Curso de profundización CISCO (Diseño e implementación de soluciones integradas LAN – WAN)

Nombre: José Hernando Bejarano Chala
Código: 79316361
Grupo: 203092_42

Universidad Nacional Abierta y a Distancia UNAD Facultad de Ciencias Básicas Tecnología e Ingeniería CEAD La Dorada Caldas
Fecha: 27-05-2018.

Curso de profundización CISCO (Diseño e implementación de soluciones integradas LAN – WAN)

Nombre: José Hernando Bejarano Chala
Código: 79316361
Correo: Jjjs5679@hotmail.com
Grupo: 203092_42

Tutor:
Diego Edinson Ramírez

Universidad Nacional Abierta y a Distancia UNAD Facultad de Ciencias Básicas Tecnología e Ingeniería CEAD La Dorada Caldas
Fecha: 27-05-2018.

Tabla de contenido

Resumen (Abstract)

El presente producto, es la elaboración del trabajo de la prueba de habilidades práctica final del curso de profundización CISCO (Diseño e Implementación de soluciones integradas LAN – WAN), cumpliendo con el currículo programado por la plataforma virtual de Networking Academy y la UNAD
El trabajo se fundamentó en el proceso de aplicar las diferentes temáticas de VLSM (Variable Length Subnet Mask), las topologías y protocolos de enrutamientos que permitan la configuración de los diferentes dispositivos de una red informática.

El problema planteado en esta práctica es el estudio de un caso, específicamente el de configurar e interconectar entre sí cada uno de los dispositivos de las sucursales distribuidas de una empresa de Tecnología ubicada en tres ciudades, conforme con los lineamientos establecidos para el direccionamiento IP, protocolos de enrutamiento y demás aspectos que forman parte de la topología de red.

Lo anterior, con el propósito de alcanzar el mejor servicio y acelerar los procesos, avalando una adecuada dirección de la información requerida por la empresa.

La actividad se enmarco en los pasos y requerimientos descritos y solicitados en la guía de la práctica de habilidades del curso de CISCO, y el apoyo del conocimiento que ofrece las plataformas Cisco Networking Academy.y fuentes documentales de la UNAD
Igualmente en el diseño, elaboración de la red y el cumplimiento de los objetivos propuestos para la presente práctica de habilidades se utilizó como soporte tecnológico la herramienta informática Packet Tracer

Finalmente, se puede concluir que para el diseño del direccionamiento de redes la aplicación de VLSM es una ventaja si se quiere un ahorro considerable de direcciones IP. A través de la presente práctica se consiguió llevar a término el proceso de análisis de las redes, así como el montaje de las mismas dentro del simulador, facilitando y agilizando la práctica en lo que respecta a los comandos de configuración y verificación. De tal forma que se comprobó el funcionamiento de las redes y se logró observar que cada una de ellas son eficaces y coinciden.

Palabras Claves: Red, Configuración, Comandos, Router, Topología, Dirección, Protocolo, Interface, Dispositivo, Conectividad y Enrutamiento.

.

Introducción.

En el presente trabajo desarrollaré la red para la empresa de TECNOLOGÍA en el cual profundizaremos mucho más en todo el tema de las redes y las telecomunicaciones.

Lo más importante es que profundicemos en estos temas, que generemos en nosotros seguridad para la implementación de propuestas de este tipo y que mejoremos día a día.

El trabajo lo desarrollaré desde cero, el cual me permito conectar diferentes sucursales en 3 ciudades diferentes que permita la conexión entre estas diferentes ciudades. El desarrollo y la implementación lo hare paso a paso y documentando cada uno de ellos con el fin de ser lo más explicativos posible. Lo importante es que tengamos claridad de los pasos a seguir y del proceso con el fin de evitar cualquier tipo de inconveniente. Estábamos en la mitad del diplomado, pero ya sentía esa satisfacción de lo aprendido.

La empresa tiene una serie de necesidades las cuales se nos presentan dentro del documente y las cuales deberemos satisfacer y solucionar una por una con el fin de que la red funcione de la mejora manera y que esta tenga una buena proyección a futuro.

Espero de mi parte la presentación del presente trabajo sea del agrado de todos ustedes y que al igual que a mi sirva para su formación y ayude a clarificar alguna duda que tengan al respecto.

Objetivo general

- Realizar el diseño de la red para las empresas de TECNOLOGÍA, indicando el proceso desarrollado para cada uno de los casos.

