

EVALUACIÓN – PRUEBA DE HABILIDADES PRÁCTICAS CCNA  
DIPLOMADO DE PROFUNDIZACIÓN CISCO

HAIR ORLANDO GONZALEZ VEGA

UNAD – UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA  
ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERÍA  
INGENIERÍA DE TELECOMUNICACIONES

BOGOTÁ D.C

2018



EVALUACIÓN – PRUEBA DE HABILIDADES PRÁCTICAS CCNA  
DIPLOMADO DE PROFUNDIZACIÓN CISCO

HAIR ORLANDO GONZALEZ VEGA

(Diseño e implementación de  
soluciones integradas LAN/WAN)

Juan Carlos Vesga

UNAD – UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA  
ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERÍA  
INGENIERÍA DE TELECOMUNICACIONES

BOGOTÁ D.C

2018

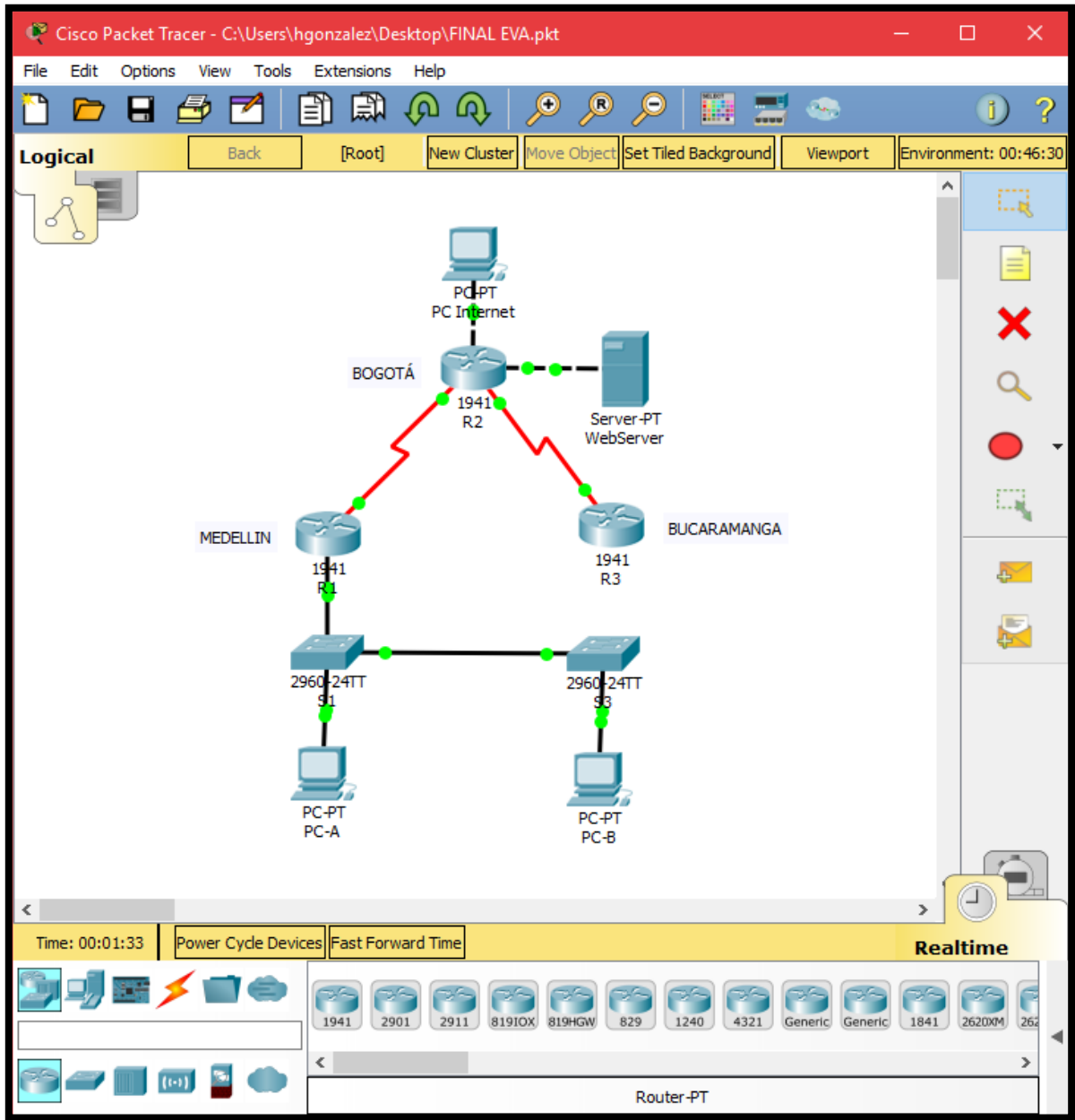
## Contenido

<b>Introducción</b> .....	3
<b>Diseño Topología</b> .....	4
<b>1. Configurar el direccionamiento IP acorde con la topología de red para cada uno de los dispositivos que forman parte del escenario.</b> .....	5
<b>2. Configurar el protocolo de enrutamiento OSPFv2 bajo los siguientes criterios:</b> .....	7
<b>3. Verificar información de OSPF</b> .....	10
<b>4. Configurar VLANs, Puertos troncales, puertos de acceso, encapsulamiento, InterVLAN Routing y Seguridad en los Switches acorde a la topología de red establecida.</b> .....	11
<b>5. En el Switch 3 deshabilitar DNS lookup</b> .....	14
<b>6. Asignar direcciones IP a los Switches acorde a los lineamientos.</b> .....	14
<b>7. Desactivar todas las interfaces que no sean utilizadas en el esquema de red.</b> .....	15
<b>8. Implement DHCP and NAT for IPv4.</b> .....	16
<b>9. Configurar NAT en R2 para permitir que los hosts puedan salir a internet</b> .....	16
<b>10. 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.</b> .....	18
<b>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.</b> .....	19
<b>12. Verificar procesos de comunicación y redireccionamiento de tráfico en los routers mediante el uso de Ping y Traceroute.</b> .....	21

