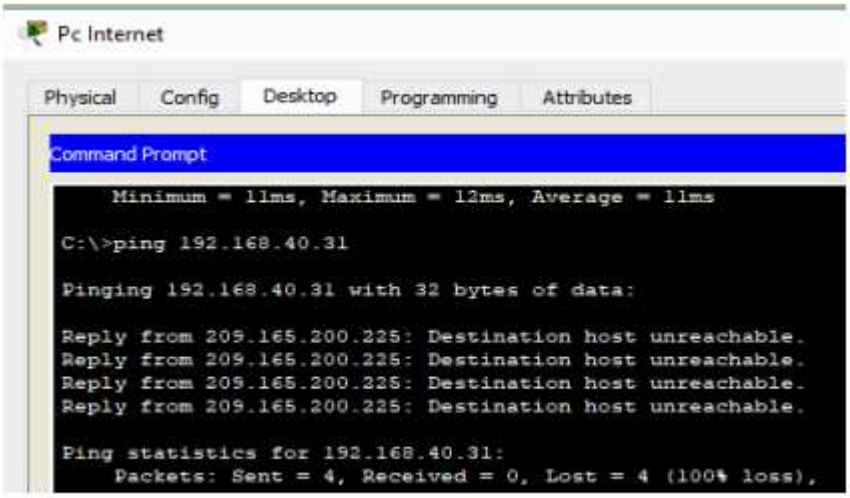


13. Verificar procesos de comunicación y redireccionamiento de tráfico en los routers mediante el uso de Ping y Traceroute.

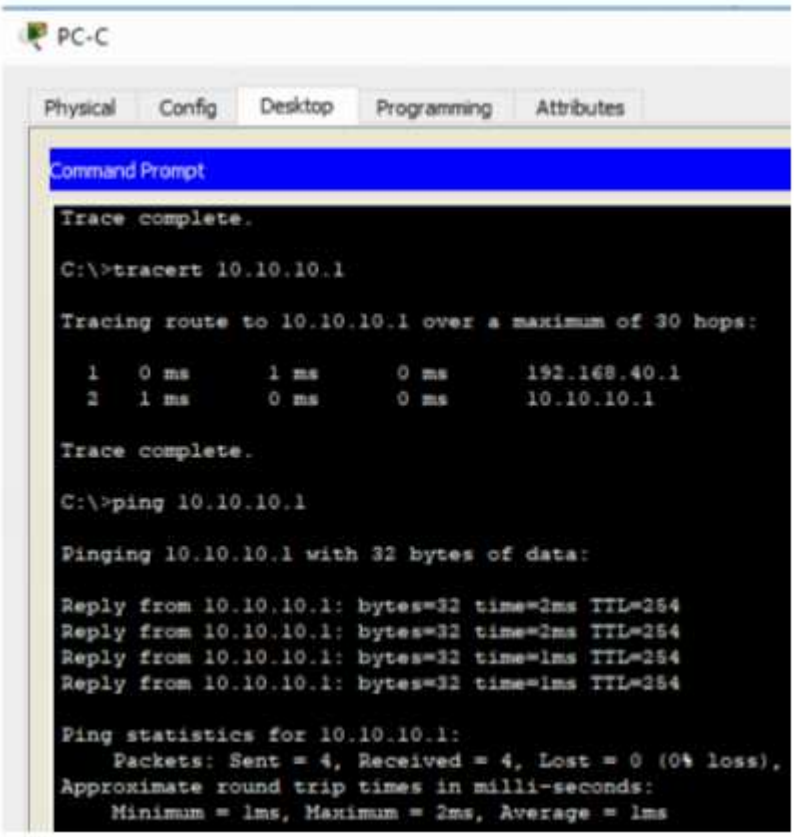
- ✓ Traceroute desde el PC-A hacia PC Internet y de la PC-A hacia la PC-C



- ✓ Ping Pc Internet hacia la red interna



- ✓ Traceroute y ping desde la PC-C hacia la interfaz f0/1 (ip 10.10.10.1)



Pasos realizados para la configuración de la red propuesta:

Configuración de los switches

```
!!SW1
config term
vlan 30
name Administración
vlan 40
name Mercadeo
vlan 200
name Mantenimiento
exit
!
!Se le asigna la ip a la vlan de mantenimiento
interf vlan 200
ip address 192.168.200.2 255.255.255.0
no shutdown
exit
!
ip default-gateway 192.168.200.1

interf f0/3
switchport mode trunk
switchport trunk native vlan 1
exit
!
interf f0/24
switchport mode trunk
switchport trunk native vlan 1
exit
!
interf range fa0/1-2, fa0/4-23, g0/1-2
switchport mode access
exit
!
interf f0/1
switchport mode access
```

```
switchport access vlan 30
exit
!
interf range f0/2, f0/4-23, g0/1-2
shutdown
end
!
copy running-config startup-config

!!SW3
config term
vlan 30
name Administración
vlan 40
name Mercadeo
vlan 200
name Mantenimiento
exit
!
!Asignación de dirección IP a la vlan de mantenimiento
interf vlan 200
ip address 192.168.200.3 255.255.255.0
no shutdown
exit
!
ip default-gateway 192.168.200.1

interf f0/3
switchport mode trunk
switchport trunk native vlan 1
exit
!
interf range fa0/1-2, fa0/4-24, g0/1-2
switchport mode access
exit
!
interf f0/1
switchport mode access
switchport access vlan 40
exit
!
interf range f0/2, f0/4-24, g0/1-2
```

```
shutdown
end
!
copy running-config startup-config
```

