



PORTADA

DIPLOMADO DE PROFUNDIZACIÓN CISCO

**ENTREGADO POR:
GERSON GUEVARA BOCANEGRA**

**PRESENTADO A:
GIOVANNI ALBERTO BRACHO**

**C.C. 93137847
GRUPO: 203092_32**

**UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD
ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERÍA
IBAGUE
2018**

TABLA DE CONTENIDO

PORTADA.....	1
Tabla de Contenido.....	2
Evaluación – Prueba de habilidades prácticas CCNA	3
Introducción	5
Descripción y desarrollo de los 2 escenarios propuestos para la prueba de habilidades:.....	6
Escenario 1	6
Escenario 2.....	12
Conclusiones	21
Referencias Bibliográficas	22

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, y busca identificar el grado de desarrollo de competencias y habilidades que fueron adquiridas a lo largo del diplomado. Lo esencial es poner 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 dos (2) 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 iproute, entre otros.

Teniendo en cuenta que la Prueba de habilidades está conformada por dos (2) escenarios, el estudiante deberá realizar el proceso de configuración de usando cualquiera de las siguientes herramientas: PacketTracer o GNS3.

Es muy importante mencionar que esta actividad es de carácter INDIVIDUAL y OBLIGATORIA.

Toda evidencia de copy-paste o plagio (de la web o de otros informes) será penalizada con severidad.

Lineamientos para la elaboración del Informe

Finalmente, el informe a presentar deberá cumplir con las normas ICONTEC 1486 para la presentación de trabajos escritos e incluir los siguientes elementos en su contenido:

Portada

Tabla de contenido

Introducción

Desarrollo de los dos escenarios

IMPORTANTE: Para cada uno de los escenarios se debe describir el paso a paso de cada punto realizado y deben digitar el código de configuración aplicado (no incluir imágenes ni capturas de pantalla). Las imágenes o capturas de pantalla sólo serán usadas para evidenciar los resultados de comandos como ping, traceroute, show iproute, entre otros.

Conclusiones

Referencias Bibliográficas

El informe deberá estar acompañado de las respectivas evidencias de configuración de los dispositivos (Packet Tracer ó GNS3), 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.

IMPORTANTE: Teniendo en cuenta que este documento deberá ser entregado al final del curso en el Repositorio Institucional, acorde con los lineamientos institucionales para grado. El procedimiento será socializado al finalizar el curso.

INTRODUCCIÓN

El presente documento constituye el trabajo final del diplomado de profundización en Cisco, como requisito exigido para la obtención del título profesional en ingeniería de sistemas de la Universidad Nacional Abierta y a Distancia (UNAD).

Cabe anotar que además de lo anterior, este trabajo pretende alcanzar como objetivo poner en práctica el conocimiento adquirido en el diplomado acerca de redes a nivel profesional, de tal forma que se garantice un adecuado manejo de la información y, la oportunidad en la entrega de la misma, para que los usuarios alcancen su plena satisfacción pudiendo así con base en ésta tomar decisiones acerca de los diferentes temas allí contenidos, buscando la optimización de los recursos con fundamento en ella.

De otra parte es conveniente aclarar que Cisco cuenta con diferentes tecnologías, en este caso haciendo énfasis en redes.

DESCRIPCIÓN Y DESARROLLO DE LOS 2 ESCENARIOS PROPUESTOS PARA LA PRUEBA DE HABILIDADES:

