

**Curso de profundización cisco (diseño e implementación de soluciones integradas lan – wan)**



**Juan Carlos Sepulveda Daza**  
**Codigo : 7185224**  
**Grupo: 203092\_17**

**Universidad nacional abierta y a distancia unad-tunja**  
**Facultad de ciencias basicas tecnologia e ingenieria**  
**Junio de 2018**

**Curso de profundización cisco (diseño e implementación de soluciones integradas lan – wan)**

**Juan Carlos Sepulveda Daza**  
**Código : 7185224**  
**Grupo: 203092\_17**

**Tutor:**

**Giovanni Alberto Bracho**

**Universidad nacional abierta y a distancia unad-tunja**  
**Facultad de ciencias básicas tecnología e ingeniería**  
**Junio del 2018**

## Introduccion

A medida que avanzan los últimos años de este siglo, se ha dado un rápido avance en cuanto a procesamiento de información y examen de forma habitual de la misma. Por eso Como profesionales es vital que cada día nos actualicemos y profundicemos mucho más los conocimientos que tenemos, puesto que cada día salen cosas diferentes y debemos estar a la vanguardia dentro de la tecnología de nuestro campo. El presente curso lo que busca es eso, que profundizar en el campo de las redes, de la mano de una de las empresas líderes en las telecomunicaciones, aspecto que favorecerá mucho nuestra vida profesional.

El desarrollo de una red para la empresa de TECNOLOGÍA nos permitirá que apliquemos toda la temática desarrollada y verificar nuestro grado de asimilación de la temática que abordamos a lo largo del mismo. Tenemos, que exigimos y demostramos que podemos solucionar cualquier tipo de inconveniente que se nos presente no importando el grado de dificultad del mismo.

CISCO es una academia muy importante, ya que todos sus estudiantes están acompañados constantemente por un material de primera mano y excelente en contenido y acompañamiento, aprovechemos cada uno de sus aspectos para favorecer nuestra formación integral.

Son muchos los temas que se han desarrollado, pero lo primordial es reconocer que todo el proceso de direccionamiento y de intercambio de información entre las diferentes redes solo es posible gracias a la intervención de los routers, por lo cual hemos profundizado en los protocolos de enrutamiento los cuales son las reglas que permiten este intercambio y además todo lo relacionado a VLSM que permite un uso eficiente de cada una de las direcciones IP.

## 2. Objetivos

### 2.1 Objetivo general

Poner en práctica cada uno de los temas desarrollados en el módulo, diseñando la configuración de Red de la empresa de TECNOLOGÍA y el esquema de enrutamiento, utilizando herramientas de simulación para alcanzar el objetivo.

### 2.2 Objetivos específicos

- ✓ Conocer el manejo de la herramienta de simulación de redes PACKET TRACER. gracias al cual podremos realizar el montaje del ejercicio práctico para la empresa.
- ✓ Diseñar y documentar un esquema de direccionamiento según los requisitos.
- ✓ Diferenciar los modos como trabajan los diferentes protocolos de enrutamiento con clase y sin clase identificando las ventajas y desventajas de cada uno.
- ✓ Aplicar VLSM, esto con el fin de hacer un uso eficiente de las direcciones IP y que el desperdicio sea el menor posible.
- ✓ Verificar la conectividad entre todos los dispositivos de la topología de la red.
- ✓ Comprender los pasos lógicos necesarios para el desarrollo e implementación de una red compleja
- ✓ Aplicar el concepto de redistribución de rutas entre los diferentes protocolos de enrutamiento.

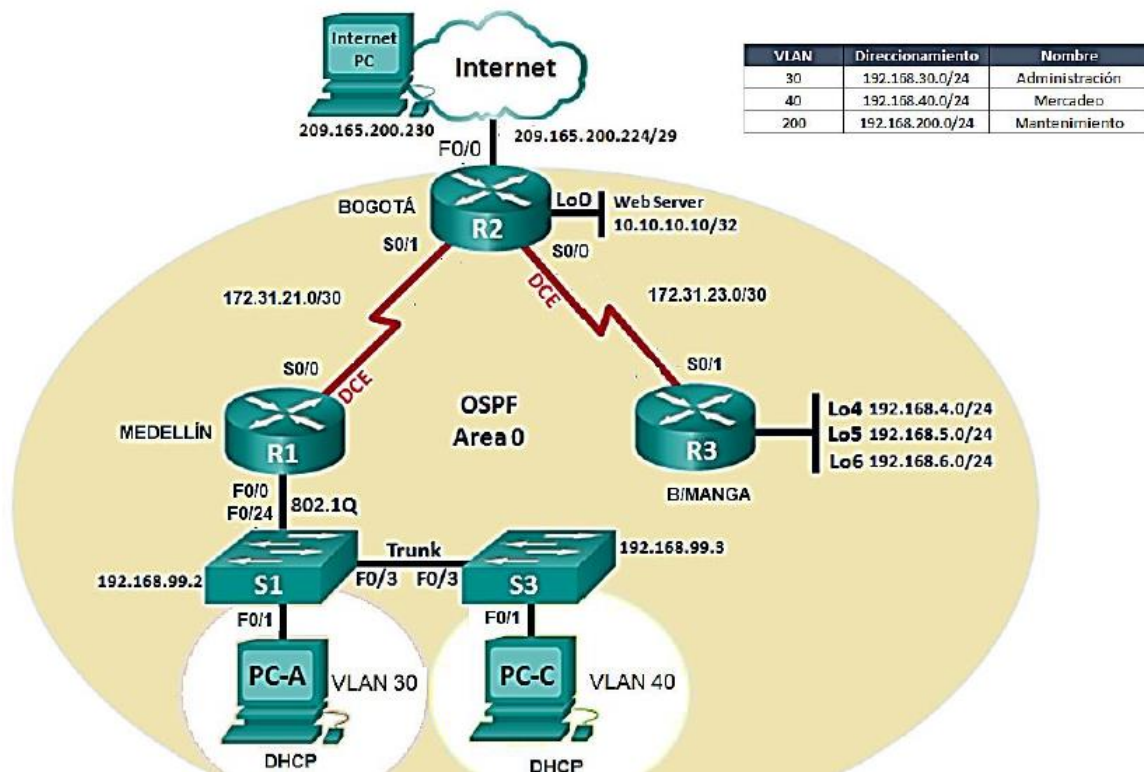
## Seminario de profundización en redes lan – wan cisco

