

DIPLOMADO DE PROFUNDIZACIÓN CISCO (DISEÑO E IMPLEMENTACIÓN DE
SOLUCIONES INTEGRADAS LAN / WAN

PRUEBA DE HABILIDADES PRÁCTICAS CCNA

JAIME YESID LANCHEROS LOPEZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD

ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍAS E

INGENIERÍAS – ECBTI

TUNJA

2018

DIPLOMADO DE PROFUNDIZACIÓN CISCO (DISEÑO E IMPLEMENTACIÓN DE
SOLUCIONES INTEGRADAS LAN / WAN

PRUEBA DE HABILIDADES PRÁCTICAS CCNA

JAIME YESID LANCHEROS LOPEZ

INFORME PRUEBA DE HABILIDADES PRÁCTICAS

DIEGO EDINSON RAMIREZ

TUTOR

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD

ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍAS E

INGENIERÍAS – ECBTI

TUNJA

2018

Nota de Aceptación

Presidente del Jurado

Jurado

Jurado

Tunja 27 de mayo de 2018

CONTENIDO

INTRODUCCIÓN	8
OBJETIVOS	9
Objetivo General	9
Objetivos Específicos	9
PLANTEAMIENTO DEL PROBLEMA	10
JUSTIFICACIÓN	10
MARCO TEÓRICO	11
MATERIALES Y MÉTODOS	13
MATERIALES	13
METODOLOGÍA.....	13
DESARROLLO DEL PROYECTO.....	14
ANÁLISIS DEL DESARROLLO DEL PROYECTO	27
CONCLUSIONES	28
RECOMENDACIONES	29
BIBLIOGRAFÍA.....	30

LISTA DE TABLAS

Tabla 1. Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway predeterminado
R1	G0/0.1	192.168.99.1	255.255.255.0	N/A
	G0/0.30	192.168.30.1	255.255.255.0	N/A
	G0/1.40	192.168.40.1	255.255.255.0	N/A
	G0/1.200	192.168.200.1	255.255.255.0	N/A
	S0/0/0	172.31.21.2	255.255.255.252	N/A
S1	VLAN 1	192.168.99.2	255.255.255.0	192.168.99.1
S3	VLAN 1	192.168.99.3	255.255.255.0	192.168.99.1
PC-A	NIC	DHCP	DHCP	DHCP
PC-B	NIC	DHCP	DHCP	DHCP
R2	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
	G0/0	209.165.200.225	255.255.255.248	N/A
	Lo0	10.10.10.10	255.255.255.255	N/A
PC-Internet	NIC	209.165.200.230	255.255.255.248	209.165.200.225
R3	S0/0/1	172.31.23.2	255.255.255.252	N/A
	Lo4	192.168.4.1	255.255.255.0	
	Lo5	192.168.5.1	255.255.255.0	
	Lo6	192.168.6.1	255.255.255.0	

LISTA DE ANEXOS

Anexo A. Evaluación – Prueba de habilidades prácticas CCNA.pk

GLOSARIO

Cisco: es una empresa estadounidense proveedora de soluciones de red y fabricante de dispositivos de interconexión de redes de área local (LAN) y redes de área extensa (WAN). Fundada en 1984, Cisco tiene su sede en San José, California, y posee oficinas en todo el mundo, incluyendo Argentina, Brasil, Chile, Colombia, México y Perú.

Router: Los routers se utilizan para conectar varias redes. Por ejemplo, puede utilizar un router para conectar sus computadoras en red a Internet y, de esta forma, compartir una conexión de Internet entre varios usuarios. El router actuará como distribuidor, seleccionando la mejor ruta de desplazamiento de la información para que la reciba rápidamente.

Switch: Los Switches se utilizan para conectar varios dispositivos a través de la misma red dentro de un edificio u oficina. Por ejemplo, un Switch puede conectar sus computadoras, impresoras y servidores, creando una red de recursos compartidos. El Switch actuaría de controlador, permitiendo a los diferentes dispositivos compartir información y comunicarse entre sí. Mediante el uso compartido de información y la asignación de recursos, los switches permiten ahorrar dinero y aumentar la productividad.

Routing: es la función de buscar un camino entre todos los posibles en una red de paquetes cuyas topologías poseen una gran conectividad. Dado que se trata de encontrar la mejor ruta posible, lo primero será definir qué se entiende por "mejor ruta" y en consecuencia cuál es la "métrica" que se debe utilizar para medirla.

OSPF (Primero la ruta libre más corta): Protocolo de enrutamiento por estado de enlace jerárquico, que se ha propuesto como sucesor de RIP en la comunidad de Internet.

INTRODUCCIÓN

Mediante el desarrollo de la presente practica se pretende interconectar una red WAN de acuerdo a una topología dada, junto con otros parámetros establecidos en la guía suministrada; esta práctica tendrá como fin aplicar conocimientos adquiridos en los módulos CCNAI y CCNAII , estudiados en el DIPLOMADO DE PROFUNDIZACIÓN CISCO (DISEÑO E IMPLEMENTACIÓN DE SOLUCIONES INTEGRADAS LAN / WAN) .

OBJETIVOS

Objetivo General

Diseñar una red WAN mediante el uso de dispositivos de red interconectados y configurados permitiendo tráfico entre éstas haciendo uso de protocolos de enrutamiento y demás aspectos que hacen parte de la topología.

Objetivos Específicos

- Configurar el direccionamiento IP acorde con la topología de red para cada uno de los dispositivos que forman parte del escenario.
- Configurar el protocolo de enrutamiento OSPFv2 según lineamientos.
- Configurar VLANs, Puertos troncales, puertos de acceso, encapsulamiento, Inter-VLAN Routing y Seguridad en los Switches acorde a la topología de red establecida.
- Implementar DHCP and NAT for IPv4Especificar las ventajas, costos, materiales, entre otros, del radioenlace.
- Configurar listas de acceso estándar y extendidas para restringir o permitir tráfico desde R1 o R3 hacia R2.
- Verificar procesos de comunicación y redireccionamiento de tráfico en los routers.