Más configuración de switches

```
##Configurando SW1
enable
conf terminal
hostname S1
enable secret class
line con 0
pass cisco
login
line vty 0 4
pass cisco
login
exit
!
service password-encryption
banner motd =¡El acceso no autorizado esta prohibido!=
copy running-config startup-config

##Configurando SW3
enable
conf terminal
no ip domain-lookup
hostname S3
enable secret class
line con 0
pass cisco
login
line vty 0 4
pass cisco
login
exit
!
service password-encryption
banner motd =¡El acceso no autorizado esta prohibido!=
copy running-config startup-config
```

Configuración inicial router, servidor y PC Internet

```
##R1(Medellin)
enable
conf term
no ip domain-lookup
hostname Medellin
interface s0/0/0
description conexion con Bogota
ip address 172.31.21.1 255.255.255.252
clock rate 128000
no shutdown
exit
!
ip route 0.0.0.0 0.0.0.0 s0/0/0
exit
!
copy running-config startup-config

##R2(Bogota) configuring
enable
conf term
no ip domain-lookup
hostname Bogota
##En el siguiente comando se presenta un error,
##por ello se procedde a configurar un servidor web
##real en la topología.

ip http server

interface s0/0/0
description conexion con Bucaramanga
ip address 172.31.23.1 255.255.255.252
clock rate 128000
no shutdown
exit
!
interface s0/0/1
description conexion con Medellin
ip address 172.31.21.2 255.255.255.252
no shutdown
exit
!
```

```
interface f0/0
description conexion a ISP
ip address 209.165.200.225 255.255.255.248
no shutdown
exit
!
interface f0/1
description conexion con servidor web
ip address 10.10.10.1 255.255.255.0
no shutdown
exit
!
ip route 0.0.0.0 0.0.0.0 f0/0
exit
!
copy running-config startup-config

##R3(Bucaramanga) configuring
enable
conf term
no ip domain-lookup
hostname Bucaramanga
interface s0/0/1
description conexion con Bogota
ip address 172.31.23.2 255.255.255.252
no shutdown
exit

!
interface loopback 4
ip address 192.168.4.1 255.255.255.0
no shutdown
exit
!
interface loopback 5
ip address 192.168.5.1 255.255.255.0
no shutdown
exit
!
interface loopback 6
ip address 192.168.6.1 255.255.255.0
no shutdown
exit
```

```
!
ip route 0.0.0.0 0.0.0.0 s0/0/1
exit
!
copy running-config startup-config
```

Configuración OSPF en diferentes dispositivos

```
!OSPF R1
enable
conf term
!OSPF e id de router
router ospf 1
router-id 1.1.1.1
!Notificando redes conectadas directamente
network 172.31.21.0 0.0.0.3 area 0
network 192.168.30.0 0.0.0.255 area 0
network 192.168.40.0 0.0.0.255 area 0
network 192.168.200.0 0.0.0.255 area 0
!Estableciendo interfaces LAN como pasiva
passive-interface f0/0.30
passive-interface f0/0.40
passive-interface f0/0.200
exit
!Ancho de banda para interfaz s0/0/0
interface s0/0/0
bandwidth 128
!Costo de metrica
ip ospf cost 7500
end
copy running-config startup-config
```

```
!OSPF R2
enable
conf term
!OSPF e id de router
router ospf 1
router-id 2.2.2.2
```

```
!Notificando redes conectadas directamente
network 172.31.21.0 0.0.0.3 area 0
network 172.31.23.0 0.0.0.3 area 0
network 10.10.10.0 0.0.0.255 area 0
!Estableciendo interfaces LAN como pasiva
passive-interface f0/1
exit
!Ancho de banda para interfaz seriales
interface s0/0/0
bandwidth 128
exit
interface s0/0/1
bandwidth 128
exit
!Costo de métrica para la serial s0/0/0
interface s0/0/0
ip ospf cost 7500
end
copy running-config startup-config

!OSPF R3
enable
conf term
!OSPF e id de router
router ospf 1
router-id 3.3.3.3
!Notificando redes conectadas directamente
network 172.31.23.0 0.0.0.3 area 0
network 192.168.4.0 0.0.3.255 area 0
!Estableciendo interfaces LAN como pasiva

passive-interface lo4
passive-interface lo5
passive-interface lo6
exit
!Ancho de banda para interfaz serial s0/0/1
interface s0/0/1
bandwidth 128
end
copy running-config startup-config
```