ESCENARIO 1

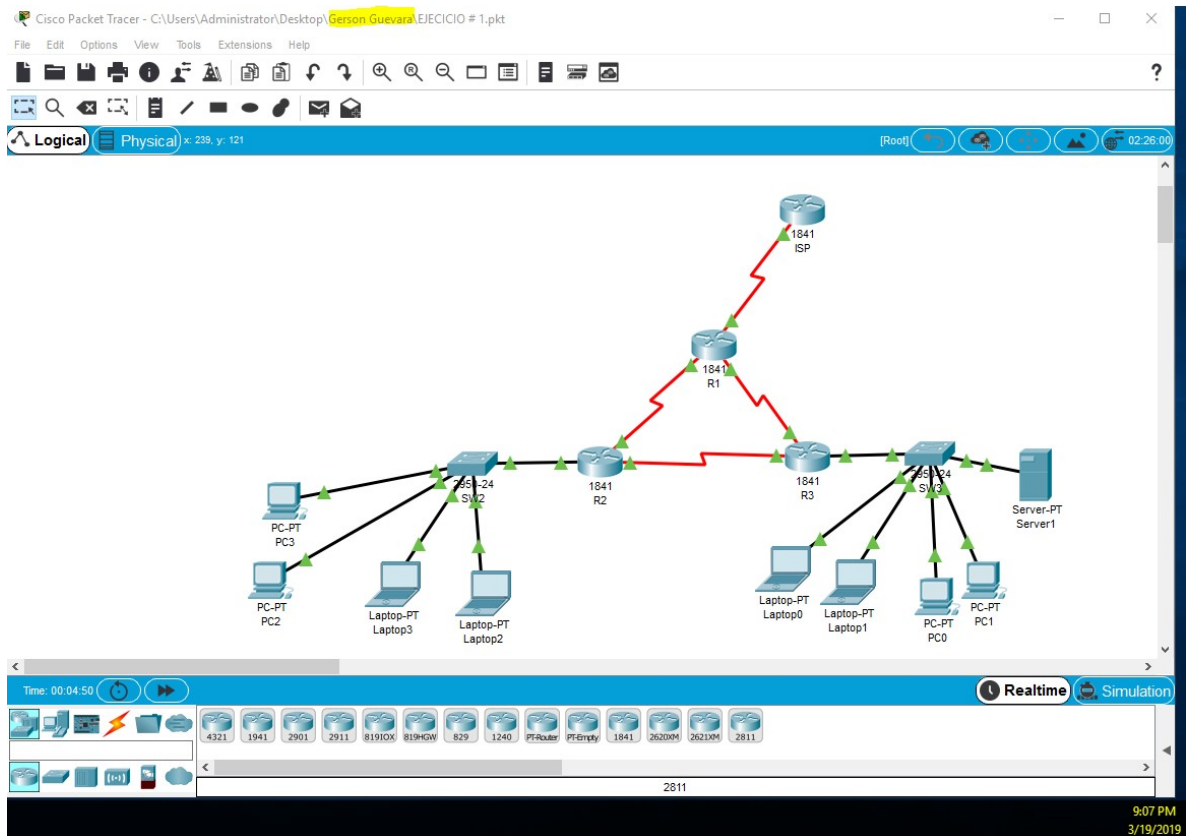


Tabla de direccionamiento:

El administrador	Interfases	Dirección IP	Máscara de subred	Gateway predeterminado
ISP	S0/0/0	200.123.211.1	255.255.255.0	N/D
	Se0/0/0	200.123.211.2	255.255.255.	N/D

R1			0	
	Se0/1/0	10.0.0.1	255.255.255. 252	N/D
	Se0/1/1	10.0.0.5	255.255.255. 252	N/D
R2	Fa0/0,1 00	192.168.20.1	255.255.255. 0	N/D
	Fa0/0,2 00	192.168.21.1	255.255.255. 0	N/D
	Se0/0/0	10.0.0.2	255.255.255. 252	N/D
	Se0/0/1	10.0.0.9	255.255.255. 252	N/D
R3	Fa0/0	192.168.30.1	255.255.255. 0	N/D
		2001:db8:130::9C0:8 0F:301	/64	N/D
	Se0/0/0	10.0.0.6	255.255.255. 252	N/D
	Se0/0/1	10.0.0.10	255.255.255. 252	N/D
SW2	VLAN 100	N/D	N/D	N/D
	VLAN 200	N/D	N/D	N/D
SW3	VLAN1	N/D	N/D	N/D

PC20	NIC	DHCP	DHCP	DHCP
PC21	NIC	DHCP	DHCP	DHCP

PC30	NIC	DHCP	DHCP	DHCP
PC31	NIC	DHCP	DHCP	DHCP
Laptop20	NIC	DHCP	DHCP	DHCP
Laptop21	NIC	DHCP	DHCP	DHCP
Laptop30	NIC	DHCP	DHCP	DHCP
Laptop31	NIC	DHCP	DHCP	DHCP

Tabla de asignación de VLAN y de puertos:

Dispositivo	VLAN	Nombre	Interfaz
SW2	100	LAPTOPS	Fa0/2-3
SW2	200	DESTOPS	Fa0/4-5
SW3	1	-	Todas las interfaces

Tabla de enlaces troncales:

Dispositivo local	Interfaz local	Dispositivo remoto
SW2	Fa0/2-3	100

Situación

En esta actividad, demostrará y reforzará su capacidad para implementar NAT, servidor de DHCP, RIPV2 y el routing entre VLAN, incluida la configuración de direcciones IP, las VLAN, los enlaces troncales y las subinterfaces. Todas las pruebas de alcance deben realizarse a través de ping únicamente.