Objetivos específicos.

- Aplicar cada uno de los conocimientos adquiridos al desarrollo de casos reales.
- Aplicar VLSM en cada uno de los diseños.
- Profundizar en la aplicación y el funcionamiento de los protocolos de enrutamiento.
- Realizar el montaje de la topologías dentro del Simulador de Packet-Tracer herramienta que va ha favorecer nuestro proceso de aprendizaje.
- Debemos realizar la configuración de cada uno de los dispositivos que hará parte de las redes aplicando los diferentes comandos para tal fin.
- Algo supremamente importante a la hora de diseñar una red es la documentación que debemos hacer de cada una de ellas, esto lo haremos con el fin de poder realizar las correcciones de una manera más sencilla.
- Siempre realizaremos la verificación de cada uno de los pasos desarrollados, esto con el fin de observar el correcto funcionamiento de lo elaborado.

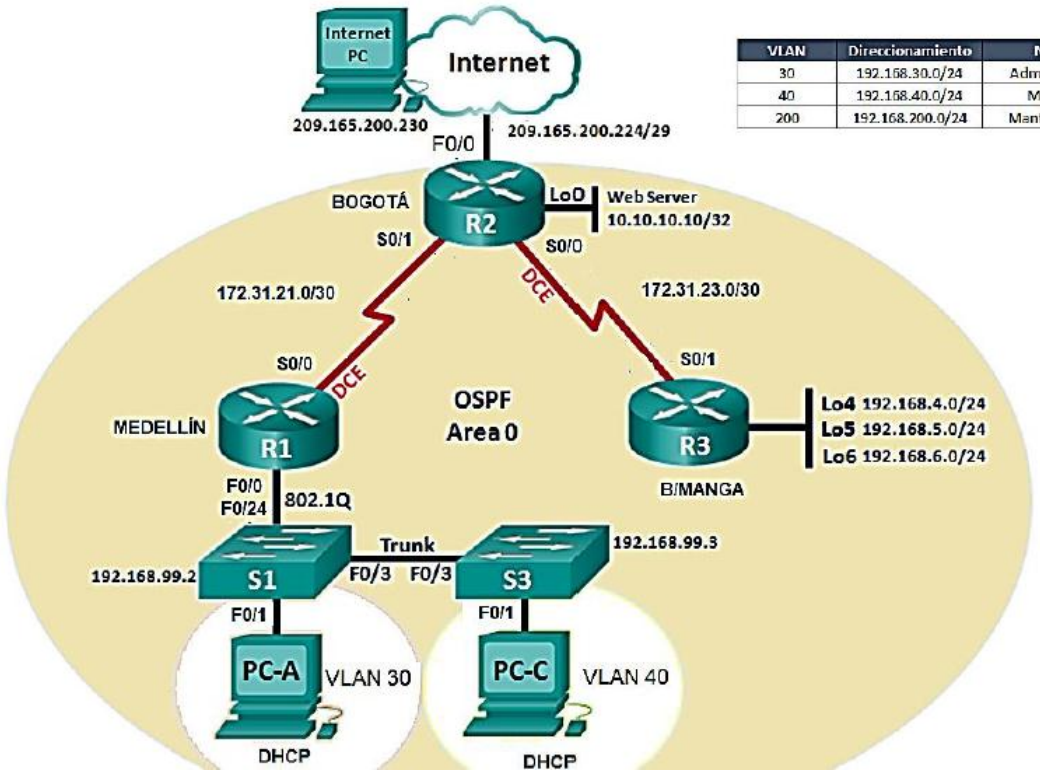
Seminario de profundización en redes LAN – WAN CISCO

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



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 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.

- EXAMEN DE HABILIDADES PRACTICAS

Iniciamos configurando el router R1 tanto las contraseñas como las interfaces.

• 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 A PERSONAL NO AUTORIZADO..
Procedemos a configurar la siguientes interface s0/0/0. 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

- 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

Banner motd & PROHIBIDO EL INGRESO A PERSONAL NO AUTORIZADO.

Procedemos a configurar las interfaces

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

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 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 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 A PERSONAL NO AUTORIZADO.

