EVALUACION

PRUEBA DE HABILIDADES PRACTICAS CCNA

MAURICIO EFRAIN PATIÑO CAÑAR

13072206

UNIVERSIDAD NACIONAL ABIERTA Y ADISTANCIA

ECEBTI

INGENIERIA DE SISTEMAS

PASTO

2018

EVALUACION

PRUEBA DE HABILIDADES PRACTICAS CCNA

MAURICIO EFRAIN PATIÑO CAÑAR

13072206

INFORME FINAL DIPLOMADO PROFUNDIZACION CISCO

INGENIERO:

GIOVANNY ALBERTO BRACHO

TUTOR

UNIVERSIDAD NACIONAL ABIERTA Y ADISTANCIA

ECEBTI

INGENIERIA DE SISTEMAS

PASTO

2018

NOTA DE ACEPTACION

_____

_____

_____

_____

_____

_____

_____

PASTO JUNIO DE 2018

AGRADECIMIENTOS

A la facultad de ingeniería de sistemas por promover el conocimiento en las áreas de la tecnología de información siendo una rama esencial para la formación de competencias para los que decidieron realizar sus estudios en esta institución.

En la aplicación de nueva tecnologías y el perfeccionamiento del conocimiento es fundamental la normatividad de la práctica y la teoría y en su momento consolidar en base a la experiencia un conocimiento valioso en el futuro profesional.

TABLA DE CONTENIDO

Configurar el direccionamiento IP acorde con la topología de red para cada uno de los dispositivos que forman parte del escenario 15

Configurar el protocolo de enrutamiento OSPFv2 bajo los siguientes criterios ... 10

Verificar información de OSPF..... 29

Configurar VLANs, Puertos troncales, puertos de acceso, encapsulamiento, Inter-VLAN Routing y Seguridad en los Switches acorde a la topología de red establecida..... 22

En el Switch 3 deshabilitar DNS lookup 19

Asignar direcciones IP a los Switches acorde a los lineamientos 18

Desactivar todas las interfaces que no sean utilizadas en el esquema de red 26

Implement DHCP and NAT for IPv4 27

Configurar R1 como servidor DHCP para las VLANs 30 y 40. 24

Reservar las primeras 30 direcciones IP de las VLAN 30 y 40 para configuraciones estáticas 31

Configurar NAT en R2 para permitir que los host puedan salir a internet 33

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 26

Verificar procesos de comunicación y re direccionamiento de tráfico en los routers mediante el uso de Ping y Traceroute 28

Resumen final tipología 41

CONCLUCIONES 44

BIBLIOGRAFIA 45

RESUMEN

En el siguiente trabajo se realiza como practica final CCNA dado que en esta tipología, se realiza una configuración mixta, donde se especifica la configuración con OSPFV2, además de configuración de dispositivos con DHCP orientada a una prueba real.

INTRODUCCIÓN

Se realiza el presente informe con la finalidad de demostrar los conocimientos adquiridos durante este periodo académico para desarrollar procesos de configuración de PAKET TRACER, los cuales se aplicaron , en esta práctica se revisa las segmentaciones de esta red para de acuerdo a esta tipología realizar este proceso de configuración.

LISTA DE FIGURAS

ARQUITECTURA A DESARROLLAR _____ 6

CONFIGURACIN PC C _____ 8

CONFIGURACIN PC C _____17

CONFIGURACION R1 _____17

CONFIGURACION R1 CON INTERFAZ
SERIAL_____18

CONECTIVIDAD R1_____22

CONECTIVIDAD R2_____22

CONFIGURACION S1_____23

CONFIGURACION S1_____24

CONFIGURACION S1_____26

CONFIGURACION S3_____27

CONFIGURACION R1_____28

CONFIGURACION R1_____29

CONFIGURACION R1_____30

CONFIGURACION R2_____31

CONFIGURACION R3_____31

VALIDACION PROTOCOLOS_____33

VALIDACION PROTOCOLOS_____34

CONFIGURAICON R1_____35

CONFIGURACION EXTERNA _____36

CONFIGURAICON R2_____37

VALIDACION PING_____38

VALIDACION PING_____39

VALIDACION TELNET_____40

VALIDACION TELNET_____41

RESUMEN FINAL TOPOLOGIA_____41

PING PC A RED_____43

PING PC A RED_____44

PROBLEMA DE INVESTIGACION

Evaluación –Prueba de habilidades prácticas CCNA

Descripción general de la prueba de habilidades

La evaluación denominada “Prueba de habilidades prácticas”, forma parte de las actividades evaluativas del Diplomado de Profundización CCNA, la cual busca identificar el grado de desarrollo de competencias y habilidades que fueron adquiridas a lo largo del diplomado y a través de la cual se pondrá a prueba los niveles de comprensión y solución de problemas relacionados con diversos aspectos de Networking.