Descripción de las actividades

- **SW1** VLAN y las asignaciones de puertos de VLAN deben cumplir con la tabla1.

```
Switch>en
Switch#conf ter
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname SW2
SW2(config)#vlan 100
SW2(config-vlan)#name LAPTOPS
SW2(config-vlan)#vlan 200
SW2(config-vlan)#name DESKTOPS
SW2(config-vlan)#exit
SW2(config)#int ra fa 0/2-3
SW2(config-if-range)#sw acc vlan 100
SW2(config-if-range)#int ra fa 0/4-5
SW2(config-if-range)#se acc vlan 200
^
% Invalid input detected at '^' marker.

SW2(config-if-range)#sw acc vlan 200
```

- Los puertos de red que no se utilizan se deben deshabilitar.

```
SW2(config)#int ra fa 0/6-24
SW2(config-if-range)#shu

Switch(config)#int ra fa 0/7-24
Switch(config-if-range)#shu
Switch(config-if-range)#shutdown
```

- **R1** debe realizar una NAT con sobre carga sobre una dirección IPv4 pública. Asegúrese de que todos los terminales pueden comunicarse con Internet pública (haga ping a la dirección ISP) y la lista de acceso estándar se llama **INSIDE-DEVS**.

```
R1(config)#int se 0/0/0
R1(config-if)#ip nat outside
R1(config-if)#int se 0/1/1
R1(config-if)#ip nat inside
R1(config-if)#int se 0/1/0
R1(config-if)#ip nat inside
R1(config-if)#exit
R1(config)#ip access-list extended INSIDE-DEVS
R1(config-ext-nacl)#permit ip 0.0.0.0 255.255.255.255 any
R1(config-ext-nacl)#exit
R1(config)#ip nat inside source list INSIDE-DEVS interface serial
0/0/0 overload
R1(config)#
```

- **R1** debe tener una ruta estática predeterminada al ISP que se configuró y que incluye esa ruta en **el dominioRIPv2**.

```
-----
R1(config)#ip route 0.0.0.0 0.0.0.0 200.123.211.1
R1(config)#router rip
R1(config-router)#version 2
R1(config-router)#network 10.0.0.0
R1(config-router)#redistribute static
R1(config-router)#exit
R1(config)#
```

- **R2** es un servidor de DHCP para los dispositivos conectados al puerto FastEthernet0/0.

```
R2(config)#ip dhcp excluded-address 192.168.20.1
R2(config)#ip dhcp excluded-address 192.168.21.1
R2(config)#
R2(config)#ip dhcp pool VLAN100
R2(dhcp-config)#network 192.168.20.0 255.255.255.0
R2(dhcp-config)#default-router 192.168.20.1
R2(dhcp-config)#
R2(dhcp-config)#ip dhcp pool VLAN200
R2(dhcp-config)#network 192.168.20.0 255.255.255.0
R2(dhcp-config)#default-router 192.168.20.1
```

- **R2** debe, además de enrutamiento a otras partes de la red, ruta entre las VLAN 100 y200.
- El Servidor0 es sólo un servidor IPv6 y sólo debe ser accesible para los dispositivos en R3 (ping).
- La NIC instalado en direcciones IPv4 e IPv6 de Laptop30, de Laptop31, de PC30 y obligación de configurados PC31 simultáneas (dual-stack). Las direcciones se deben configurar mediante DHCP y DHCPv6.
- La interfaz FastEthernet 0/0 del R3 también deben tener direcciones IPv4 e IPv6 configuradas (dual- stack).

```
R3(config)#ip dhcp excluded-address 192.168.30.1
R3(config)#!
R3(config)#ip dhcp pool R3
R3(dhcp-config)# network 192.168.30.0 255.255.255.0
R3(dhcp-config)# default-router 192.168.30.1
```

<input checked="" type="radio"/> DHCP <input type="radio"/> Static	
IP Address	192.168.30.2
Subnet Mask	255.255.255.0
Default Gateway	192.168.30.1
DNS Server	0.0.0.0
IPv6 Configuration	
<input type="radio"/> DHCP <input checked="" type="radio"/> Auto Config <input type="radio"/> Static	
IPv6 Address	2001:DB8:130:0:201:42FF:FEC5:EAC5 / 64
Link Local Address	FE80::201:42FF:FEC5:EAC5
IPv6 Gateway	FE80::20B:BEFF:FEDA:3101
IPv6 DNS Server	

- R1, R2 y R3 intercambian información de routing mediante RIP versión 2.