## Introducción

Describe la arquitectura, los componentes y el funcionamiento de los routers, explica los principios de enrutamiento incluyendo a los mismos protocolos de enrutamiento dinámicos y estáticos. Se analizan, configuran, verifican y solucionan los problemas de los protocolos de enrutamiento principales: RIPv1, RIPv2, EIGRP y OSPF. Al finalizar el curso, los estudiantes podrán reconocer, corregir fallas y problemas de enrutamiento comunes. El objetivo es adquirir las competencias necesarias para mejorar el acceso a los equipos y aprender a configurar básicamente los aspectos físicos (hardware) y lógicos (software) de una Red, con laboratorio de procedimientos básicos, configuración, implementación y resolución de problemas.

# Diseño Topología



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

## Configuración Routers

Se configuran las interfaces con el direccionamiento realizado anteriormente.

### R1

```
interface GigabitEthernet0/0
 ip address 192.168.99.1 255.255.255.248
 duplex auto
 speed auto
!
interface GigabitEthernet0/1
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface Serial0/0/0
 ip address 172.131.21.1 255.255.255.252
```

### R2

```
Serial0/0/0      Up    --    172.131.23.1/30
Serial0/0/1      Up    --    172.131.21.2/30
```

```
interface GigabitEthernet0/0
 ip address 209.165.200.225 255.255.255.248

interface GigabitEthernet0/1
 ip address 10.10.10.1 255.255.255.0
```

## R3

Para este Router es necesario configurar 3 interfaces de loopback para simular redes LAN.

```
Serial0/0/1          Up          --          172.131.23.2/30
```

```
R3(config)#int lo4|
```

```
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
```

```
R3(config-if)#ip address 192.168.4.1 255.255.255.0
```

```
R3(config-if)#no sh
```

```
R3(config-if)#int lo5
```

```
R3(config-if)#
```

```
%LINK-5-CHANGED: Interface Loopback5, changed state to up
```

