CURSO DE PROFUNDIZACION CISCO (DISEÑO E IMPLEMENTACIÓN DE SOLUCIONES INTEGRADAS LAN – WAN)

Estudiante: PEREZ VARGAS FREDY YOVAN PEREZ
Grupo: 203092_49

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD-SOGAMOSO
FACULTAD DE CIENCIAS BASICAS TECNOLOGIA E INGENIERIA
SOGAMOSO
2019

CURSO DE PROFUNDIZACION CISCO (DISEÑO E IMPLEMENTACIÓN DE SOLUCIONES INTEGRADAS LAN – WAN)

Estudiante: PEREZ VARGAS FREDY YOVAN PEREZ
Grupo: 203092_49

TUTOR:
GERARDO GRANADOS ACUÑA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD-SOGAMOSO
FACULTAD DE CIENCIAS BASICAS TECNOLOGIA E INGENIERIA
SOGAMOSO
2019

TABLA DE CONTENIDO

INTRODUCCION

Mediante el desarrollo del presente trabajo buscamos realizar la implementación de la red para los escenarios 1 y 2. Esperamos ser un punto de apoyo para la misma y una fortaleza para su futuro y su crecimiento a nivel local y nacional.

Es importante poder ayudar, pero al igual en el punto que nos encontramos, el desarrollo de esta propuesta también va a ser excelente para nuestra formación profesional, pues gracias a esta propuesta podremos practicar lo aprendido hasta el momento y que mejor manera que desarrollando directamente sobre un caso real que pueda exigirnos a cada día mejorara más.

La propuesta como vemos el archivo entregado donde los plasman el ejercicio será desarrollada desde cero, no hay nada de esta red sobre lo cual podamos trabajar, debemos analizar la situación actual de la empresa para poder tomar decisiones al respecto. Todo el diseño y el montaje lo realizaremos bajo dispositivos CISCO.

Espero el trabajo sea del agrado de todos ustedes y que les contribuya igualmente a solucionar algunas dudas que en el momento tenga.

El proyecto nos va a favorecer muchísimo puesto que será la forma de que apliquemos todo ese conocimiento que a lo largo del Diplomado hemos adquirido, queremos generar en nosotros esa confianza que necesitamos para poder abordar proyectos de cualquier dificultad.

Las redes han cambiado de forma significativa nuestra forma de vivir, nuestra forma de relacionarnos. Estas nos han permitido realizar muchas cosas que antes pensábamos imposibles pero que ahora las tenemos y las podemos hacer con gran facilidad. Utilizamos la red de distintas formas, entre ellas las aplicaciones Web, la telefonía IP, la videoconferencia, los juegos interactivos, el comercio electrónico, la educación y mucho más.

OBJETIVOS

Objetivo general

- ✓ Desarrollo e implementación de la red de datos para los escenarios 1 y 2.

- ✓ Diseño de la Topología de los escenarios indicados, la cual tiene una serie de sedes a nivel de diferentes ciudades, siguiendo una serie de pautas y necesidades que se nos establece dentro del documento.

Objetivos específicos

- ✓ Diseñar la red de datos para la empresa la cual se ajuste a las necesidades reales de la empresa.
- ✓ Practicar todo lo aprendido hasta el momento, lo cual nos genere esta confianza que necesitamos para el desarrollo de este tipo de propuesta.
- ✓ Aplicaremos VLSM en todo el diseño de la red, la intención es mitigar el desperdicio de direcciones IP.
- ✓ Realizar la documentación general de la red.
- ✓ Practicarnos en la configuración de protocolos de enrutamiento, reconociendo las posibilidades de cada uno de ellos.
- ✓ Comprender mucho mejor la utilización de los diferentes comandos de configuración

ESCENARIO 1

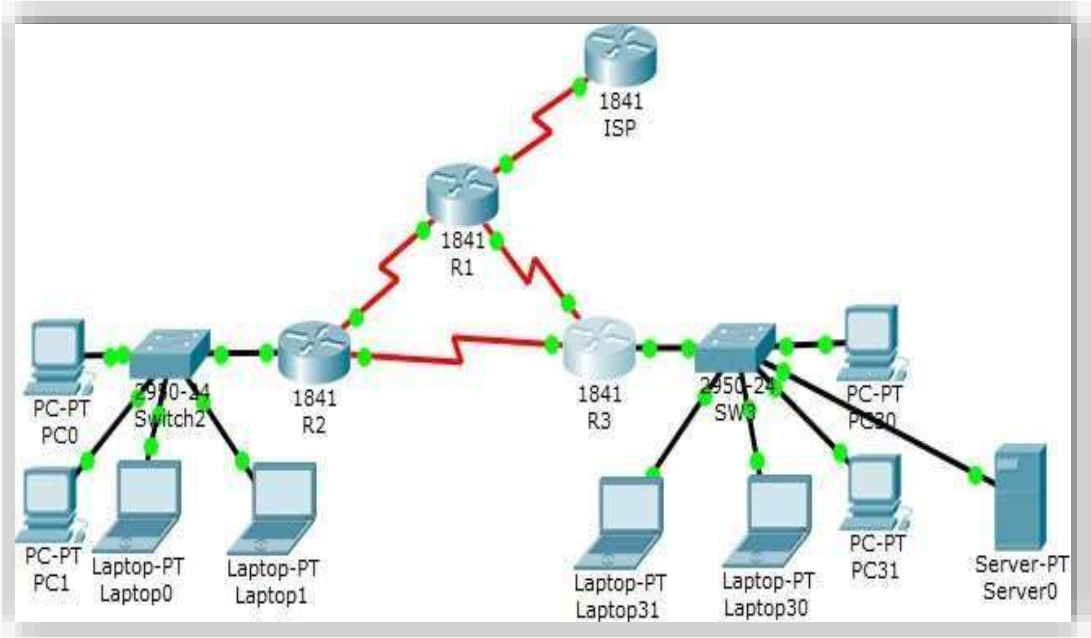


Tabla de direccionamiento

El administrador	Interfaces	Dirección IP	Máscara de subred	Gateway predeterminado
ISP	S0/0/0	200.123.211.1	255.255.255.0	N/D
R1	Se0/0/0	200.123.211.2	255.255.255.0	N/D
	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
	Fa0/0,100	192.168.20.1	255.255.255.0	N/D

R2	Fa0/0,200	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::9C0:80F: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	Interf az
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 tabla 1.
- Los puertos de red que no se utilizan se deben deshabilitar.
- La información de dirección IP R1, R2 y R3 debe cumplir con la tabla 1.
- Laptop20, Laptop21, PC20, PC21, Laptop30, Laptop31, PC30 y PC31 deben obtener información IPv4 del servidor DHCP.
- R1 debe realizar una NAT con sobrecarga 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 debe tener una ruta estática predeterminada al ISP que se configuró y que incluye esa ruta en el dominio RIPv2.
- R2 es un servidor de DHCP para los dispositivos conectados al puerto FastEthernet0/0.
- R2 debe, además de enrutamiento a otras partes de la red, ruta entre las VLAN 100 y 200.
- El Servidor0 es sólo un servidor IPv6 y solo debe ser accesibles 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).
- R1, R2 y R3 intercambian información de routing mediante RIP versión 2.
- R1, R2 y R3 deben saber sobre las rutas de cada uno y la ruta predeterminada desde R1.

Verifique la conectividad. Todos los terminales deben poder hacer ping entre sí y a la dirección IP del ISP. Los terminales bajo el R3 deberían poder hacer IPv6-ping entre

ellos y el servidor.

Desarrollo del escenario 1.

- SW1 VLAN y las asignaciones de puertos de VLAN deben cumplir con la tabla 1.
- Los puertos de red que no se utilizan se deben deshabilitar.
- La información de dirección IP R1, R2 y R3 debe cumplir con la tabla 1.

SW 2

SW2>enable
SW2#config
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line. End with CNTL/Z.
SW2(config)#vlan 100
SW2(config-vlan) #name LAPTOPS
SW2(config-vlan) #vlan 200
SW2(config-vlan) #name DESTOPS
SW2(config-vlan) #exit SW2(config)#do wr

- Asignamos las VLAN a las interfaces correspondientes.

SW2#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SW2(config)#int range f0/2-3
SW2(config-if-range) #switchport mude access
SW2(config-if-range) #switchport access vlan 100
SW2(config-if-range) #int range f0/4-5
SW2(config-if-range) #switchport mode access
SW2(config-if-range) #switchport access vlan 200
SW2(config-if-range) #
SW2(config-if-range) #exit
SW2(config)#exit

- Deshabilitamos los rangos que no estamos utilizando

SW2#config
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line. End with CNTL/Z.
SW2(config)#
SW2(config)#interface range f0/6-24
SW2(config-if-range) #shutdown

- Configuramos en enlace troncal

SW2#configure
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line. End with CNTL/Z.
SW2(config)#interface f0/1
SW2(config-if)#switchport mode trunk
SW2(config-if) #exit
SW2(config)#do wr Building configuration...

SW 3

- Configuramos la VLAN 1

SW3(config)#vlan 1
SW3(config-vlan) #exit
SW3(config)#int range f0/1-24
SW3(config-if-range) #switchport mode access
SW3(config-if-range) #switchport access vlan 1
SW3(config-if-range) #exit
SW3(config)#do wr

- Todos los puertos que no utilicemos los debemos deshabilitar

SW3#configu
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line. End with CNTL/Z.
SW3(config)#
SW3(config)#int range f0/6-23
SW3(config-if-range) #shutdown

- Configuramos la interface como enlace troncal

SW3#config
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line. End with CNTL/Z.
SW3(config)#int f0/1
SW3(config-if) #switchport mode trunk

- Procedemos a configurar las INTERFACES de los routers

R1

R1>enable
R1#config

Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#int s0/0/0
R1(config-if)#ip address 200.123.211.2 255.255.255.0
R1(config-if)#exit
R1(config)#int s0/1/0
R1(config-if)#ip address 10.0.0.1 255.255.255.252
R1(config-if)#int s0/1/1
R1(config-if) #ip address 10.0.0.5 255.255.255.252
R1(config-if) #do wr

R2

R2>enable
R2#config
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line. End with CNTL/Z. R2(config)#interface f0/0.100
R2(config-subif) #
R2(config-subif) #encapsulation dot1Q 100
R2(config-subif) #ip address 192.168.20.1 255.255.255.0 R2(config-subif) #exit
R2(config)# R2(config)#interface f0/0.200 R2(config-subif) #
R2(config-subif) #encapsulation dot1Q 200
R2(config-subif) #ip address 192.168.21.1 255.255.255.0 R2(config-subif) #exit
R2(config)# R2(config)#interface s0/0/0
R2(config-if) #ip address 10.0.0.2 255.255.255.252 R2(config-if) #interface s0/0/1
R2(config-if) #ip address 10.0.0.9 255.255.255.252 R2(config-if) #
R2(config-if) #do wr Building configuration... [OK]
R2(config-if) #

R3

R3#
R3#config
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#
R3(config)#interface f0/0

R3(config-if)#ip addres 192.168.30.1 255.255.255.0
R3(config-if) #exit
R3(config)#ipv6 unicast-routing
R3(config)#int s0/0/0
R3(config-if) #ip addres 10.0.0.6 255.255.255.252
R3(config-if) #exit
R3(config)# R3(config)#int s0/0/1
R3(config-if) #ip addres 10.0.0.10 255.255.255.252
R3(config-if) #