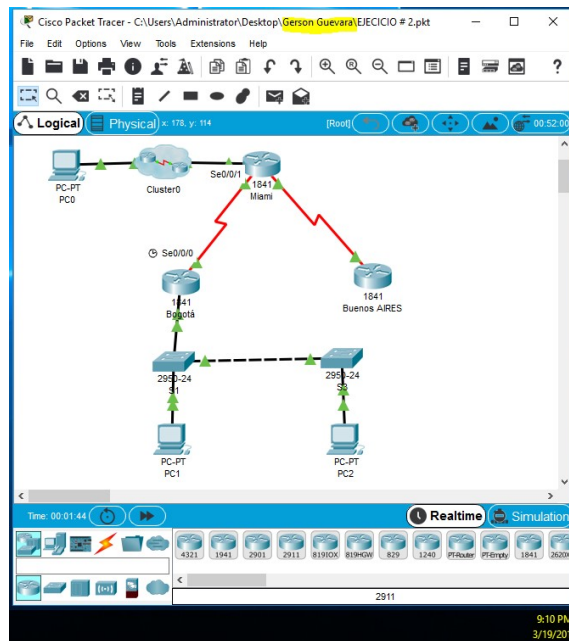
```
R1(config)#router rip
R1(config-router)# version 2
R1(config-router)# network 10.0.0.0
R1(config-router)#exit
R1(config)#
```

```
R2(config)#router rip
R2(config-router)# version 2
R2(config-router)# network 10.0.0.0
R2(config-router)# network 192.168.20.0
R2(config-router)# network 192.168.21.0
```

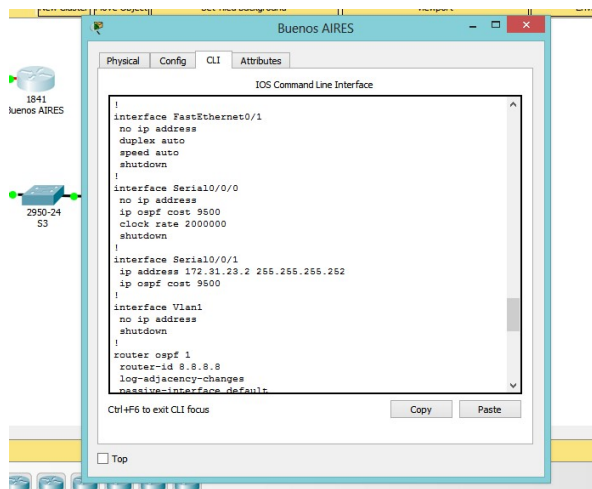
```
R3(config)#router rip
R3(config-router)# version 2
R3(config-router)# network 10.0.0.0
R3(config-router)# network 192.168.30.0
```