Para esta actividad, el estudiante dispone de cerca de dos semanas para realizar las tareas asignadas en cada uno de los escenarios propuestos, acompañado de los respectivos procesos de documentación de la solución, correspondientes al registro de la configuración de cada uno de los dispositivos, la descripción detallada del paso a paso de cada una de las etapas realizadas durante su desarrollo, el registro de los procesos de verificación de conectividad mediante el uso de comandos ping, traceroute, show ip route, entre otros.

La prueba de habilidades podrá ser desarrollada en el **Laboratorio SmartLab** o mediante el uso de **herramientas de Simulación (Puede ser Packet Tracer o GNS3)**. El estudiante es libre de escoger bajo qué mediación tecnológica resolverá cada escenario. No obstante, es importante mencionar que **aquellos estudiantes que hagan uso del laboratorio SmartLab se les considerará un estímulo adicional a la hora de evaluar el informe, teniendo en cuenta que su trabajo fue realizado sobre equipos reales y con ello será la oportunidad poner a prueba las habilidades y competencias adquiridas durante el diplomado.** Adicionalmente, es importante considerar, que esta actividad puede ser realizada en varias sesiones sobre este entorno, teniendo en cuenta que disponen de casi 15 días para su desarrollo.

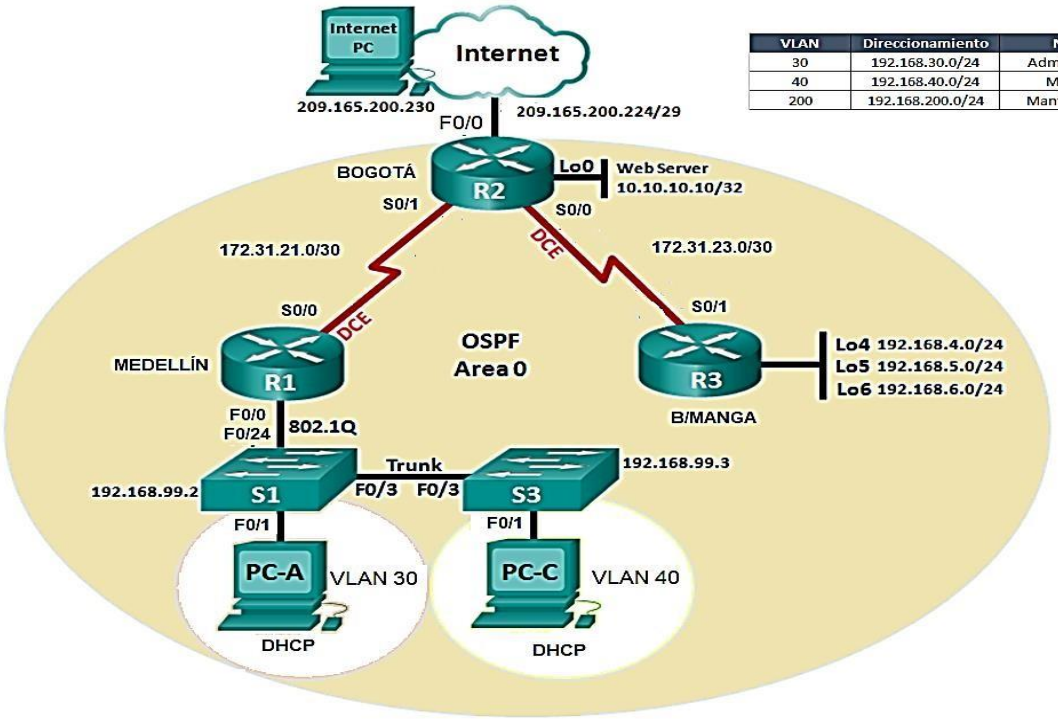
Finalmente, el informe deberá cumplir con las normas ICONTEC para la presentación de trabajos escritos, teniendo en cuenta que este documento deberá ser entregado al final del curso en el Repositorio Institucional, acorde con los lineamientos institucionales para grado. Proceso que les será socializado al finalizar el curso.

Es muy importante mencionar que esta actividad es de carácter INDIVIDUAL. El informe deberá estar acompañado de las respectivas evidencias de configuración de los dispositivos, las cuales generarán veracidad al trabajo

realizado. **El informe deberá ser entregado en el espacio creado para tal fin en el Campus Virtual de la UNAD**.

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.



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:

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

OSPFv2 area 0

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.

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

- 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.

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

DESARROLLO DE LA GUIA DE ACTIVIDADES

Para el desarrollo de la guía de actividades se tomó un método ortodoxo para la configuración dado que en el orden que lo presentan los resultados no sería óptimos por lo tanto en cada aparte se informara el punto de la guía a resolver.