PLANTEAMIENTO DEL PROBLEMA

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.

JUSTIFICACIÓN

Diseñar, analizar, configurar e investigar son aspectos aplicables en la solución al planteamiento expuesto, el cual será abordado con base en conocimientos adquiridos durante el pregrado y todo lo aprendido en los cursos de CCNAI y CCNAII.

MARCO TEÓRICO

Las Vlan son redes de área local virtuales las cuales permiten división lógica del dominio de Broadcast a nivel de la Capa 2 del modelo OSI. También podemos decir que una VLAN es una agrupación lógica de dispositivos que se pueden comunicar en sí.

Las VLAN están definidas por los estándares IEEE 802.1D, 802.1p, 802.1Q y 802.10.

Se han definido diversos tipos de VLAN, según criterios de conmutación y el nivel en el que se lleve a cabo. Así, la VLAN de nivel 1 (también denominada VLAN basada en puerto) define una red virtual según los puertos de conexión del conmutador. La VLAN de nivel 2 (también denominada VLAN basada en la dirección MAC) define una red virtual según las direcciones MAC de las estaciones. Este tipo de VLAN es más flexible que la VLAN basada en puerto, ya que la red es independiente de la ubicación de la estación.

Además de las anteriores, existe la VLAN de nivel 3, que incluye diferentes tipos. La VLAN basada en la dirección de red conecta subredes según la dirección IP de origen de los datagramas. Este tipo de solución brinda gran flexibilidad, en la medida en que la configuración de los conmutadores cambia automáticamente cuando se mueve una estación. En contrapartida, puede haber una ligera disminución del rendimiento, ya que la información contenida en los paquetes debe analizarse detenidamente. La VLAN basada en protocolo permite crear una red virtual por tipo de protocolo (por ejemplo, TCP/IP, IPX, AppleTalk, etc.). Por lo tanto, se pueden agrupar todos los equipos que utilizan el mismo protocolo en la misma red.

Una tabla de enrutamiento es un archivo almacenado en la memoria RAM del enrutador cuya

finalidad es almacenar la información de las rutas sobre redes conectadas directamente y

redes remotas. La tabla de enrutamiento contiene asociaciones red/siguiente salto que le dicen al enrutador que un destino (identificado por el concepto “red”) puede alcanzarse enviando el paquete hacia otro enrutador (que representa el concepto “siguiente salto”) en el camino al destino final.

Protocolos de enrutamiento sin clase.

Sí envían la información de la máscara de subred con la dirección de red en las actualizaciones de enrutamiento. Las redes actuales ya no se signan basándose en clases y la máscara de subred no puede determinarse por el valor del primer octeto. Los protocolos de enrutamiento sin clase son necesarios en la mayoría de las redes actuales debido a que soportan VLSM20, las redes discontinuas, etc....

Este tipo de protocolos son RIPv2, EIGRP, OSPF, IS-IS y BGP

OSPFv2 (open shortest path first) fue creado a finales de los ochenta. Se diseñó para cubrir las necesidades de las grandes redes IP que otros protocolos como RIP no podían soportar, incluyendo VLSM, autenticación de origen de ruta, convergencia rápida, etiquetado de rutas conocidas mediante protocolos de enrutamiento externo y publicaciones de ruta de multidifusión. El protocolo OSPF versión 2 en la implementación más actualizada, aparece especificado en la RFC 2328.

- Las listas de acceso ACL son un mecanismo para clasificar los paquetes que circulan a través de un router; éstas a su vez están formadas por un grupo de declaraciones que permiten (“permit”) o deniegan (“deny”) paquetes, son aplicables interfaces (entrada/salida router), políticas QoS y traducciones NAT. Las ACL se clasifican en estándar y extendidas.

MATERIALES Y MÉTODOS

MATERIALES

- Computador de escritorio con Sistema Operativo Windows 7
- Software packet tracer ver. 6.3
- acceso a internet Banda Ancha
- Documentación cisco CCNAI- CCNAII

METODOLOGÍA

- Se realiza diseño de red de acuerdo a topología sugerida.
- se configura direccionamiento IP
- son creadas Vlan en router 1 y Switch 1 y 3
- se realiza tabla de enrutamiento
- es aplicado protocolo OSPFv2
- se configuran listas de acceso
- se valida conectividad

DESARROLLO DEL PROYECTO

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

```

interface Serial0/0/0
 ip address 172.31.21.2 255.255.255.252
 clock rate 128000
!

R2(config)#inter s0/0/0
R2(config-if)#ip add 172.31.23.1 255.255.255.252
R2(config-if)#clock rate 128000
^
% Invalid input detected at '^' marker.

R2(config-if)#clock rate 128000
R2(config-if)#no sh

%LINK-5-CHANGED: Interface Serial0/0/0, changed state to down
R2(config-if)#inter s0/0/1
R2(config-if)#ip add 172.31.21.1 255.255.255.252
R2(config-if)#no sh

R3(config)#int s0/0/1
R3(config-if)#ip add 172.31.23.2 255.255.255.252
R3(config-if)#exit
R3(config)#int loo
R3(config)#int loopback 4

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

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

R3(config-if)#ip add 192.168.4.1 255.255.255.0
R3(config-if)#int loopback 5

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

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

R3(config-if)#ip add 192.168.5.1 255.255.255.0
R3(config-if)#int loopback 6

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

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

R3(config-if)#ip add 192.168.6.1 255.255.255.0

