

PRUEBA DE HABILIDADES CCNA

CLAUDIA PATRICIA CELY MONTAÑEZ
C.C: 1.056.830.258

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERIA
DIPLOMADO DE PROFUNDIZACIÓN CISCO
TUNJA
2018

PRUEBA DE HABILIDADES CCNA

ACTIVIDAD INDIVIDUAL

CLAUDIA PATRICIA CELY MONTAÑEZ
C.C: 1.056.830.258

GIOVANNI ALBERTO BRACHO
TUTOR

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERIA
DIPLOMADO DE PROFUNDIZACIÓN CISCO
TUNJA
2018

Nota de Aceptación

Presidente del Jurado

Jurado

Jurado

Tunja 27 de mayo de 2018

LISTA DE ANEXOS

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

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.

RESUMEN

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.

ABSTRACT

A Technology company has three branches distributed in the cities of Bogotá, Medellín and Bucaramanga, where the student will be the administrator of the network, which must configure and interconnect each of the devices that are part of the scenario, in accordance with the guidelines established for IP addressing, routing protocols and other aspects that are part of the network topology.

CONTENIDO

INTRODUCCIÓN	9
OBJETIVOS.....	10
Objetivo General.....	10
Objetivos Específicos	10
DESCRIPCIÓN GENERAL DE LA PRUEBA DE HABILIDADES	11
DESCRIPCIÓN DEL ESCENARIO PROPUESTO PARA LA PRUEBA DE HABILIDADES.....	12
TOPOLOGÍA DE RED	13
DESARROLLO DE LA ACTIVIDAD	13
TPOLOGIA DE RED (Realización propia)	13
ANÁLISIS DEL DESARROLLO DEL PROYECTO.....	26
CONCLUSIONES	27
RECOMENDACIONES.....	28
BIBLIOGRAFÍA.....	29

INTRODUCCIÓN

Mediante el desarrollo de la presente practica se pretende interconectar una red WAN de acuerdo con una topología dada, junto con otros parámetros establecidos en la guía suministrada; esta práctica tendrá como fin aplicar conocimientos adquiridos en los módulos CCNA I y CCNA II, 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.
- Implement 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

EVALUACIÓN –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.

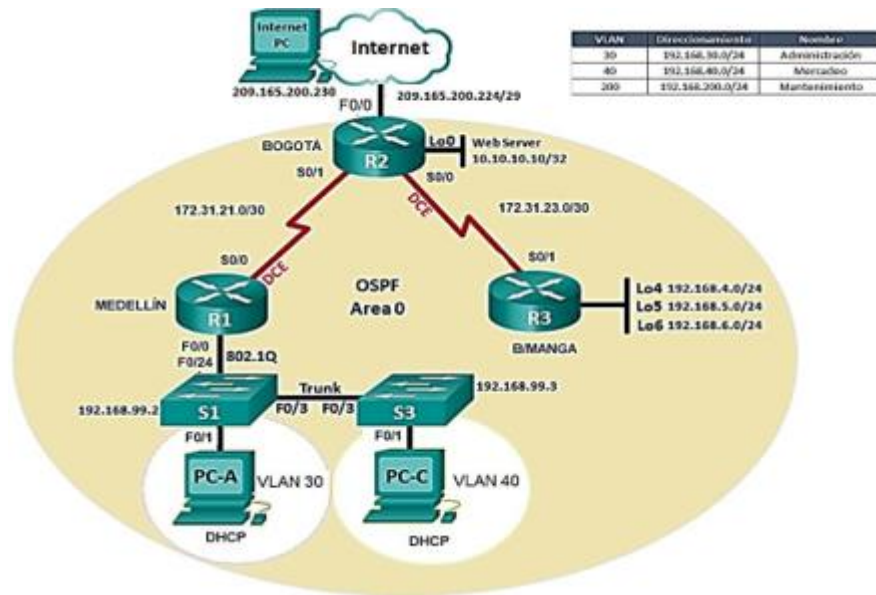
Finalmente, el informe deberá cumplir con las normas ICONTEC para la presentación de trabajos escritos, teniendo en cuenta que este documento deberá ser entregado al final del curso en el Repositorio Institucional, acorde con los lineamientos institucionales para grado. Proceso que les será socializado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