### Descripción del escenario propuesto para la prueba de habilidades

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

### Topología de red

#### Topología de red



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 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

## 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 R1 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 R2 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 R1 o R3 hacia R2.
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.
13. Verificar procesos de comunicación y redireccionamiento de tráfico en los routers mediante el uso de Ping y Traceroute.

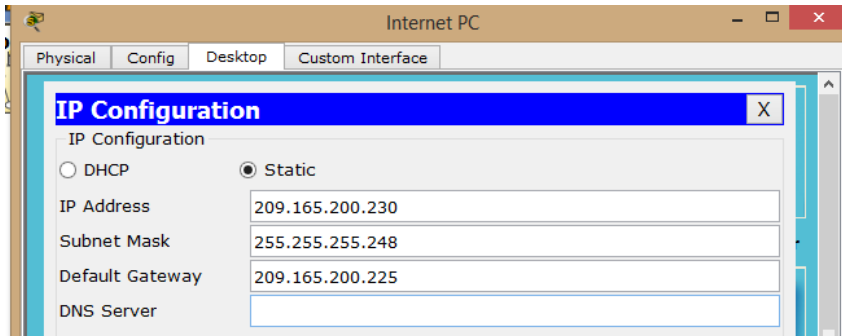
## DESARROLLO DE LA GUIA – EXAMEN DE HABILIDADES PRÁCTICAS.

### • CONFIGURAMOS LA IP INTERNET.

IP: 209.165.200.230

Mask: 255.255.255.248

Gateway: 209.165.200.225



### • Configuramos R1.

No ip domain lookup

Hostname R1

Enable secret class

Line console 0

    Password cisco

    Login

Line vty 0 4

    Password class

    Login

Service password encryption

Banner motd & **PROHIBIDO EL INGRESO.**

Universidad Abierta y  
Nacional a Distancia

UNAD

## IOS Command Line Interface

```
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#No ip domain lookup
Router(config)#Hostname R1
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
R1(config-line)#Service password encryption
R1(config-line)#
% Invalid input detected at '^' marker.

R1(config-line)#service?
% Unrecognized command
R1(config-line)#exit
R1(config)#Service password encryption
R1(config)#
% Invalid input detected at '^' marker.

R1(config)#service pass?
password-encryption
R1(config)#service pass
R1(config)#service password-encryption
R1(config)#bann?
banner
R1(config)#banner-
R1(config)#banner-?
% Unrecognized command
R1(config)#banner-mo?
% Unrecognized command
R1(config)#banner mo?
motd
R1(config)#banner mo
R1(config)#banner motd ?
LINE c banner-text c, where 'c' is a delimiting character
R1(config)#banner motd &PROHIBIDO EL INGRESO
Enter TEXT message. End with the character '&'.

```

Configure interface s0/0/0

Description **CONECTA CON R2.**

Ip address 172.31.21.1 255.255.255.252

Clock rate 128000

No shutdown

- Configuramos una ruta por defecto

Ip route 0.0.0.0 0.0.0.0 s0/0/0

```
R1#
R1#enable
R1#
R1#
R1#configure interface
R1#
% Invalid input detected at '^' marker.

R1#config
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#
R1(config)#interface s0/0/0
R1(config-if)#Description conecta con R2.
R1(config-if)#Description CONECTA CON R2.
R1(config-if)#172.31.21.1 255.255.255.252
R1(config-if)#
% Invalid input detected at '^' marker.

R1(config-if)#Ip address 172.31.21.1 255.255.255.252
R1(config-if)#clock rate 128000
R1(config-if)#no shutdown

%LINK-5-CHANGED: Interface Serial10/0/0, changed state to down
R1(config-if)#
R1(config-if)#ip route 0.0.0.0 0.0.0.0 s0/0/0
%Default route without gateway, if not a point-to-point interface, may impact
performance
R1(config-if)#
R1(config)#
R1(config)#

```

- **Configuramos R2.**

No ip domain-lookup

Hostname R2



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 ACCESO**

```
Interface s0/0/1
Description CONEXION CON R1
Ip address 172.31.21.2 255.255.255.252
no shutdown
```

```
interface s0/0/0
description CONEXION CON R3
ip address 172.31.23.1 255.255.255.252
clock rate 128000
no shutdown
```

```
interface g0/1 "es la simulación de INTERNET"
description CONEXION A INTERNET
ip address 209.165.200.225 255.255.255.248
no shutdown
```

- como siguiente paso debemos configurara el servicios WEB

```
interface g0/0
ip address 10.10.10.1 255.255.255.0
no shutdown
description CONEXIÓN CON WEB SERVER
```