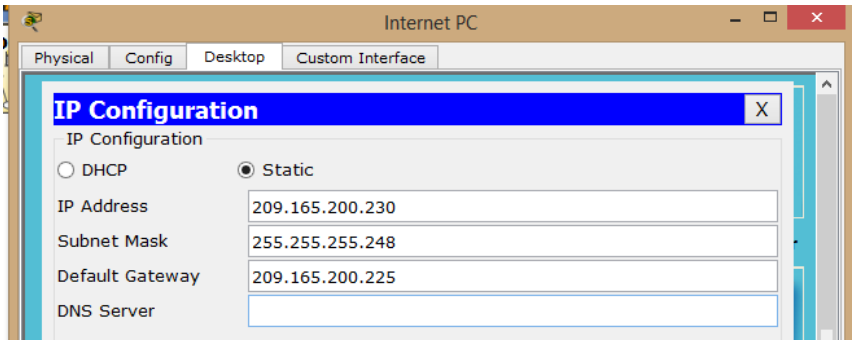
***Configurar el direccionamiento IP acorde con la topología de red para cada uno de los dispositivos que forman parte del escenario**

Se instala un servidor de manera real

- Se elimina las configuraciones básicas de los router
  - Erase start-up config
- Se elimina la configuración de las VLAN.
  - Delete vlan.dat
- Se reinicia
  - Reload.

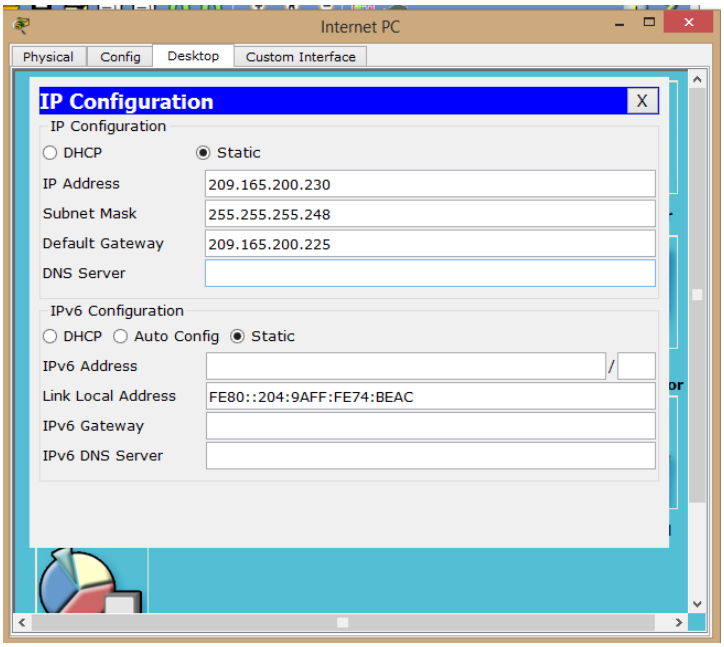
Se inicia las configuraciones de internet

IP: 209.165.200.230
Mask: 255.255.255.248
Gateway: 209.165.200.225



En esta imagen observamos la configuración de PC

En esta imagen observamos la configuración de PC



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.

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
                ^
% Invalid input detected at '^' marker.

R1(config-line)#service?
% Unrecognized command
R1(config-line)#exit
R1(config)#Service password encryption
                ^
% 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 '&'.
```

SE OBSERVA LA CONFIGURACION DE R1 CON ENCRIPTACION

Configure interface s0/0/0
Description CONECTA CON R2.
Ip address 172.31.21.1 255.255.255.252
Clock rate 128000
No shutdown
Ip route 0.0.0.0 0.0.0.0 s0/0/0