```

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

OSPFv2 área 0	Configuración Ítem 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 128 Kb/s
 seriales en
 Ajustar el costo en la métrica de S0/0 a 7500

```
R1#conf term
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#router ospf 1
R1(config-router)#router-id 1.1.1.1
R2(config)#router ospf 1
R2(config-router)#router-id 2.2.2.2
R3(config)#router ospf 1
R3(config-router)#router-id 3.3.3.3

Last flood scan time is 0 msec, maximum is 0 msec
Neighbor Count is 1, Adjacent neighbor count is 1
  Adjacent with neighbor 2.2.2.2
Suppress hello for 0 neighbor(s)
GigabitEthernet0/0.30 is up, line protocol is up
Internet address is 192.168.30.1/24, Area 0
Process ID 1, Router ID 1.1.1.1, Network Type BROADCAST, Cost: 1
Transmit Delay is 1 sec, State WAITING, Priority 1
No designated router on this network
No backup designated router on this network
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
  No Hellos (Passive interface)
Index 3/3, flood queue length 0
Next 0x0(0)/0x0(0)
Last flood scan length is 1, maximum is 1
Last flood scan time is 0 msec, maximum is 0 msec
Neighbor Count is 0, Adjacent neighbor count is 0
Suppress hello for 0 neighbor(s)
GigabitEthernet0/0.40 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 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

Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#int s0/0/0
R1(config-if)#bandwidth 128
R1(config-if)#

R2(config)#interface s0/0/0
R2(config-if)#bandwidth 128
R2(config-if)#interface s0/0/1
R2(config-if)#bandwidth 128
R2(config-if)#
```

```

R3(config)#int s0/0/1
R3(config-if)#bandwidth 128
R3(config-if)#

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

R2(config)#interface s0/0/0
R2(config-if)#ip ospf cost 7500
R2(config-if)#

```

Verificar información de OSPF

Visualizar tablas de enrutamiento y routers conectados por OSPFv2

```

10.0.0.0/32 is subnetted, 1 subnets
C    10.10.10.11/32 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    172.31.21.1/32 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
192.168.4.0/32 is subnetted, 1 subnets
O    192.168.4.1/32 [110/7501] via 172.31.23.2, 00:04:57, Serial0/0/0
192.168.5.0/32 is subnetted, 1 subnets
O    192.168.5.1/32 [110/7501] via 172.31.23.2, 00:04:57, Serial0/0/0
192.168.6.0/32 is subnetted, 1 subnets
O    192.168.6.1/32 [110/7501] via 172.31.23.2, 00:04:57, Serial0/0/0
O    192.168.30.0/24 [110/782] via 172.31.21.2, 00:20:26, Serial0/0/1
O    192.168.40.0/24 [110/782] via 172.31.21.2, 00:20:26, Serial0/0/1
O    192.168.99.0/24 [110/782] via 172.31.21.2, 00:20:26, 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    209.165.200.225/32 is directly connected, GigabitEthernet0/0
S*  0.0.0.0/0 [1/0] via 10.10.10.11
R2#
R2#

10.0.0.0/32 is subnetted, 1 subnets
O    10.10.10.11/32 [110/7501] via 172.31.21.1, 00:11:45, 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 [110/15000] via 172.31.21.1, 00:10:31, Serial0/0/0
192.168.4.0/32 is subnetted, 1 subnets
O    192.168.4.1/32 [110/15001] via 172.31.21.1, 00:10:31, Serial0/0/0
192.168.5.0/32 is subnetted, 1 subnets
O    192.168.5.1/32 [110/15001] via 172.31.21.1, 00:10:31, Serial0/0/0
192.168.6.0/32 is subnetted, 1 subnets
O    192.168.6.1/32 [110/15001] via 172.31.21.1, 00:10:31, Serial0/0/0
192.168.30.0/24 is variably subnetted, 2 subnets, 2 masks
C    192.168.30.0/24 is directly connected, GigabitEthernet0/0.30
L    192.168.30.1/32 is directly connected, GigabitEthernet0/0.30
192.168.40.0/24 is variably subnetted, 2 subnets, 2 masks
C    192.168.40.0/24 is directly connected, GigabitEthernet0/0.40
L    192.168.40.1/32 is directly connected, GigabitEthernet0/0.40
192.168.99.0/24 is variably subnetted, 2 subnets, 2 masks
C    192.168.99.0/24 is directly connected, GigabitEthernet0/0.1
L    192.168.99.1/32 is directly connected, GigabitEthernet0/0.1
192.168.200.0/24 is variably subnetted, 2 subnets, 2 masks
C    192.168.200.0/24 is directly connected, GigabitEthernet0/0.200
L    192.168.200.1/32 is directly connected, GigabitEthernet0/0.200
209.165.200.0/29 is subnetted, 1 subnets
O    209.165.200.224/29 [110/7501] via 172.31.21.1, 00:11:45, Serial0/0/0
R1#

```

```

10.0.0.0/32 is subnetted, 1 subnets
O   10.10.10.11/32 [110/782] via 172.31.23.1, 00:26:15, Serial0/0/1
172.31.0.0/16 is variably subnetted, 3 subnets, 2 masks
O   172.31.21.0/30 [110/1562] via 172.31.23.1, 00:26:15, 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
192.168.4.0/24 is variably subnetted, 2 subnets, 2 masks
C   192.168.4.0/24 is directly connected, Loopback4
L   192.168.4.1/32 is directly connected, Loopback4
192.168.5.0/24 is variably subnetted, 2 subnets, 2 masks
C   192.168.5.0/24 is directly connected, Loopback5
L   192.168.5.1/32 is directly connected, Loopback5
192.168.6.0/24 is variably subnetted, 2 subnets, 2 masks
C   192.168.6.0/24 is directly connected, Loopback6
L   192.168.6.1/32 is directly connected, Loopback6
O   192.168.30.0/24 [110/1563] via 172.31.23.1, 00:26:15, Serial0/0/1
O   192.168.40.0/24 [110/1563] via 172.31.23.1, 00:26:15, Serial0/0/1
O   192.168.99.0/24 [110/1563] via 172.31.23.1, 00:26:15, Serial0/0/1
209.165.200.0/29 is subnetted, 1 subnets
O   209.165.200.224/29 [110/782] via 172.31.23.1, 00:26:15, Serial0/0/1
S*  0.0.0.0/0 [1/0] via 172.31.23.1
R3#
R3#