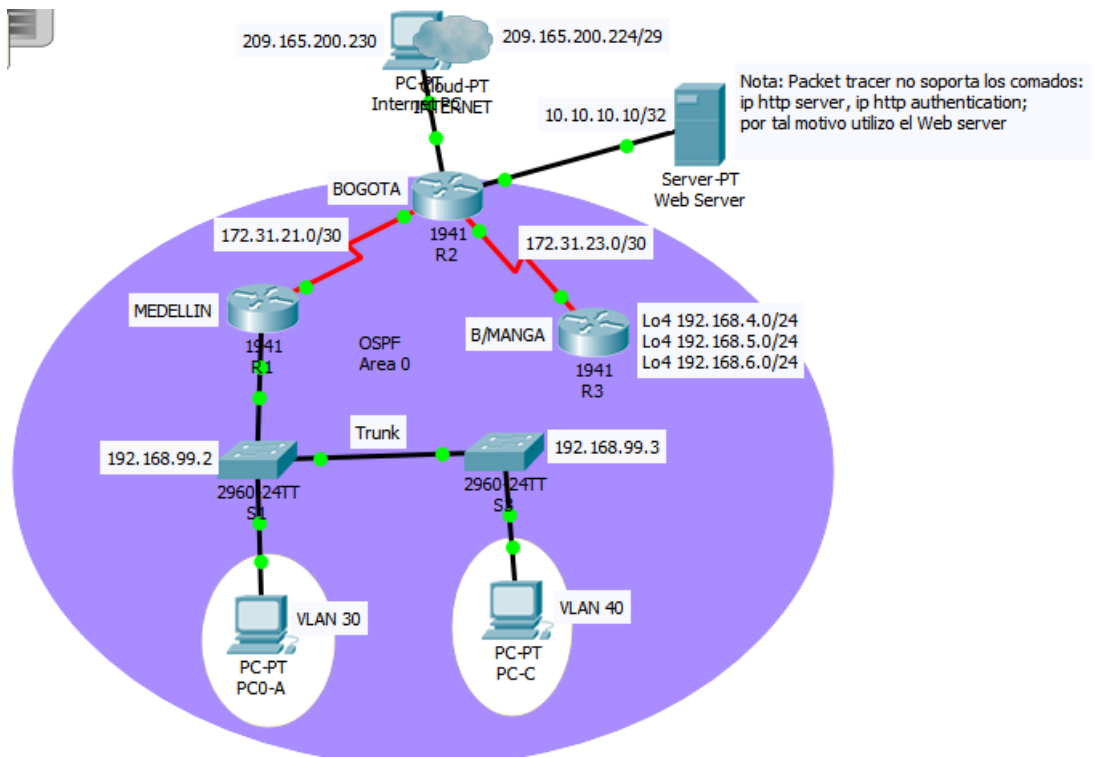
Escenario: Una empresa de Tecnología posee tres sucursales distribuidas en las ciudades de Bogotá, Medellín y Bucaramanga, en donde el estudiante será el administrador de la red, el cual deberá configurar e interconectar entre sí cada uno de los dispositivos que forman parte del escenario, acorde con los lineamientos establecidos para el direccionamiento IP, protocolos de enrutamiento y demás aspectos que forman parte de la topología de red.

TOPOLOGÍA DE RED



DESARROLLO DE LA ACTIVIDAD

TPOLOGIA DE RED (Realización propia)



1. 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

```

Descripción: Se configura el direccionamiento IP acorde con la topología de red para cada uno de los dispositivos que forman parte del escenario

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

OSPFv2 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

```

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

```

```
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
```

Verificar información de OSPF

- Visualizar tablas de enrutamiento y routers conectados por OSPFv2

```
R2#show ip route ospf
    192.168.4.0/32 is subnetted, 1 subnets
O       192.168.4.1 [110/782] via 172.31.23.2, 00:14:08, Serial0/0/1
    192.168.5.0/32 is subnetted, 1 subnets
O       192.168.5.1 [110/782] via 172.31.23.2, 00:14:08, Serial0/0/1
    192.168.6.0/32 is subnetted, 1 subnets
O       192.168.6.1 [110/782] via 172.31.23.2, 00:14:08, Serial0/0/1
O       192.168.30.0 [110/7501] via 172.31.21.1, 00:23:30, Serial0/0/0
O       192.168.40.0 [110/7501] via 172.31.21.1, 00:23:30, Serial0/0/0
O       192.168.200.0 [110/7501] via 172.31.21.1, 00:23:30, Serial0/0/0
```

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