```
R1#
R1#enable
R1#
R1#
R1#configure interface
             ^
% 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
               ^
% 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 Serial0/0/0, 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)#
R1(config)#
```

CONFIGURACION DE R1 CON INTERFACE SERIAL

APLICACIÓN DE CLOCK RATE

CONFIGURACION R2

- **Asignar direcciones IP a los Switches acorde a los lineamientos se resuelve este ítem con estas configuraciones.**

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
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
interface g0/0
ip address 10.10.10.1 255.255.255.0
no shutdown

description CONEXIÓN CON WEB SERVER
ip addres 10.10.10.10
mask: 255.255.255.0
Gateway: 10.10.10.1

ip route 0.0.0.0 0.0.0.0 g0/1

CONFIGURACION R3

- **EN EL SWITCH 3 DESHABILITAR DNS LOOKUP**

- **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.**

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

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

CONFIGURACION SWITCH

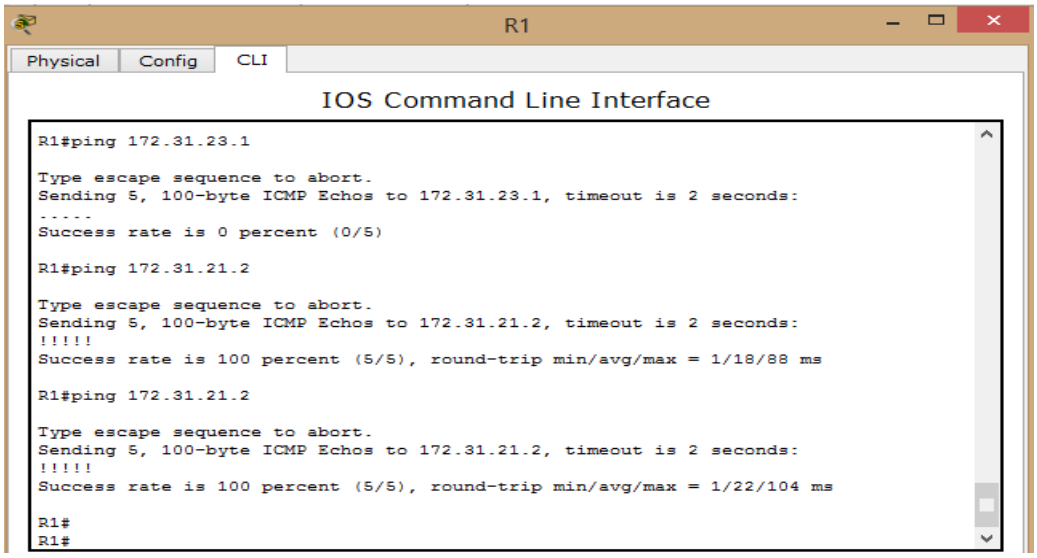
```
No ip domain-lookup
hostname S1
enable secret class
line console 0
        password cisco
        login
line vty 0 4
        password cisco
        login
service password-encryption
banner motd & PROHIBIDO EL INGRESO
```

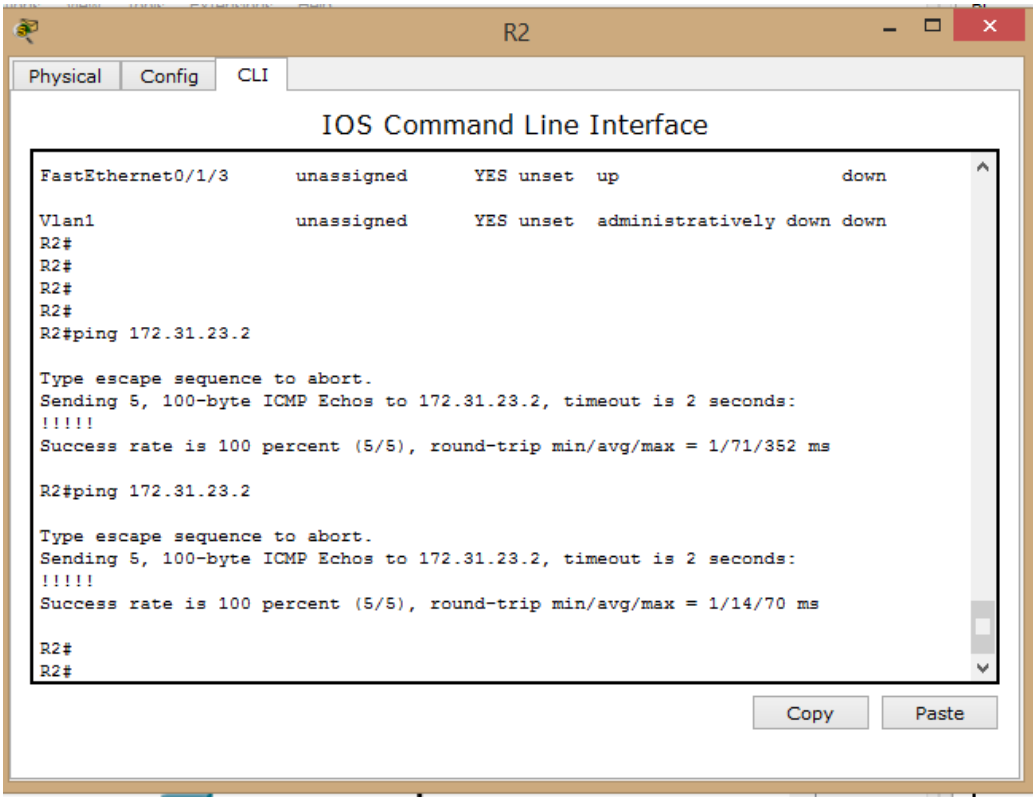
CONFIGURACION SWITCH 3

```
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.

