

PRUEBA DE HABILIDADES DIPLOMADO DE PROFUNDIZACION CCNA

NEISBI LISETH PIRABAN PARRA

C.C: 46451821 de Duitama

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
ESCUELA DE CIENCIAS BASICAS TECNOLOGIA E INGENIERIA

INGENIERIA DE SISTEMAS

SOGAMOSO

2018

PRUEBA DE HABILIDADES DIPLOMADO DE PROFUNDIZACION CCNA

NEISBI LISETH PIRABAN PARRA

C.C: 46451821

Trabajo de grado para optar por el título profesional de
Ingeniería de Sistemas

Tutor académico

Ingeniero: Giovanni Alberto Bracho

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
ESCUELA DE CIENCIAS BASICAS TECNOLOGIA E INGENIERIA
INGENIERIA DE SISTEMAS
SOGAMOSO

2018

NOTA DE ACEPTACION

Presidente del jurado

Jurado

Jurado

Sogamoso, de 15 enero de 2018

DEDICATORIA

Dedico este proyecto en primera medida a Dios que es el pilar y quía espiritual, mis hijos, familiares, amigos que están a mi lado en todo momento y mis tutores por entregar todo su conocimiento para mi aprendizaje que me servirá para un futuro profesional.

Contenido

INTRODUCCION.....	7
OBJETIVO GENERAL	8
OBJETIVOS ESPECIFICOS.....	8
CONTENIDO.....	9
Parte 1: armar la red y configurar los parámetros básicos de los dispositivos.....	12
Paso 1: realizar el cableado de red tal como se muestra en la topología.	13
Paso 2: inicializar y volver a cargar los routers según sea necesario.	13
Paso 3: configurar los parámetros básicos para cada router.....	16
Paso 4: Configurar la internet PC.....	17
Parte 2: Configurar el protocolo de enrutamiento OSPFv2 bajo los siguientes criterios:OSPFv2 área 0.....	17
Verificar información de OSPF.....	17
• Asignar ID a los routers. Emita el comando ip router ospf para iniciar un proceso OSPFv2 en el router.	17
• Asigne la ID de router OSPF 1.1.1.1 al R1.....	18
• Inicie el proceso de routing de OSPF y asigne la ID de router 2.2.2.2 al R2 y la ID de router 3.3.3.3 al R3.	18
• Emita el comando show ip ospf para verificar las ID de router de todos los routers.....	18
todas las redes aparezcan en la tabla de routing de todos los routers.....	20
• Visualizar lista resumida de interfaces por OSPF en donde se ilustre el costo de cada interface; visualizar el OSPF Process ID, Router ID, Address summarizations..	20
• Routing Networks, and passive interfaces configuradas en cada router.	21
Parte 3: Configurar VLANs, Puertos troncales, puertos de acceso, encapsulamiento, Inter- VLAN Routing y Seguridad en los Switches acorde a la topología de red establecida.	24
Parte 4: En el Switch 3 deshabilitar DNS lookup	24
Parte 5: Asignar direcciones IP a los Switches acorde a los lineamientos.	24
Parte 6: Desactivar todas las interfaces que no sean utilizadas en el esquema	24
de red.....	24
Parte 7: Implemente DHCP and NAT para IPv4	24
Parte 8: Configurar R1 como servidor DHCP para las VLANs 30 y 40.	24

Parte 9: Reservar las primeras 30 direcciones IP de las VLAN 30 y 40 para configuraciones estáticas.....	24
Parte 10: Configurar NAT en R2 para permitir que los host puedan salir a internet	25
Parte 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.	26
Parte 11: Configurar al menos dos listas de acceso de tipo extendido o nombradas a su criterio en para restringir o permitir tráfico desde R1 o R3 hacia R2.....	30
Parte 13: Verificar procesos de comunicación y re direccionamiento de tráfico en los routers mediante el uso de Ping y Traceroute.....	31
CONCLUSIONES	35
BIBLIOGRAFIA	36

INTRODUCCION

El siguiente trabajo representa la forma de demostrar, de cómo cisco y la universidad da a sus alumnos las herramientas para llevar a cabo el desarrollo de la educación a distancia. Como método para adquirir el título de ingeniero de sistemas, se hace un curso de profundización en cisco.

De esta manera se da por terminado el curso mediante el desarrollo de una evaluación de práctica de habilidades por las cuales son simuladas por la herramienta de simulación de packet Tracer. Como modelo para simular redes, dado que en la actualidad las redes han adquirido una importancia y su expansión e innovación van transformando nuestra sociedad actual; entrar al mundo de las redes se vislumbra un camino de evolución e innovación en las redes.