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

```
ip address 192.168.5.1 255.255.255.0
```

```
R3(config-if)#int lo6
```

```
R3(config-if)#
```

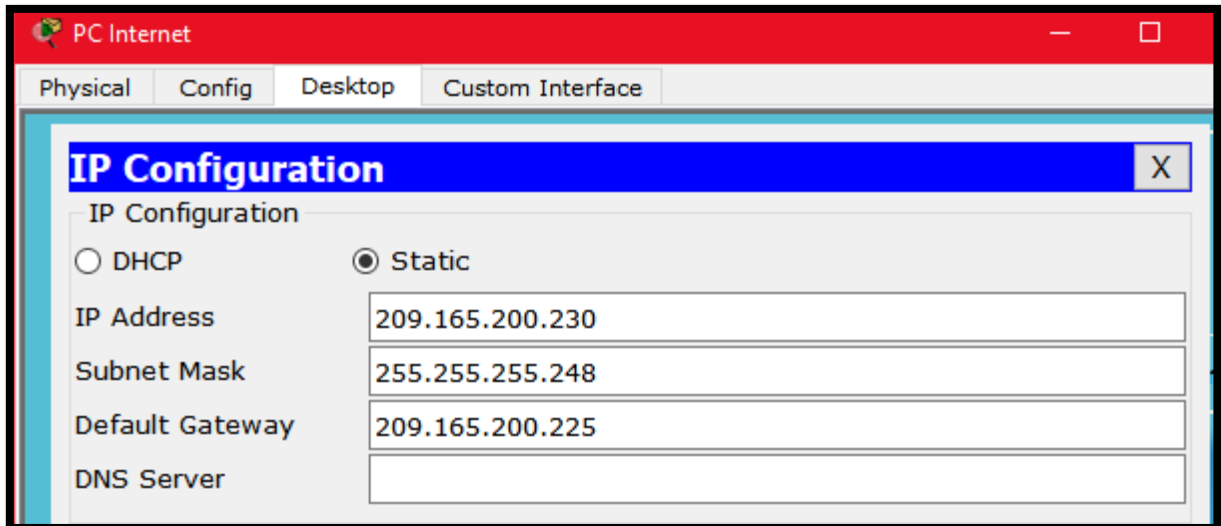
```
%LINK-5-CHANGED: Interface Loopback6, changed state to up
```

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

```
ip address 192.168.6.1 255.255.255.0
```

## PC Internet

Se le coloca a este PC una dirección IP estática.



2. 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	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

- En este paso configuramos el protocolo OSPF y agregamos todas las redes directamente conectadas a cada router. Además de configurar los demás parámetros indicados.

### R1

```
R1(config)#router ospf 1
R1(config-router)#router
R1(config-router)#router-id 1.1.1.1
```



```
R1(config-router)#network 192.168.30.0 0.0.0.255 area 0
R1(config-router)#network 192.168.40.0 0.0.0.255 area 0
R1(config-router)#network 192.168.200.0 0.0.0.255 area 0

network 172.31.21.0 0.0.0.3 area 0

R1(config-router)#passive-interface g0/0.30
R1(config-router)#passive-interface g0/0.40
R1(config-router)#passive-interface g0/0.200

R1(config)#interface Serial0/0/0
R1(config-if)#clock rate 128000
R1(config-if)#band
R1(config-if)#bandwidth ?
    <1-10000000> Bandwidth in kilobits
R1(config-if)#bandwidth 128
R1(config-if)#ip osp
R1(config-if)#ip ospf c
R1(config-if)#ip ospf cost 7500
```

## R2

```
router ospf 1
  router-id 2.2.2.2
  log-adjacency-changes
  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

Router(config)#int s0/0/0
Router(config-if)#band
Router(config-if)#bandwidth 128
Router(config-if)#IP OS
Router(config-if)#IP OSpf C
Router(config-if)#IP OSpf Cost 7500

R2(config)#int s0/0/1
R2(config-if)#bandwidth 128
R2(config-if)#IP OSpf Cost 7500
```