```

R2#show ip ospf interface

Serial0/0/0 is up, line protocol is up
  Internet address is 172.31.21.2/30, Area 0
  Process ID 1, Router ID 2.2.2.2, Network Type POINT-TO-POINT, Cost: 7500
  Transmit Delay is 1 sec, State POINT-TO-POINT, Priority 0
  No designated router on this network
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:02
  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)
Serial0/0/1 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: 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
--More--

```

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

```

R1#show ip protocols

Routing Protocol is "ospf 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 1.1.1.1
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    172.31.21.0 0.0.0.3 area 0
    192.168.30.0 0.0.0.255 area 0
    192.168.40.0 0.0.0.255 area 0
    192.168.200.0 0.0.0.255 area 0
  Passive Interface(s):
    GigabitEthernet0/1.30
    GigabitEthernet0/1.40
    GigabitEthernet0/1.200
  Routing Information Sources:
    Gateway         Distance      Last Update
    1.1.1.1          110          00:28:29
    2.2.2.2          110          00:28:28
    3.3.3.3          110          00:28:29
  Distance: (default is 110)
--More--

```

```

R2#show ip protocols

Routing Protocol is "ospf 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 2.2.2.2
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    172.31.21.0 0.0.0.3 area 0
    172.31.23.0 0.0.0.3 area 0
    10.10.10.0 0.0.0.255 area 0
  Passive Interface(s):
    GigabitEthernet0/1
  Routing Information Sources:
    Gateway         Distance       Last Update
    1.1.1.1          110           00:04:41
    2.2.2.2          110           00:10:27
    3.3.3.3          110           00:03:34
  Distance: (default is 110)

```

```

R3#show ip protocols

Routing Protocol is "ospf 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 3.3.3.3
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    172.31.23.0 0.0.0.3 area 0
    192.168.4.0 0.0.3.255 area 0
  Passive Interface(s):
    Loopback4
    Loopback5
    Loopback6
  Routing Information Sources:
    Gateway         Distance       Last Update
    1.1.1.1          110           00:00:51
    2.2.2.2          110           00:00:51
    3.3.3.3          110           00:00:51
  Distance: (default is 110)

```

3. 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-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-5-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-5-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-5-CHANGED: Interface Serial0/0/0, changed state to up

```

```

hostname S1
!
enable secret 5 $1$mERr$9cTjUIEqNGurQiFU.ZeCi1
!
!
!
no ip domain-lookup
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
interface FastEthernet0/1
!
interface FastEthernet0/2
!
interface FastEthernet0/3
switchport mode trunk

```

```

interface Vlan30
mac-address 0001.c79a.9101
ip address 192.168.99.2 255.255.255.0
!
ip default-gateway 192.168.99.1
!
banner motd ^CUnauthorized Access is Prohibited!^C

```

```

hostname S3
!
enable secret 5 $1$mERr$9cTjUIEqNGurQiFU.ZeCi1
!
!
!
no ip domain-lookup
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
interface FastEthernet0/1
!
interface FastEthernet0/2
!
interface FastEthernet0/3
  switchport mode trunk

```

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

4. En el Switch 3 deshabilitar DNS lookup

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

Descripción: Se deshabilita el DNS lookup del switch 3

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

```

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

```

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

```
%LINK-5-CHANGED: Interface FastEthernet0/20, changed state to administrati  
own  
%LINK-5-CHANGED: Interface FastEthernet0/21, changed state to administrati  
own  
%LINK-5-CHANGED: Interface FastEthernet0/22, changed state to administrati  
own  
%LINK-5-CHANGED: Interface FastEthernet0/23, changed state to administrati  
own  
%LINK-5-CHANGED: Interface FastEthernet0/24, changed state to administrati  
own  
%LINK-5-CHANGED: Interface GigabitEthernet1/1, changed state to administra  
down  
%LINK-5-CHANGED: Interface GigabitEthernet1/2, changed state to administra  
down  
S3(config-if-range)#end  
S3#  
%SYS-5-CONFIG_I: Configured from console by console  
S3#
```