- R1 debe realizar una NAT con sobrecarga 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 s0/1/1
R1(config-if) #ip nat inside
R1(config-if) #exit
R1(config)#int s0/1/0
R1(config-if) #ip nat inside
R1(config-if) #exit
R1(config)#
R1(config)#int s0/0/0
R1(config-if)#ip nat outside
R1(config-if) #exit
R1(config)#ip nat pool INSIDE-DEVS 200.123.211.2 200.123.211.128 NETMASK 255.255.255.0
R1(config)#access-list 1 permit 192.168.0.0 0.0.255.255
R1(config)#access-list 1 permit 10.0.0.0 0.255.255.255
R1(config)#ip nat inside source list 1 interface serial 0/0/0 overload
R1(config)#ip nat inside source static tcp 192.168.30.6 80 200.123.211.1 80
R1(config)#

```
R1#show ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
tcp 200.123.211.1:80   192.168.30.6:80    ---                ---

R1#
```

```
R1#show ip nat stati
R1#show ip nat statistics
Total translations: 1 (1 static, 0 dynamic, 1 extended)
Outside Interfaces: Serial0/0/0
Inside Interfaces: Serial0/1/0 , Serial0/1/1
Hits: 0  Misses: 4
Expired translations: 0
Dynamic mappings:
```

- **R2** es un servidor de DHCP para los dispositivos conectados al puerto

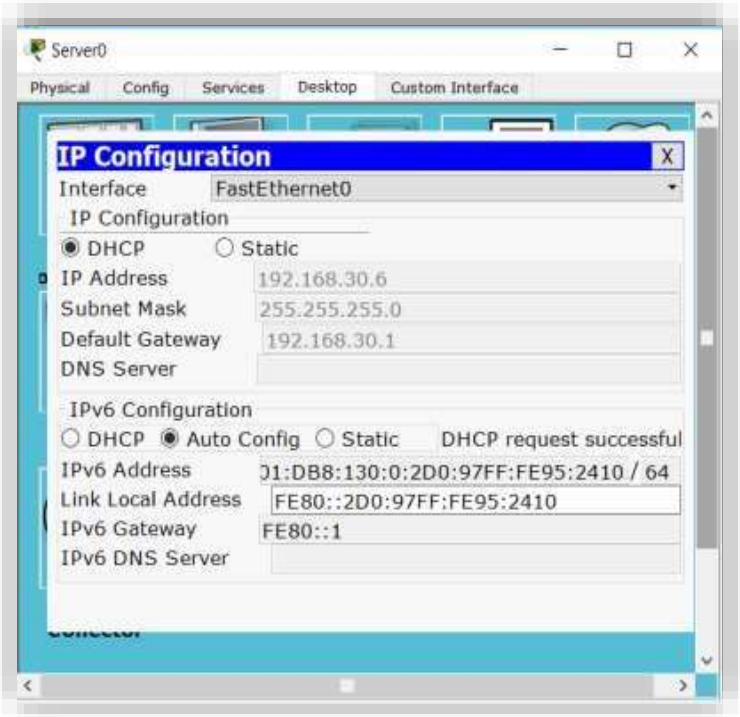
FastEthernet0/0.

```
R2(config)# R2(config)#ip dhcp exc? excluded-address
R2(config)#ip dhcp exc
R2(config)#ip dhcp excluded-address 10.0.0.2 10.0.0.9
R2(config)#ip dhcp pool INSIDE-DEVS
R2(dhcp-config) #network 192.168.20.1 255.255.255.0
R2(dhcp-config) #network 192.168.21.1 255.255.255.0
R2(dhcp-config) #defaul?
default-router
R2(dhcp-config)#defaul
R2(dhcp-config)#default-router 192.168.1.1
R2(dhcp-config)#dns-server 0.0.0.0
R2(dhcp-config)#exit
R2(config)#
```

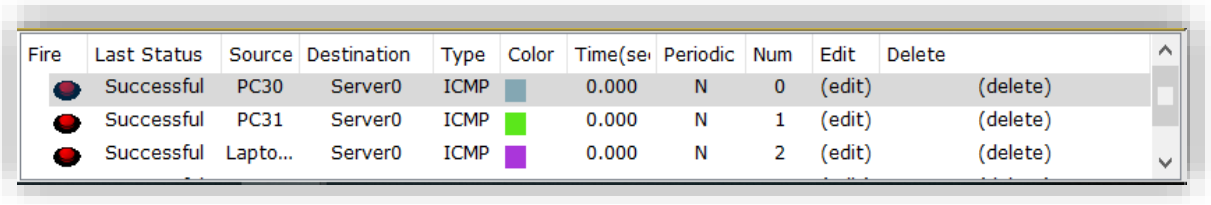
- R2 debe, además de enrutamiento a otras partes de la red, ruta entre las VLAN 100 y 200.

```
R2(config)#int vlan 100
R2(config-if)#ip addres 192.168.20.1 255.255.255.0
% 192.168.20.0 overlaps with FastEthernet0/0.100
R2(config-if)#int vlan 200
R2(config-if)#ip addres 192.168.21.1 255.255.255.0
% 192.168.21.0 overlaps with FastEthernet0/0.200
```

El Servidor0 es sólo un servidor IPv6 y solo debe ser accesibles para los dispositivos en R3 (ping).



Dentro de la misma red nos debe funcionar los PING



Fire	Last Status	Source	Destination	Type	Color	Time(se	Periodic	Num	Edit	Delete
	Successful	PC30	Server0	ICMP		0.000	N	0	(edit)	(delete)
	Successful	PC31	Server0	ICMP		0.000	N	1	(edit)	(delete)
	Successful	Lapto...	Server0	ICMP		0.000	N	2	(edit)	(delete)

- La interfaz FastEthernet 0/0 del R3 también deben tener direcciones IPv4 e IPv6 configuradas (dual- stack).

R3(config)#ipv6 uni?
unicast-routing
R3(config)#ipv6 uni
R3(config)#ipv6 unicast-routing R3(config)#int f0/0
R3(config-if)#ipv6 enable
R3(config-if)#ip address 192.168.30.1 255.255.255.0
R3(config-if)#ipv6 address 2001:db8::9c0:80f:301/64
R3(config-if)#no shutdown
R3(config-if)#

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

```
R1(config)# R1(config)#router rip
R1(config-router)#version 2
R1(config-router)#do show ip route connected
C 10.0.0.0/30 is directly connected, Serial0/1/0
C 10.0.0.4/30 is directly connected, Serial0/1/1
C 200.123.211.0/24 is directly connected, Serial0/0/0
R1(config-router)#
R1(config-router)#network 10.0.0.0
R1(config-router) #network 10.0.0.4
R1(config-router) #end
R1#

R2#config
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#
R2(config)#router rip
R2(config-router) #version 2
R2(config-router) #do show ip route connected
C 10.0.0.0/30 is directly connected, Serial0/0/0
C 10.0.0.8/30 is directly connected, Serial0/0/1
C 192.168.20.0/24 is directly connected, FastEthernet0/0.100
C 192.168.21.0/24 is directly connected, FastEthernet0/0.200
R2(config-router) #
R2(config-router)#network 10.0.0.0
R2(config-router) #network 10.0.0.8
R2(config-router)#end
R2#
%SYS-5-CONFIG_I: Configured from console by console

R2#
R3>enable
R3#config
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#router rip
R3(config-router)#version 2
R3(config-router)#do show ip route connected
C 10.0.0.4/30 is directly connected, Serial0/0/0
C 10.0.0.8/30 is directly connected, Serial0/0/1
C 192.168.30.0/24 is directly connected, FastEthernet0/0
R3(config-router)#network 10.0.0.4
R3(config-router)#network 10.0.0.8
```

R3(config-router)#end

R3#
%SYS-5-CONFIG_I: Configured from console by console

R3#

- R1, R2 y R3 deben saber sobre las rutas de cada uno y la ruta predeterminada desde R1.

R1#show ip route
Codes: C - connected, S - static, I - IGRP, 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

10.0.0.0/30 is subnetted, 3 subnets
C 10.0.0.0 is directly connected, Serial0/1/0
C 10.0.0.4 is directly connected, Serial0/1/1
R 10.0.0.8 [120/1] via 10.0.0.6, 00:00:16, Serial0/1/1
[120/1] via 10.0.0.2, 00:00:02, Serial0/1/0
R 192.168.30.0/24 [120/1] via 10.0.0.6, 00:00:16, Serial0/1/1
C 200.123.211.0/24 is directly connected, Serial0/0/0
R1#

R2>show ip route
Codes: C - connected, S - static, I - IGRP, 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

10.0.0.0/30 is subnetted, 3 subnets
C 10.0.0.0 is directly connected, Serial0/0/0

R 10.0.0.4 [120/1] via 10.0.0.1, 00:00:08, Serial0/0/0
C 10.0.0.8 is directly connected, Serial0/0/1
C 192.168.20.0/24 is directly connected, FastEthernet0/0.100 C 192.168.21.0/24 is directly connected, FastEthernet0/0.200

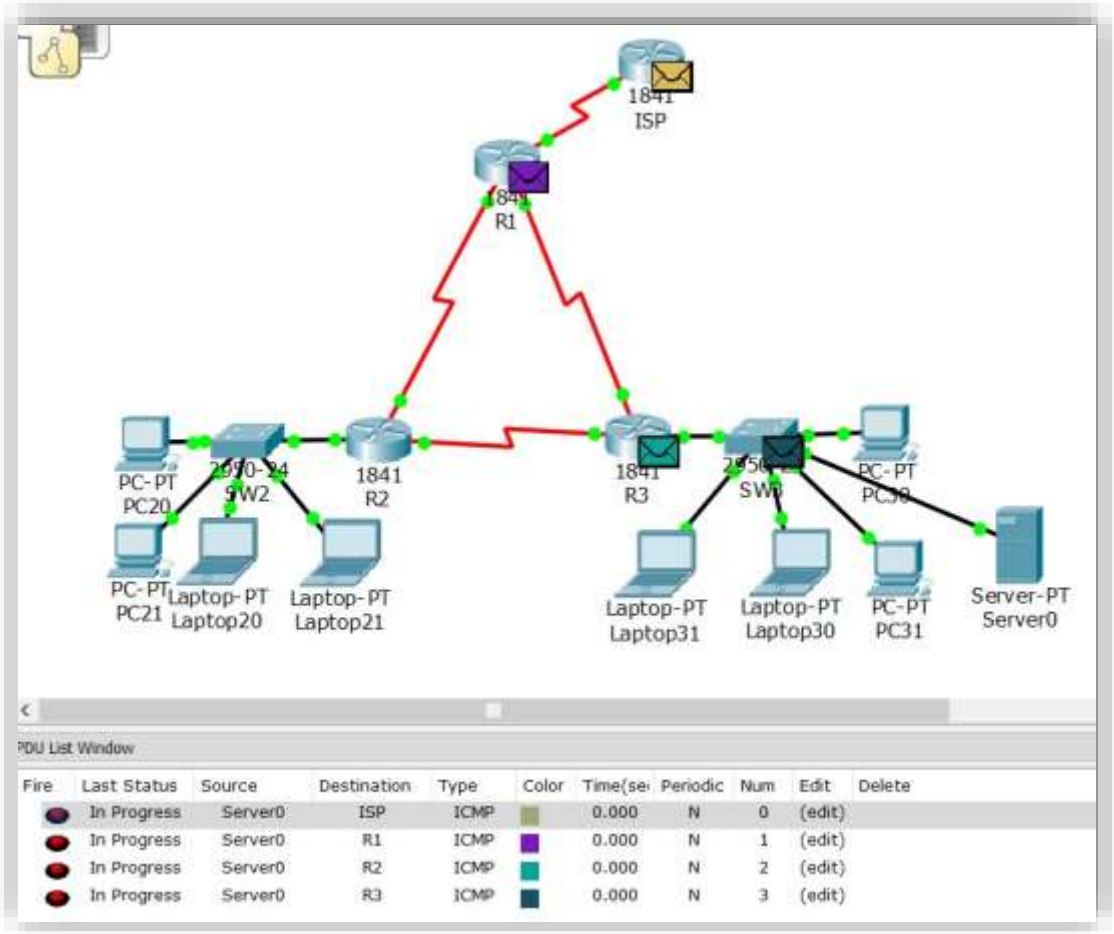
R 192.168.30.0/24 [120/2] via 10.0.0.1, 00:00:08, Serial0/0/0
R 200.123.211.0/24 [120/1] via 10.0.0.1, 00:00:08, Serial0/0/0
R2>