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 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

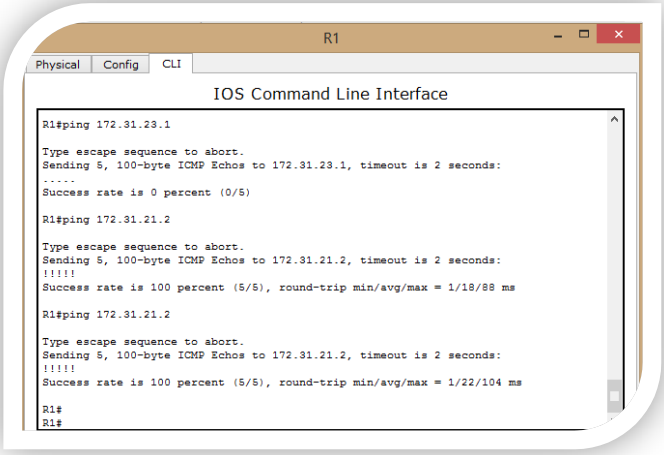
No ip domain-lookup
hostname S1
enable secret class
line console 0
    password cisco
    login
line vty 0 4
    password cisco
    login
service password-encryption
banner motd & PROHIBIDO EL INGRESO A PERSONAL NO AUTORIZADO.

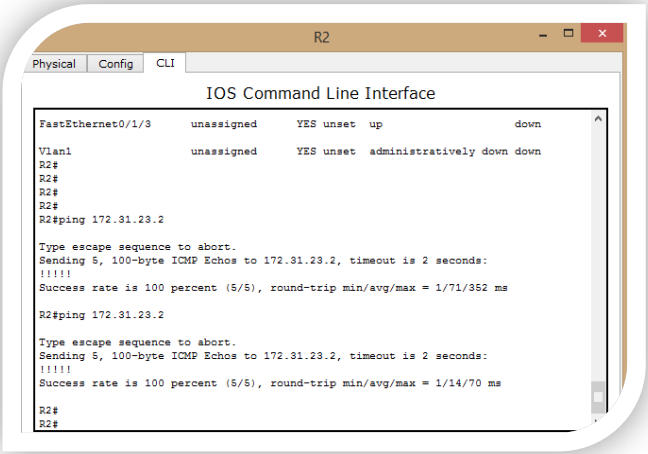
- Configuramos switch 3

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 ingreso
```

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





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

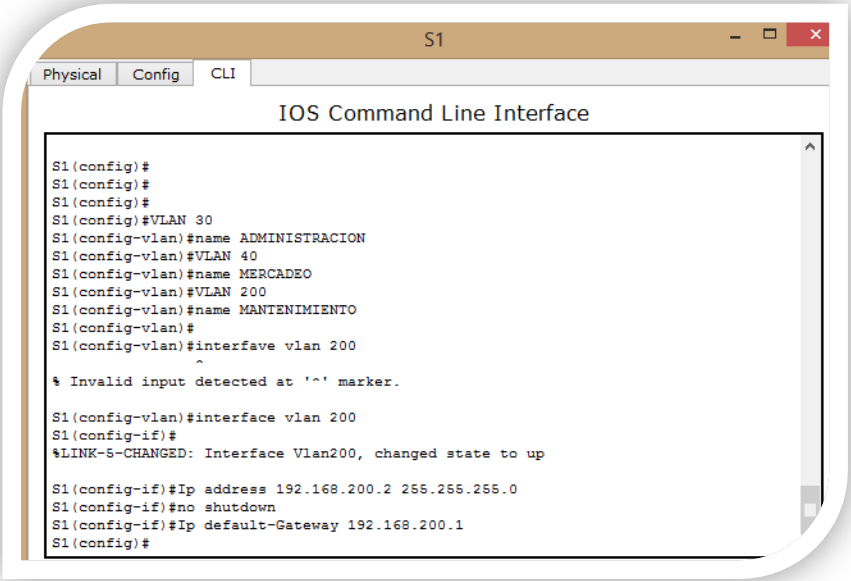
- Configuramos la seguridad, las VLANS y el ruteo entre las VLANS

Iniciamos con el SWITCH 1
VLAN 30 Name ADMINISTRACION VLAN 40 Name MERCADEO VLAN 200 Name MANTENIMIENTO