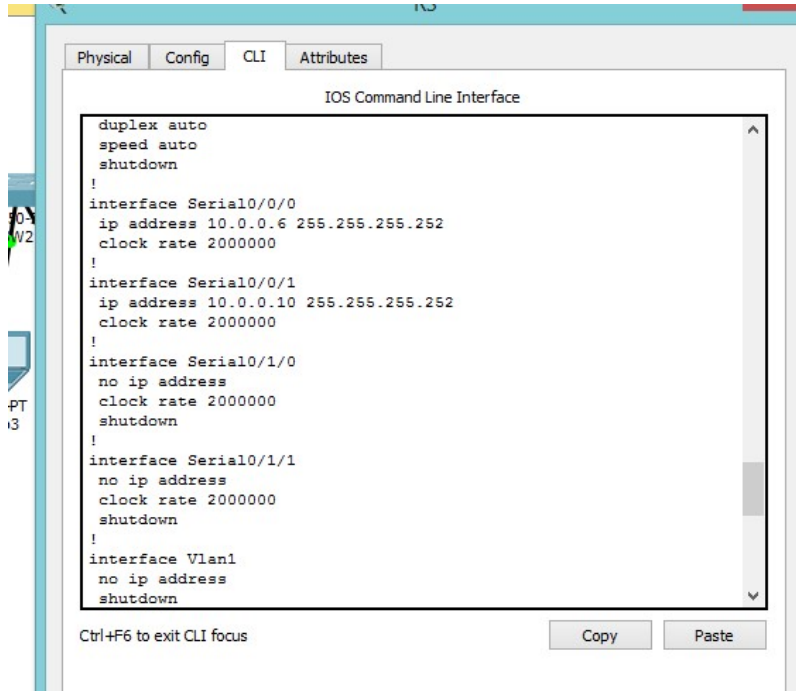
ESCENARIO 2

Escenario: Una empresa de Tecnología posee tres sucursales distribuidas en las ciudades de Miami, Bogotá y Buenos Aires, 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.



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





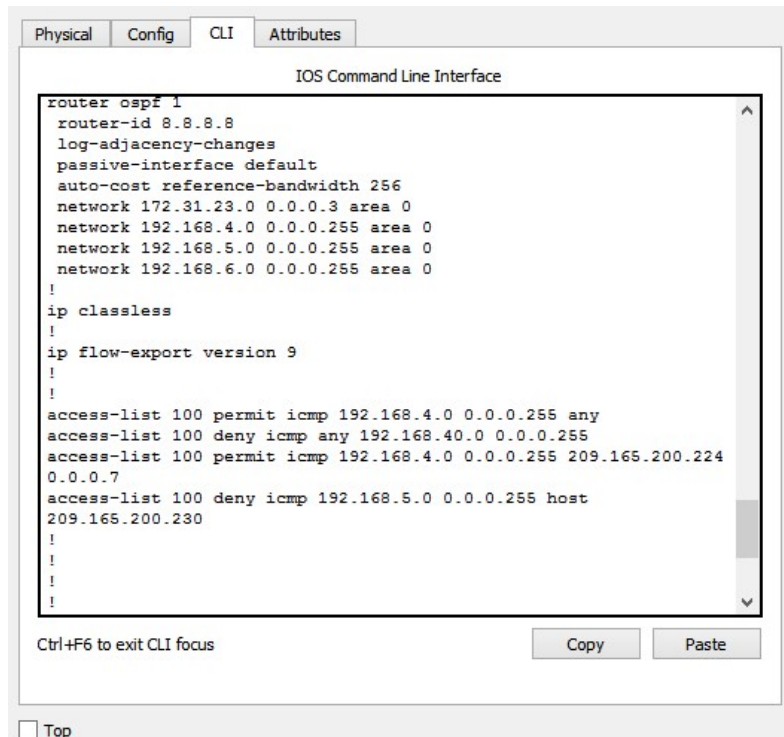
Physical Config CLI Attributes

IOS Command Line Interface

```
duplex auto
speed auto
shutdown
!
interface Serial0/0/0
ip address 10.0.0.6 255.255.255.252
clock rate 2000000
!
interface Serial0/0/1
ip address 10.0.0.10 255.255.255.252
clock rate 2000000
!
interface Serial0/1/0
no ip address
clock rate 2000000
shutdown
!
interface Serial0/1/1
no ip address
clock rate 2000000
shutdown
!
interface Vlan1
no ip address
shutdown
```

Ctrl+F6 to exit CLI focus

Copy Paste



Physical Config CLI Attributes

IOS Command Line Interface

```
router ospf 1
router-id 8.8.8.8
log-adjacency-changes
passive-interface default
auto-cost reference-bandwidth 256
network 172.31.23.0 0.0.0.3 area 0
network 192.168.4.0 0.0.0.255 area 0
network 192.168.5.0 0.0.0.255 area 0
network 192.168.6.0 0.0.0.255 area 0
!
ip classless
!
ip flow-export version 9
!
!
access-list 100 permit icmp 192.168.4.0 0.0.0.255 any
access-list 100 deny icmp any 192.168.4.0 0.0.0.255
access-list 100 permit icmp 192.168.4.0 0.0.0.255 209.165.200.224
0.0.0.7
access-list 100 deny icmp 192.168.5.0 0.0.0.255 host
209.165.200.230
!
!
!
```