R3

```
R3(config)#router ospf
R3(config)#router ospf 1
R3(config-router)#rou
R3(config-router)#router-id 3.3.3.3

R3(config-router)#network 192.168.4.0 0.0.3.255 area 0
R3(config-router)#network 172.31.23.0 0.0.0.3 area 0

R3(config-router)#passive-interface lo4
R3(config-router)#passive-interface lo5
R3(config-router)#passive-interface lo6

R3(config-if)#bandwidth 128
R3(config-if)#ip ospf
R3(config-if)#ip ospf co
R3(config-if)#ip ospf cost 7500
```

### 3. Verificar información de OSPF

- Visualizar tablas de enrutamiento y routers conectados por OSPFv2

```

R1#sh ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

    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       172.31.21.1/32 is directly connected, Serial0/0/0
O       172.31.23.0/30 [110/15000] via 172.31.21.2, 00:08:51, Serial0/0/0
    192.168.99.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.99.0/29 is directly connected, GigabitEthernet0/0
L       192.168.99.1/32 is directly connected, GigabitEthernet0/0
R1#sh ip ospf neighbor

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

```

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

#### SHOW IP OSPF INTERFACE BRIEF

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

```

R1#sh 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):
    GigabitEthernet0/0.30
    GigabitEthernet0/0.40
    GigabitEthernet0/0.200
  Routing Information Sources:
    Gateway         Distance      Last Update
    2.2.2.2          110          00:10:20
    3.3.3.3          110          00:20:14
  Distance: (default is 110)

```

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

## S1

Se crean las vlans respectivas, y se ponen los puertos indicados en modo troncal y acceso en cada switch.

```
S-1(config)#do sh vlan
```

VLAN Name	Status	Ports
1 default	active	Fa0/2, Fa0/4, Fa0/5, Fa0/6 Fa0/7, Fa0/8, Fa0/9, Fa0/10 Fa0/11, Fa0/12, Fa0/13, Fa0/14 Fa0/15, Fa0/16, Fa0/17, Fa0/18 Fa0/19, Fa0/20, Fa0/21, Fa0/22 Fa0/23, Gig0/1, Gig0/2
30 Administracion	active	Fa0/1
40 Mercadeo	active	
200 Mantenimiento	active	

```

S-1(config)#int f0/3
S-1(config-if)#sw
S-1(config-if)#switchport mode trunk
S-1(config-if)#sw
S-1(config-if)#switchport tr
S-1(config-if)#switchport trunk nat
S-1(config-if)#switchport trunk native vlan 1

S-1(config-if)#int f0/24
S-1(config-if)#sw
S-1(config-if)#switchport mode tru
S-1(config-if)#switchport mode trunk
S-1(config-if)#sw
S-1(config-if)#switchport tr
S-1(config-if)#switchport trunk nat
S-1(config-if)#switchport trunk native vlan 1

S-1(config)#int f0/1
S-1(config-if)#sw
S-1(config-if)#switchport mode a
S-1(config-if)#switchport mode access
S-1(config-if)#sw
S-1(config-if)#switchport acc
S-1(config-if)#switchport access vlan 30

```

## S2

```
S-2(config-vlan)#do sh vlan
```

VLAN Name	Status	Ports
1 default	active	Fa0/2, Fa0/4, Fa0/5, Fa0/6 Fa0/7, Fa0/8, Fa0/9, Fa0/10 Fa0/11, Fa0/12, Fa0/13, Fa0/14 Fa0/15, Fa0/16, Fa0/17, Fa0/18 Fa0/19, Fa0/20, Fa0/21, Fa0/22 Fa0/23, Fa0/24, Gig0/1, Gig0/2
30 Administracion	active	
40 Mercadeo	active	Fa0/1
200 Mantenimiento	active	

```

S-2(config)#int f0/3
S-2(config-if)#sw
S-2(config-if)#switchport mode tr
S-2(config-if)#switchport mode trunk
S-2(config-if)#sw
S-2(config-if)#switchport trun
S-2(config-if)#switchport trunk nat
S-2(config-if)#switchport trunk native vlan 1

S-2(config-if)#int f0/1
S-2(config-if)#sw
S-2(config-if)#switchport mode acce
S-2(config-if)#switchport mode access
S-2(config-if)#sw
S-2(config-if)#switchport acces
S-2(config-if)#switchport access vlan 40