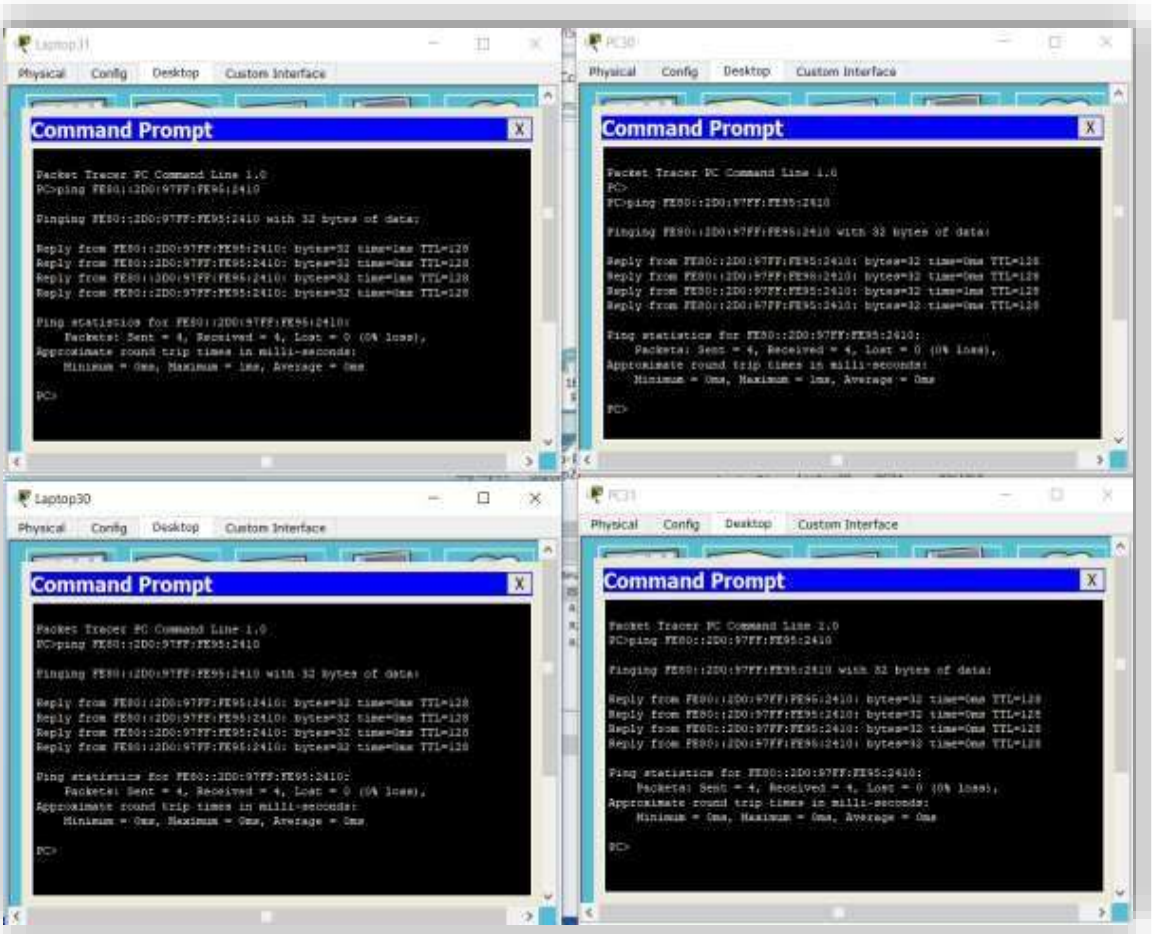
R3#
R3#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS 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

10.0.0.0/30 is subnetted, 3 subnets
R 10.0.0.0 [120/1] via 10.0.0.5, 00:00:17, Serial0/0/0
[120/1] via 10.0.0.9, 00:00:21, Serial0/0/1
C 10.0.0.4 is directly connected, Serial0/0/0
C 10.0.0.8 is directly connected, Serial0/0/1
C 192.168.30.0/24 is directly connected, FastEthernet0/0
R 200.123.211.0/24 [120/1] via 10.0.0.5, 00:00:17, Serial0/0/0
R3#

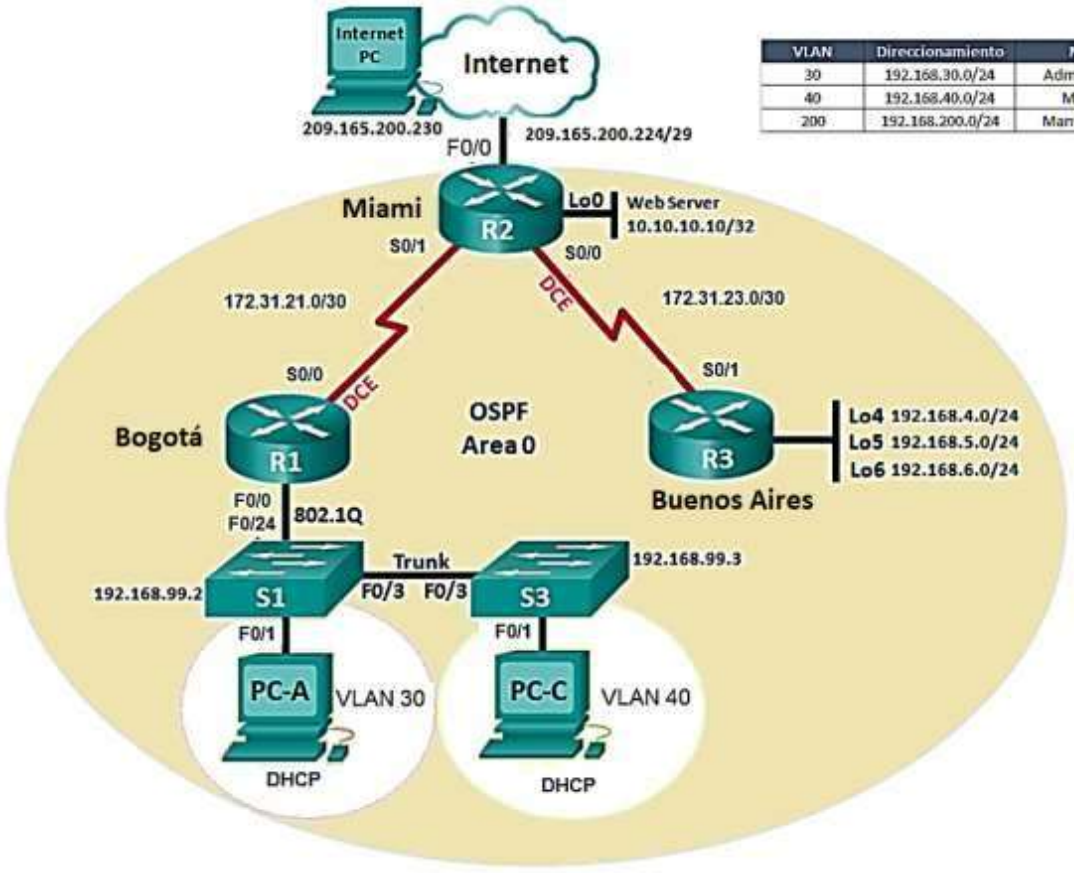
- Verifique la conectividad. Todos los terminales deben poder hacer ping entre sí y a la dirección IP del ISP. Los terminales bajo el R3 deberían poder hacer IPv6-ping entre ellos y el servidor.


1841
ISP
R1
PC-PT
PC20
1841
R2
1841
R3
PC-PT
PC21
Laptop-PT
Laptop20
Laptop-PT
Laptop21
Laptop-PT
Laptop31
Laptop-PT
Laptop30
PC-PT
PC31
Server-PT
Server0
PDU List Window
Fire
Last Status
Source
Destination
Type
Color
Time(se
Periodic
Num
Edit
Delete
In Progress
Server0
ISP
ICMP
0.000
N
0
(edit)
In Progress
Server0
R1
ICMP
0.000
N
1
(edit)
In Progress
Server0
R2
ICMP
0.000
N
2
(edit)
In Progress
Server0
R3
ICMP
0.000
N
3
(edit)


Laptop11
Physical
Config
Desktop
Custom Interface
Command Prompt
Packet Tracer PC Command Line 1.0
PC>ping FE80::2D0:97FF:FE95:2410
Pinging FE80::2D0:97FF:FE95:2410 with 32 bytes of data:
Reply from FE80::2D0:97FF:FE95:2410: bytes=32 time<1ms TTL=128
Reply from FE80::2D0:97FF:FE95:2410: bytes=32 time=0ms TTL=128
Reply from FE80::2D0:97FF:FE95:2410: bytes=32 time<1ms TTL=128
Reply from FE80::2D0:97FF:FE95:2410: bytes=32 time=0ms TTL=128
Ping statistics for FE80::2D0:97FF:FE95:2410:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 1ms, Average = 0ms
PC>
PC30
Physical
Config
Desktop
Custom Interface
Command Prompt
Packet Tracer PC Command Line 1.0
PC>
PC>ping FE80::2D0:97FF:FE95:2410
Pinging FE80::2D0:97FF:FE95:2410 with 32 bytes of data:
Reply from FE80::2D0:97FF:FE95:2410: bytes=32 time=0ms TTL=128
Reply from FE80::2D0:97FF:FE95:2410: bytes=32 time=0ms TTL=128
Reply from FE80::2D0:97FF:FE95:2410: bytes=32 time<1ms TTL=128
Reply from FE80::2D0:97FF:FE95:2410: bytes=32 time=0ms TTL=128
Ping statistics for FE80::2D0:97FF:FE95:2410:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 1ms, Average = 0ms
PC>
Laptop30
Physical
Config
Desktop
Custom Interface
Command Prompt
Packet Tracer PC Command Line 1.0
PC>ping FE80::2D0:97FF:FE95:2410
Pinging FE80::2D0:97FF:FE95:2410 with 32 bytes of data:
Reply from FE80::2D0:97FF:FE95:2410: bytes=32 time=0ms TTL=128
Reply from FE80::2D0:97FF:FE95:2410: bytes=32 time=0ms TTL=128
Reply from FE80::2D0:97FF:FE95:2410: bytes=32 time=0ms TTL=128
Reply from FE80::2D0:97FF:FE95:2410: bytes=32 time=0ms TTL=128
Ping statistics for FE80::2D0:97FF:FE95:2410:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms
PC>
PC31
Physical
Config
Desktop
Custom Interface
Command Prompt
Packet Tracer PC Command Line 1.0
PC>ping FE80::2D0:97FF:FE95:2410
Pinging FE80::2D0:97FF:FE95:2410 with 32 bytes of data:
Reply from FE80::2D0:97FF:FE95:2410: bytes=32 time=0ms TTL=128
Reply from FE80::2D0:97FF:FE95:2410: bytes=32 time=0ms TTL=128
Reply from FE80::2D0:97FF:FE95:2410: bytes=32 time=0ms TTL=128
Reply from FE80::2D0:97FF:FE95:2410: bytes=32 time=0ms TTL=128
Ping statistics for FE80::2D0:97FF:FE95:2410:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms
PC>

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.



VLAN	Direccionamiento	Nombre
30	192.168.30.0/24	Administración
40	192.168.40.0/24	Mercadeo
200	192.168.200.0/24	Mantenimiento

1. Configurar 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 area 0

Configuration Item or Task	**Specification**
Router ID BOGOTA.	1.1.1.1
Router ID MIAMI.	5.5.5.5
Router ID BUENOS AIRES.	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.

3. Configurar 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

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

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

7. Implement DHCP and NAT for IPv4

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

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

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.

10. Configurar NAT en MIAMI. para permitir que los host puedan salir a internet

11. Configurar al menos dos listas de acceso de tipo estándar a su criterio en para restringir o permitir tráfico desde BOGOTA. o BUENOS AIRES. hacia MIAMI..

12. Configurar al menos dos listas de acceso de tipo extendido o nombradas a su criterio en para restringir o permitir tráfico desde BOGOTA. o BUENOS AIRES. hacia MIAMI..

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

DESARROLLO DE LA GUÍA.