Ctrl+F6 to exit CLI focus

Copy Paste

Top

```
R3(config)#hostname R3
R3(config)#interface Loopback4
R3(config-if)# ip address 192.168.4.1 255.255.255.0
R3(config-if)#interface Loopback5
R3(config-if)# ip address 192.168.5.1 255.255.255.0
R3(config-if)#interface Loopback6
R3(config-if)# ip address 192.168.6.1 255.255.255.0
R3(config-if)#interface Serial0/0/1
R3(config-if)# ip address 172.31.23.2 255.255.255.252
R3(config-if)#exit

S1(config)#int fa 0/24
S1(config-if)#sw mo tr
S1(config-if)#int fa 0/3
S1(config-if)#sw mo tr
S1(config-if)#int vlan 99
S1(config-if)# ip address 192.168.99.2 255.255.255.
S1(config-if)#vlan 30
S1(config-vlan)#name Administracion
S1(config-vlan)#vlan 40
S1(config-vlan)#name Mercadeo
S1(config-vlan)#vlan 200
S1(config-vlan)#name Mantenimiento
S1(config-vlan)#
S1(config-vlan)#exit
S1(config)#int fa 0/1
S1(config-if)#sw acc vlan 30
```

Physical Config CLI Attributes

IOS Command Line Interface

```
!  
!  
!  
no ip domain-lookup  
ip domain-name ccna-unad.com  
!  
!  
spanning-tree mode pvst  
spanning-tree extend system-id  
!  
interface FastEthernet0/1  
  switchport access vlan 40  
!  
interface FastEthernet0/2  
  shutdown  
!  
interface FastEthernet0/3  
  switchport mode trunk  
!  
interface FastEthernet0/4  
  shutdown  
!  
interface FastEthernet0/5  
  shutdown  
!
```

Ctrl+F6 to exit CLI focus

Copy Paste

Top

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

OSPFv2 area 0

Configuration Item or Task	Specification
Router ID R1	1.1.1.1
Router ID R2	5.5.5.5
Router ID R3	8.8.8.8
Configurar todas las interfaces LAN como pasivas	
Establecer el ancho de banda para enlaces seriales en	256 Kb/s
Ajustar el costo en la métrica de S0/0 a	9500

- Verificar información de OSPF

Visualizar tablas de enrutamiento y routers conectados por OSPFv2

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

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

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

- En el Switch 3 deshabilitar DNS lookup

```

S3(config)#no ip domain-lookup
S3(config)#

```

Asignar direcciones IP a los Switches acorde a los lineamientos.

```

S1(config-if)#int vlan 99
S1(config-if)# ip address 192.168.99.2 255.255.255.0

S3(config-if)#int vlan 99
S3(config-if)#ip address 192.168.99.3 255.255.255.0

```

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

```

S3(config)#int fa 0/2
S3(config-if)#sh
S3(config-if)#int ra fa 0/4-23
...

S1(config)#int fa 0/2
S1(config-if)#sh
S1(config-if)#int ra fa 0/4-23
S1(config-if-range)#sh

```

Implementar DHCP y NAT con IPv4

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

```
R1(config)#ip dhcp excluded-address 192.168.30.1
R1(config)#ip dhcp excluded-address 192.168.40.1
R1(config)#ip dhcp pool ADMINISTRACION
R1(dhcp-config)# network 192.168.30.0 255.255.255.0
R1(dhcp-config)# default-router 192.168.30.1
R1(dhcp-config)# dns-server 10.10.10.11
R1(dhcp-config)#ip dhcp pool MERCADEO
R1(dhcp-config)# network 192.168.40.0 255.255.255.0
R1(dhcp-config)# default-router 192.168.40.1
R1(dhcp-config)# dns-server 10.10.10.11
R1(dhcp-config)#ip domain-name ccna-unad.com
```