OBJETIVO GENERAL

Analizar y solucionar la prueba de habilidades practicas CCNA, propuesta por la universidad para demostrar las habilidades que se desarrollaron en el transcurso del proceso de enseñanza del curso.

OBJETIVOS ESPECIFICOS

- Utilizando la herramienta Packet Tracer conceptualizar la temática de la práctica propuesta por el curso.
- Diseñar la topología propuesta por la prueba.
- Realizar los ejercicios propuestos de acuerdo a los ítems planteados.
- Consolidar las prácticas con sus debidas evidencias.

CONTENIDO

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.

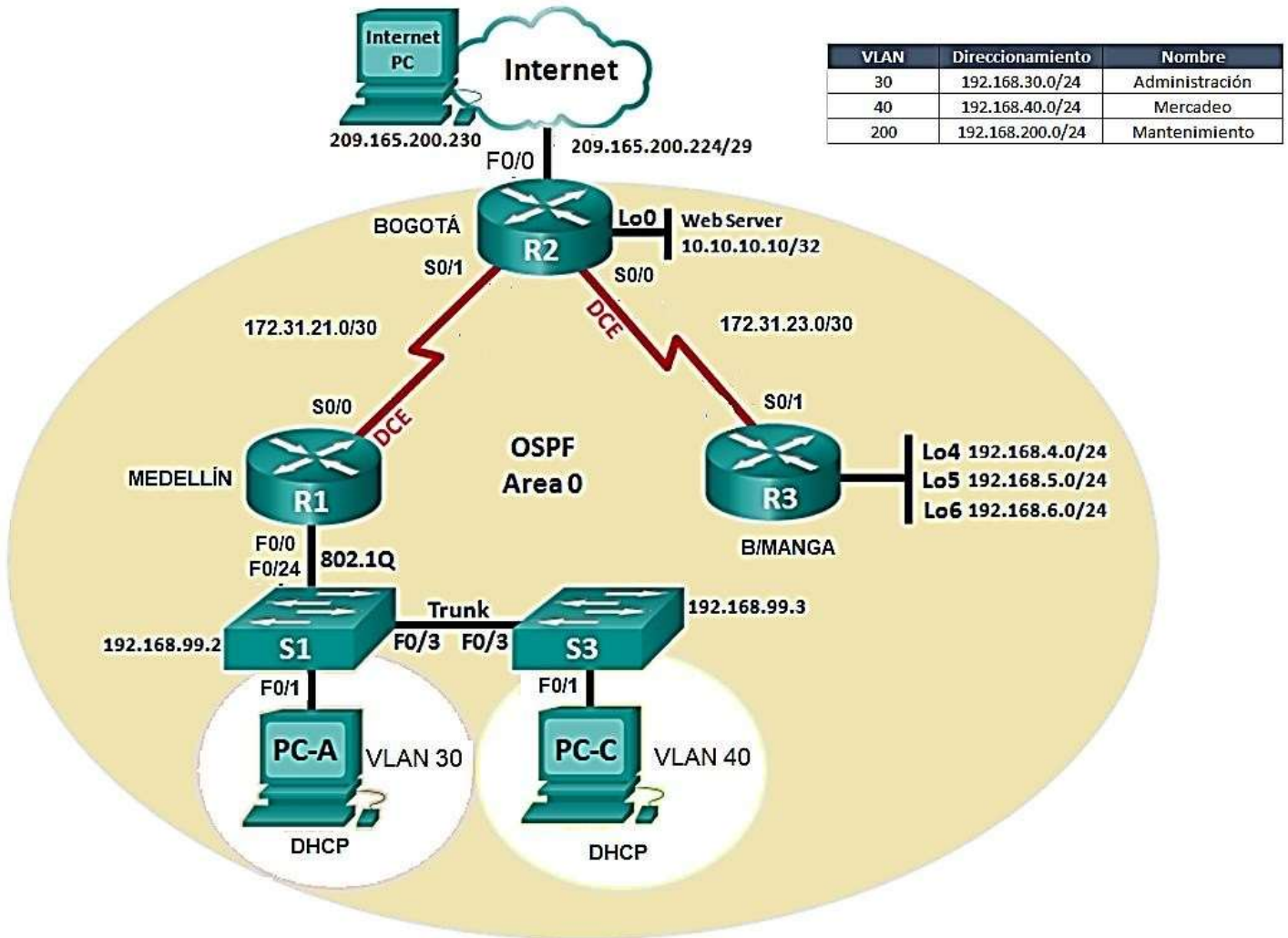
La prueba de habilidades podrá ser desarrollada en el Laboratorio SmartLab o mediante el uso de herramientas de Simulación (Puede ser Packet Tracer o GNS3). El estudiante es libre de escoger bajo qué mediación tecnológica resolverá cada escenario. No obstante, es importante mencionar que aquellos estudiantes que hagan uso del laboratorio SmartLab se les considerarán 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

Topología de red



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.