- configuramos el servidor web

```
ip address 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.
```

```

R2#show ip interface brief
Interface                IP-Address      OK? Method Status  Protocol
GigabitEthernet0/0      10.10.10.1      YES manual up      up
GigabitEthernet0/1      209.165.200.225 YES manual up      up
Serial0/0/0              172.31.23.1     YES manual up      up
Serial0/0/1              172.31.21.2     YES manual up      up

```

- **Configuramos el ROUTER 3.**

No ip domain-lookup

Hostname R3

Enable secret class

Line console 0

    Password cisco

    login

Line vty 0 4

    Password cisco

    Login

Service password-encryption

Banner motd & **PROHIBIDO EL INGRESO**

Interface **s0/0/1**

Description **CONEXIÓN CON R2**

Ip address 172.31.23.2 255.255.255.252

No shutdown

- Vamos a crear las interfaces loopback

Interface loopback 4

Ip address 192.168.4.1 255.255.255.0

No shutdown

Interface loopback 5

Ip address 192.168.5.1 255.255.255.0

No shutdown

Interface loopback 6

Ip address 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

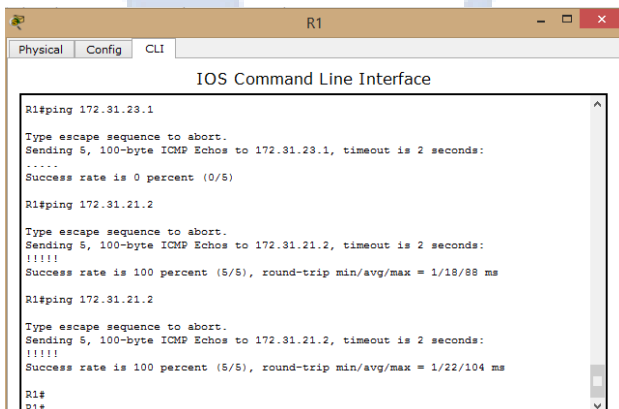
- **Configuramos switch 1**

```
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
```

- **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 ingreso
```

- En este punto debemos verificar la conectividad de los dispositivos.



The screenshot shows a terminal window titled 'R1' with tabs for 'Physical', 'Config', and 'CLI'. The main content is the 'IOS Command Line Interface' where the following commands and outputs are visible:

```
R1#ping 172.31.23.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.31.23.1, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
R1#ping 172.31.21.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.31.21.2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/18/88 ms
R1#ping 172.31.21.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.31.21.2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/22/104 ms
R1#
R1#
```

```

R2
-----
Physical Config CLI
IOS Command Line Interface
FastEthernet0/1/3 unassigned YES unset up down
Vlan1 unassigned YES unset administratively down down
R2#
R2#
R2#
R2#ping 172.31.23.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.31.23.2, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/71/352 ms
R2#ping 172.31.23.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.31.23.2, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/14/70 ms
R2#
R2#

```

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

```

S1#show 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
1002 fddi-default           act/unsup
1003 token-ring-default    act/unsup
1004 fddinet-default       act/unsup
1005 trnet-default        act/unsup

```

- 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

```



```

S1(config)#
S1(config)#
S1(config)#
S1(config)#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)#interfave vlan 200
S1(config-vlan)#
% Invalid input detected at '^' marker.
S1(config-vlan)#interface vlan 200
S1(config-if)#
%LINK-5-CHANGED: Interface Vlan200, changed state to up
S1(config-if)#Ip address 192.168.200.2 255.255.255.0
S1(config-if)#no shutdown
S1(config-if)#Ip default-Gateway 192.168.200.1
S1(config)#

```

- Forzamos el trunking 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

```

S1(config-if)#ip address 192.168.200.2 255.255.255.0
S1(config-if)#no shutdown
S1(config-if)#Ip default-Gateway 192.168.200.1
S1(config-if)#
S1(config)#
S1(config)#
S1(config)#interface f0/3
S1(config-if)#Switchport mode trunk

S1(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to
down
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to
up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan200, changed state to up

S1(config-if)#Switchport trunk native vlan 1
S1(config-if)#
S1(config-if)#exit
S1(config)#Interface f0/24
S1(config-if)#Switchport mode trunk
S1(config-if)#Switchport trunk native vlan 1
S1(config-if)#

```

- Configuramos todos los 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

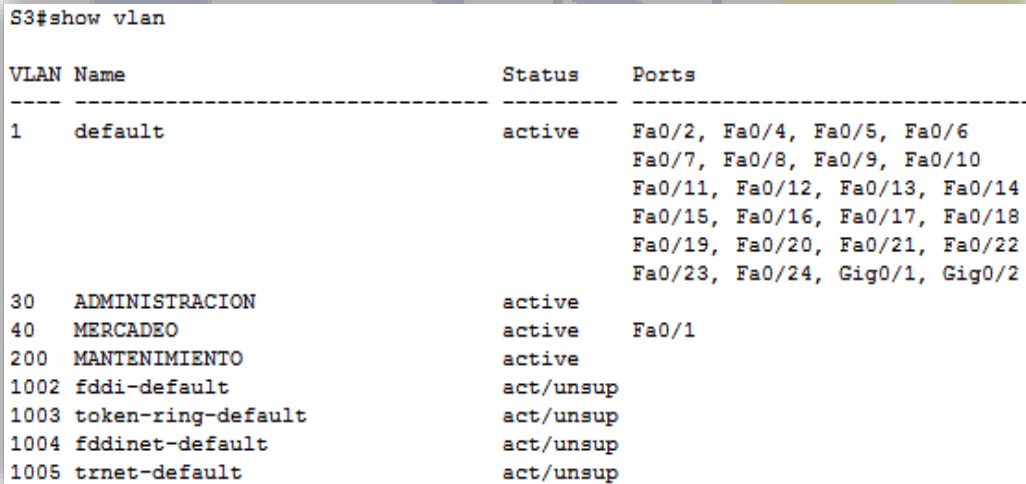
Interface range fa0/2, fa0/4-23, g0/1-2  
Shutdown