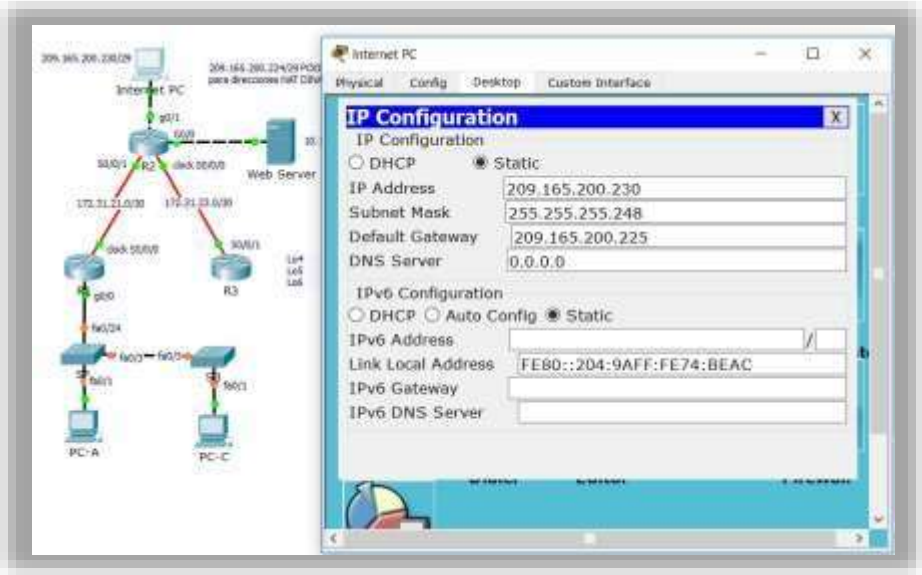
Examen de ENTRENAMIENTO.

Debemos poner un servidor WEB, pues paquet racer no lo admite como comando, debemos ponerlo de manera real.

- Debemos borrar la configuración de los dispositivos switches
- Erase start-up config
- Borra a base de datos de las VLAN.
- Delete vlan.dat
- Reiniciamos
- Reload.

CONFIGURAMOS LA IP INTERNET.

IP: 209.165.200.230
Mask: 255.255.255.248
Gateway: 209.165.200.225



Configuramos BOGOTA..

No ip domain lookup
Hostname BOGOTA.
Enable secret class
Line console 0
    Password cisco
    Login

Line vty 0 4
    Password class
    Login
Service password encryption

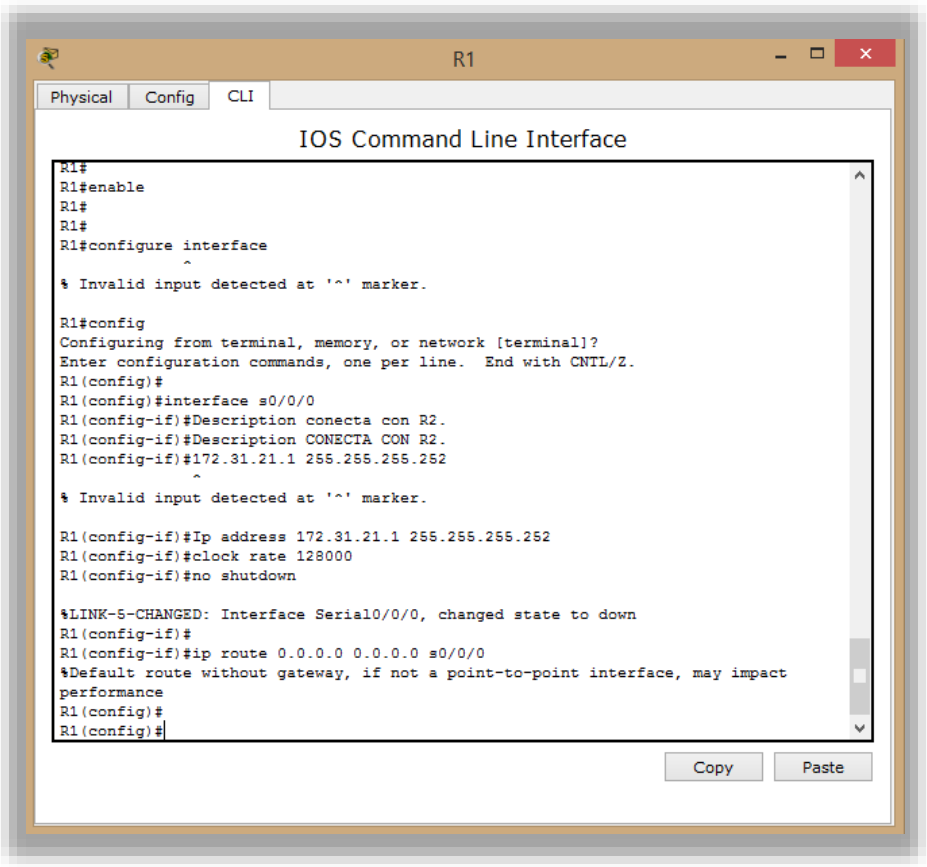
Banner motd &PROHIBIDO EL INGRESO DE PERSONAL NO AUTORIZADO.&

```
R1(config)#enable secret class
R1(config)#line console 0
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#line vty 0 4
R1(config-line)#password cisco
R1(config-line)#login
```

Configure interface s0/0/0
Description INTERFAZ QUE CONECTA CON MIAMI.
Ip address 172.31.21.1 255.255.255.252
Clock rate 256000
No shutdown

- Configuramos una ruta por defecto

Ip route 0.0.0.0 0.0.0.0 s0/0/0



Configuramos MIAMI..

No ip domain-lookup
Hostname MIAMI.
Enable secret class

Line console 0
Password cisco
Login
Line vty 0 4
Password cisco
Login

Service password-encryption

Ip http server “comando no soportado por PACKET TRACER”
Banner motd &PROHIBIDO EL INGRESO DE PERSONAL NO AUTORIZADO.&

Interface s0/0/1
Description INTERFAZ QUE CONECTA CON BOGOTA.
Ip address 172.31.21.2 255.255.255.252
no shutdown

interface s0/0/0
description INTERFAZ QUE CONECTA CON BUENOS AIRES.
ip address 172.31.23.1 255.255.255.252
clock rate 256000
no shutdown

interface g0/1 “es la simulación de INTERNET”
description INTERFAZ QUE CONECTA CON INTERNET
ip address 209.165.200.225 255.255.255.248
no shutdown

- como siguiente paso debemos configurara el servidos WEB

interface g0/0
ip address 10.10.10.1 255.255.255.0
no shutdown
description INTERFAZ QUE CONECTA CON WEB SERVER

- configuramos el servidor web

ip addres 10.10.10.10
mask: 255.255.255.0
Gateway: 10.10.10.1

- configuramos una ruta por defecto

ip route 0.0.0.0 0.0.0.0 g0/1 “que salga hacia internet.

- Configuramos el ROUTER 3.

No ip domain-lookup
Hostname BUENOS AIRES.
Enable secret class
Line console 0
Password cisco
login
Line vty 0 4
Password cisco
Login
Service password-encryption

Banner motd &PROHIBIDO EL INGRESO DE PERSONAL NO AUTORIZADO.&

Interface s0/0/1

Description INTERFAZ QUE CONECTA CON MIAMI.
Ip address 172.31.23.2 255.255.255.252
No shutdown

- Vamos a crear las interfaces loopback

Interface loopback 4
Ip addres 192.168.4.1 255.255.255.0
No shutdown

Interface loopback 5
Ip addres 192.168.5.1 255.255.255.0
No shutdown

Interface loopback 6
Ip addres 192.168.6.1 255.255.255.0
No shutdown

-Configurar ruta por defecto por serial 1 Ip route 0.0.0.0 0.0.0.0 s0/0/1

- Configuramos switch 1

No ip domain-lookup
hostname S1
enable secret class
line console 0
password cisco
login
line vty 0 4
password cisco
login
service password-encryption
banner motd &PROHIBIDO EL INGRESO DE PERSONAL NO AUTORIZADO.&

- Configuramos switch 3

No ip domain-lookup
hostname S3
enable secret class line console 0
password cisco

login

line vty 0 4
password cisco
login
service password-encryption
banner motd &PROHIBIDO EL INGRESO DE PERSONAL NO AUTORIZADO.&

En este punto debemos verificar la conectividad de los dispositivos.

tep 7: Verify network connectivity.

Use the **ping** command to test connectivity between network devices.

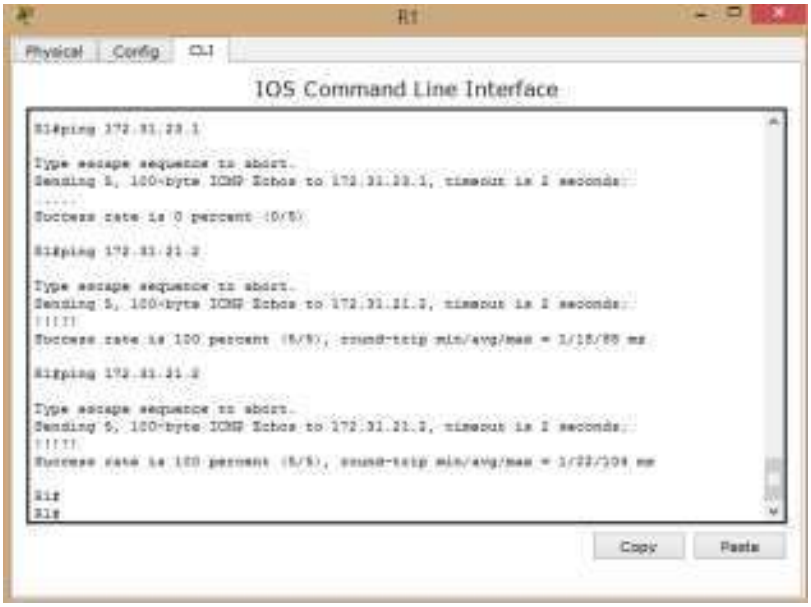
Use the following table to methodically verify connectivity with each network device. Take c
establish connectivity if a test fails:

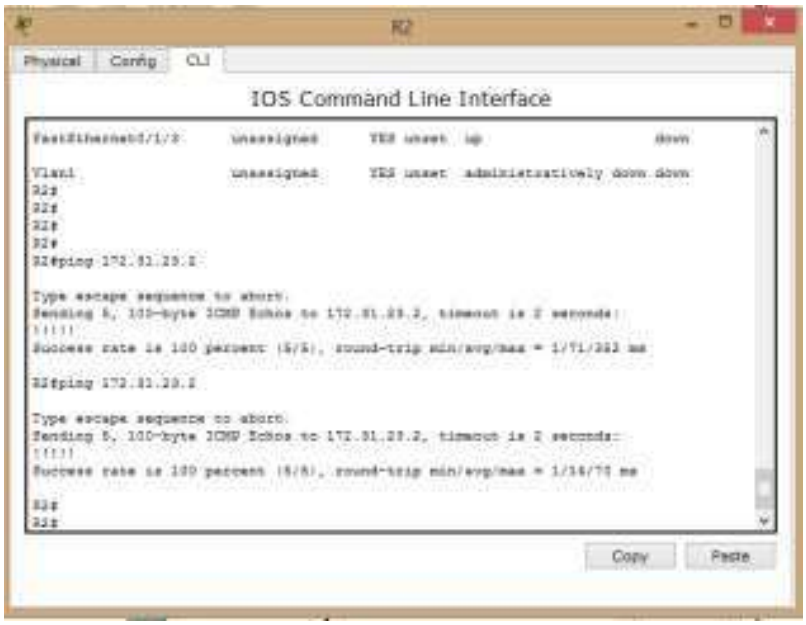
From	To	IP Address	Ping Results
R1	R2, S0/0/0		
R2	R3, S0/0/1		
Internet PC	Default Gateway		

Note: It may be necessary to disable the PC firewall for pings to be successful.