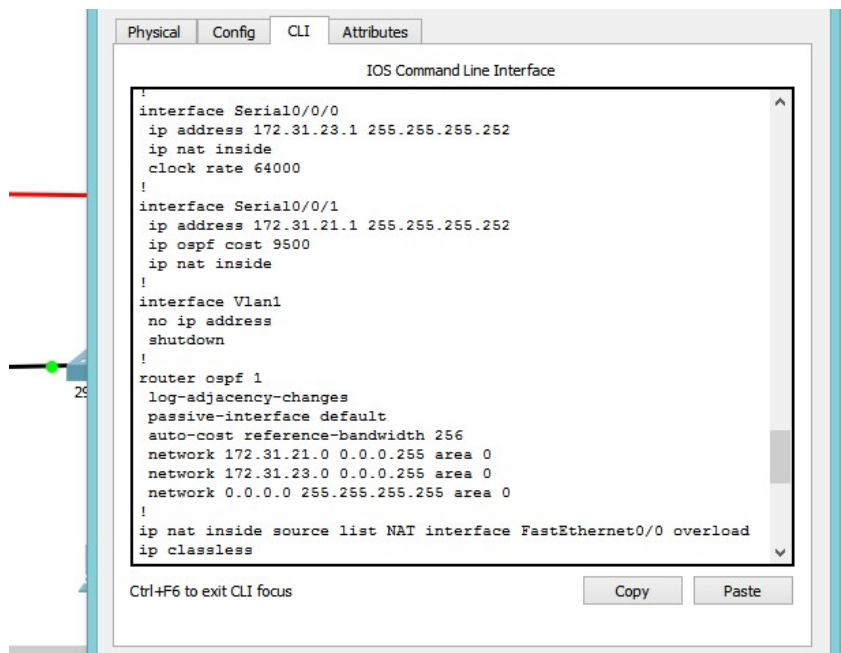
- Reservar las primeras 30 direcciones IP de las VLAN 30 y 40 para configuraciones estáticas.

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

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

```
R2(config)#interface FastEthernet0/0
R2(config-if)# ip nat outside
R2(config-if)#interface Serial0/0/0
R2(config-if)# ip nat inside
R2(config-if)#interface Serial0/0/1
R2(config-if)# ip nat inside
R2(config-if)#ip access-list extended NAT
R2(config-ext-nacl)# permit ip host 0.0.0.0 any
R2(config-ext-nacl)#ip nat inside source list NAT interface
FastEthernet0/0 overload
```

- 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.



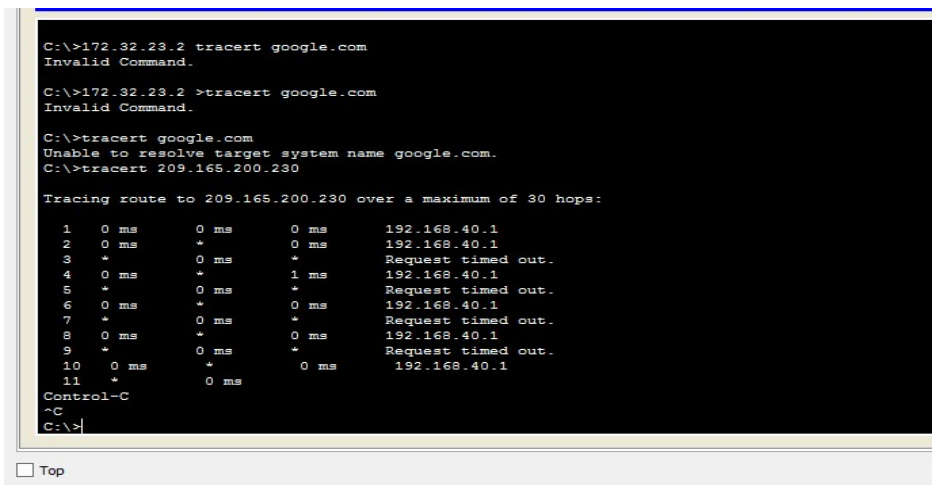
```
!
interface Serial0/0/0
 ip address 172.31.23.1 255.255.255.252
 ip nat inside
 clock rate 64000
!
interface Serial0/0/1
 ip address 172.31.21.1 255.255.255.252
 ip ospf cost 9500
 ip nat inside
!
interface Vlan1
 no ip address
 shutdown
!
router ospf 1
 log-adjacency-changes
 passive-interface default
 auto-cost reference-bandwidth 256
 network 172.31.21.0 0.0.0.255 area 0
 network 172.31.23.0 0.0.0.255 area 0
 network 0.0.0.0 255.255.255.255 area 0
!
ip nat inside source list NAT interface FastEthernet0/0 overload
ip classless
```

```
R3(config)#access-list 100 permit icmp 192.168.4.0 0.0.0.255 209.165.200.224 0.0.0.7
R3(config)#access-list 100 deny icmp 192.168.5.0 0.0.0.255 host 209.165.200.230
```

- 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 1 deny 192.168.6.0 0.0.0.255
R2(config)#access-list 1 permit host 192.168.40.2
```

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



```
C:\>172.32.23.2 tracert google.com
Invalid Command.