```

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

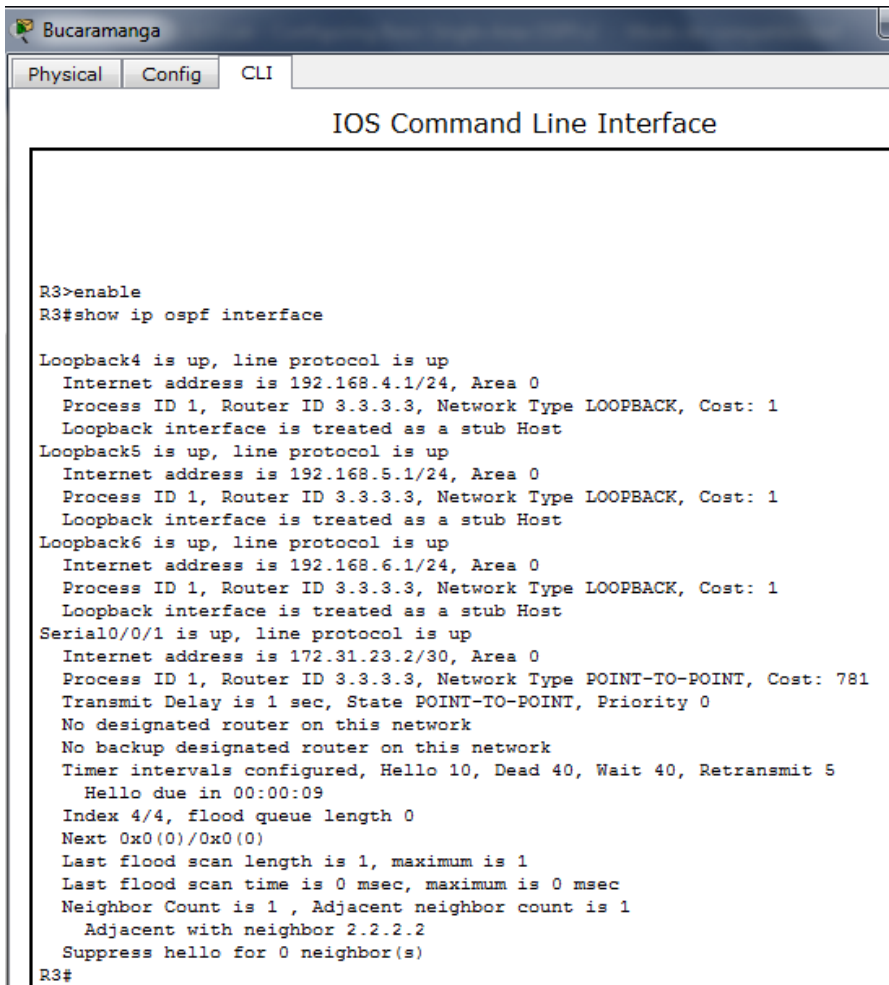
Comando no soportado para packet tracer
show ip ospf interface brief

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

```
Medellin
Physical Config CLI
IOS Command Line Interface

Process ID 1, Router ID 1.1.1.1, Network Type BROADCAST, Cost: 1
Transmit Delay is 1 sec, State DR, Priority 1
Designated Router (ID) 1.1.1.1, Interface address 192.168.99.1
No backup designated router on this network
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
  No Hellos (Passive interface)
Index 1/1, flood queue length 0
Next 0x0(0)/0x0(0)
Last flood scan length is 1, maximum is 1
Last flood scan time is 0 msec, maximum is 0 msec
Neighbor Count is 0, Adjacent neighbor count is 0
Suppress hello for 0 neighbor(s)
GigabitEthernet0/0.30 is up, line protocol is up
Internet address is 192.168.30.1/24, Area 0
Process ID 1, Router ID 1.1.1.1, Network Type BROADCAST, Cost: 1
Transmit Delay is 1 sec, State DR, Priority 1
Designated Router (ID) 1.1.1.1, Interface address 192.168.30.1
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)
GigabitEthernet0/0.40 is up, line protocol is up
Internet address is 192.168.40.1/24, Area 0
Process ID 1, Router ID 1.1.1.1, Network Type BROADCAST, Cost: 1
Transmit Delay is 1 sec, State DR, Priority 1
Designated Router (ID) 1.1.1.1, Interface address 192.168.40.1
No backup designated router on this network
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
  No Hellos (Passive interface)
Index 3/3, flood queue length 0
Next 0x0(0)/0x0(0)
Last flood scan length is 1, maximum is 1
Last flood scan time is 0 msec, maximum is 0 msec
Neighbor Count is 0, Adjacent neighbor count is 0
Suppress hello for 0 neighbor(s)
GigabitEthernet0/0.50 is up, line protocol is up
```

```
Bogotá
Physical Config CLI
IOS Command Line Interface
Index 1/2, 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)
Serial0/0/1 is up, line protocol is up
Internet address is 172.31.21.1/30, 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 00:00:02
Index 2/2, flood queue length 0
Next 0x0(0)/0x0(0)
Last flood scan length is 1, maximum is 1
Last flood scan time is 0 msec, maximum is 0 msec
Neighbor Count is 1, Adjacent neighbor count is 1
Adjacent with neighbor 1.1.1.1
Suppress hello for 0 neighbor(s)
Serial0/0/0 is up, line protocol is up
Internet address is 172.31.23.1/30, Area 0
Process ID 1, Router ID 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 00:00:02
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)
Loopback0 is up, line protocol is up
Internet address is 10.10.10.11/32, Area 0
Process ID 1, Router ID 2.2.2.2, Network Type LOOPBACK, Cost: 1
Loopback interface is treated as a stub Host
R2#
```



```
R3>enable
R3#show ip ospf interface

Loopback4 is up, line protocol is up
  Internet address is 192.168.4.1/24, Area 0
  Process ID 1, Router ID 3.3.3.3, Network Type LOOPBACK, Cost: 1
  Loopback interface is treated as a stub Host
Loopback5 is up, line protocol is up
  Internet address is 192.168.5.1/24, Area 0
  Process ID 1, Router ID 3.3.3.3, Network Type LOOPBACK, Cost: 1
  Loopback interface is treated as a stub Host
Loopback6 is up, line protocol is up
  Internet address is 192.168.6.1/24, Area 0
  Process ID 1, Router ID 3.3.3.3, Network Type LOOPBACK, Cost: 1
  Loopback interface is treated as a stub Host
Serial0/0/1 is up, line protocol is up
  Internet address is 172.31.23.2/30, Area 0
  Process ID 1, Router ID 3.3.3.3, Network Type POINT-TO-POINT, Cost: 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 00:00:09
  Index 4/4, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1 , Adjacent neighbor count is 1
    Adjacent with neighbor 2.2.2.2
  Suppress hello for 0 neighbor(s)
R3#
```