7. Implement DHCP and NAT for IPv4

```
R1#conf t  
Enter configuration commands, one per line. End with CNTL/Z.  
R1(config)#ip dhcp excluded-address 192.168.30.1 192.168.30.30  
R1(config)#ip dhcp excluded-address 192.168.40.1 192.168.40.30  
R1(config)#
```

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

```

R1(config)#ip dhcp pool ADMINISTRACION
R1(dhcp-config)#
R1(dhcp-config)#?
  default-router  Default routers
  dns-server      Set name server
  exit            Exit from DHCP pool configuration mode
  network         Network number and mask
  no              Negate a command or set its defaults
  option          Raw DHCP options
R1(dhcp-config)#dns-server 10.10.10.11
R1(dhcp-config)#domain-name ccna-unad.com
^
% Invalid input detected at '^' marker.

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

R1(dhcp-config)#domain-name ccna-unad.com
^
% Invalid input detected at '^' marker.

R1(dhcp-config)#default-router 192.168.40.1
R1(dhcp-config)#

```

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

```

R1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#ip dhcp excluded-address 192.168.30.1 192.168.30.30
R1(config)#ip dhcp excluded-address 192.168.40.1 192.168.40.30
R1(config)#

```

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.

```

R1(config)#ip dhcp pool ADMINISTRACION
R1(dhcp-config)#
R1(dhcp-config)#?
  default-router  Default routers
  dns-server      Set name server
  exit            Exit from DHCP pool configuration mode
  network         Network number and mask
  no              Negate a command or set its defaults
  option          Raw DHCP options
R1(dhcp-config)#dns-server 10.10.10.11
R1(dhcp-config)#domain-name ccna-unad.com
  ^
% Invalid input detected at '^' marker.

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

R1(dhcp-config)#domain-name ccna-unad.com
  ^
% Invalid input detected at '^' marker.

R1(dhcp-config)#default-router 192.168.40.1
R1(dhcp-config)#

```

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

```

R2(config)#user webuser privilege 15 secret cisco12345
R2(config)#ip http server
  ^
% Invalid input detected at '^' marker.

R2(config)#ip http authentication local
  ^
% Invalid input detected at '^' marker.

R2(config)#

```

Descripción: Packet tracer no soporta los comandos que están encerrados en los cuadros color rojo es por eso que voy a utilizar el servidor web como se muestra en la topología que desarrolle

Nota: Configure NAT Estatica

```
R2(config)#ip nat inside source static 10.10.10.10 209.165.200.229
R2(config)#int g0/0
R2(config-if)#ip nat outside
R2(config-if)#int g0/1
R2(config-if)#ip nat inside
R2(config-if)#
```

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.

```
R2(config)#ip Access-list standard ADMIN
R2(config-std-nacl)#permit host 172.31.21.1
R2(config-std-nacl)#permit host 172.31.23.2
```

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.

```
R2(config)#access-list 101 permit tcp any host 209.165.200.229 eq www
R2(config)#access-list 101 permit icmp any any echo-reply
R2(config)#int g0/0
R2(config-if)#ip access-group 101 in
R2(config-if)#int s0/0/0
R2(config-if)#ip access-group 101 out
R2(config-if)#int s0/0/1
R2(config-if)#ip access-group 101 out
R2(config-if)#int g0/1
R2(config-if)#ip access-group 101 out
R2(config-if)#
```

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

```
R1#en
R1#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 = 1/22/102 ms

R1#
```

```
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 = 1/2/8 ms

R2#
```

```
R2#ping 172.31.21.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.31.21.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/5 ms

R2#
```

```
-----
R3#ping 172.31.23.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.31.23.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/5 ms

R3#
```

```
-----
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=0ms TTL=255
Reply from 209.165.200.225: bytes=32 time=0ms TTL=255
Reply from 209.165.200.225: bytes=32 time=0ms TTL=255
Reply from 209.165.200.225: bytes=32 time=0ms TTL=255

Ping statistics for 209.165.200.225:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

PC>
```

Descripción: Finalmente se verifica los procesos de comunicación y redireccionamiento de tráfico en los routers mediante el uso de Ping y Traceroute.

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 investigando 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

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

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

BNamericas, Cisco Systems, Inc. Recuperado de:

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

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__fl_g&hl=es419&sa=X&ved=0ahUKEwiTu4Hm_KPbAhXB3VMKHdSECV4Q6AEIcjAl#v=onepage&q=ospf&f=false