CONECTIVIDAD





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

VLAN 30

Name ADMINISTRACION

VLAN 40

Name MERCADEO

VLAN 200

Name MANTENIMIENTO

asignar la dirección IP a la Vlan MANTENIMIENTO

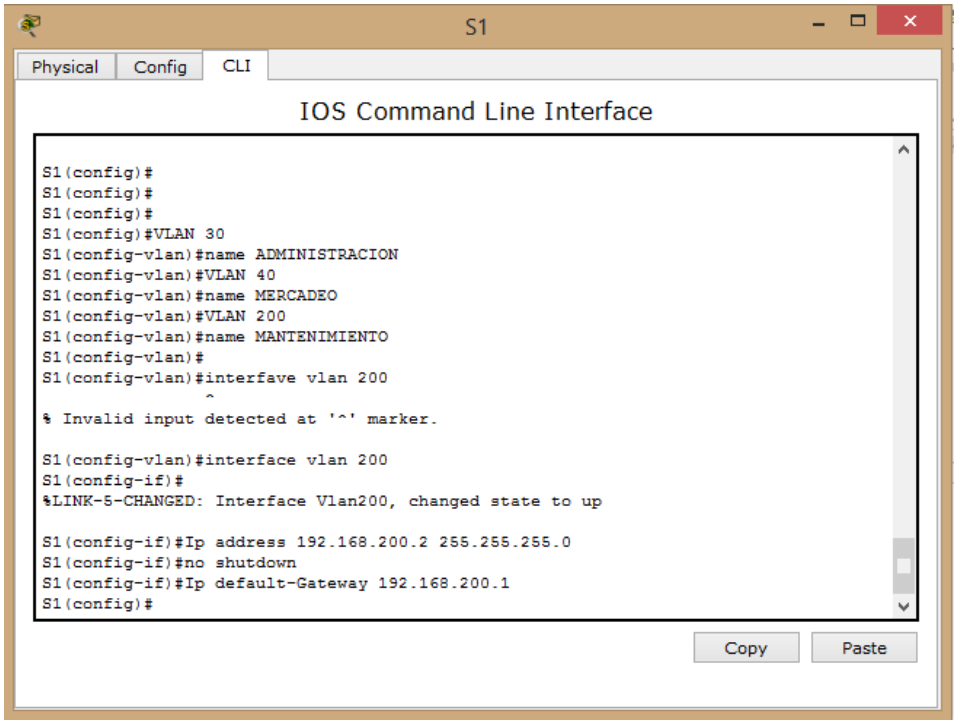
Interface VLAN 200

Ip address 192.168.200.2 255.255.255.0

No shutdown

Ip default-Gateway

192.168.200.1



CONFIGURACION S1 PARA DIRECCIONAMIENTO

interface f0/3, usamos la vlan nativa 1

Interface f0/3

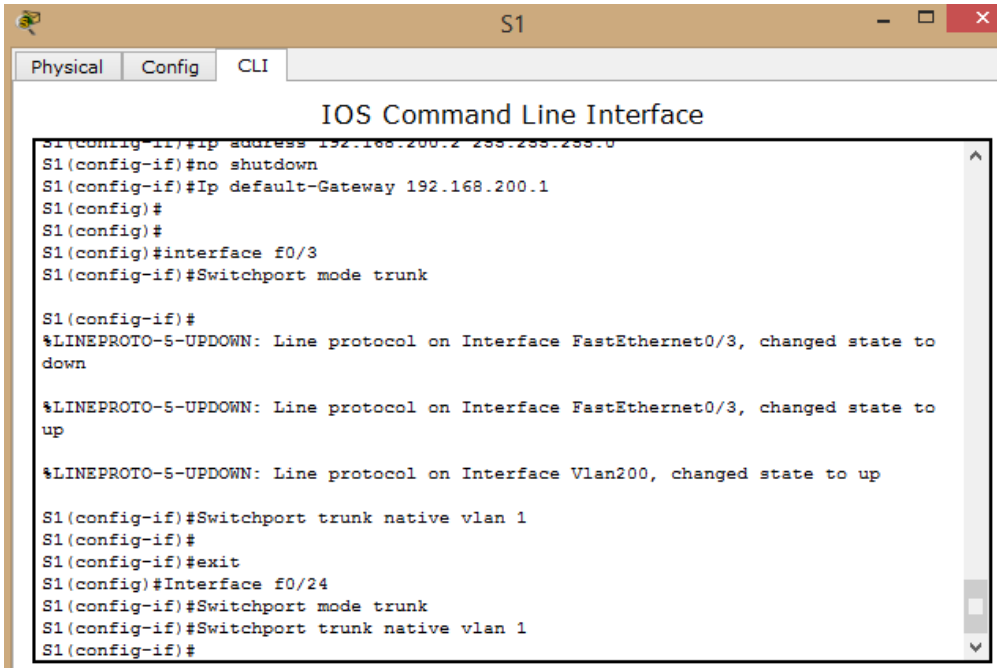
Switchport mode trunk

Switchport trunk native vlan 1

Interface f0/24

Switchport mode trunk

Switchport trunk native vlan 1



SE CONFIGURA LA INTERFAS DE MANERA NATIVA

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

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

Switchport mode Access

Interface fa0/1

Switchport mode Access

Switchport Access VLAN 30

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

Shutdown

CONFIGURACION SWITCH 3

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)#
```

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.

Se usa la interfaz f0/3 como troncal y la vlan 1 como nativa

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

Se configuran las interfaces en modo acceso empleando el comando rango

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

Se asigna a la interface fa0/1 a la vlan 40

En este aparte se soluciona el siguiente item
Desactivar todas las interfaces que no sean utilizadas en el esquema de red.

Interface fa0/1
Switchport mode access
Switchport Access VLAN 40
Se apagan los puertos que no se necesitan
Interface range fa0/2, fa0/4-24, g0/1-2
Shutdown

```
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
                 ^
% 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
```

CONFIGURACION S1 INTEFACE FA

CONFIGURACION SUB INTERFACES

En este aparte se soluciona el siguiente item

Implementar DHCP and NAT for IPv4

CONFIGURACION R1

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

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)#
```

CONFIGURACION

DE IP PROCESO DE

ENCAPSULACION

VALIDACION PING

Verificar procesos de comunicación y re direccionamiento de tráfico en los routers mediante el uso de Ping y Traceroute.