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

```

R1(config-if)#inter G0/0.1
R1(config-subif)#
%LINK-S-CHANGED: Interface GigabitEthernet0/0.1, changed state to up

R1(config-subif)#encapsulation dot1Q 1
R1(config-subif)#ip add 192.168.99.1 255.255.255.0
R1(config-subif)#inter G0/0.30
R1(config-subif)#
%LINK-S-CHANGED: Interface GigabitEthernet0/0.30, changed state to up

R1(config-subif)#encapsulation dot1Q 30
R1(config-subif)#ip add 192.168.99.2 255.255.255.0
% 192.168.99.0 overlaps with GigabitEthernet0/0.1
R1(config-subif)#ip add 192.168.30.1 255.255.255.0
R1(config-subif)#inter G0/0.40
R1(config-subif)#
%LINK-S-CHANGED: Interface GigabitEthernet0/0.40, changed state to up

R1(config-subif)#encapsulation dot1Q 40
R1(config-subif)#ip add 192.168.40.1 255.255.255.0
R1(config-subif)#
R1#
%SYS-5-CONFIG_I: Configured from console by console

R1#config term
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#inter G0/0.200
R1(config-subif)#
%LINK-S-CHANGED: Interface GigabitEthernet0/0.200, changed state to up

R1(config-subif)#encapsulation dot1Q 200
R1(config-subif)#ip add 192.168.200.1 255.255.255.0
R1(config-subif)#exit
R1(config)#inter G0/0
R1(config-if)#no sh
R1(config-if)#
%LINK-S-CHANGED: Interface Serial0/0/0, changed state to up

hostname S1
!
!
!
!
!
spanning-tree mode pvst
!
interface FastEthernet0/1
  switchport access vlan 30
  switchport mode access
!
interface FastEthernet0/2
!
interface FastEthernet0/3
  switchport mode trunk
!
interface FastEthernet0/4
!
interface FastEthernet0/5
!
interface FastEthernet0/6
,

```

```

!
interface FastEthernet0/24
  switchport mode trunk
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
  ip address 192.168.99.2 255.255.255.0
!
ip default-gateway 192.168.99.1
.

```

```

!
hostname S3
!
!
!
no ip domain-lookup
!
!
spanning-tree mode pvst
!
interface FastEthernet0/1
  switchport access vlan 40
  switchport mode access
!
interface FastEthernet0/2
!
interface FastEthernet0/3
  switchport mode trunk
!
interface FastEthernet0/4
!
interface FastEthernet0/5
!
interface FastEthernet0/6
!
interface GigabitEthernet0/2
!
interface Vlan1
  ip address 192.168.99.3 255.255.255.0
!
ip default-gateway 192.168.99.1
!
!
!

```

D. En el Switch 3 deshabilitar DNS lookup

```

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

```

E. Asignar direcciones IP a los Switches acorde a los lineamientos. S1 interface Vlan1

```

ip address 192.168.99.2 255.255.255.0
ip default-gateway 192.168.99.1
S2 interface Vlan1
ip address 192.168.99.3 255.255.255.0
ip default-gateway 192.168.99.1

```

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

Port	Link	VLAN	IP Address	MAC Address
FastEthernet0/1	Up	30	--	0060.5CE2.AE01
FastEthernet0/2	Down	1	--	0060.5CE2.AE02
FastEthernet0/3	Up	--	--	0060.5CE2.AE03
FastEthernet0/4	Down	1	--	0060.5CE2.AE04
FastEthernet0/5	Down	1	--	0060.5CE2.AE05
FastEthernet0/6	Down	1	--	0060.5CE2.AE06
FastEthernet0/7	Down	1	--	0060.5CE2.AE07
FastEthernet0/8	Down	1	--	0060.5CE2.AE08
FastEthernet0/9	Down	1	--	0060.5CE2.AE09
FastEthernet0/10	Down	1	--	0060.5CE2.AE0A
FastEthernet0/11	Down	1	--	0060.5CE2.AE0B
FastEthernet0/12	Down	1	--	0060.5CE2.AE0C
FastEthernet0/13	Down	1	--	0060.5CE2.AE0D
FastEthernet0/14	Down	1	--	0060.5CE2.AE0E
FastEthernet0/15	Down	1	--	0060.5CE2.AE0F
FastEthernet0/16	Down	1	--	0060.5CE2.AE10
FastEthernet0/17	Down	1	--	0060.5CE2.AE11
FastEthernet0/18	Down	1	--	0060.5CE2.AE12
FastEthernet0/19	Down	1	--	0060.5CE2.AE13
FastEthernet0/20	Down	1	--	0060.5CE2.AE14
FastEthernet0/21	Down	1	--	0060.5CE2.AE15
FastEthernet0/22	Down	1	--	0060.5CE2.AE16
FastEthernet0/23	Down	1	--	0060.5CE2.AE17
FastEthernet0/24	Up	--	--	0060.5CE2.AE18
GigabitEthernet0/1	Down	1	--	0060.5CE2.AE19
GigabitEthernet0/2	Down	1	--	0060.5CE2.AE1A
Vlan1	Up	1	192.168.99.2/24	00D0.58BE.E5E8
Hostname: S1				