Instructor Sign-off Part 2: _____

Points: _____ **of 28**





Todos los PING son satisfactorios, con lo cual se verifica la correcta configuración de cada una delas INTERFACES.

- Configuramos la seguridad, las VLANS y el ruteo entre las VLANS

- Iniciamos con el SWITCH 1

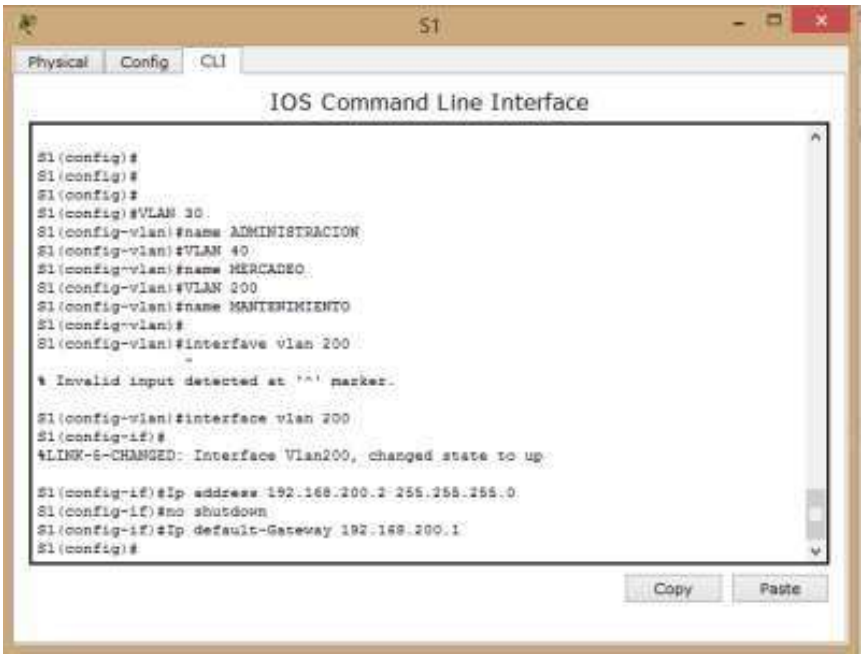
VLAN 30
Name ADMINISTRACION

VLAN 40
Name MERCADEO

VLAN 200
Name MANTENIMIENTO

- Asignar la dirección IP a la Vlan MANTENIMIENTO

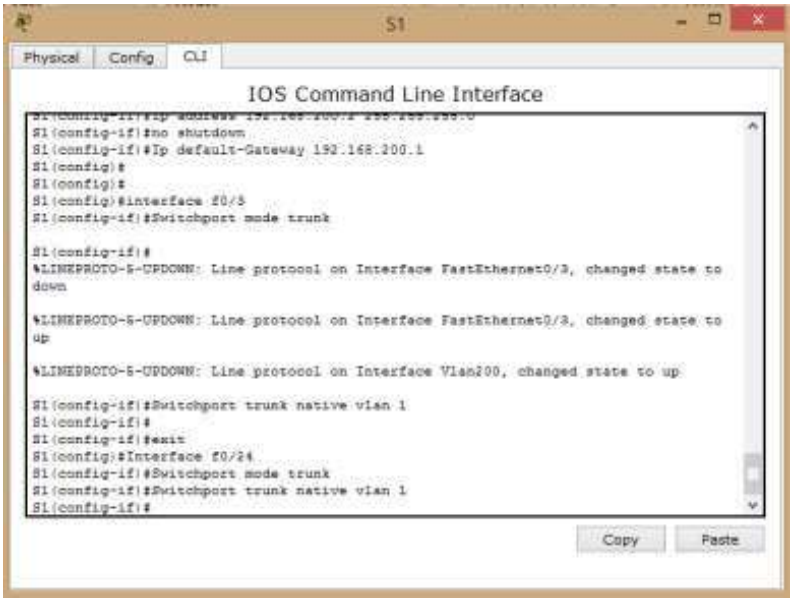
Interface VLAN 200
Ip address 192.168.200.2 255.255.255.0
No shutdown
Ip default-Gateway 192.168.200.1



- Forzamos el tranking en la interface f0/3, usamos la vlan nativa 1

Interface f0/3
Switchport mode trunk
Switchport trunk native vlan 1

Interface f0/24
Switchport mode trunk
Switchport trunk native vlan 1



- Configuramos todos demás puertos como puertos de acceso.

Interface range fa0/2, fa0/4-23, g0/1-2
Switchport mode Access

Interface fa0/1
Switchport mode Access
Switchport Access VLAN 30

- Apagamos los puertos que no los estemos utilizando

Interface range fa0/2, fa0/4-23, g0/1-2
Shutdown

Configuramos el S3

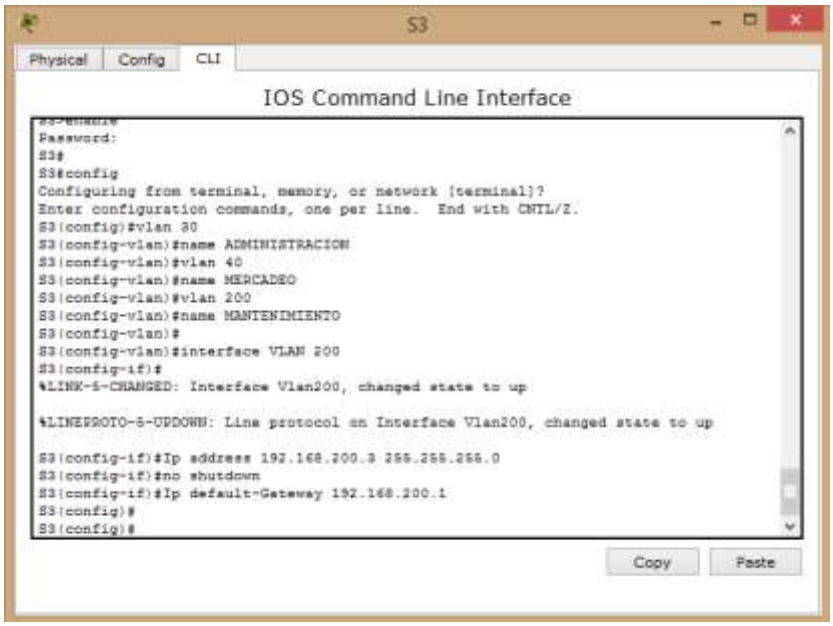
VLAN 30
Name ADMINISTRACION

VLAN 40
Name MERCADEO

VLAN 200
Name MANTENIMIENTO

-

Interface VLAN 200
Ip address 192.168.200.3 255.255.255.0
No shutdown exit
Ip default-Gateway 192.168.200.1



Usamos la f0/3 como troncal y la vlan 1 como nativa

Interface fa0/3
Switchport mode trunk
Switchport trunk native vlan 1

- Configuramos las interfaces en modo acceso empleando el comando rango

Interface range fa0/2, fa0/4-24, g1/1-2
Switchport mode Access

- Asignamos la interface fa0/1 a la vlan 40

Interface fa0/1
Switchport mode access
Switchport Access VLAN 40

- Apagar todos los puertos que no utilicemos

Interface range fa0/2, fa0/4-24, g0/1-2
Shutdown

- Configuramos el BOGOTA., procedemos a configurar las subinterfaces

Configuration Item or Task	Specification
Configure 802.1Q subinterface .31 on G0/1	Description Accounting LAN Assign VLAN 31. Assign the first available address to this interface.
Configure 802.1Q subinterface .33 on G0/1	Description Engineering LAN Assign VLAN 33. Assign the first available address to this interface.
Configure 802.1Q subinterface .99 on G0/1	Description Management LAN Assign VLAN 99. Assign the first available address to this interface.
Activate interface G0/1	

interface g0/0.30
description ADMINISTRACION LAN
encapsulation dot1q 30
ip address 192.168.30.1 255.255.255.0

interface g0/0.40
description MERCADEO LAN
encapsulation dot1q 40
ip address 192.168.40.1 255.255.255.0

interface g0/0.200
description MANTENIMIENTO LAN
encapsulation dot1q 200
ip address 192.168.200.1 255.255.255.0

- Activamos ahora la interface física g0/0

Interface g0/0
No shutdown

- Procedemos a verificar la conectividad de la red empleando el comendo PING

From	To	IP Address	Ping Results
S1	R1 VLAN 99 address		
S3	R1, VLAN 99 address		
S1	R1, VLAN 31 address		
S3	R1, VLAN 33 address		

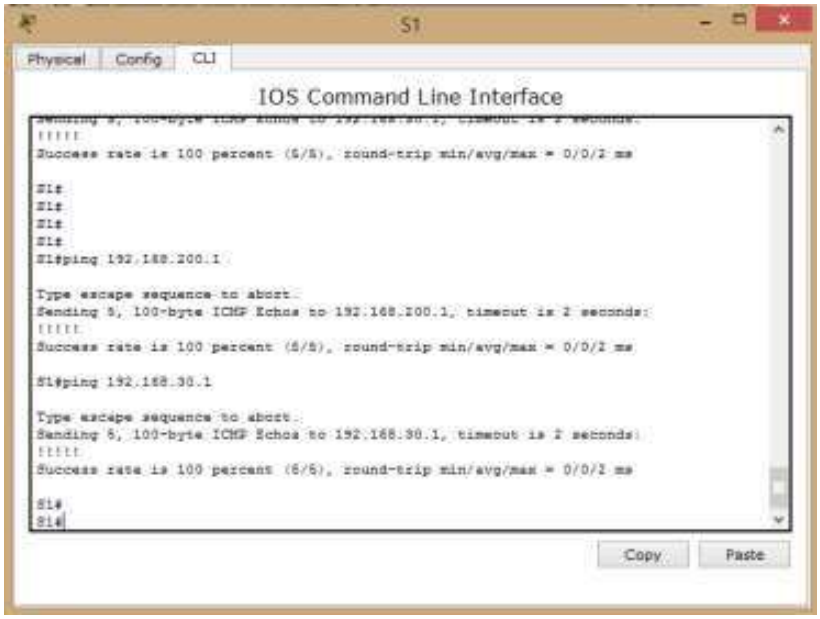
Todos estos comandos deben ser satisfactorios

S1
Ping 192.168.200.1
Ping 192.168.30.1

Network 192.168.30.0 0.0.0.255 area 0
Network 192.168.40.0 0.0.0.255 area 0
Network 192.168.200.0 0.0.0.255 area 0

- Establecemos todas las interfaces LAN como pasivas

Passive-interface g0/0.30
Passive-interface g0/0.40
Passive-interface g0/0.200



- Cambiamos el costo por defecto

Auto-cost reference-bandwitdh 1000 “este comando no es soportado por el simuladors

- Cambiamos el ancho de banda de las interface seriales

Interface s0/0/0
Bandwidth 256
Ip ospf cost 9500

- Configuramos OPSF V2 en el router MIAMI.

Router ospf 1
Router-id 5.5.5.5
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

- Establecemos las LAN como pasivas

Passive-interface g0/0

Interface s0/0/0
Bandwidth 256
Interface s0/0/1
Bandwidth 256

Ajustar la métrica de serial s0/0/0

Interface s0/0/0
Ip ospf cost 9500

- Configuramos OPSF V2 en el router BUENOS AIRES.

Router ospf 1
Router-id 8.8.8.8

Network 172.31.23.0 0.0.0.3 area 0
Network 192.168.4.0 0.0.3.255 area 0

- Debemos hacer que todas las interfaces loopback sean pasivas

Passive-interface lo4
Passive-interface lo5
Passive-interface lo6

Interface s0/0/1
Bandwidth 256

- Debemos verificar los comandos OSPF.