```
#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

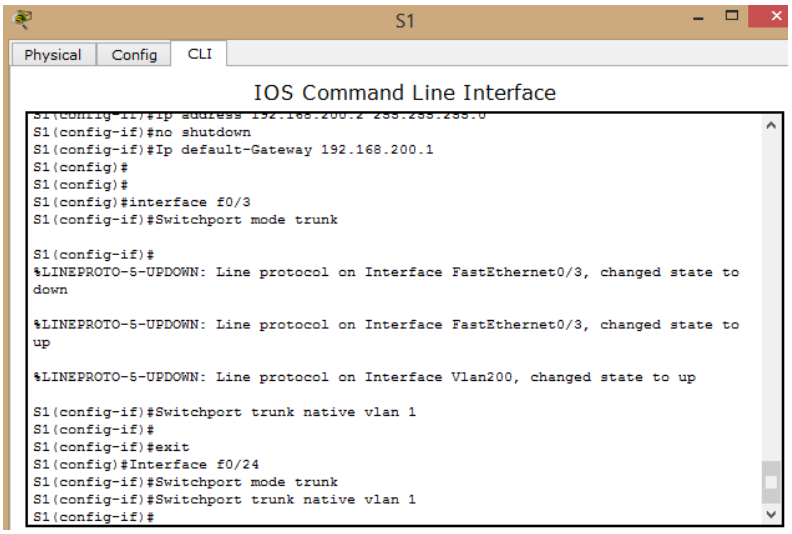
Interface VLAN 200
Ip address 192.168.200.2 255.255.255.0
No shutdown
Ip default-Gateway 192.168.200.1



- 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 los demás puertos como puertos de acceso.

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

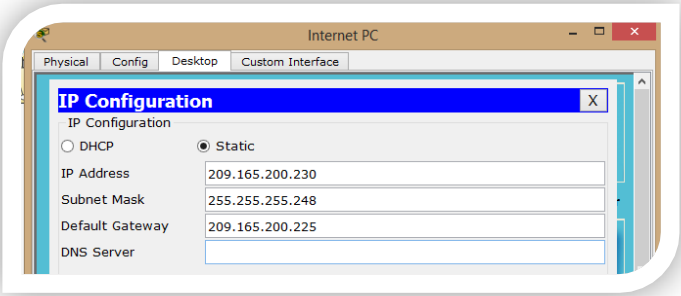
Interface fa0/1
Switchport mode Access
Switchport Access VLAN 30

- Apagamos los puertos que no los estemos utilizando

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

- Configuramos la IP Internet.

IP: 209.165.200.230
Mask: 255.255.255.248
Gateway: 209.165.200.225



- Configuramos el S3

Procedemos a realizar la configuración de las diferentes VLAN dentro del dispositivo SWITCH 1

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

```
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)#
```

- Usuamos 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
```

- 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#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 comendo PING

Todos estos comandos deben ser satisfactorios

S1

- Ping 192.168.200.1
- Ping 192.168.30.1

```
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#
```

S3

- Ping 192.168.200.1
- Ping 192.168.40.1

```
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#
```

• 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#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)#
```

- 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

```
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)#
```

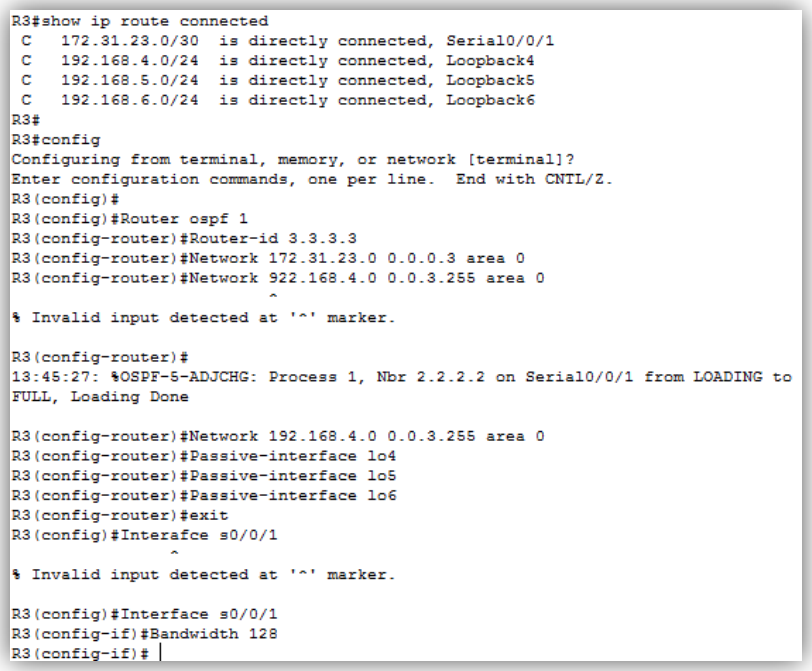
- Configuramos OPSF V2 en el router R3

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#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 CNTL/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)#Interafce s0/0/1
             ^
% Invalid input detected at '^' marker.