Información básica/situación

El protocolo OSPF (Open Shortest Path First), es un protocolo de routing de estado de enlace para las redes IP. Se definió OSPFv2 para redes IPv4, y OSPFv3 para redes IPv6¹.

En esta práctica de laboratorio, configurará la topología de la red con routing OSPFv2, asignará ID de router, configurará interfaces pasivas y utilizará varios comandos de CLI para ver y verificar la información de routing OSPFv2.

Nota: asegúrese de que los routers se hayan borrado y no tengan configuraciones de inicio. Si no está seguro, realice las verificaciones pertinentes con el instructor.

Recursos necesarios

3 routers (Cisco 1941 con IOS de Cisco versión 15.2(4)M3, amagan universal o similar).

3 computadoras (Windows 7, Vista o XP con un programa de emulación de terminal, como Tera Term).

Cables de consola para configurar los dispositivos con IOS de Cisco mediante los puertos de consola .

Cables Ethernet y seriales, como se muestra en la topología.

2 switch(cisco 2960 com IOS de cisco15.0 (2), imagen lanbasek9 o similar).

Parte 1: armar la red y configurar los parámetros básicos de los dispositivos.

Establecerá la topología de la red y configurará los parámetros básicos en los equipos host, switch y los routers.

Paso 1: Realizar el cableado de red tal como se muestra en la topología.

Paso 2: Inicializar y volver a cargar los routers según sea necesario.

¹ Enunciados de un anterior trabajo colaborativo

Paso 3: Configurar los parámetros básicos para cada router.

Paso 4: Configurar la internet PC.

Parte 2: Configurar el protocolo de enrutamiento OSPFv2 bajo criterios.

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

Parte 4 : En el Switch 3 deshabilitar DNS lookup.

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

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

Parte 7: Implementar DHCP and NAT for IPv4

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

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

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

Parte 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.

Parte 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.

Parte 13: Verificar procesos de comunicación y re direccionamiento de tráfico en los routers mediante el uso de Ping y Traceroute.

DESARROLLO

Parte 1: armar la red y configurar los parámetros básicos de los dispositivos

En la primera parte, establecerá la topología de la red y configurará los parámetros básicos en los equipos host, switch y los routers.

Paso 1: realizar el cableado de red tal como se muestra en la topología.

Paso 2: inicializar y volver a cargar los routers según sea necesario.


```
no ip address
duplex auto
speed auto
shutdown
interface GigabitEthernet0/1
no ip address
duplex auto
speed auto
shutdown
interface Serial0/0/0
no ip address
clock rate 2000000
shutdown
interface Serial0/0/1
no ip address
clock rate 2000000
shutdown

interface Vlan1
no ip address
shutdown
ip classless
ip flow-export version 9
line con 0
line aux 0
line vty 0 4
login
```

```
end
```

Se verifica algo más

Nos mostrara la configuración de almacenado de la NVRAM.(se verifico en todos los router).

```
Router#sh startup-config
startup-config is not present
Router#
```

Paso 3: configurar los parámetros básicos para cada router.

- a. Desactive la búsqueda del DNS.
- b. Configure el nombre del dispositivo como se muestra en la topología.
- c. Asigne class como la contraseña del modo EXEC privilegiado.
- d. Asigne cisco como la contraseña de vty.
- e. Configure un mensaje MOTD para advertir a los usuarios que se prohíbe el acceso no autorizado.
- f. Configure logging synchronous para la línea de consola.
- g. Cifre las contraseñas de texto no cifrado.
- h. Copie la configuración en ejecución en la configuración de inicio

Paso 4: Configurar la internet PC.