- Show ip ospf neighbor
- Show ip protocols
- Show ip route ospf
- Do show ip route connected

- Show ip ospf neighbor

```
MIAMI#Show ip ospf neighbor


Neighbor ID     Pri   State           Dead Time   Address
Interface
8.8.8.8           0   FULL/  -        00:00:38    172.31.23.2
Serial0/0/0
1.1.1.1           0   FULL/  -        00:00:38    172.31.21.1
Serial0/0/1
MIAMI#
```

```
BOGOTA#Show ip ospf neighbor


Neighbor ID     Pri   State           Dead Time   Address
Interface
5.5.5.5           0   FULL/  -        00:00:37    172.31.21.2
Serial0/0/0
BOGOTA#
```

```
BUENOS-AIRES#Show ip ospf neighbor


Neighbor ID     Pri   State           Dead Time   Address
Interface
5.5.5.5           0   FULL/  -        00:00:37    172.31.23.1
Serial0/0/1
BUENOS-AIRES#
```

- Show ip route ospf

```
MIAMI#Show ip route ospf
     192.168.4.0/32 is subnetted, 1 subnets
O       192.168.4.1 [110/9501] via 172.31.23.2, 00:18:01, Serial0/0/0
     192.168.5.0/32 is subnetted, 1 subnets
O       192.168.5.1 [110/9501] via 172.31.23.2, 00:18:01, Serial0/0/0
     192.168.6.0/32 is subnetted, 1 subnets
O       192.168.6.1 [110/9501] via 172.31.23.2, 00:18:01, Serial0/0/0
O    192.168.30.0 [110/391] via 172.31.21.1, 00:18:01, Serial0/0/1
O    192.168.40.0 [110/391] via 172.31.21.1, 00:18:01, Serial0/0/1
O    192.168.200.0 [110/391] via 172.31.21.1, 00:18:01, Serial0/0/1
MIAMI#
```

```
BOGOTA#Show ip route ospf
     10.0.0.0/24 is subnetted, 1 subnets
O       10.10.10.0 [110/9501] via 172.31.21.2, 00:18:13, Serial0/0/0
     172.31.0.0/16 is variably subnetted, 3 subnets, 2 masks
O       172.31.23.0 [110/19000] via 172.31.21.2, 00:18:13, Serial0/0/0
     192.168.4.0/32 is subnetted, 1 subnets
O       192.168.4.1 [110/19001] via 172.31.21.2, 00:18:13, Serial0/0/0
     192.168.5.0/32 is subnetted, 1 subnets
O       192.168.5.1 [110/19001] via 172.31.21.2, 00:18:13, Serial0/0/0
     192.168.6.0/32 is subnetted, 1 subnets
O       192.168.6.1 [110/19001] via 172.31.21.2, 00:18:13, Serial0/0/0
     209.165.200.0/29 is subnetted, 1 subnets
O       209.165.200.224 [110/9501] via 172.31.21.2, 00:18:13,
Serial0/0/0
BOGOTA#
```

```
BUENOS-AIRES#Show ip route ospf
     10.0.0.0/24 is subnetted, 1 subnets
O       10.10.10.0 [110/391] via 172.31.23.1, 00:18:07, Serial0/0/1
     172.31.0.0/16 is variably subnetted, 3 subnets, 2 masks
O       172.31.21.0 [110/780] via 172.31.23.1, 00:18:07, Serial0/0/1
O    192.168.30.0 [110/781] via 172.31.23.1, 00:17:57, Serial0/0/1
O    192.168.40.0 [110/781] via 172.31.23.1, 00:17:57, Serial0/0/1
O    192.168.200.0 [110/781] via 172.31.23.1, 00:17:57, Serial0/0/1
     209.165.200.0/29 is subnetted, 1 subnets
O       209.165.200.224 [110/391] via 172.31.23.1, 00:18:07, Serial0/0/1
BUENOS-AIRES#
```

- Comando para verificar la configuración en ejecución

- show running-config

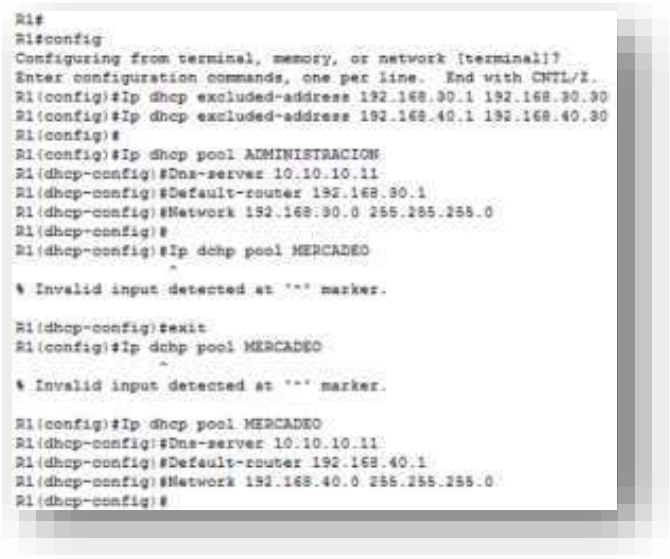
- Debemos implementar DHCP en el router BOGOTA..

- Procedemos en este caso a reservar las 30 primaras direcciones, tanto de la VLAN 30 como la VLAN 40.

Ip dhcp excluded-address 192.168.30.1 192.168.30.30
Ip dhcp excluded-address 192.168.40.1 192.168.40.30

Ip dhcp pool ADMINISTRACION
Dns-server 10.10.10.11
Domain-name ccna-unad.com “comando no soportado
Default-router 192.168.30.1
Network 192.168.30.0 255.255.255.0

Ip dhcp pool MERCADEO
Dns-server 10.10.10.11
Domain-name ccna-unad.com “comando no soportado
Default-router 192.168.40.1
Network 192.168.40.0 255.255.255.0



14. Configurar NAT en MIAMI. para permitir que los host puedan salir a internet

15. Configurar al menos dos listas de acceso de tipo estándar a su criterio en para restringir o permitir tráfico desde BOGOTA. o BUENOS AIRES. hacia MIAMI..

- Configuramos NAT ESTATICO y DINAMICO e MIAMI. con el fin de que los host puedan salir a internet.

Step 2: Configure Static and Dynamic NAT on R2.

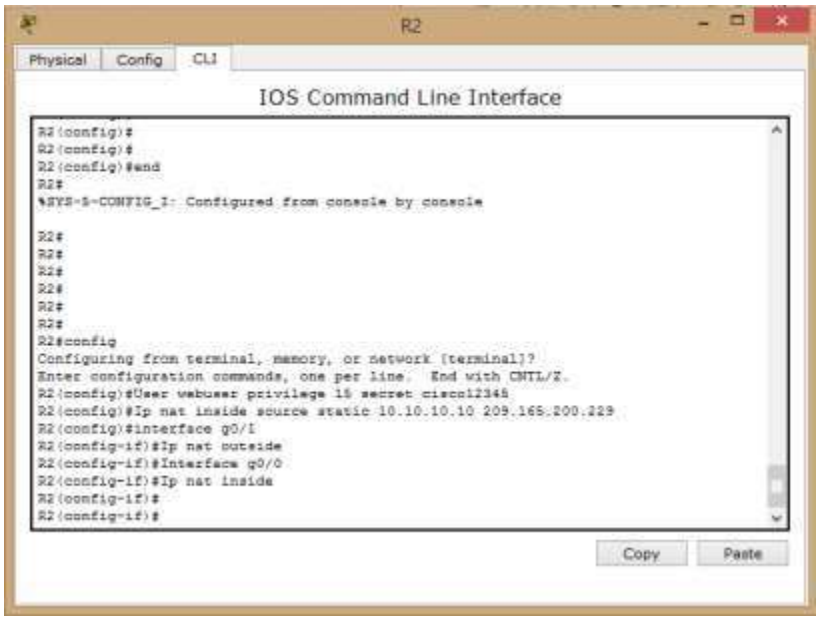
Configuration tasks for R2 include the following:

Configuration Item or Task	Specification
Create a local database with 1 user account	Username: **webuser** Password: **cisco12345** Privilege level: **15**
Enable HTTP server service	
Configure the HTTP server to use the local database for authentication	
Create a static NAT to the Web Server	Inside Global Address: **209.165.200.229**
Assign the inside and outside interface for the static NAT	
Configure the dynamic NAT inside private ACL	Access List: 1 Allow the Accounting and Engineering networks o R1 to be translated. Allow a summary of the LANs (loopback) networks on R3 to be translated.
Define the pool of usable public IP addresses	Pool Name: **INTERNET** Pool of addresses include: **209.165.200.225 – 209.165.200.228**
Define the dynamic NAT translation	

- Asignamos la interface interna y externa

Interface g0/1
Ip nat outside

Interface g0/0
Ip nat inside



- Creamos algunas restricciones empleando las ACL.

- Configuramos la NAT DINAMICA con una ACL.
- Creamos la acces-list número 1
- Solo debemos permitir que la traducción sea para las redes de ADMINISTRACIÓN Y MERCADEO que están en BOGOTA. – pero la traducción se hace en MIAMI..

Configure terminal

Access-list 1 permit 192.168.30.0 0.0.0.255
Access-list 1 permit 192.168.40.0 0.0.0.255

- Permitir que las loopback que están conectadas al BUENOS AIRES. también sean traducidas empleando una ruta RESUMIDA.

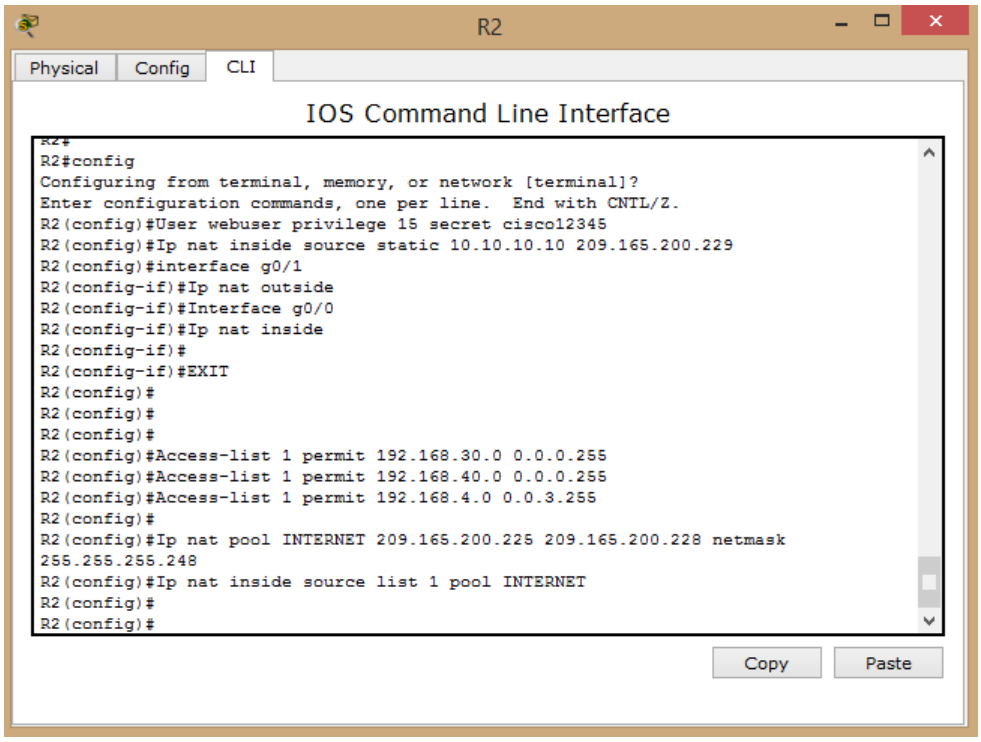
Access-list 1 permit 192.168.4.0 0.0.3.255

- Definimos el POOL de direcciones que se van a utilizar para el NAT DINAMICO.