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

- 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     Serial0/0/1
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
     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
     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
     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#
```

- Debemos implementar DHCP en el router R1.

- 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
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
Default-router 192.168.40.1
Network 192.168.40.0 255.255.255.0

```
onfig
onfiguring 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 dchp pool MERCADEO
               ^
% Invalid input detected at '^' marker.

R1(dhcp-config)#exit
R1(config)#Ip dchp 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)#
```

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

- Configuramos NAT ESTATICO y DINAMICO e **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 sourse 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
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)#
```

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.

- 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.

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.

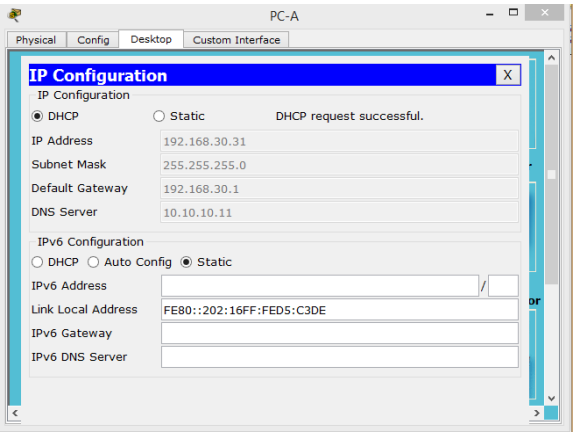
Ip nat pool INTERNET 209.165.200.225 209.165.200.228 netmask 255.255.255.248

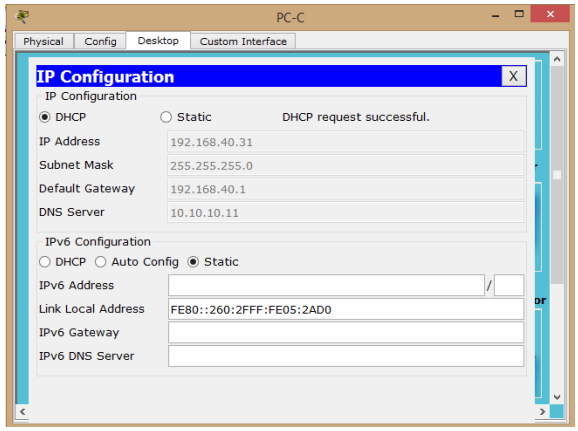
- Definimos la traducción NAT dinamico

Ip nat inside source list 1 pool INTERNET

```
R2(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)#
```

- Procedemos a verificar lo hecho hasta este momento.





- Ping entre PC-A y PC-C

- Satisfactorio.

- 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

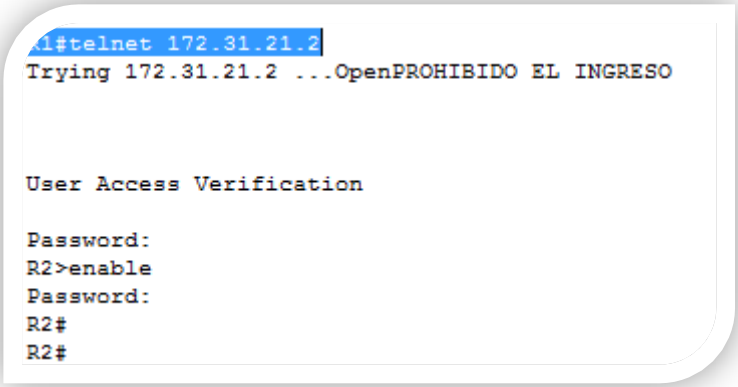
Line vty 0 4

Access-class ADMIN-MANTENIMIENTO in

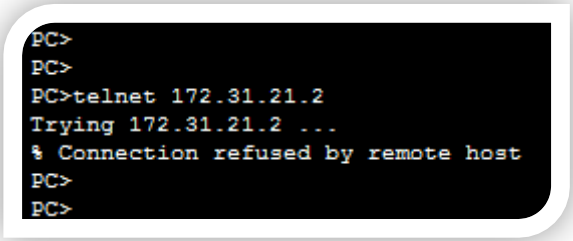
- Debemos verificar que las ACL está trabajando como queremos

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.