- **Configuramos el S3**

VLAN 30  
Name ADMINISTRACION

VLAN 40  
Name MERCADEO

VLAN 200  
Name MANTENIMIENTO



```
S3#show 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	
1002	fddi-default	act/unsup	
1003	token-ring-default	act/unsup	
1004	fddinet-default	act/unsup	
1005	trnet-default	act/unsup	

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

```
S3
Physical Config CLI
IOS Command Line Interface
S3>enable
Password:
S3#
S3#config
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line. End with CNTRL/Z.
S3(config)#vlan 30
S3(config-vlan)#name ADMINISTRACION
S3(config-vlan)#vlan 40
S3(config-vlan)#name MERCADEO
S3(config-vlan)#vlan 200
S3(config-vlan)#name MANTENIMIENTO
S3(config-vlan)#
S3(config-vlan)#interface VLAN 200
S3(config-if)#
%LINK-5-CHANGED: Interface Vlan200, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan200, changed state to up
S3(config-if)#Ip address 192.168.200.3 255.255.255.0
S3(config-if)#no shutdown
S3(config-if)#Ip default-Gateway 192.168.200.1
S3(config)#
S3(config)#
```

- 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 utilizemos

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

```
S3
Physical Config CLI
IOS Command Line Interface
S3#config
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line. End with CNTL/Z.
S3(config)#vlan 30
S3(config-vlan)#name ADMINISTRACION
S3(config-vlan)#vlan 40
S3(config-vlan)#name MERCADEO
S3(config-vlan)#vlan 200
S3(config-vlan)#name MANTENIMIENTO
S3(config-vlan)#
S3(config-vlan)#interface VLAN 200
S3(config-if)#
%LINK-5-CHANGED: Interface Vlan200, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan200, changed state to up

S3(config-if)#Ip address 192.168.200.3 255.255.255.0
S3(config-if)#no shutdown
S3(config-if)#Ip default-Gateway 192.168.200.1
S3(config)#
S3(config)#
S3(config)#Interface fa0/3
S3(config-if)#Switchport mode trunk
S3(config-if)#Switchport trunk native vlan 1
S3(config-if)#
S3(config-if)#Interface range fa0/2, fa0/4-24, g0/1-2
S3(config-if-range)#Switchport mode Access
S3(config-if-range)#exit
S3(config)#Interface fa0/1
S3(config-if)#Switchport mode access
S3(config-if)#Swirchport Access VLAN 40
S3(config-if)#Swirchport Access VLAN 40
^
% Invalid input detected at '^' marker.

S3(config-if)#Switchport Access VLAN 40
S3(config-if)#
S3(config-if)#Interface range fa0/2, fa0/4-24, g0/1-2
S3(config-if-range)#shutdown
```

- Configuramos el R1, procedemos a configurar las subinterfaces

```
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
```



```
R1
Physical Config CLI
IOS Command Line Interface
R1#
R1#config
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#interface g0/0.30
R1(config-subif)#description ADMINISTRACION LAN
R1(config-subif)#encapsulation dot1q 30
R1(config-subif)#ip address 192.168.30.1 255.255.255.0
R1(config-subif)#no shutdown
R1(config-subif)#
R1(config-subif)#interface g0/0.40
R1(config-subif)#description MERCADEO LAN
R1(config-subif)#encapsulation dot1q 40
R1(config-subif)#encapsulation dot1q 40
R1(config-subif)#ip address 192.168.40.1 255.255.255.0
R1(config-subif)#
R1(config-subif)#interface g0/0.200
R1(config-subif)#description MANTENIMIENTO LAN
R1(config-subif)#encapsulation dot1q 200
R1(config-subif)#ip address 192.168.200.1 255.255.255.0
R1(config-subif)#
R1(config-subif)#exit
R1(config)#interface g0/0
R1(config-if)#no shutdown

R1(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up
%LINK-5-CHANGED: Interface GigabitEthernet0/0.30, changed state to up
%LINK-5-CHANGED: Interface GigabitEthernet0/0.40, changed state to up
%LINK-5-CHANGED: Interface GigabitEthernet0/0.200, changed state to up
R1(config-if)#
```

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

Todos estos comandos deben ser satisfactorios

PING desde el SWITCH S1

- Ping 192.168.200.1
- Ping 192.168.30.1

```
S1
Physical Config CLI
IOS Command Line Interface
Sending 5, 100-byte ICMP Echos to 192.168.30.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/2 ms
S1#
S1#
S1#
S1#
S1#ping 192.168.200.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.200.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/2 ms
S1#ping 192.168.30.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.30.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/2 ms
S1#
S1#
```

PING desde el SWITCH S3

- Ping 192.168.200.1
- Ping 192.168.40.1

```
S3
Physical Config CLI
IOS Command Line Interface
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/2 ms
S3#
S3#
S3#
S3#
S3#
S3#
S3#ping 192.168.200.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.200.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/21/103 ms
S3#ping 192.168.40.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.40.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/1 ms
S3#
S3#
```

- Procedemos a configurar OSPF V2 en el router R1

Router ospf 1

Router-id 1.1.1.1

```
Network 172.31.21.0 0.0.0.3 area 0
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 interface LAN como pasivas