S1
Ping 192.168.200.1
Ping 192.168.30.1

```
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#
```

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.

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

ACTIVACION PASIVA

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)#
```

Auto-cost reference-bandwitdh 1000 …

CAMBIO DE ANCHO DE BANDA

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

CONFIGURACION OSPF 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

ESTABLECER LAN COMO PASIVAS

Passive-interface g0/0

Interface s0/0/0
Bandwidth 128
Interface s0/0/1
Bandwidth 128
ESTABLECES METRICA PARA INTERFAS
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)#
```

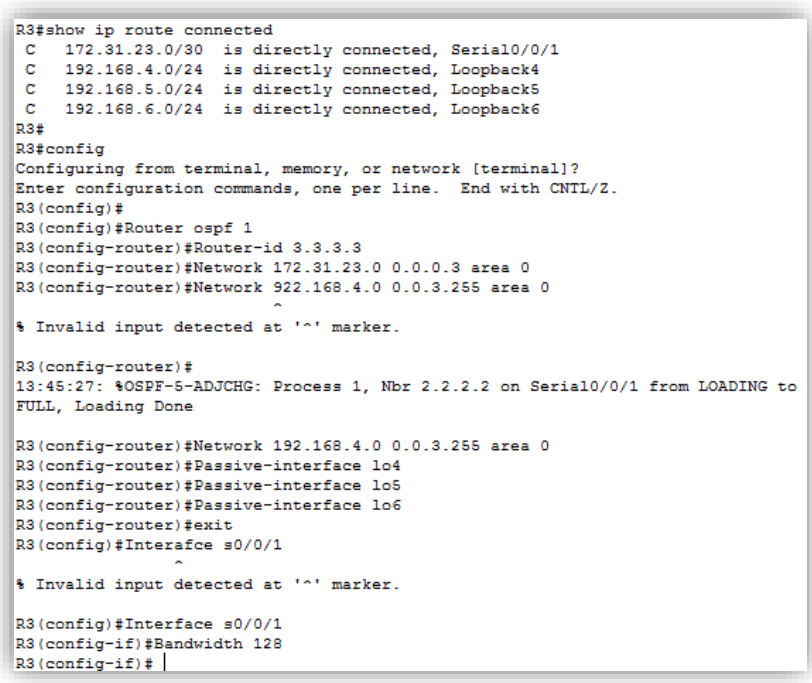
CONFIGURACION R3 OSPFV2

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)#
```

VALIDACION PROTOCOLOS

- 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#
```

```
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#
```

```
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#
```

```
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#
```

COMANDOS PARA VERIFICAR CONFIGURACION EN EJECUCION

- show running-config

CONFIGURACION DHSP R1.

RESERVA VALIDACIONES DE LAS 30 PRIMERAS DIRECCION 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
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
Default-router 192.168.40.1
Network 192.168.40.0 255.255.255.0

```
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 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)#
```