```

## R1

- En este router se configuran las subinterfaces para cada una de las vlan creadas, se configuran las IP's para cada una y la encapsulación.

```

R1(config)#int g0/0.30
R1(config-subif)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0.30, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0.30, changed
state to up
desc
R1(config-subif)#description Administracion
R1(config-subif)#enc
R1(config-subif)#encapsulation dot
R1(config-subif)#encapsulation dot1Q 30
R1(config-subif)#ip add 192.168.30.1 255.255.255.0
^
% Invalid input detected at '^' marker.

R1(config-subif)#ip add 192.168.30.1 255.255.255.0

```

```

R1(config)#int g0/0.40
R1(config-subif)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0.40, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0.40, changed
state to up
description Mercadeo
R1(config-subif)#encap
R1(config-subif)#encapsulation dot
R1(config-subif)#encapsulation dot1Q 40
R1(config-subif)#ip add 192.168.40.1 255.255.255.0

R1(config)#int g0/0.200
R1(config-subif)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0.200, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0.200, changed
state to up
descr
R1(config-subif)#description Mantenimiento
R1(config-subif)#enc
R1(config-subif)#encapsulation do
R1(config-subif)#encapsulation dot1Q 200
R1(config-subif)#ip add
R1(config-subif)#ip address 192.168.200.1 255.255.255.0

```

## 5. En el Switch 3 deshabilitar DNS lookup

```
S-2(config)#no ip domain-lookup
```

## 6. Asignar direcciones IP a los Switches acorde a los lineamientos.

Se configura una dirección IP a la vlan 200 de cada switch.

**S1**

```

interface Vlan200
 ip address 192.168.200.2 255.255.255.0
 !
 ip default-gateway 192.168.200.1

```

**S2**

```
interface Vlan200
  ip address 192.168.200.3 255.255.255.0
  !
ip default-gateway 192.168.200.1
```

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

Desactivamos todas las interfaces que no estamos usando.

**S1**

```
S-1(config)#int range f0/4 - 23
S-1(config-if-range)#sh
```

```
S-1(config-if)#int g0/1
S-1(config-if)#sh
```

```
%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to administratively
down
```

```
S-1(config-if)#int g0/2
S-1(config-if)#sh
```

```
%LINK-5-CHANGED: Interface GigabitEthernet0/2, changed state to administratively
down
```

**S2**

```
S-2(config-if-range)#int range f0/4 - 24
S-2(config-if-range)#sh
```

```
S-2(config)#int range g0/1 - 2
S-2(config-if-range)#sh
```



## 8. Implement DHCP and NAT for IPv4

- Configurar R1 como servidor DHCP para las VLANs 30 y 40.
- Reservar las primeras 30 direcciones IP de las VLAN 30 y 40 para configuraciones estáticas.
  - Se habilita el servicio dhcp, se excluyen el rango de direcciones indicadas, se crea el pool de direcciones, se le asigna un nombre, se agrega la dirección del router por defecto que fue la que agregamos a las subinterfaces de las vlans, configuramos la dirección del servidor dns.

```
R1(config)#service dhcp
R1(config)#service dn
R1(config)#ip dh
R1(config)#ip dhcp ex
R1(config)#ip dhcp excluded-address 192.168.30.1 192.168.30.30
R1(config)#ip dhc
R1(config)#ip dhcp poo
R1(config)#ip dhcp pool Administracion
R1(dhcp-config)#def
R1(dhcp-config)#default-router 192.168.30.1
R1(dhcp-config)#dns
R1(dhcp-config)#dns-server 10.10.10.11

R1(dhcp-config)#network 192.168.30.0 255.255.255.0

R1(config)#ip dhcp excluded-address 192.168.40.1 192.168.40.30
R1(config)#ip dhcp
R1(config)#ip dhcp po
R1(config)#ip dhcp pool Mercadeo
R1(dhcp-config)#ne
R1(dhcp-config)#network 192.168.40.0 255.255.255.0
R1(dhcp-config)#de
R1(dhcp-config)#default-router 192.168.40.11
```