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

```
R1
Physical Config CLI
IOS Command Line Interface
% Invalid input detected at '^' marker.
R1#show ip route connected
C 172.31.21.0/30 is directly connected, Serial0/0/0
C 192.168.30.0/24 is directly connected, GigabitEthernet0/0.30
C 192.168.40.0/24 is directly connected, GigabitEthernet0/0.40
C 192.168.200.0/24 is directly connected, GigabitEthernet0/0.200
R1#
R1#
R1#
R1#config
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#Router ospf 1
R1(config-router)#Router-id 1.1.1.1
R1(config-router)#Network 172.31.21.0 0.0.0.3 area 0
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
R1(config-router)#
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-router)#
R1(config-router)#
R1(config-router)#
```

- Cambiamos el ancho de banda de las interface seriales

```
Interface s0/0/0  
Bandwidth 128  
Ip ospf cost 7500
```

- Configuramos OPSF V2 en el router R2

```
Router ospf 1  
Router-id 2.2.2.2  
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 128  
Interface s0/0/1  
Bandwidth 128
```

Ajustar la métrica de serial s0/0/0

```
Interface s0/0/0  
Ip ospf cost 7500
```

Universidad Abierta y  
Nacional a Distancia



```
R2
Physical Config CLI
IOS Command Line Interface
R2>enable
Password:
R2#
R2#
R2#show ip route connected
C 10.10.10.0/24 is directly connected, GigabitEthernet0/0
C 172.31.21.0/30 is directly connected, Serial0/0/1
C 172.31.23.0/30 is directly connected, Serial0/0/0
C 209.165.200.224/29 is directly connected, GigabitEthernet0/1
R2#
R2#Router ospf 1
^
! Invalid input detected at '^' marker.

R2#config
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#Router ospf 1
R2(config-router)#Router-id 2.2.2.2
R2(config-router)#Network 172.31.21.0 0.0.0.3 area 0
R2(config-router)#
13:40:51: %OSPF-5-ADJCHG: Process 1, Nbr 1.1.1.1 on Serial0/0/1 from LOADING to FULL,
Loading Done
Network 172.31.23.0 0.0.0.3 area 0
R2(config-router)#Network 10.10.10.0 0.0.0.255 area 0
R2(config-router)#
R2(config-router)#
R2(config-router)#Passive-interface g0/0
R2(config-router)#
R2(config-router)#exit
R2(config)#Interface s0/0/0
R2(config-if)#Bandwidth 128
R2(config-if)#Interface s0/0/1
R2(config-if)#Bandwidth 128
R2(config-if)#Interface s0/0/0
R2(config-if)#Ip ospf cost 7500
R2(config-if)#
```

d Abierta y  
a Distancia

- Configuramos OPSF V2 en el router R3

Router ospf 1

Router-id 3.3.3.3

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 128

```

R3
Physical Config CLI
IOS Command Line Interface
R3#
R3#
R3#show ip route connected
C 172.31.23.0/30 is directly connected, Serial0/0/1
C 192.168.4.0/24 is directly connected, Loopback4
C 192.168.5.0/24 is directly connected, Loopback5
C 192.168.6.0/24 is directly connected, Loopback6
R3#
R3#config
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line. End with CNTRL/Z.
R3(config)#
R3(config)#Router ospf 1
R3(config-router)#Router-id 3.3.3.3
R3(config-router)#Network 172.31.23.0 0.0.0.3 area 0
R3(config-router)#Network 922.168.4.0 0.0.3.255 area 0
^
% Invalid input detected at '^' marker.

R3(config-router)#
13:45:27: %OSPF-5-ADJCHG: Process 1, Nbr 2.2.2.2 on Serial0/0/1 from LOADING to FULL, Loading Done

R3(config-router)#Network 192.168.4.0 0.0.3.255 area 0
R3(config-router)#Passive-interface lo4
R3(config-router)#Passive-interface lo5
R3(config-router)#Passive-interface lo6
R3(config-router)#exit
R3(config)#Interface s0/0/1
^
% Invalid input detected at '^' marker.

R3(config)#Interface s0/0/1
R3(config-if)#Bandwidth 128
R3(config-if)#

```

Abierta y a Distancia

**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



R2#Show ip ospf neighbor

Neighbor ID	Pri	State	Dead Time	Address	Interface
1.1.1.1	0	FULL/ -	00:00:32	172.31.21.1	Serial0/0/1
3.3.3.3	0	FULL/ -	00:00:36	172.31.23.2	Serial0/0/0

R2#

R1#show ip ospf neighbor

Neighbor ID	Pri	State	Dead Time	Address	Interface
2.2.2.2	0	FULL/ -	00:00:31	172.31.21.2	Serial0/0/0

R1#

R1#

R3#Show ip ospf neighbor

Neighbor ID	Pri	State	Dead Time	Address	Interface
2.2.2.2	0	FULL/ -	00:00:36	172.31.23.1	Serial0/0/0