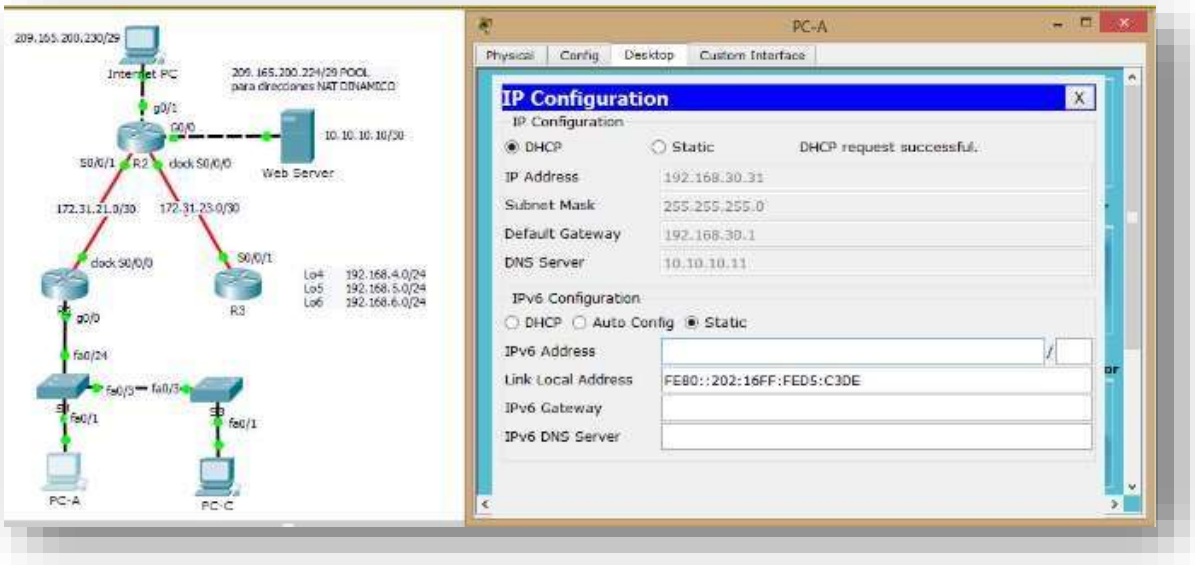
Ip nat pool INTERNET 209.165.200.225 209.165.200.228 netmask 255.255.255.248

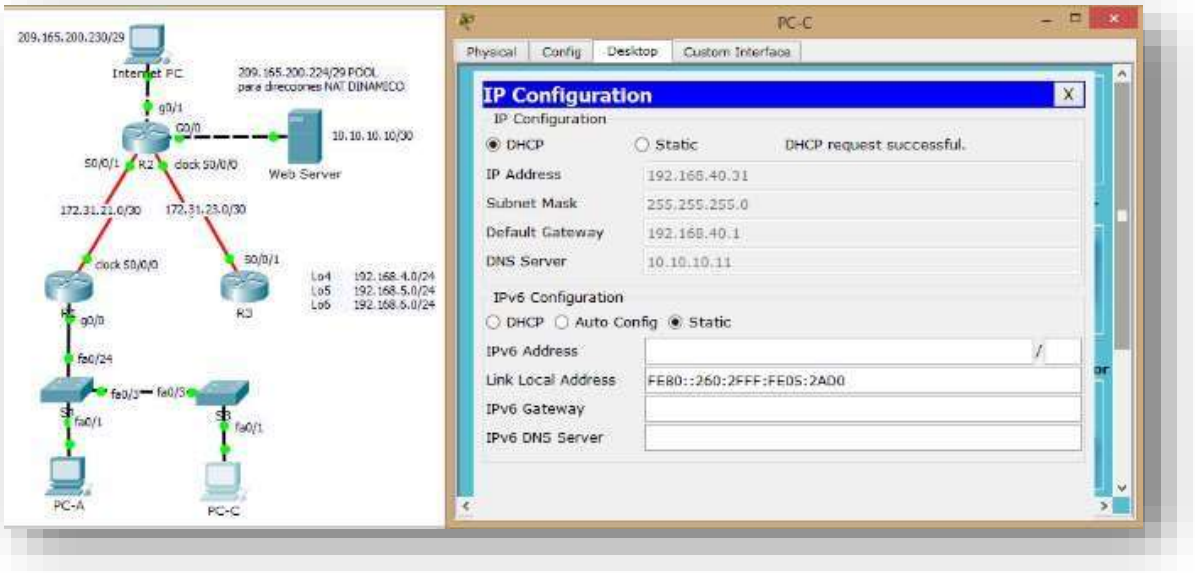
- Definimos la traducción NAT dinámico

Ip nat inside source list 1 pool INTERNET

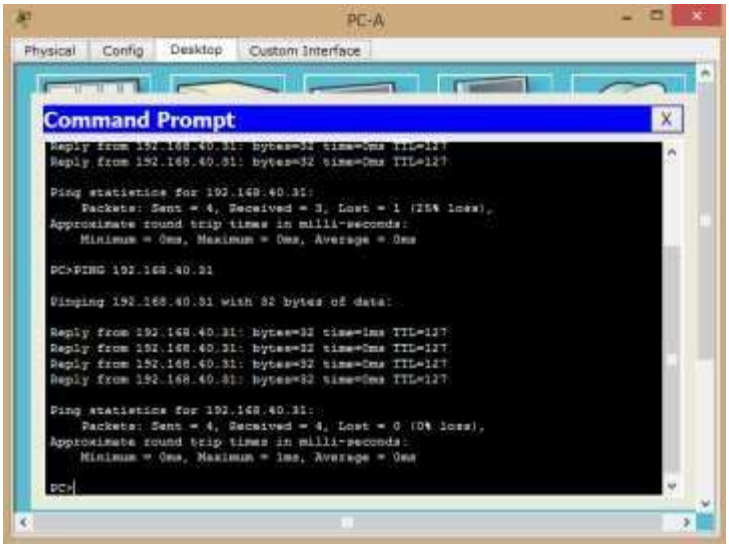


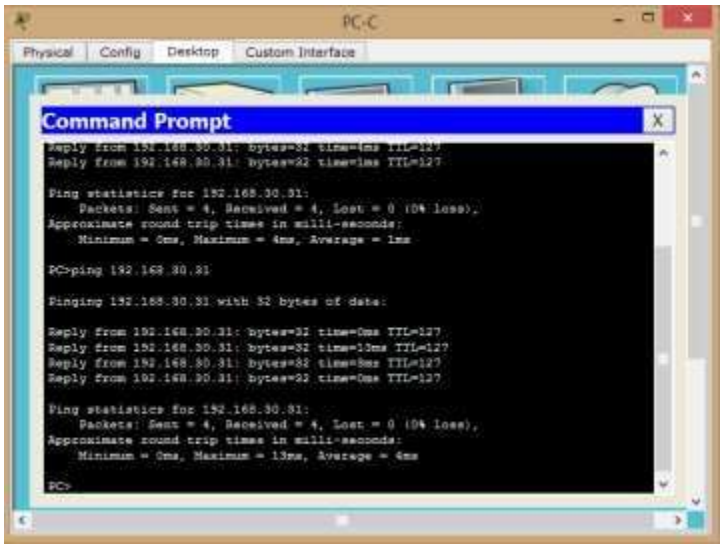
Procedemos a verificar lo hecho hasta este momento.





Ping entre PC-A y PC-C





- Configurar y verificar las ACL en el router MIAMI. en la cual solo le damos acceso al router BOGOTA..

- Configuramos una ACL que me permita que solo BOGOTA. pueda hacer TELNET a MIAMI..

Ip Access-list standard ADMIN-MANTENIMIENTO
Permit host 172.31.21.1

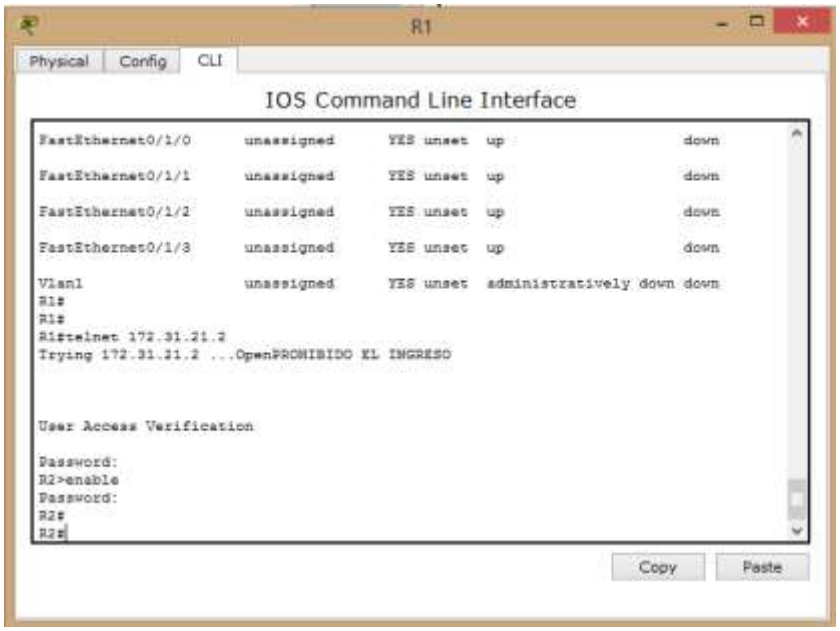
- Ahora si debemos aplicar la ACL nombrada a la línea VTY

Line vty 0 4
Access-class ADMIN-MANTENIMIENTO in

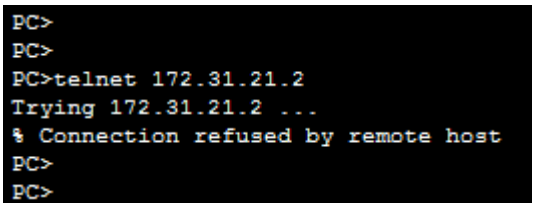
- Debemos verificar que las ACL está trabajando como queremos

Vemos claramente que si empleamos TELNET desde el ROUTER BOGOTA. este es satisfactorio, si lo hacemos desde cualquier otro equipo este no puede ser posible.

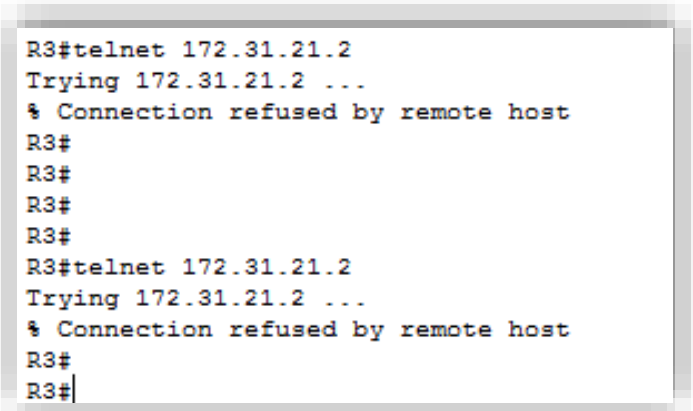
- Si hacemos TELNET al router MIAMI. desde el router BOGOTA. este es SATISFACTORIO, tal como lo indica nuestra ACL.



- Si hacemos TELNET desde un equipo de cualquiera de las VLAN.



- Si hacemos TELNET desde BUENOS AIRES..



- Aseguramos la red del tráfico de INTERNET, de este modo estas no son posibles.

- En MIAMI.