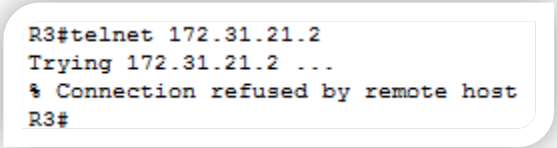
- Si hacemos TELNET al router R2 desde el router R1 este es SATISFACTORIO, tal como lo indica nuestra ACL.



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



- Si hacemos TELNET desde 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.

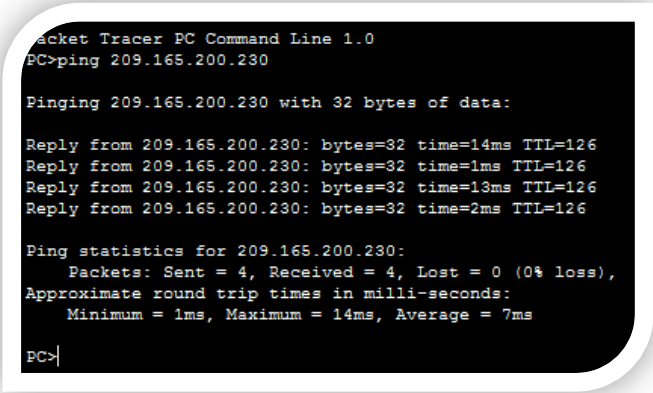
Interface g0/1
Ip Access-group 101 in
Interface s0/0/0
Ip Access-group 101 out
Interface s0/0/1
Ip Access-group 101 out
Interface g0/0
Ip Access-group 101 out

- Procedemos a verificar que las ACL están funcionando

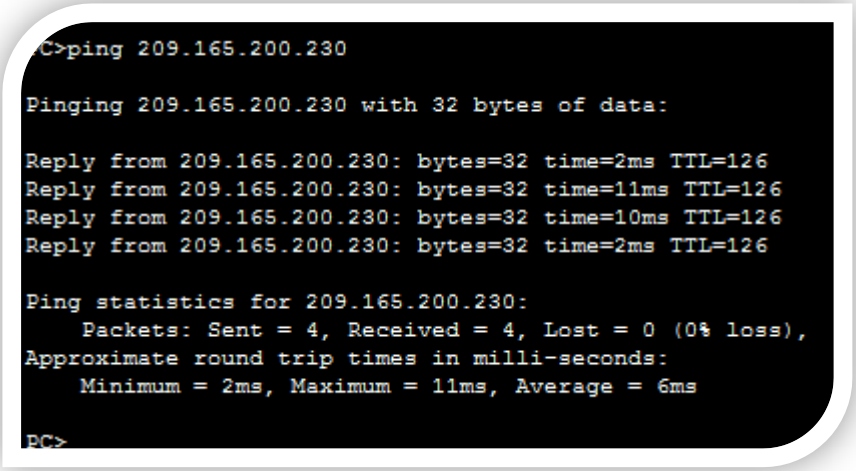
```
R1#ping 209.165.200.230

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#
```