Port	Link	VLAN	IP Address	MAC Address
FastEthernet0/1	Up	40	--	0060.3EDB.6001
FastEthernet0/2	Down	1	--	0060.3EDB.6002
FastEthernet0/3	Up	--	--	0060.3EDB.6003
FastEthernet0/4	Down	1	--	0060.3EDB.6004
FastEthernet0/5	Down	1	--	0060.3EDB.6005
FastEthernet0/6	Down	1	--	0060.3EDB.6006
FastEthernet0/7	Down	1	--	0060.3EDB.6007
FastEthernet0/8	Down	1	--	0060.3EDB.6008
FastEthernet0/9	Down	1	--	0060.3EDB.6009
FastEthernet0/10	Down	1	--	0060.3EDB.600A
FastEthernet0/11	Down	1	--	0060.3EDB.600B
FastEthernet0/12	Down	1	--	0060.3EDB.600C
FastEthernet0/13	Down	1	--	0060.3EDB.600D
FastEthernet0/14	Down	1	--	0060.3EDB.600E
FastEthernet0/15	Down	1	--	0060.3EDB.600F
FastEthernet0/16	Down	1	--	0060.3EDB.6010
FastEthernet0/17	Down	1	--	0060.3EDB.6011
FastEthernet0/18	Down	1	--	0060.3EDB.6012
FastEthernet0/19	Down	1	--	0060.3EDB.6013
FastEthernet0/20	Down	1	--	0060.3EDB.6014
FastEthernet0/21	Down	1	--	0060.3EDB.6015
FastEthernet0/22	Down	1	--	0060.3EDB.6016
FastEthernet0/23	Down	1	--	0060.3EDB.6017
FastEthernet0/24	Down	1	--	0060.3EDB.6018
GigabitEthernet0/1	Down	1	--	0060.3EDB.6019
GigabitEthernet0/2	Down	1	--	0060.3EDB.601A
Vlan1	Up	1	192.168.99.3/24	0001.C719.3570
Hostname: S3				

G. Implement DHCP and NAT for IPv4

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

```
ip dhcp pool Administracion
 network 192.168.30.0 255.255.255.0
 default-router 192.168.30.1
 dns-server 10.10.10.11
ip dhcp pool Mercadeo
 network 192.168.40.0 255.255.255.0
 default-router 192.168.40.1
 dns-server 10.10.10.11
```

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

```
ip dhcp excluded-address 192.168.30.1 192.168.30.31
ip dhcp excluded-address 192.168.40.1 192.168.40.31
```

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

```
R2(config)#ip nat inside source static 172.31.21.2 209.165.200.226
R2(config)#int S0/0/0
R2(config-if)#int S0/0/1
R2(config-if)#ip nat inside
R2(config-if)#int g0/0
R2(config-if)#ip nat outside
R2(config-if)#exit
R2(config)#exit
R2#
%SYS-5-CONFIG_I: Configured from console by console

R2#show ip nat translations
Pro Inside global   Inside local       Outside local      Outside global
--- 209.165.200.226  172.31.21.2       ---               ---

R2#conf term
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#ip nat inside source static 172.31.23.2 209.165.200.227
R2(config)#int S0/0/0
R2(config-if)#ip nat inside
R2(config-if)#int g0/0
R2(config-if)#ip nat outside
R2(config-if)#end
R2#
%SYS-5-CONFIG_I: Configured from console by console

R2#show ip nat translations
Pro Inside global   Inside local       Outside local      Outside global
```

K. 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.

```

R2>enable
R2#conf term
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#access-list 1 permit 192.168.30.0 0.0.0.255
R2(config)#access-list 1 deny any
R2(config)#interface serial0/0/1
R2(config-if)#ip access-group 1 out
R2(config-if)#exit
R2(config)#access-list 2 permit 192.168.40.0 0.0.0.255
R2(config)#access-list 2 deny any
R2(config)#interface serial0/0/1
R2(config-if)#ip access-group 2 out
R2(config-if)#

```

- L. 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.

```

R2(config)#access-list 100 deny tcp 192.168.30.0 0.0.0.255 eq 23 172.31.21.1
0.0.0.3 eq 23
R2(config)#access-list 100 deny tcp 192.168.40.0 0.0.0.255 eq 23 172.31.21.1
0.0.0.3 eq 23
R2(config)#access-list 100 deny tcp 192.168.30.0 0.0.0.255 eq 23 172.31.21.1
0.0.0.3 eq 23
R2(config)#access-list 100 permit ip any any
R2(config)#int s0/0/1
R2(config-if)#ip access-group 100 in
R2(config-if)#exit
R2(config)#access-list 101 deny tcp 192.168.40.0 0.0.0.255 eq 23 172.31.21.1
0.0.0.3 eq 23
R2(config)#access-list 101 permit ip any any
R2(config)#ip access-group 101 in
^
* Invalid input detected at '^' marker.

R2(config)#int s0/0/1
R2(config-if)#ip access-group 101 in
R2(config-if)#exit
R2(config)#access-list 101 permit ssh 192.168.200.0 0.0.0.255 eq 22 172.31.21.1
0.0.0.3 eq 22

```

```

R2(config)#access-list 102 permit tcp 192.168.200.0 0.0.0.255 eq 22 172.31.21.1
0.0.0.3 eq 22
R2(config)#access-list 102 permit ip any any
R2(config)#int s0/0/1
R2(config-if)#ip access-group 102 in
R2(config-if)#access-list 103 deny tcp 172.31.23.2 0.0.0.3 eq 23 172.31.23.1
0.0.0.3 eq 23
R2(config)#access-list 103 permit ip any any
R2(config)#int s0/0/0
R2(config-if)#ip access-group 103 in
R2(config-if)#