Item de configuracion	Especificación
Id Address	209.165.200.230
Subnet Mask	255.255.255.248
Default Gateway	209.165.200.225

Parte 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	1000
Establecer el ancho de banda para enlaces seriales en	128 Kb/s
Ajustar el costo en la métrica de S0/0 a	7500

Verificar información de OSPF

- Asignar ID a los routers. Emita el comando ip router ospf para iniciar un proceso OSPFv2 en el router.

```
R1(config)# ip router ospf 1
```

- Asigne la ID de router OSPF 1.1.1.1 al R1.

```
R2(config-router)# router-id 1.1.1.1
```

- Inicie el proceso de routing de OSPF y asigne la ID de router 2.2.2.2 al R2 y la ID de router 3.3.3.3 al R3.
- Emita el comando show ip ospf para verificar las ID de router de todos los routers.

```
R1#show ip ospf
```

```
Routing Process "ospf 1" with ID 1.1.1.1
Supports only single TOS(TOS0) routes
Supports opaque LSA
SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
Minimum LSA interval 5 secs. Minimum LSA arrival 1 secs
Number of external LSA 0. Checksum Sum 0x000000
Number of opaque AS LSA 0. Checksum Sum 0x000000
Number of DCbitless external and opaque AS LSA 0
Number of DoNotAge external and opaque AS LSA 0
Number of areas in this router is 1. 1 normal 0 stub 0 nssa
External flood list length 0
Area BACKBONE(0) (Inactive)
Number of interfaces in this area is 0
Area has no authentication
SPF algorithm executed 1 times
Area ranges are
Number of LSA 1. Checksum Sum 0x004d0e
Number of opaque link LSA 0. Checksum Sum 0x000000
Number of DCbitless LSA 0
Number of indication LSA 0
Number of DoNotAge LSA 0
Flood list length 0
```

```
R2#show ip ospf
```

```
Routing Process "ospf 1" with ID 2.2.2.2
Supports only single TOS(TOS0) routes
Supports opaque LSA
SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
Minimum LSA interval 5 secs. Minimum LSA arrival 1 secs
Number of external LSA 0. Checksum Sum 0x000000
Number of opaque AS LSA 0. Checksum Sum 0x000000
Number of DCbitless external and opaque AS LSA 0
Number of DoNotAge external and opaque AS LSA 0
Number of areas in this router is 1. 1 normal 0 stub 0 nssa
External flood list length 0
Area BACKBONE(0)
Number of interfaces in this area is 2
Area has no authentication
SPF algorithm executed 37 times
Area ranges are
Number of LSA 2. Checksum Sum 0x0176fd
Number of opaque link LSA 0. Checksum Sum 0x000000
Number of DCbitless LSA 0
Number of indication LSA 0
Number of DoNotAge LSA 0
Flood list length 0
```

```
R3#show ip ospf
```

```
Routing Process "ospf 1" with ID 3.3.3.3
Supports only single TOS(TOS0) routes
Supports opaque LSA
SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
Minimum LSA interval 5 secs. Minimum LSA arrival 1 secs
Number of external LSA 0. Checksum Sum 0x000000
Number of opaque AS LSA 0. Checksum Sum 0x000000
Number of DCbitless external and opaque AS LSA 0
Number of DoNotAge external and opaque AS LSA 0
Number of areas in this router is 1. 1 normal 0 stub 0 nssa
```


- Routing Networks, and passive interfaces configuradas en cada router.

```

R1
Physical Config CLI
IOS Command Line Interface

show ip protocols
Number of LSA 2, Checksum Sum 0x017afb
Number of opaque link LSA 0, Checksum Sum 0x000000
Number of DCbitless LSA 0
Number of indication LSA 0
Number of DoNotAge LSA 0
Flood list length 0

R1#
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 0.0.0.0 area 0
    172.31.23.0 0.0.0.0 area 0
    192.168.4.0 0.0.0.255 area 0
  Passive Interface(s):
    GigabitEthernet0/0
  Routing Information Sources:
    Gateway         Distance      Last Update
    1.1.1.1           110           00:26:29
    2.2.2.2           110           00:26:29
  Distance: (default is 110)
  
```

R2

Physical Config CLI

IOS Command Line Interface

```
R2#
R2#show ip route ospf
R2#show ip ospf protocols
      ^
% Invalid input detected at '^' marker.

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:
    172.168.21.0 0.0.0.3 area 0
    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
    10.10.8.0 0.0.3.255 area 0
    192.168.4.0 0.0.3.255 area 0
    10.10.10.8 0.0.0.3 area 0
  Passive Interface(s):
    GigabitEthernet0/1
  Routing Information Sources:
    Gateway         Distance      Last Update
    2.2.2.2          110          00:25:20
  Distance: (default is 110)
```