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

- Se configura NAT para que traduzca internamente la dirección del servidor web a una pública.

```
R2(config)#ip nat inside source static 10.10.10.10 209.165.200.229
```

- Se aplica NAT a las interfaces correspondientes.

```
R2(config)#int g0/0
R2(config-if)#ip nat out
R2(config-if)#ip nat outside
R2(config-if)#int g0/1
R2(config-if)#ip nat insi
R2(config-if)#ip nat inside
```

- Se configura una lista de acceso que permita el tráfico de las redes que harán Nateo.

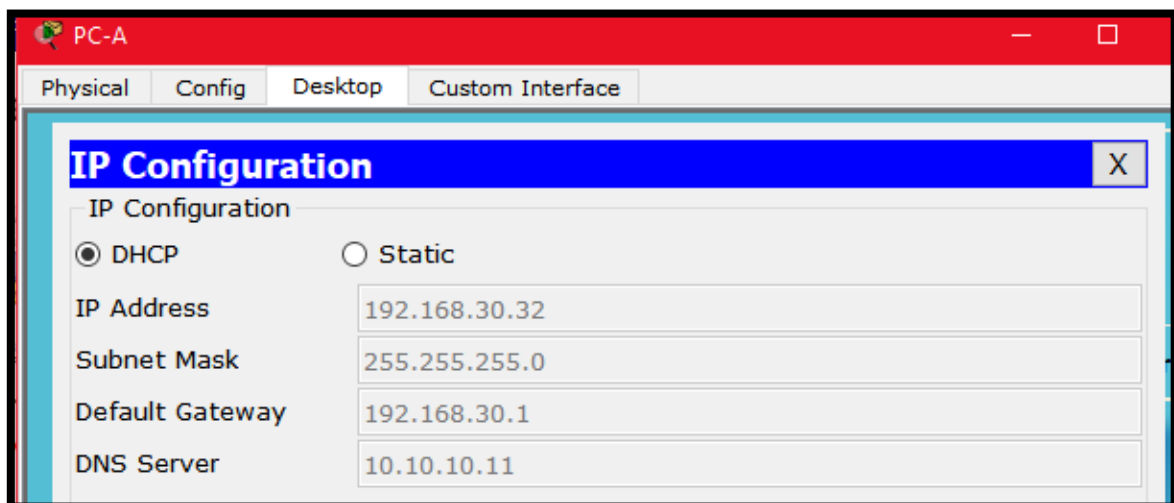
```
R2(config)#ac
R2(config)#access-list 1 permit 192.168.30.0 0.0.0.255
R2(config)#access-list 1 permit 192.168.40.0 0.0.0.255
R2(config)#access-list 1 permit 192.168.4.0 0.0.3.255
```