```

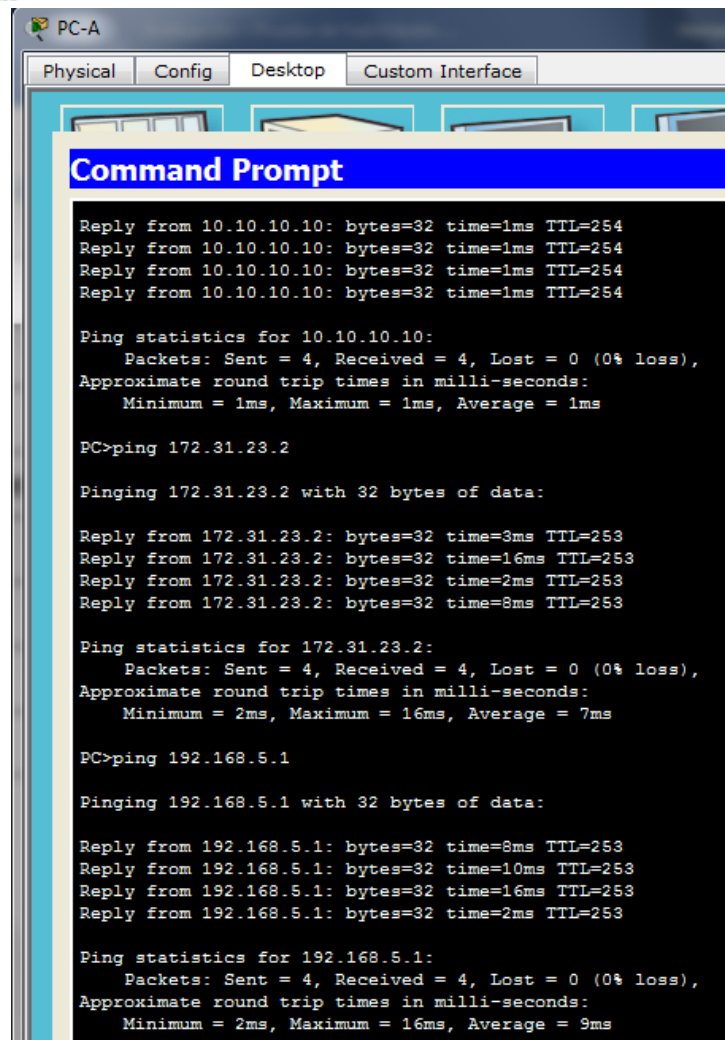
- M. Verificar procesos de comunicación y redireccionamiento de tráfico en los routers mediante el uso de Ping y Traceroute.

```

1 172.31.23.1 6 msec 0 msec 0 msec
2 172.31.21.2 6 msec 1 msec 1 msec
R3#

```

```
1 172.31.21.1 2 msec 1 msec 0 msec
2 172.31.23.2 0 msec 3 msec 0 msec
R1#show runn
```