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

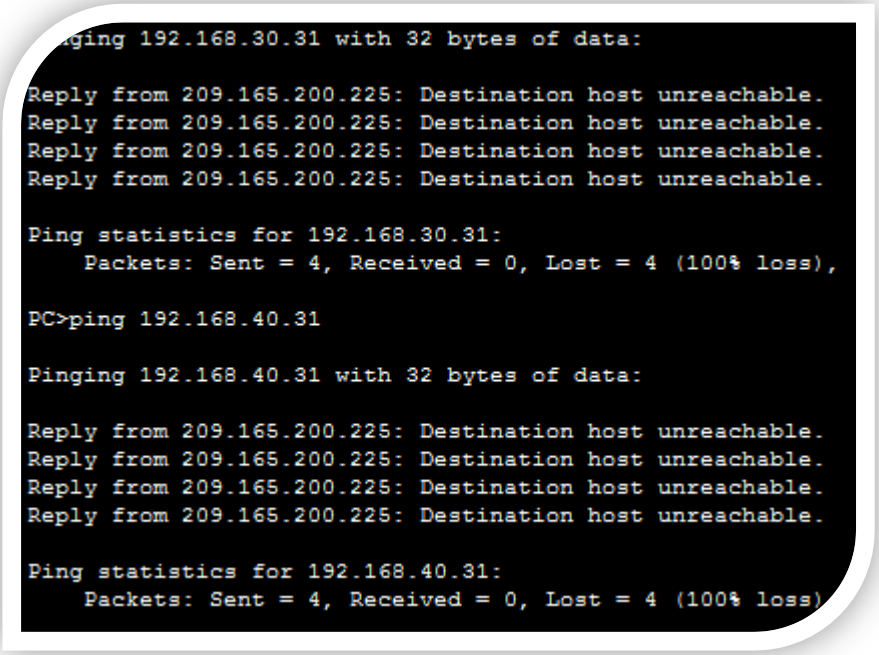
- Desde la PC-A

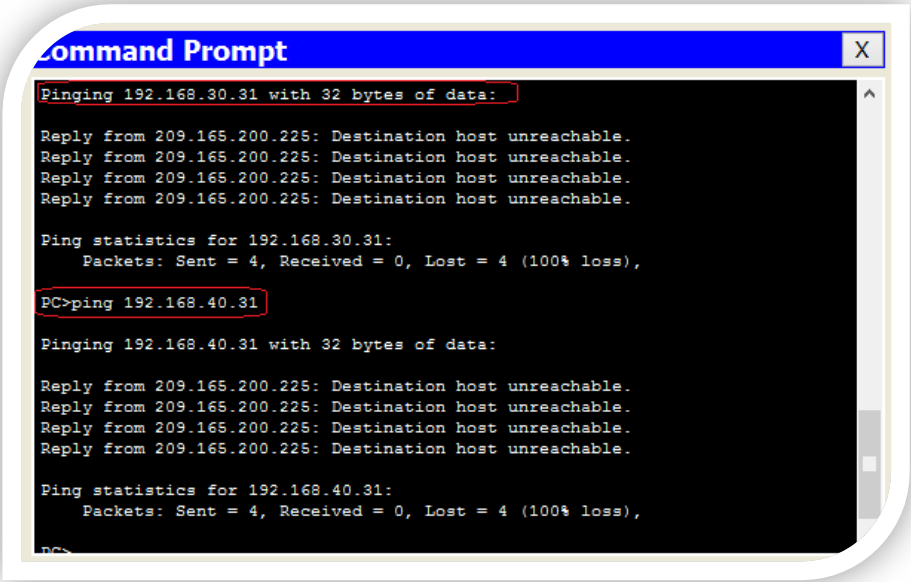


- Desde la PC-C



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


ging 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)