R1

Physical Config CLI

IOS Command Line Interface

```

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
Suppress hello for 0 neighbor(s)
R1#
R1#show ip route ospf
R1#
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
    172.31.23.0 0.0.0.3 area 0
    192.168.4.0 0.0.3.255 area 0
  Passive Interface(s):
    GigabitEthernet0/0
  Routing Information Sources:
    Gateway         Distance      Last Update
    1.1.1.1          110          00:00:23
  Distance: (default is 110)
  
```

```

% Invalid input detected at '^' marker.
R1(config-router)#end
R1#
%SYS-5-CHSR1_1: Configured from console by console
R1#show ip ospf interface
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 5.5.5.5
  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
    172.31.21.0 0.0.0.3 area 0
    192.168.4.0 0.0.3.255 area 0
    10.10.10.0 0.0.0.3 area 0
  Passive Interface(s):
    GigabitEthernet0/0
  Routing Information Sources:
    Gateway         Distance      Last Update
    5.5.5.5          110          00:10:21
  Distance: (default is 110)
  
```

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

Parte 4: En el Switch 3 deshabilitar DNS lookup

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

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

Parte 7: Implemente DHCP and NAT para IPv4

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

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

```
R1>ena
R1#config t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#ip dhcp exc
R1(config)#ip dhcp excluded-address 192.168.30.1 192.168.31.30
R1(config)#ip dhcp excluded-address 192.168.40.1 192.168.31.30
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)#defa
R1(dhcp-config)#default-router 192.168.30.1
R1(dhcp-config)#network 192.168.30.0 255.255.255.0
R1(dhcp-config)#ip dhcp pool administracion
R1(dhcp-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.

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

```
R2#config t
```

```
Enter configuration commands, one per line. End with CNTL/Z.
```

```
R2(config)#acce
```

```
R2(config)#access-list 1 permit 192.168.30.0 0.0.0.255
```

```
R2(config)#access-list 1 permit 192.168.40.0 0.0.0.255
```

```
R2(config)#access-list 1 permit 192.168.4.0 0.0.3.255
```

```
R2(config)#ip nat pool INTERNET 209.165.200.256 209.165.200.228  
netmask
```

```
^
```

```
% Invalid input detected at '^' marker.
```

```
R2(config)#ip nat pool INTERNET 209.165.200.256 209.165.200.228  
netmask 255.255.255.248
```

```
^
```

```
% Invalid input detected at '^' marker.
```

```
R2(config)#ip nat pool INTERNET 209.165.200.256 209.165.200.228  
netmask R2(config)#ip nat pool INTERNET 209.165.200.256
```

```
209.165.200.228 netmask R2(config)#ip nat pool INTERNET
```

```
209.165.200.256 209.165.200.228 netmask R2(config)#ip nat pool
```

```
INTERNET 209.165.200.256 209.165.200.228 netmask R2(config)#ip nat
```

```
pool INTERNET 209.165.200.225 209.165.200.228 netmask
```

```
255.255.255.248
```

```
R2(config)#
```

Parte 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#sho run
```

```
Building configuration...
```

```
Current configuration : 1838 bytes
```

```
version 15.1
```

```
no service timestamps log datetime msec
```

```
no service timestamps debug datetime msec
```

```
no service password-encryption
```

```
hostname R2
```

```
no ip cef
```

```
no ipv6 cef
```

```
username webuser privilege 15 secret 5
```

```
$1$mERr$WvpW0n5HghRrqnrxXCUUI.
```

```
license udi pid CISCO1941/K9 sn FTX1524BK5N
```

```
no ip domain-lookup
```

```
spanning-tree mode pvst
```

```
interface GigabitEthernet0/0
```

```
description connetion to ISP
```

```
ip address 209.165.200.230 255.255.255.252
```

```
ip nat outside
```

```
duplex auto
```

```
speed auto
```

```
interface GigabitEthernet0/1
```

```
description connection a web server
```

```
ip address 10.10.10.10 255.255.255.252
```

```
ip nat inside
```

```
duplex auto
```

```
speed auto
```

```
interface Serial0/0/0
```

```
description connection R3
```

```
bandwidth 128
```

```
ip address 172.31.23.1 255.255.255.252
```

```
ip ospf cost 7500
```

```
clock rate 128000
```

```
interface Serial0/0/1
```

```
bandwidth 128
```

```
ip address 172.31.21.1 255.255.255.252
```

```
clock rate 128000
```

```
interface Vlan1
```

```
no ip address
```

```
shutdown
```

```
router ospf 1
router-id 2.2.2.2
log-adjacency-changes
passive-interface GigabitEthernet0/1
network 172.168.21.0 0.0.0.3 area 0
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
network 10.10.8.0 0.0.3.255 area 0
network 192.168.4.0 0.0.3.255 area 0
network 10.10.10.8 0.0.0.3 area 0

router rip

ip nat pool INTERNET 209.165.200.225 209.165.200.228 netmask
255.255.255.248
ip nat inside source list 1 pool INTERNET
ip classless
ip route 0.0.0.0 0.0.0.0 GigabitEthernet0/0

ip flow-export version 9

access-list 1 permit 192.168.30.0 0.0.0.255
access-list 1 permit 192.168.40.0 0.0.0.255
access-list 1 permit 192.168.4.0 0.0.3.255
ip access-list standard ADMIN
```