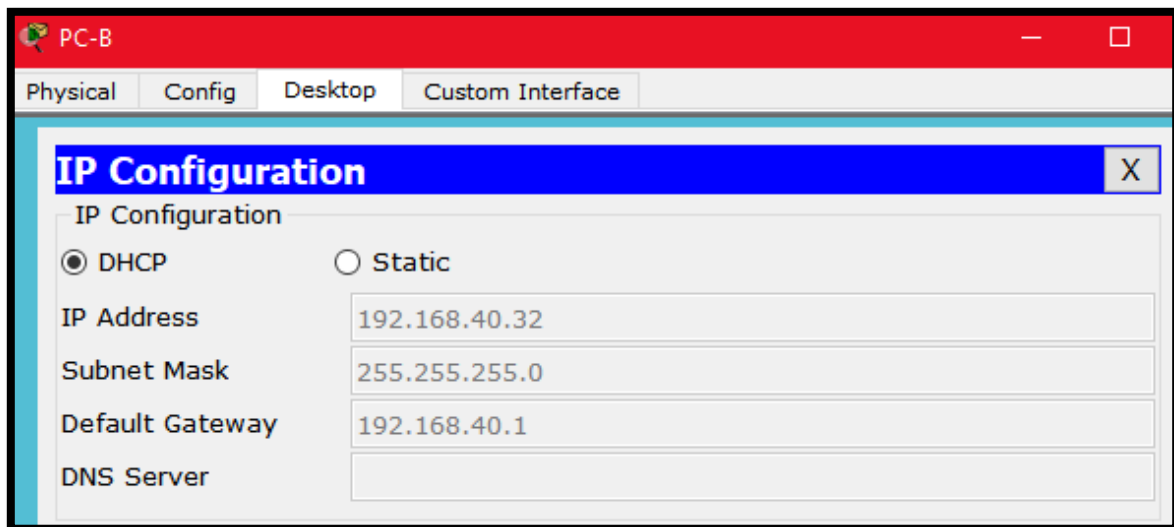
- Se configura el pool de direcciones disponibles públicas.

```
R2(config)#ip nat pool Internet 209.165.200.225 209.165.200.228 netmask
255.255.255.248
```

```
R2(config)#ip nat inside source list 1 pool Internet
```

- Confirmamos en los PC que se este asignando una dirección a través del DHCP.



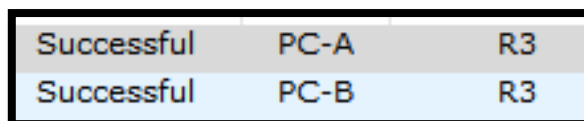


- Verificamos que los dos PC tengan conectividad entre ellos.



10. 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.

- ACL que deniegue el tráfico desde el PC-A a Bucaramanga
  - Verificamos que tengamos ping antes de implementar la ACL.



- Se crea la ACL 2 permitiendo el tráfico desde la red de la VLAN 40 y deniegue el tráfico desde el host de la VLAN 30.

```
R3(config)#access-list 2 permit 192.168.40.0 0.0.0.255
R3(config)#access-list 2 deny host 192.168.30.32
```

- Se aplica la ACL en la interfaz indicada.

```
R3(config-if)#ip access-group 2 in
```

- Confirmamos el resultado de la ACL.

Failed	PC-A	R3
Successful	PC-B	R3

- ACL que deniegue el tráfico desde el PC-B a PC INTERNET y permita el tráfico desde el PC-A
  - Configuramos una ACL que permita el tráfico desde el host de la VLAN 30 y deniegue el tráfico desde el host de la VLAN 40.



```
R2(config)#access-list 3 permit host 192.168.30.32
```

```
R2(config)#access-list 3 deny host 192.168.40.32
```

- Se aplica la ACL en la interfaz indicada.

```
R2(config-if)#ip access-group 3 out
```

- Confirmamos el resultado de la ACL.

	Successful	PC-A	PC Internet
	Failed	PC-B	PC Internet

## 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.

- ACL que deniegue el tráfico IP desde la red 192.168.40.0 hacia el servidor web, pero que permita el tráfico IP hacia el servidor desde 192.168.30.0.

Configuramos una nueva lista de acceso extendida donde vamos a denegar el tráfico tcp desde la red de la VLAN 40 hacia el servidor web.

- Permitimos el tráfico tcp desde la red de la VLAN 30 hacia el servidor web.
- Permitimos el tráfico icmp desde la red de la VLAN 30 hacia el servidor web.
- Permitimos el tráfico icmp desde la red de la VLAN 40 hacia el servidor web.