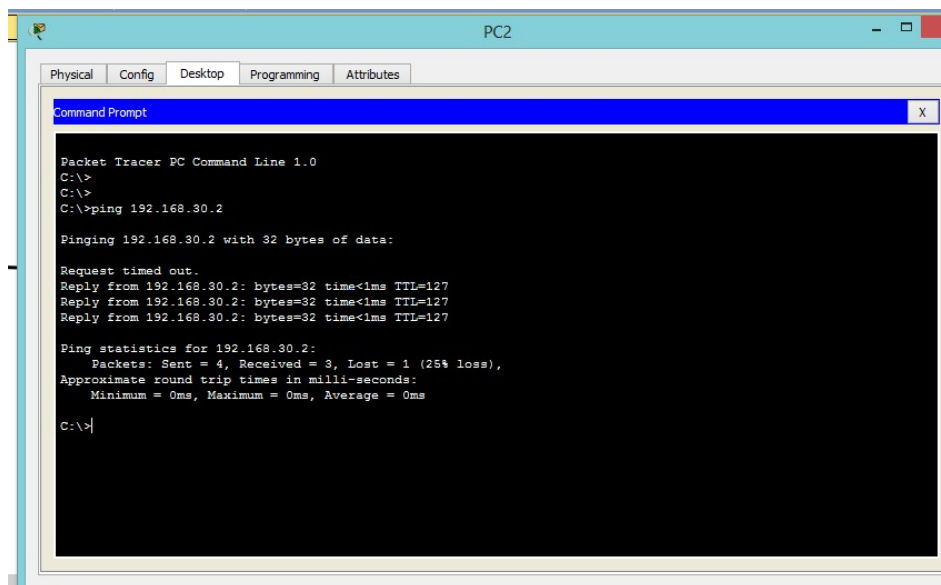
C:\>172.32.23.2 >tracert google.com
Invalid Command.

C:\>tracert google.com
Unable to resolve target system name google.com.
C:\>tracert 209.165.200.230

Tracing route to 209.165.200.230 over a maximum of 30 hops:

  0  0 ms  0 ms  0 ms  192.168.40.1
  1  0 ms  *    0 ms  192.168.40.1
  2  *    0 ms  *    Request timed out.
  3  0 ms  *    1 ms  192.168.40.1
  4  *    0 ms  *    Request timed out.
  5  0 ms  *    0 ms  192.168.40.1
  6  *    0 ms  *    Request timed out.
  7  0 ms  *    0 ms  192.168.40.1
  8  *    0 ms  *    Request timed out.
  9  0 ms  *    0 ms  192.168.40.1
 10 *    *    0 ms  192.168.40.1
 11 *    *    *    Request timed out.

Control-C
^C
C:\>
```



```
PC2
Physical Config Desktop Programming Attributes
Command Prompt
Packet Tracer PC Command Line 1.0
C:\>
C:\>
C:\>ping 192.168.30.2

Pinging 192.168.30.2 with 32 bytes of data:

Request timed out.
Reply from 192.168.30.2: bytes=32 time<1ms TTL=127
Reply from 192.168.30.2: bytes=32 time<1ms TTL=127
Reply from 192.168.30.2: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.30.2:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

CONCLUSIONES

A título de conclusiones podemos enumerar:

- El diplomado fundamentó los conocimientos en redes de acuerdo con la tecnología Cisco.
- La tecnología Cisco es considerada en el mundo de los sistemas como una de las más avanzadas y es reconocida a nivel mundial como una de las mejores y más seguras.
- Su ámbito de aplicación es supremamente amplio ya que puede ser utilizada en cualquier tipo de empresa o negocio ya sea industrial, bancario, servicios, etc.

REFERENCIAS BIBLIOGRÁFICAS

- Referencias de Comando, Cisco
https://www.cisco.com/c/es_mx/support/ios-nx-os-software/ios-15-2s/products-command-reference-list.html