permit host 172.31.21.1

banner motd ^C acceso prohibido^C

line con 0

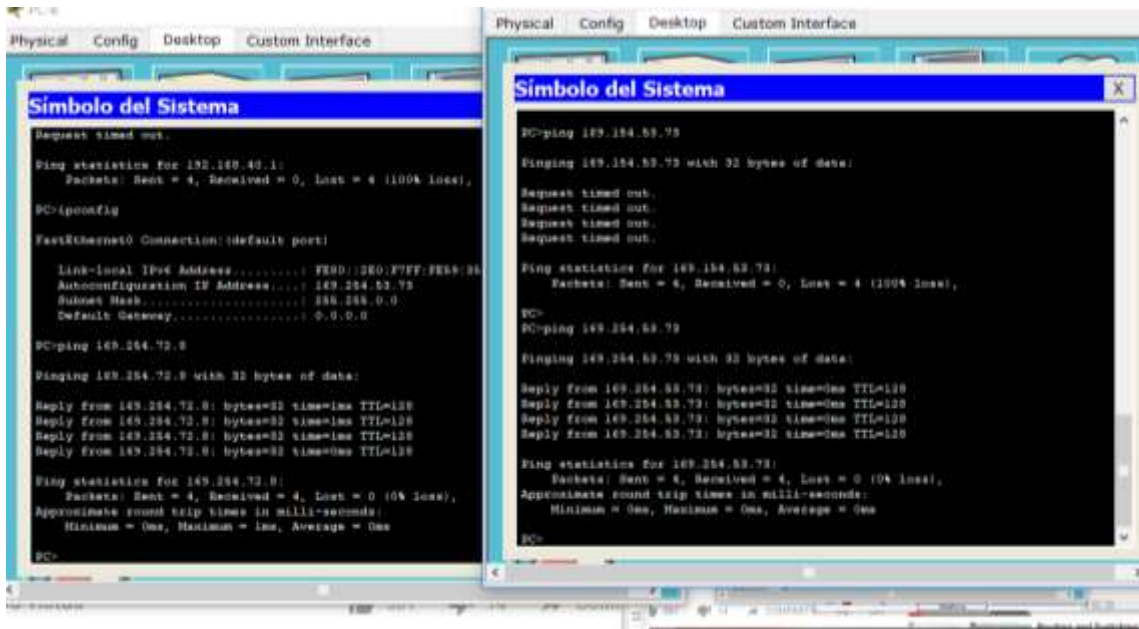
line aux 0

line vty 0 4

access-class ADMIN in

login

end



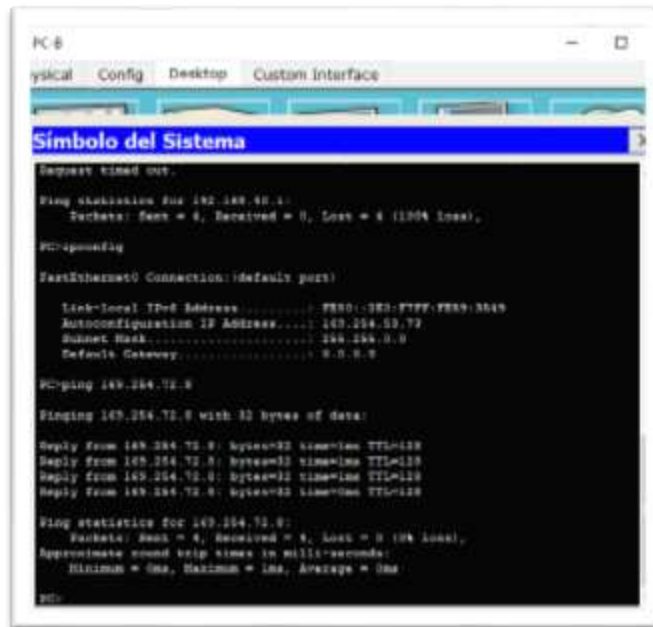
Parte 11: Configurar al menos dos listas de acceso de tipo extendido o nombradas a su criterio en para restringir o permitir tráfico desde R1 o R3 hacia R2.

```

R2#show access-
R2#show access-lists
Standard IP access list 1
10 permit 192.168.30.0 0.0.0.255
20 permit 192.168.40.0 0.0.0.255
30 permit 192.168.4.0 0.0.3.255
Standard IP access list ADMIN
10 permit host 172.31.21.1 (2 match(es))
R2#
  