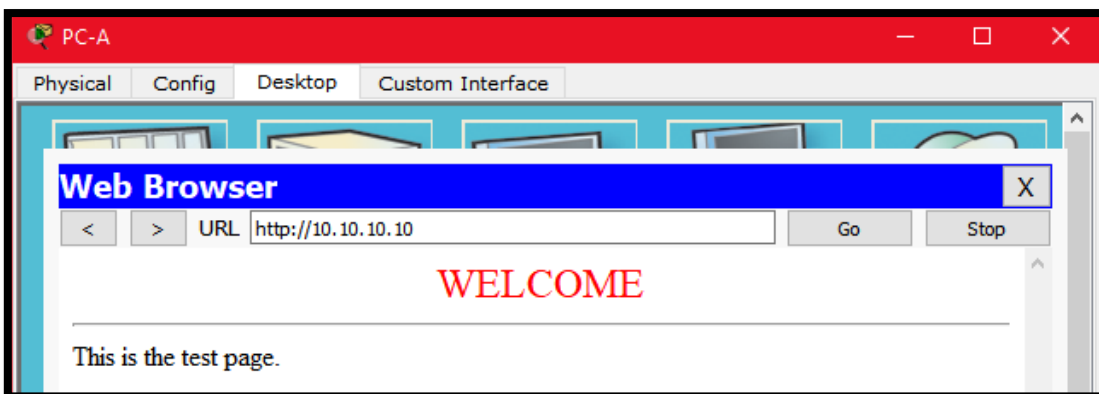
```
10 deny tcp 192.168.40.0 0.0.0.255 host 10.10.10.10 (94 match(es))
20 permit tcp 192.168.30.0 0.0.0.255 host 10.10.10.10 (20 match(es))
30 permit icmp 192.168.30.0 0.0.0.255 host 10.10.10.10
40 permit icmp 192.168.40.0 0.0.0.255 host 10.10.10.10
```

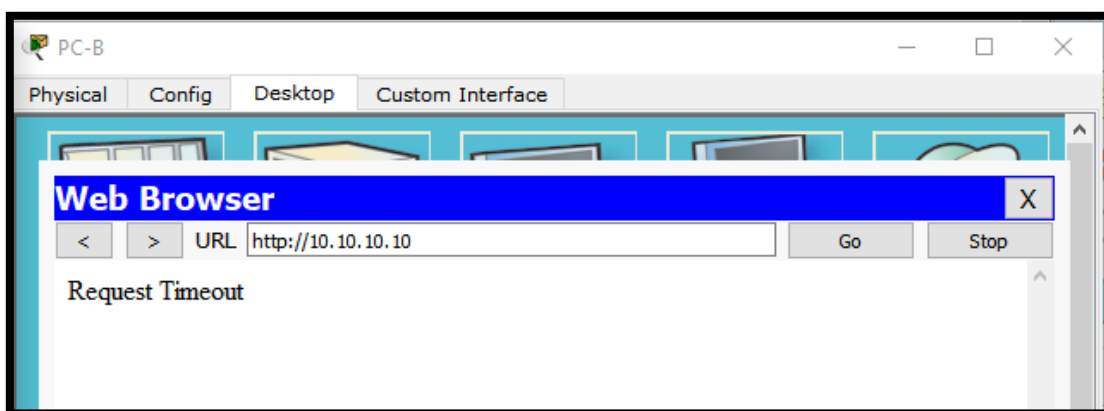
- Se aplica la ACL en la interfaz indicada.

```
R2(config)#int g0/1
R2(config-if)#ip acc
R2(config-if)#ip access-group 101 out
```

- Confirmamos el resultado de la ACL.

Successful	PC-A	WebServer	ICMP
Successful	PC-B	WebServer	ICMP





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

Successful	PC-B	PC-A	ICMP
Successful	PC-A	PC Internet	ICMP
Successful	PC-A	WebServer	ICMP
Failed	PC-B	PC Internet	ICMP
Successful	PC-B	WebServer	ICMP