R3#

- Show ip route ospf

```
R3#Show ip route ospf
 10.0.0.0/24 is subnetted, 1 subnets
O   10.10.10.0 [110/782] via 172.31.23.1, 00:04:08, Serial0/0/1
 172.31.0.0/16 is variably subnetted, 3 subnets, 2 masks
O   172.31.21.0 [110/1562] via 172.31.23.1, 00:04:08, Serial0/0/1
O   192.168.30.0 [110/1563] via 172.31.23.1, 00:04:08, Serial0/0/1
O   192.168.40.0 [110/1563] via 172.31.23.1, 00:04:08, Serial0/0/1
O   192.168.200.0 [110/1563] via 172.31.23.1, 00:04:08, Serial0/0/1
R3#
```

```
R2#Show ip route ospf
 192.168.4.0/32 is subnetted, 1 subnets
O   192.168.4.1 [110/7501] via 172.31.23.2, 00:05:09, Serial0/0/0
 192.168.5.0/32 is subnetted, 1 subnets
O   192.168.5.1 [110/7501] via 172.31.23.2, 00:04:59, Serial0/0/0
 192.168.6.0/32 is subnetted, 1 subnets
O   192.168.6.1 [110/7501] via 172.31.23.2, 00:04:59, Serial0/0/0
O   192.168.30.0 [110/782] via 172.31.21.1, 00:09:00, Serial0/0/1
O   192.168.40.0 [110/782] via 172.31.21.1, 00:09:00, Serial0/0/1
O   192.168.200.0 [110/782] via 172.31.21.1, 00:09:00, Serial0/0/1
R2#
R2#
```

```
R1#Show ip route ospf
 10.0.0.0/24 is subnetted, 1 subnets
O   10.10.10.0 [110/7501] via 172.31.21.2, 00:10:38, Serial0/0/0
 172.31.0.0/16 is variably subnetted, 3 subnets, 2 masks
O   172.31.23.0 [110/15000] via 172.31.21.2, 00:08:56, Serial0/0/0
O   192.168.4.0/32 is subnetted, 1 subnets
O   192.168.4.1 [110/15001] via 172.31.21.2, 00:05:32, Serial0/0/0
O   192.168.5.0/32 is subnetted, 1 subnets
O   192.168.5.1 [110/15001] via 172.31.21.2, 00:05:22, Serial0/0/0
O   192.168.6.0/32 is subnetted, 1 subnets
O   192.168.6.1 [110/15001] via 172.31.21.2, 00:05:22, Serial0/0/0
R1#
R1#
```

- Comando para verificar la configuración en ejecución
- show running-config

• Debemos implementar DHCP en el router R1.

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

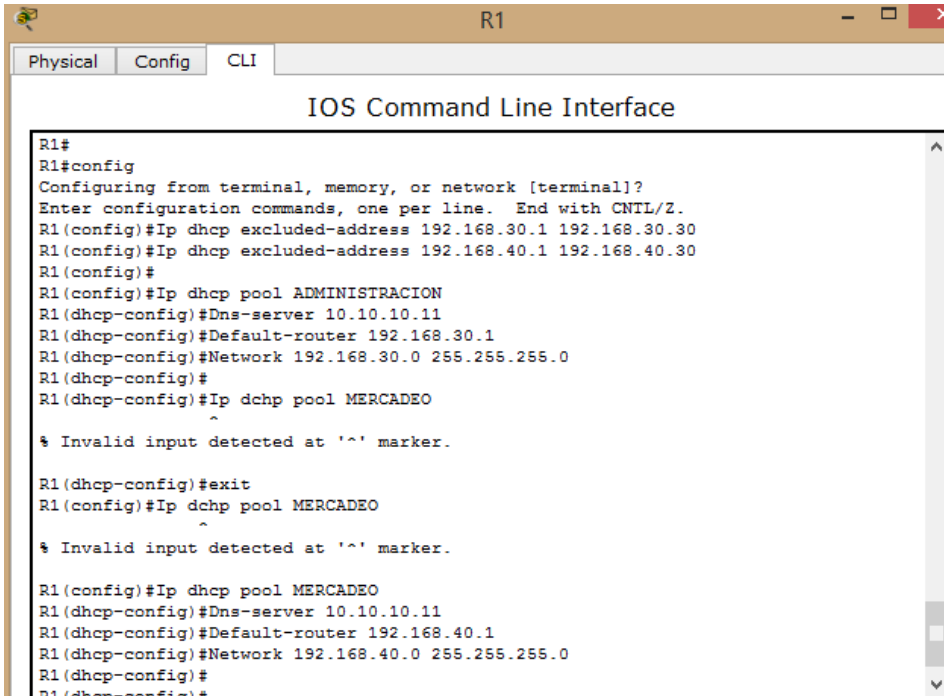
```
ip dhcp excluded-address 192.168.30.1 192.168.30.30
ip dhcp excluded-address 192.168.40.1 192.168.40.30
```

```
ip dhcp pool ADMINISTRACION
Dns-server 10.10.10.11
Default-router 192.168.30.1
Network 192.168.30.0 255.255.255.0
```

bierta y  
istancia

D

Ip dhcp pool **MERCADEO**  
Dns-server 10.10.10.11  
Default-router 192.168.40.1  
Network 192.168.40.0 255.255.255.0



```
R1#
R1#config
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#Ip dhcp excluded-address 192.168.30.1 192.168.30.30
R1(config)#Ip dhcp excluded-address 192.168.40.1 192.168.40.30
R1(config)#
R1(config)#Ip dhcp pool ADMINISTRACION
R1(dhcp-config)#Dns-server 10.10.10.11
R1(dhcp-config)#Default-router 192.168.30.1
R1(dhcp-config)#Network 192.168.30.0 255.255.255.0
R1(dhcp-config)#
R1(dhcp-config)#Ip dhcp pool MERCADEO
^
% Invalid input detected at '^' marker.
R1(dhcp-config)#exit
R1(config)#Ip dhcp pool MERCADEO
^
% Invalid input detected at '^' marker.
R1(config)#Ip dhcp pool MERCADEO
R1(dhcp-config)#Dns-server 10.10.10.11
R1(dhcp-config)#Default-router 192.168.40.1
R1(dhcp-config)#Network 192.168.40.0 255.255.255.0
R1(dhcp-config)#
R1(dhcp-config)#
```

Abierta y  
Distancia

10. Configurar NAT en R2 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 R1 o R3 hacia R2.

- Configuramos NAT ESTÁTICO y DINÁMICO en R2 con el fin de que los host puedan salir a internet.