CONFIGURACION NAT EN R2 ESTATICO Y DANIMICO

se usa servidor web

User webuser privilege 15 secret cisco12345

Ip nat inside sourse static 10.10.10.10 209.165.200.229

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)#
```

RESTRICCIONES ACL

CONFIGURACION NAT DINAMICA CON ACL.
SE CREA LA acces-list NUMERO 1

- LA TRADUCCION ES UNICAMENTE PARA ADMINISTRACIÓN Y MERCADEO ESTA EN R1 TRADUCTOR 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

EMPLEANDO RUTA RESUMIDA PARA R3

Access-list 1 permit 192.168.4.0 0.0.3.255

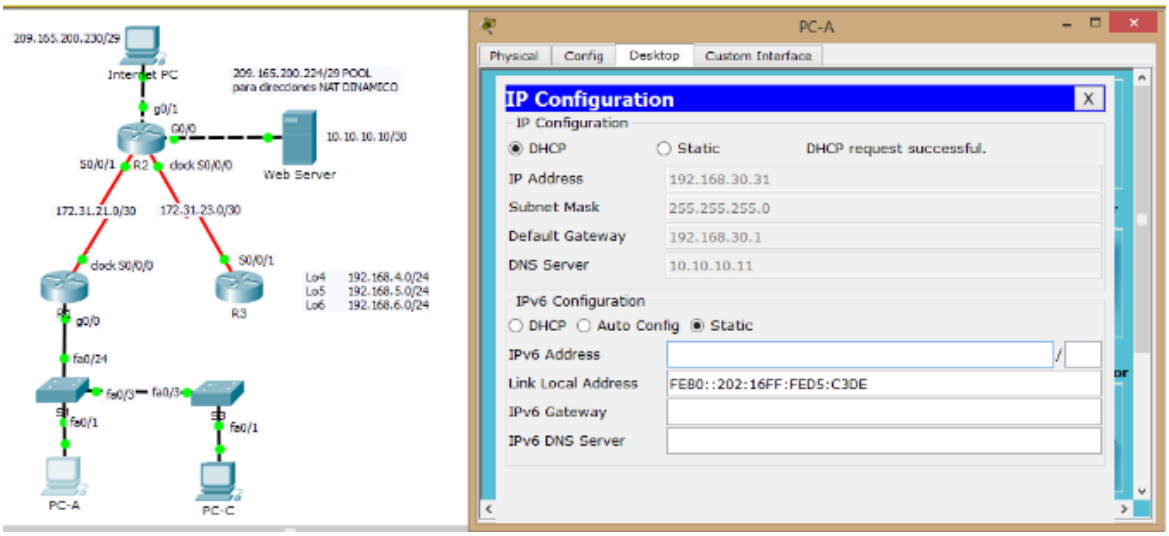
Definir el POOL de direcciones que se van a utilizar para el NAT DINAMICO.

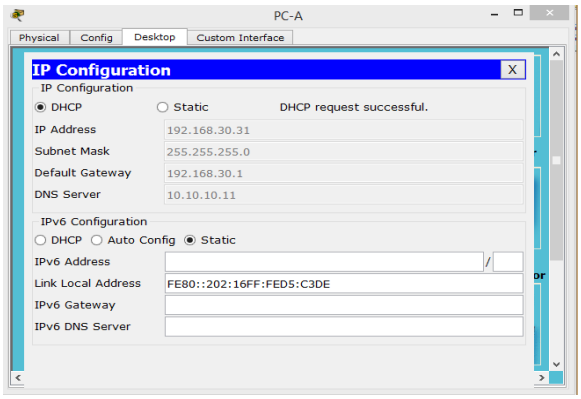
Ip nat pool INTERNET 209.165.200.225 209.165.200.228 netmask 255.255.255.248

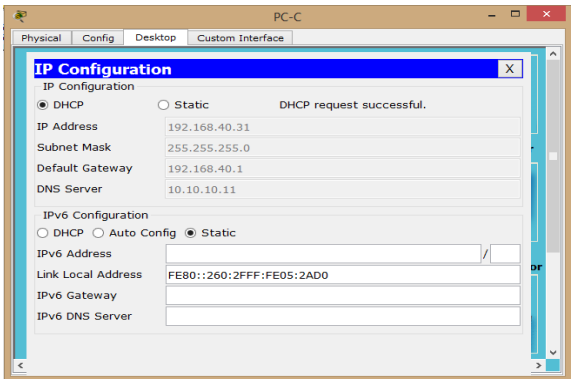
traducción NAT dinamico

Ip nat inside source list 1 pool INTERNET

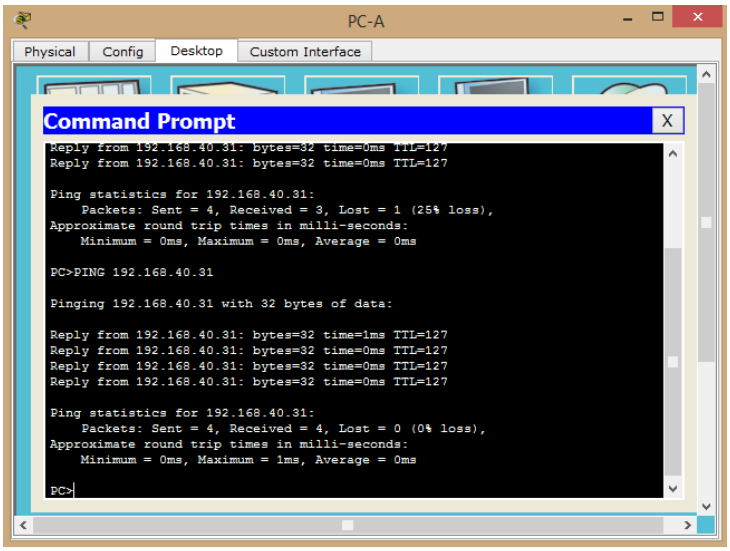
```
R2(config)#
R2(config)#Access-list 1 permit 192.168.30.0 0.0.0.255
R2(config)#Access-list 1 permit 192.168.40.0 0.0.0.255
R2(config)#Access-list 1 permit 192.168.4.0 0.0.3.255
R2(config)#
R2(config)#Ip nat pool INTERNET 209.165.200.225 209.165.200.228 netmask
255.255.255.248
R2(config)#Ip nat inside source list 1 pool INTERNET
R2(config)#
```


209.165.200.230/29
Internet PC
209.165.200.224/29 POOL
para direcciones NAT DINAMICO
g0/1
G0/0
10.10.10.10/30
Web Server
S0/0/1
R2
dock S0/0/0
172.31.21.0/30
172.31.23.0/30
dock S0/0/0
S0/0/1
R3
Lo4 192.168.4.0/24
Lo5 192.168.5.0/24
Lo6 192.168.6.0/24
g0/0
fa0/24
fa0/3
fa0/3
fa0/1