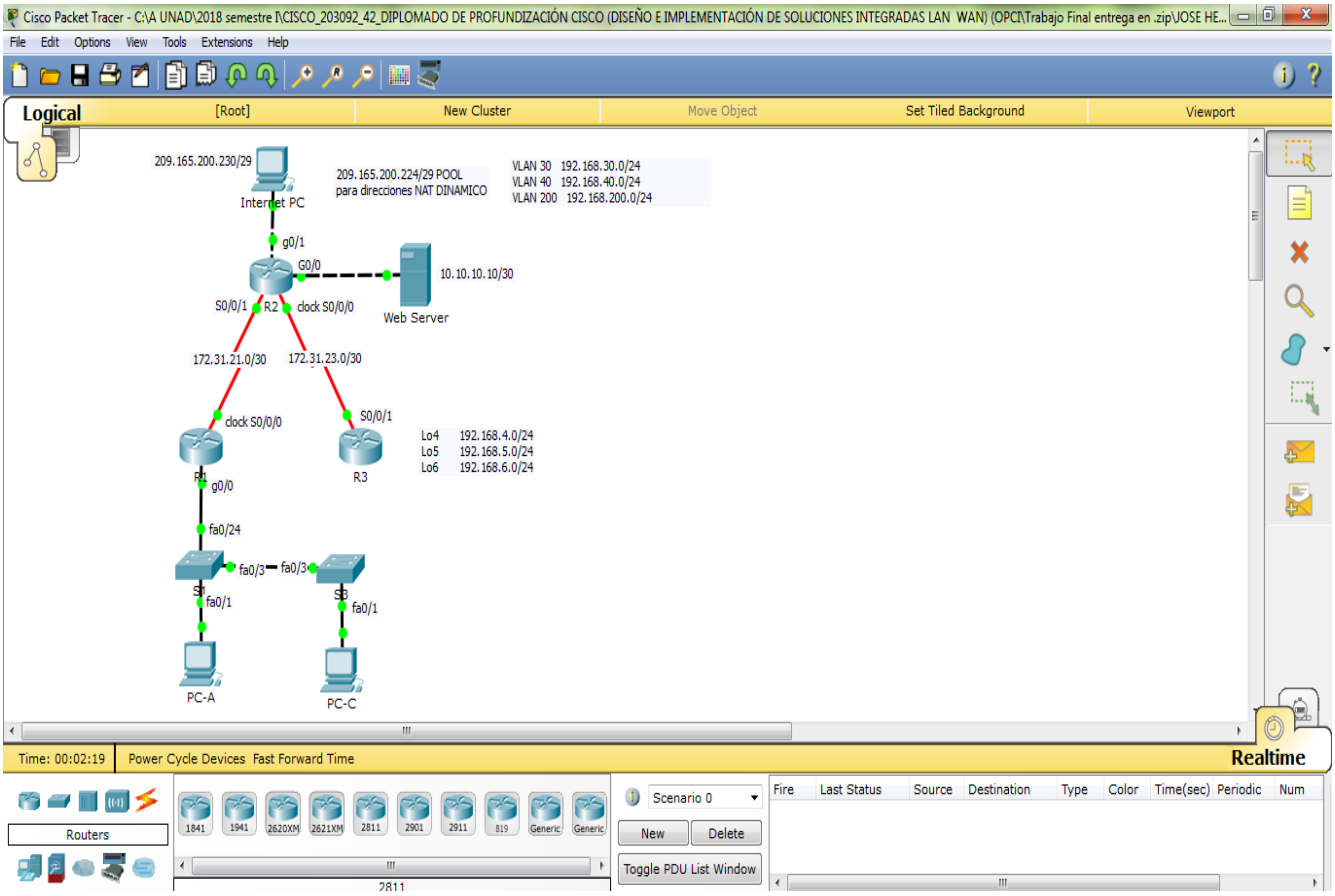

Command Prompt
X
Pinging 192.168.30.31 with 32 bytes of data:
Reply from 209.165.200.225: Destination host unreachable.
Reply from 209.165.200.225: Destination host unreachable.
Reply from 209.165.200.225: Destination host unreachable.
Reply from 209.165.200.225: Destination host unreachable.
Ping statistics 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),

PING Y TRACEROUTE.

Aplico este comando con el fin de verificar que tal está funcionando nuestra red en lo que tiene que ver con la conectividad, además estos comandos son muy útiles a la hora de solucionar algún tipo de inconveniente.

Vemos que todos los puntos de la red están respondiendo, con esto concluimos que todo el proceso de diseño y montaje de la red está bien elaborado.

Simulador



Conclusiones

- Al diseño del direccionamiento de cada una de las redes aplicamos VLSM y nos hemos dado cuenta que el ahorro de direcciones IP es inmenso.
- Realicé la implementar de cada uno de los aspectos indicados dentro del simulador.
- Todo el proceso desarrollado exigió mucho de nosotros mismo, pero es gratificando observar el grado de aprendizaje obtenido.
- Luego de realizar el proceso de análisis de las redes, se procedió a realizar el montaje de las mismas dentro del simulador, el cual nos permitió practicarnos en todo lo que tiene que ver con comandos de configuración y verificación.
- Documentamos cada uno de los pasos con el fin de corregir posibles inconvenientes que se nos presentaron y gracias a esta etapa los pudimos solucionar empleando el tiempo adecuado.
- Verificamos el funcionamiento de las redes con la utilización de los comandos estipulados para este fin, observamos que cada una de ellas son funcionales y CONVERGEN. Entre estos comando utilizamos PING y TRACERT y comandos de verificación de configuración dentro de los routers como SHOW IP ROUTE, SHOW RUNNING-CONFIG, etc….
- Siento seguridad a la hora de desarrollar proyectos de este tipo y de mediana envergadura.
- Packet Tracer es una herramienta excelente a la hora de ayudarnos a realizar la configuración de redes como las indicadas, podemos practicar y practicar.

Bibliografía.

- Universidad Nacional Abierta y a Distancia, UNAD.
- Modulo CISCO.
- http://www.slideshare.net
- http://www.cisco.com
- http://www.slideshare.net/samuelhuertasorjuela/comandos-de-configuracion-de-dispositivos-cisco
- http://www.cisco.com