```



Parte 13: Verificar procesos de comunicación y re direccionamiento de tráfico en los routers mediante el uso de Ping y Traceroute.

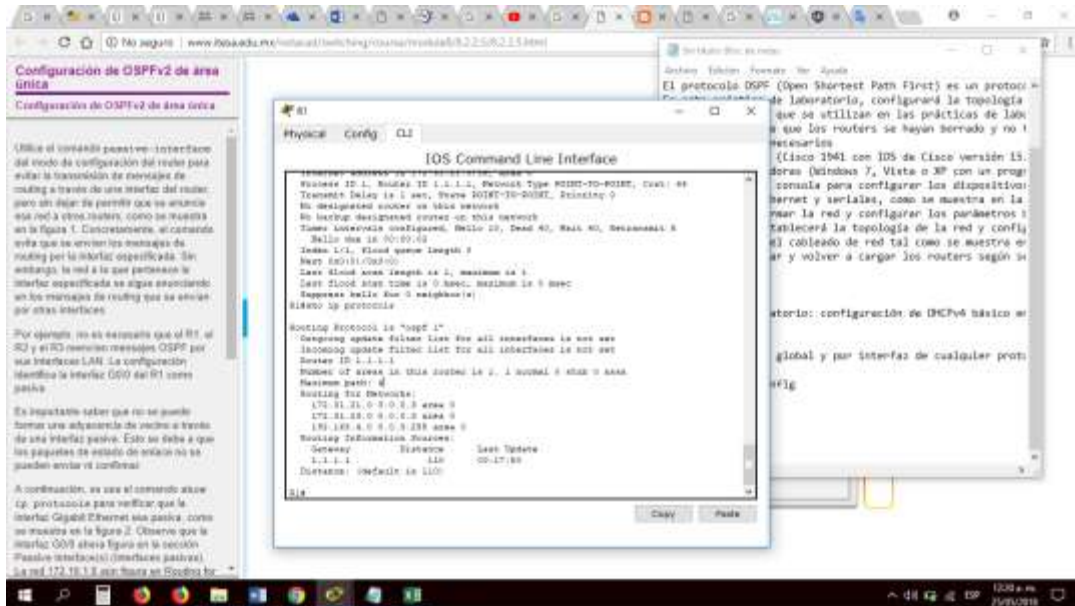


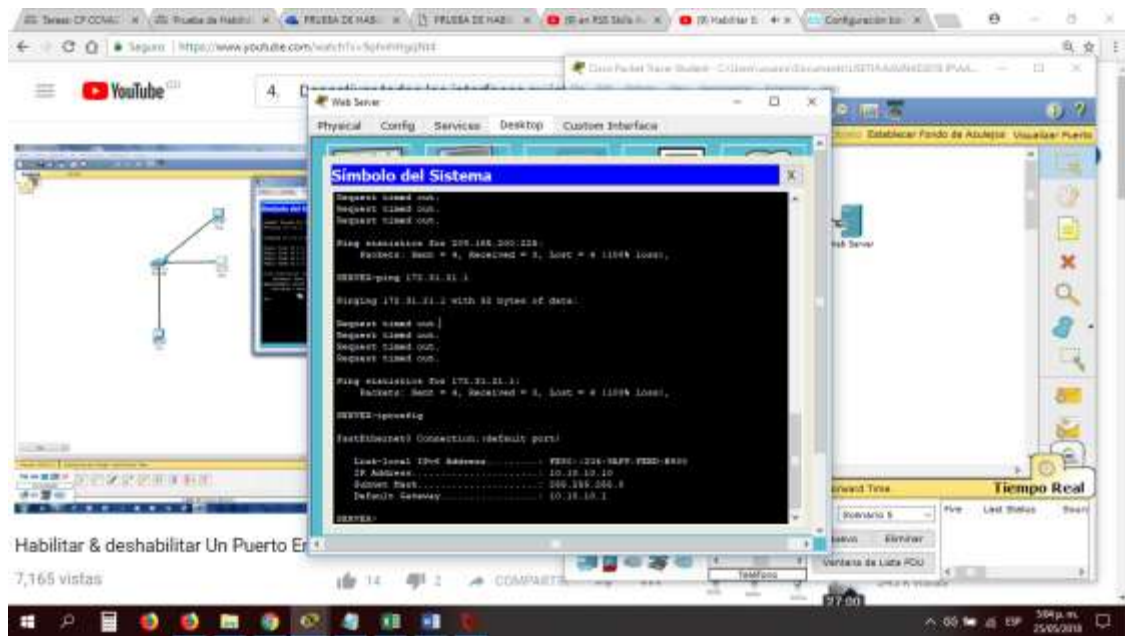
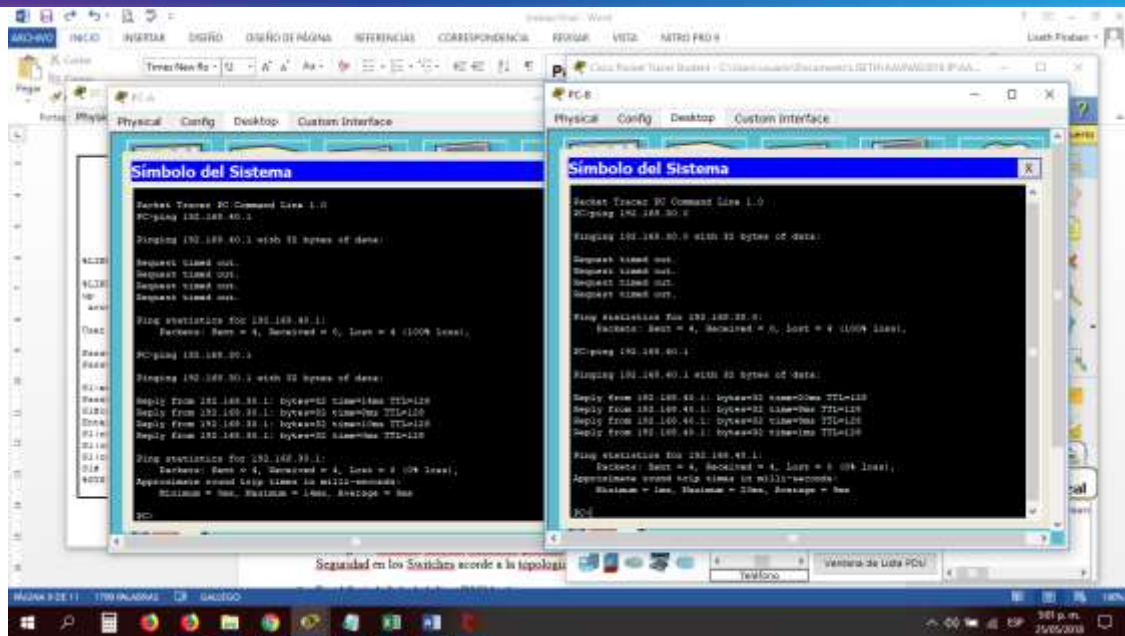
R1#telnet 172.31.21.1

Trying 172.31.21.1 ...Open

[Connection to 172.31.21.1 closed by foreign host]

R1#





CONCLUSIONES

Este curso fue dirigido por aquellos docentes que intervenían con el proceso de enseñanza.

Para un óptimo desempeño de la practica fue necesario prepararse, viendo vídeos y paginas sugeridas por la temática del curso.

Se diseñó una metodología para conceptualizar la topología para el modelo a desarrollar

Se encontró problemas en algunos problemas planteados para el escenario sugerido.

En algunas ocasiones algunos ejercicios se tornaban difíciles y otros con fácil ejecución; claro está que los errores hacen parte del conocimiento como aprendiz.

Se logra consolidar el desarrollo de la prueba de habilidades CCNA; donde amplié los conocimientos adquiridos durante el proceso de enseñanza.

BIBLIOGRAFIA

OSPF (Abrir la ruta más corta en primer lugar) Preguntas Frecuentes PDF [en línea],[revisado 1 de junio 2018].Disponible en internet:

https://www.cisco.com/c/es_mx/support/docs/ip/open-shortest-path-first-ospf/9237-9.pdf

Configuración de Listas de Acceso IP [en línea],[revisado 28 de mayo de 2018].Disponible en internet:

https://www.cisco.com/c/es_mx/support/docs/security/ios-firewall/23602-confaccesslists.html