Configuración subinterfaces del router Medellin

```
enable
config terminal
interface f0/0.30
description LAN Administración
encapsulation dot1q 30
ip address 192.168.30.1 255.255.255.0
exit
!
interface f0/0.40
description LAN Mercadeo
encapsulation dot1q 40
ip address 192.168.40.1 255.255.255.0
exit
!
interface f0/0.200
description LAN Mantenimiento
encapsulation dot1q 200
ip address 192.168.200.1 255.255.255.0
exit
!
interface f0/0
no shutdown
exit
copy running-config startup-config
```

Configuración DHCP y NAT

```
!!DHCP en R1
enable
conf term
!Habilitando servicio dhcp (por lo general está
!habilitado)
service dhcp
!Reservando las primeras 30 direcciones vlan 30
ip dhcp excluded-address 192.168.30.1 192.168.30.30
!Reservando las primeras 30 direcciones vlan 40
ip dhcp excluded-address 192.168.40.1 192.168.40.30
!Creando pool dhcp para la vlan 30
```

```
ip dhcp pool ADMINISTRACION
dns-server 10.10.10.11
domain-name ccna-unad.com
default-router 192.168.30.1
network 192.168.30.0 255.255.255.0
exit
ip dhcp pool MERCADEO
dns-server 10.10.10.11
domain-name ccna-unad.com
default-router 192.168.40.1
network 192.168.40.0 255.255.255.0
end
copy running-config startup-config


!!NAT en R2
enable
conf term
!Creando NAT-POOL
ip nat pool NAT-POOL1 209.165.200.225 209.165.200.229 netmask 255.255.255.248
access-list 1 permit 192.168.30.0 0.0.0.255
access-list 1 permit 192.168.40.0 0.0.0.255
ip nat inside source list 1 pool NAT-POOL1
interf s0/0/1
ip nat inside
exit
interf f0/0
ip nat outside
end

!!ACLs en R2
!!Creando lista de acceso estándar para solo permitir
!!acceso telnet/ssh desde el router 1 al router 2.
conf term
ip access-list standard Admin-Telnet
permit host 172.31.21.1
exit
line vty 0 4
access-class Admin-Telnet in
end

!!ACL extendida en R2
```

```
conf term
!!Previniendo ping desde la lan externa hacia la interna y
!!permintiendo lo inverso
access-list 101 permit icmp any any echo-reply
interf f0/0
ip access-group 101 in
interf f0/1
ip access-group 101 out
interf s0/0/1
ip access-group 101 out
interf s0/0/0
ip access-group 101 out
```

Verificando OSPF

```
enable
show ip ospf neighbor
show ip ospf interface
show ip protocols
```

CONCLUSIONES

Después de haber realizado el presente trabajo se puede concluir que las redes de datos son fundamentales para que la tecnología llegue a cualquier lugar, de allí la necesidad de conocer sus bases e ir diariamente en busca de actualizaciones que permitan la modernización en infraestructura y configuración, lo que sin lugar a dudas, traerá mayores beneficios, menos inversión y mejora en la transferencia de datos. Por otra parte, se observó que todos las áreas que rodean la creación de redes con fundamentales, se debe tener en cuenta cada detalle, desde la topología, medios a utilizar, selección, configuración de dispositivos intermedios y finales, así como, la verificación constante de la parametrización dada a cada componente, esto seguramente minimizará en una auditoría y puesta en marcha general cualquier falla en la conexión.

BIBLIOGRAFÍA

- CISCO. (2014). Exploración de la red. Fundamentos de Networking. Recuperado de: https://static-course-assets.s3.amazonaws.com/ITN50ES/module1/index.html#1.0.1.1

- Shaughnessy, T., Velte, T., & Sáchez García, J. I. (2000). Manual de CISCO.

- Ariganello, E., & Sevilla, B. (2011). Redes CISCO - guía de estudio para la certificación CCNP (No. 004.6 A73).

- Benchimol, D. (2010). Redes Cisco-Instalacion y administracion de hardware y software.

- Teare, D., Vachon B., Graziani, R. (2015). CISCO Press (Ed). Path Control Implementation. Implementing Cisco IP Routing (ROUTE) Foundation Learning Guide CCNP ROUTE 300-101. Recuperado de https://1drv.ms/b/s!AmIJYeiNT1IlnMfy2rhPZHwEoWx

- Teare, D., Vachon B., Graziani, R. (2015). CISCO Press (Ed). Implementing a Border Gateway Protocol (BGP) Solution for ISP Connectivity. Implementing Cisco IP Routing (ROUTE) Foundation Learning Guide CCNP ROUTE 300-101. Recuperado de https://1drv.ms/b/s!AmIJYei-NT1IlnMfy2rhPZHwEoWx

- Teare, D., Vachon B., Graziani, R. (2015). CISCO Press (Ed). Implementing Routing Facilities for Branch Offices and Mobile Workers. Implementing Cisco IP Routing (ROUTE) Foundation Learning Guide CCNP ROUTE 300-101. Recuperado de https://1drv.ms/b/s!AmIJYei-NT1IlnMfy2rhPZHwEoWx