The screenshot shows a Windows-style window titled "PC-A" with tabs for "Physical", "Config", "Desktop", and "Custom Interface". The active tab is "Custom Interface", which displays a "Command Prompt" window. The Command Prompt shows the output of several ping commands. The first ping is to 10.10.10.10, showing four successful replies with 1ms round-trip times and a TTL of 254. The second ping is to 172.31.23.2, showing four successful replies with round-trip times of 3ms, 16ms, 2ms, and 8ms, and a TTL of 253. The third ping is to 192.168.5.1, showing four successful replies with round-trip times of 8ms, 10ms, 16ms, and 2ms, and a TTL of 253. Each ping result includes statistics for packets sent, received, and lost, as well as approximate round-trip times in milliseconds.

```
PC-A
Physical Config Desktop Custom Interface
Command Prompt
Reply from 10.10.10.10: bytes=32 time=1ms TTL=254
Reply from 10.10.10.10: bytes=32 time=1ms TTL=254
Reply from 10.10.10.10: bytes=32 time=1ms TTL=254
Reply from 10.10.10.10: bytes=32 time=1ms TTL=254

Ping statistics for 10.10.10.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 1ms, Average = 1ms

PC>ping 172.31.23.2

Pinging 172.31.23.2 with 32 bytes of data:

Reply from 172.31.23.2: bytes=32 time=3ms TTL=253
Reply from 172.31.23.2: bytes=32 time=16ms TTL=253
Reply from 172.31.23.2: bytes=32 time=2ms TTL=253
Reply from 172.31.23.2: bytes=32 time=8ms TTL=253

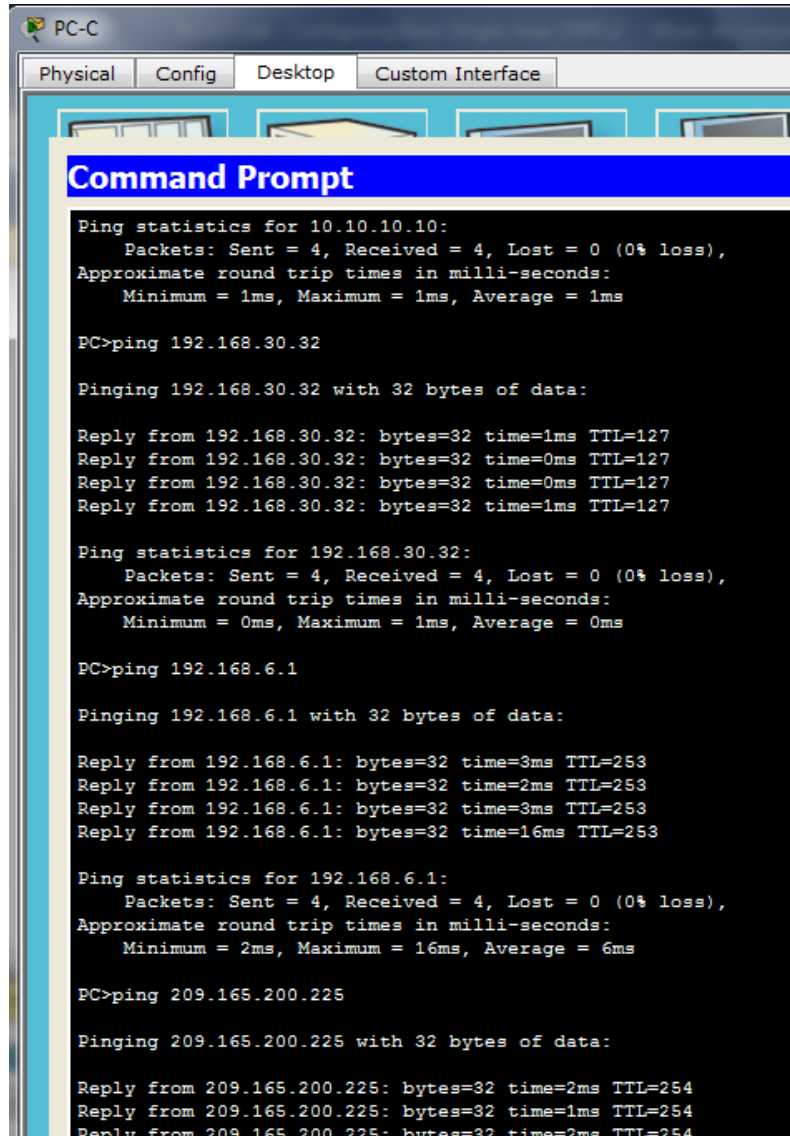
Ping statistics for 172.31.23.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 16ms, Average = 7ms

PC>ping 192.168.5.1

Pinging 192.168.5.1 with 32 bytes of data:

Reply from 192.168.5.1: bytes=32 time=8ms TTL=253
Reply from 192.168.5.1: bytes=32 time=10ms TTL=253
Reply from 192.168.5.1: bytes=32 time=16ms TTL=253
Reply from 192.168.5.1: bytes=32 time=2ms 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 = 16ms, Average = 9ms
```



```
PC-C
Physical Config Desktop Custom Interface

Command Prompt

Ping statistics for 10.10.10.10:
  Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
  Minimum = 1ms, Maximum = 1ms, Average = 1ms

PC>ping 192.168.30.32

Pinging 192.168.30.32 with 32 bytes of data:

Reply from 192.168.30.32: bytes=32 time=1ms TTL=127
Reply from 192.168.30.32: bytes=32 time=0ms TTL=127
Reply from 192.168.30.32: bytes=32 time=0ms TTL=127
Reply from 192.168.30.32: bytes=32 time=1ms TTL=127

Ping statistics for 192.168.30.32:
  Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
  Minimum = 0ms, Maximum = 1ms, Average = 0ms

PC>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=16ms 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 = 16ms, Average = 6ms

PC>ping 209.165.200.225

Pinging 209.165.200.225 with 32 bytes of data:

Reply from 209.165.200.225: bytes=32 time=2ms TTL=254
Reply from 209.165.200.225: bytes=32 time=1ms TTL=254
Reply from 209.165.200.225: bytes=32 time=2ms TTL=254
```

ANÁLISIS DEL DESARROLLO DEL PROYECTO

Mediante las listas de acceso estándar y extendidas se limita el acceso a los dispositivos de red, evitando de esta manera manipulación no autorizada desde cualquier host; tan solo tienen acceso los administradores ya que esta red queda habilitada para dichas funciones.

CONCLUSIONES

Al finalizar la actividad se da cumplimiento a los objetivos planteados en los cuales se afianzaron conocimientos aplicando todo lo aprendido e investigado durante el curso , dando como resultado un producto en el cual convergen diversos temas propios del diseño de redes de área local e internet , los cuales de cara al ámbito profesional servirán de orientación y análisis en el diseño , implementación y administración de cualquier red de telecomunicaciones.

RECOMENDACIONES

La seguridad en las redes es un factor prioritario por lo que es preciso implementar políticas con el fin de preservar la integridad de la información, mediante el uso de las herramientas lógicas como las listas de acceso ACL, la aplicación de protocolos de seguridad en los dispositivos de red, controlar las conexiones a la red tales como: puertos de Switch's, router mediante bloqueo por MAC etc.

BIBLIOGRAFÍA

Artículo web

Jara, C. A. (2012). Sistemas de Transporte de Datos. Práctica 1: Encaminamiento dinámico con IPv4. Sistemas de Transporte de Datos. Recuperado de:

https://rua.ua.es/dspace/bitstream/10045/23719/2/Practica_1_STD.pdf

Artículo web

HERNANDEZ, T., SALAZAR, P., & SOTO, S. (2017). Sistema inteligente para validar una lista de control de acceso (ACL) en una red de comunicaciones. Revista de Simulación, 1(2), 24-31. Recuperado de :

http://www.ecorfan.org/taiwan/research_journals/Simulacion_Computacional/vol1num2/Revista_de_Simulaci%C3%B3n_Computacional_V1_N2.pdf#page=31

Artículo web

BNamericas, Cisco Systems, Inc. Recuperado de:

<https://www.bnamericas.com/company-profile/es/cisco-systems-inc-cisco>

Libro

Ariganello Ernesto. REDES CISCO. Guía de estudio para la certificación CCNA Routing y Switching, 4ª edición actualizada, Madrid, España, 2016. Recuperado de:

https://books.google.com.co/books?id=tpBFDwAAQBAJ&pg=PT338&lpg=PT338&dq=define+Switching&source=bl&ots=k5M4t9_I0K&sig=7L9ukMJ3XdgMnu0mpD5gy_flg&hl=es-

[419&sa=X&ved=0ahUKEwiTu4Hm_KPbAhXB3VMKHdSECV4Q6AEIcjAI#v=one
page&q=ospf&f=false](#)