User webuser privilege 15 secret cisco12345

- En este caso debemos usar el servidor web.

Ip nat inside source static 10.10.10.10 209.165.200.229

- Asignamos la interface interna y externa

Interface g0/1  
Ip nat outside

Interface g0/0  
Ip nat inside

```
R2 (config)#
R2 (config)#
R2 (config)#end
R2#
%SYS-5-CONFIG_I: Configured from console by console

R2#
R2#
R2#
R2#
R2#
R2#
R2#config
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line. End with CNTRL/Z.
R2 (config)#User webuser privilege 15 secret cisco12345
R2 (config)#Ip nat inside source static 10.10.10.10 209.165.200.229
R2 (config)#interface g0/1
R2 (config-if)#Ip nat outside
R2 (config-if)#Interface g0/0
R2 (config-if)#Ip nat inside
R2 (config-if)#
R2 (config-if)#
```

- 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 R1 – pero la traducción se hace en R2.

### 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 R3 tambien 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

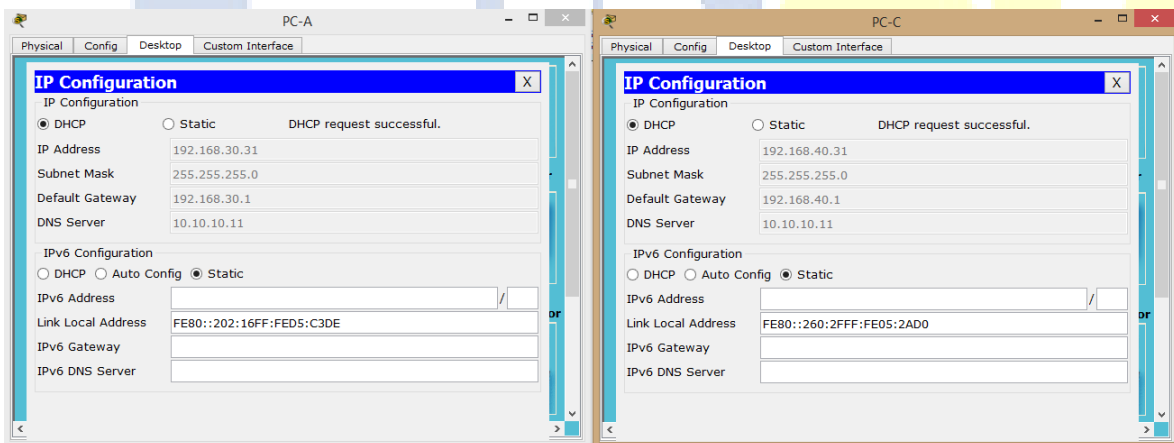
- Definimos la traducción NAT dinamico

Ip nat inside source list 1 pool INTERNET

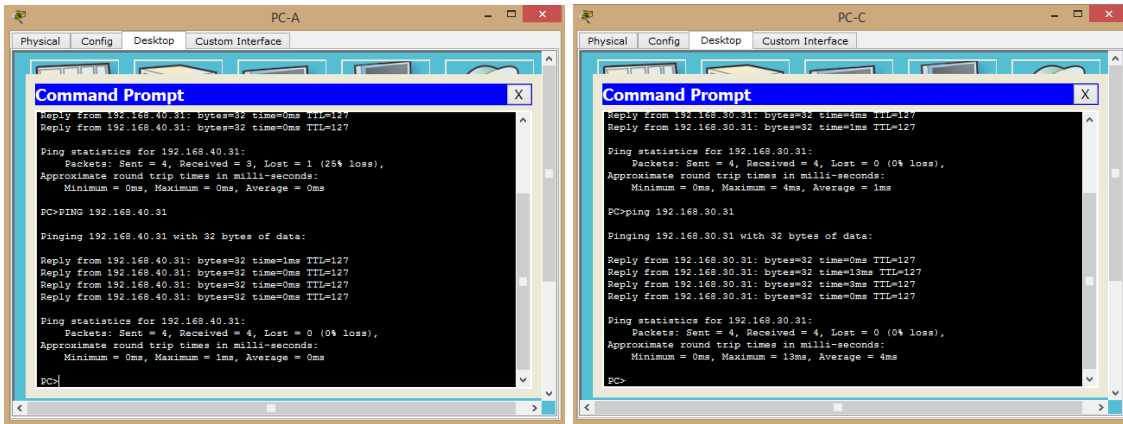


```
R2#
R2#config
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#User webuser privilege 15 secret cisco12345
R2(config)#Ip nat inside source static 10.10.10.10 209.165.200.229
R2(config)#interface g0/1
R2(config-if)#Ip nat outside
R2(config-if)#Interface g0/0
R2(config-if)#Ip nat inside
R2(config-if)#
R2(config-if)#EXIT
R2(config)#
R2(config)#
R2(config)#
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)#
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
R2(config)#
R2(config)#
```

- Procedemos a verificar lo hecho hasta este momento.



- Ping entre PC-A y PC-C



- Configurar y verificar las ACL en el router R2 en la cual solo le damos acceso al router R1.

- Configuramos una ACL que me permita que solo R1 pueda hacer TELNET a R2.