Access-list 101 permit tcp any host 209.165.229.230 eq www

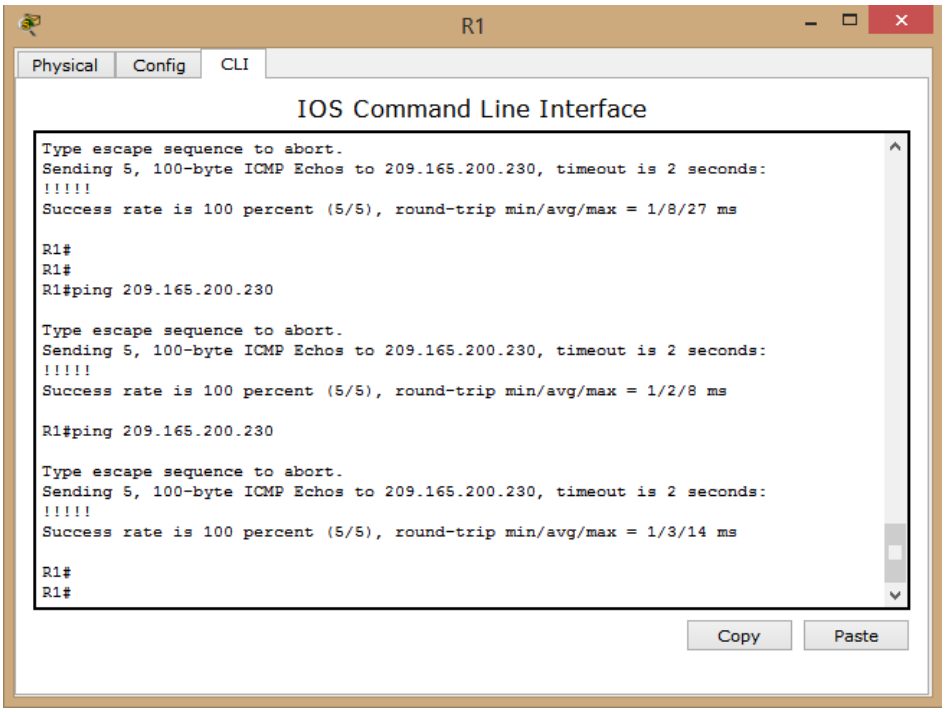
- Prevenir el tráfico desde INTERNET que no puedan hacer PING a la red interna

Access-list 101 permit icmp any any echo-reply

- Debemos aplicar las ACL a las interfaces adecuadas.

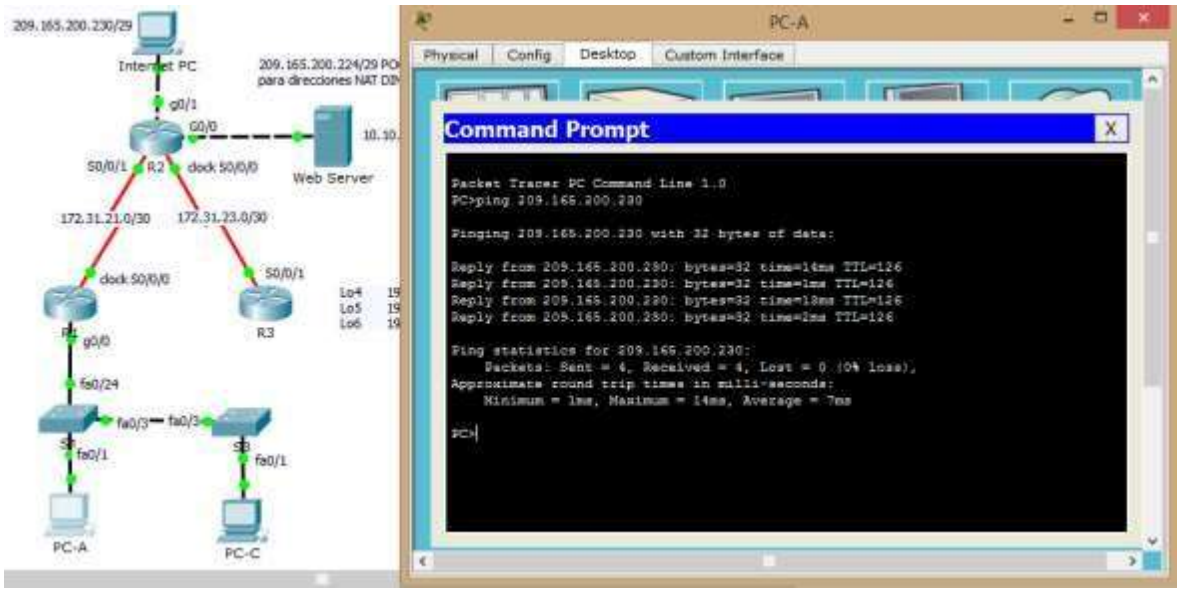
Interface g0/1
Ip Access-group 101 in Interface s0/0/0
Ip Access-group 101 out Interface s0/0/1
Ip Access-group 101 out Interface g0/0
Ip Access-group 101 out

- Procedemos a verificar que las ACL están funcionando

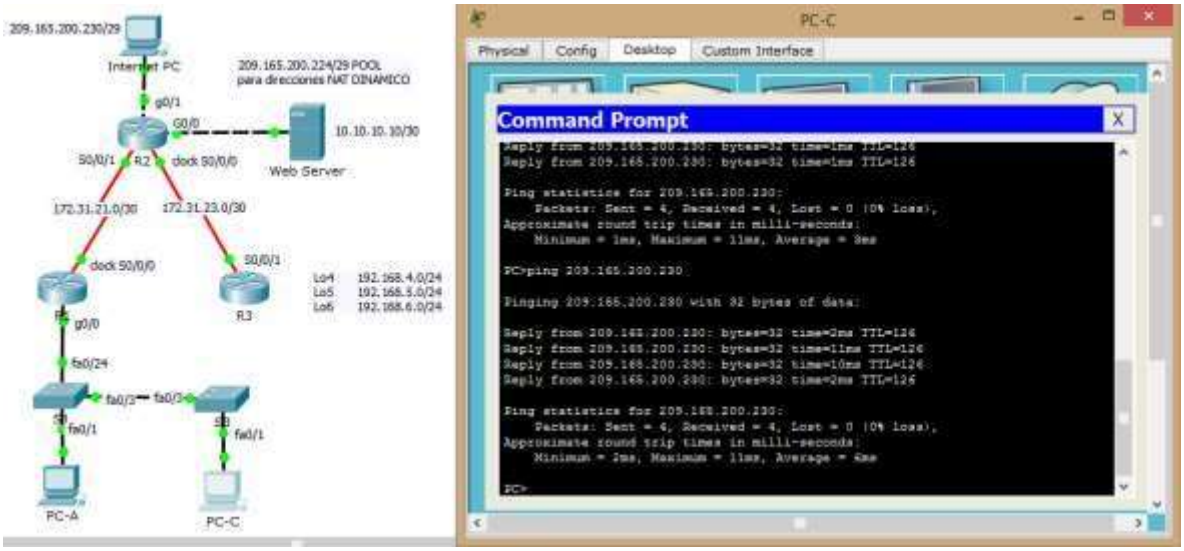


- Vamos a realizar el mismo proceso, pero en este CASO desde los PC de las VLAN.

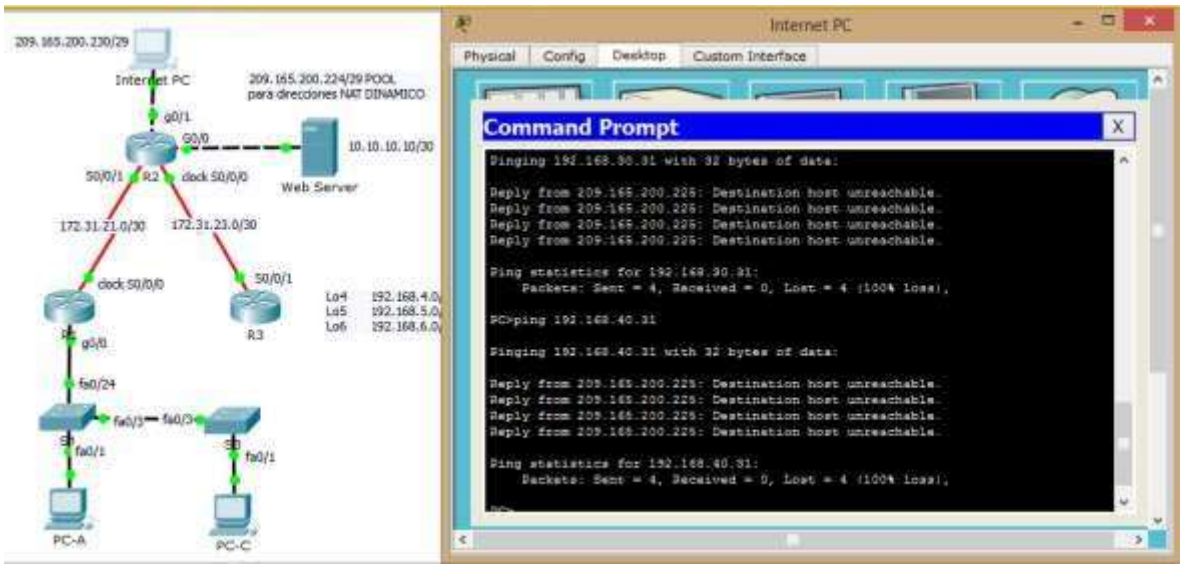
- Desde la PC-A



- Desde la PC-C



- PING desde PC INTERNET hacia la PC-A y la PC-C


209.165.200.230/29
Internet PC
209.165.200.224/29 POOL
para direcciones NAT DINAMICO
g0/1
S0/0
10.10.10.10/30
Web Server
S0/0/1
R2
clock S0/0/0
172.31.21.0/30
172.31.23.0/30
clock S0/0/0
S0/0/1
R3
Lo4
Lo5
Lo6
g0/0
fa0/24
fa0/3
fa0/3
fa0/1
fa0/1
PC-A
PC-C
Internet PC
Physical
Config
Desktop
Custom Interface
Command Prompt
X
Pinging 192.168.30.31 with 32 bytes of data:
Reply from 209.165.200.225: Destination host unreachable.
Reply from 209.165.200.225: Destination host unreachable.
Reply from 209.165.200.225: Destination host unreachable.
Reply from 209.165.200.225: Destination host unreachable.
Ping statistics for 192.168.30.31:
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
PC>ping 192.168.40.31
Pinging 192.168.40.31 with 32 bytes of data:
Reply from 209.165.200.225: Destination host unreachable.
Reply from 209.165.200.225: Destination host unreachable.
Reply from 209.165.200.225: Destination host unreachable.
Reply from 209.165.200.225: Destination host unreachable.
Ping statistics for 192.168.40.31:
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

CONCLUSIÓNES

- Lo importante para desarrollar confianza en nosotros para en la implementación de este tipo de propuestas es practicar mucho.
- El protocolo DHCP está diseñado fundamentalmente para ahorrar tiempo gestionando direcciones IP en una red grande. El servicio DHCP se encuentra activo en un servidor que concentra todas las direcciones IP de la red.
- Los usuarios al usar DHCP, este agiliza y enseña toda la información que necesita para funcionar incluso dirección IP, el servidor de inicio y la información de configuración de red. Ya que las solicitudes DHCP pueden enviar por subredes, se podría contrarrestar el uso de servidores de inicio en la red cuando se utiliza el inicio de red DHCP
- Cada vez más debemos fortalecer nuestros conocimientos profundizando constantemente en los cambios que cada uno de ellos ha tenido.
- En todo el diseño de la red aplicamos VLSM gracias al cual el desperdicio de direcciones IP es mínimo y ajustado realmente a las necesidades Ip de cada una de las subredes.
- Bueno, definitivamente todo lo trabajado y el material didáctico utilizado en el transcurso del diplomado han sido de vital importancia para llegar donde estamos, todo lo hemos utilizado en este punto del curso, los cuadros, los comandos, etc.
- El diseño que realice para la empresa funciona a la perfección, se realizaron todas las pruebas de caso y todas arrojan resultado favorable.
- La vida que tenemos está muy relacionada con la tecnología, esta ocupa parte fundamental dentro de nuestras vidas tanto familiares como laborales.
- Ya no tenemos barreras ni de tiempo ni mucho menos de espacio, podemos acceder a los que queramos en el lugar donde se encuentre.
- Veo con mucha seguridad que el Diplomado me ha aportado mucho para mi vida laboral.
- Veo que la temática desarrollada ha ayudado a mi formación integral.
- He desarrollado este proyecto desde cero y me agrada el grado de conocimiento que tengo relacionado a los dispositivos y su configuración.

BIBLIOGRAFÍA Y WEBGRAFIA.

- http://www.cisco.com/
- CISCO. (2014). OSPF de una sola área. Principios de Enrutamiento y Conmutación.

Recuperado:
- https://static-courseassets.s3.amazonaws.com/RSE50ES/module8/index.html#8.0.1.1
- MODULO CISCO