Ip Access-list standard **ADMIN-MANTENIMIENTO**  
Permit host 172.31.21.1

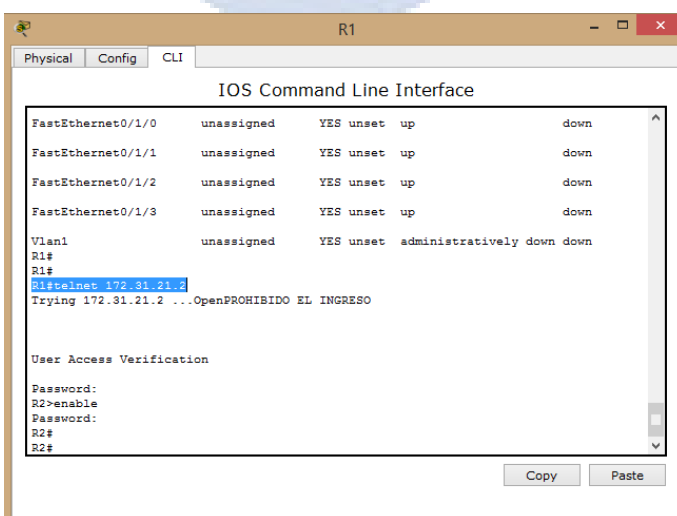
- Ahora si debemos aplicar la ACL nombrada a la línea VTY

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 R1 este es satisfactorio, si lo hacemos desde cualquier otro equipo este no puede ser posible.

- Si hacemos TELNET al router R2 desde el router R1 este es SATISFACTORIO, tal como lo indica nuestra ACL.



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

```
PC>
PC>
PC>telnet 172.31.21.2
Trying 172.31.21.2 ...
% Connection refused by remote host
PC>
PC>
```

- Si hacemos TELNET desde R3.

```
R3#telnet 172.31.21.2
Trying 172.31.21.2 ...
% Connection refused by remote host
R3#
```

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

- En R2

```
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

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 209.165.200.230, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/8/27 ms

R1#
R1#
R1#ping 209.165.200.230

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 209.165.200.230, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/8 ms

R1#ping 209.165.200.230

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 209.165.200.230, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/3/14 ms

R1#
R1#
```

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

```
PC-A
Physical Config Desktop Custom Interface
Command Prompt
Packet Tracer PC Command Line 1.0
PC>ping 209.165.200.230

Pinging 209.165.200.230 with 32 bytes of data:

Reply from 209.165.200.230: bytes=32 time=14ms TTL=126
Reply from 209.165.200.230: bytes=32 time=1ms TTL=126
Reply from 209.165.200.230: bytes=32 time=13ms TTL=126
Reply from 209.165.200.230: bytes=32 time=2ms TTL=126

Ping statistics for 209.165.200.230:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 14ms, Average = 7ms

PC>|
```

- Desde la PC-C

```
PC-C
Physical Config Desktop Custom Interface
Command Prompt
Reply from 209.165.200.230: bytes=32 time=1ms TTL=126
Reply from 209.165.200.230: bytes=32 time=1ms TTL=126

Ping statistics for 209.165.200.230:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 11ms, Average = 3ms

PC>ping 209.165.200.230

Pinging 209.165.200.230 with 32 bytes of data:

Reply from 209.165.200.230: bytes=32 time=2ms TTL=126
Reply from 209.165.200.230: bytes=32 time=11ms TTL=126
Reply from 209.165.200.230: bytes=32 time=10ms TTL=126
Reply from 209.165.200.230: bytes=32 time=2ms TTL=126

Ping statistics for 209.165.200.230:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 11ms, Average = 6ms

PC>
```

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

```
Internet PC
Physical Config Desktop Custom Interface
Command Prompt
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),

PC>
```

### CONFIGURACION DE LOS ROUTERS.

En este paso indico cual es la configuración que se ingresó en cada uno de los routers.

- PING Y TRACERT.
- Comando PING.

Con este comando observamos si tenemos respuesta desde los diferentes puntos de la red.

- **Comando TRACERT.**

Con este comando adicionalmente verificamos la respuesta de los dispositivos intermedios entre los dos puntos.

**Verificación de funcionamiento con el simulador.**



## CONCLUSIONES

- La red que hemos diseñado funciona a la perfección, hay comunicación entre cada una de las partes de la red.
- Se nos presentaron inconvenientes pero con la ayuda del material de apoyo y de algunos comandos que el mismo nos suministra logramos corregir cada uno de ellos.
- PACKET TRACER se convirtió en nuestra mano derecha, todo lo podemos probar es este simulador una y otra vez hasta que todo funcione.
- Luego de desarrollar todas las actividades del diplomado en especial luego de haber desarrollado esta propuesta veo que el curso me ha servido de mucho, puedo emprender proyectos de este tipo sin ningún problema.
- Hemos realizado la documentación de nuestra red, aspecto que nos va a favorecer mucho a la hora de solucionar algún tipo de inconveniente.
- La red es CONVERGENTE.
- Veo que es posible unificar la temática que hemos desarrollado en la solución e implementación de una propuesta real.
- A todo el direccionamiento IP de la red aplicamos VLSM lo cual nos permitió optimizar el número de direcciones por cada subsistema de acuerdo a los requerimientos específicos.
- Se Comprendo muy bien el funcionamiento de cada uno de los protocolos de enrutamiento que intervienen en la red, gracias a ellos puedo optimizar su funcionamiento.
- Se documentó cada uno de los pasos realizados en la red y en cada uno de los dispositivos, lo cual permitió y posibilitó en gran medida el encontrar errores de configuración.
- Para una red grande es prácticamente imposible el manejo manual de las rutas para entrega de paquetes, en estos casos debemos utilizar el direccionamiento dinámico
- Nuestra red es totalmente funcional.

## BIBLIOGRAFÍA

- Módulo de estudio CNNA1 Exploration.
- Módulo de estudio CNNA1 Exploration.