fa0/1
PC-A
PC-C
PC-A
Physical
Config
Desktop
Custom Interface
IP Configuration
IP Configuration
DHCP
Static
DHCP request successful.
IP Address 192.168.30.31
Subnet Mask 255.255.255.0
Default Gateway 192.168.30.1
DNS Server 10.10.10.11
IPv6 Configuration
DHCP
Auto Config
Static
IPv6 Address
Link Local Address FE80::202:16FF:FED5:C3DE
IPv6 Gateway
IPv6 DNS Server


PC-A
Physical
Config
Desktop
Custom Interface
IP Configuration
IP Configuration
DHCP
Static
DHCP request successful.
IP Address 192.168.30.31
Subnet Mask 255.255.255.0
Default Gateway 192.168.30.1
DNS Server 10.10.10.11
IPv6 Configuration
DHCP
Auto Config
Static
IPv6 Address
Link Local Address FE80::202:16FF:FED5:C3DE
IPv6 Gateway
IPv6 DNS Server


PC-C
Physical
Config
Desktop
Custom Interface
IP Configuration
IP Configuration
DHCP
Static
DHCP request successful.
IP Address 192.168.40.31
Subnet Mask 255.255.255.0
Default Gateway 192.168.40.1
DNS Server 10.10.10.11
IPv6 Configuration
DHCP
Auto Config
Static
IPv6 Address
Link Local Address FE80::260:2FFF:FE05:2AD0
IPv6 Gateway
IPv6 DNS Server

PING ENTRE PC A PC C



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.

Configurar validar 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.

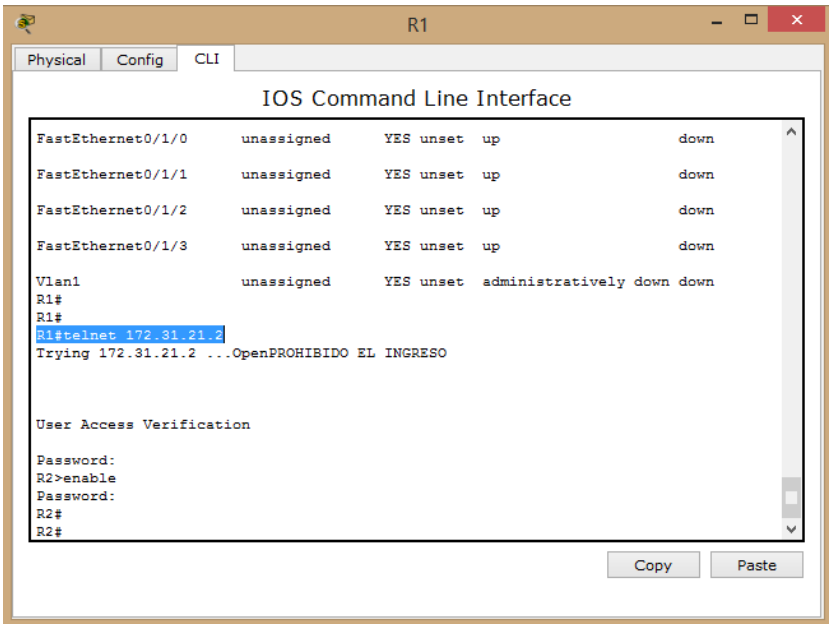
Ip Access-list standard ADMIN-MANTENIMIENTO
Permit host 172.31.21.1

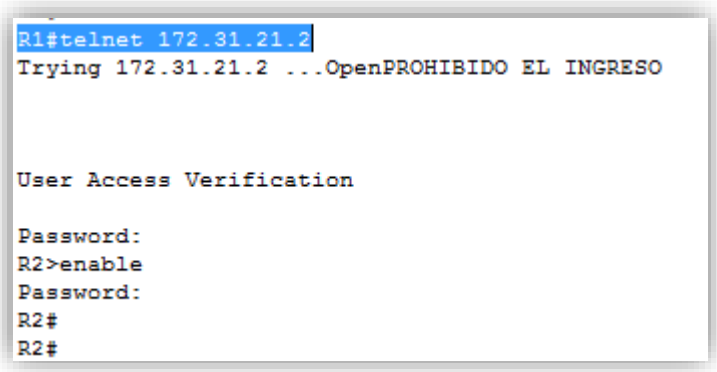
Line vty 0 4
Access-class ADMIN-MANTENIMIENTO in

Debemos verificar que las ACL están trabajando ok

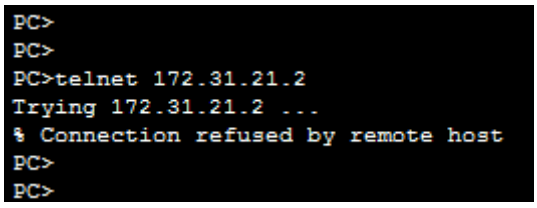
Vemos claramente que si empleamos TELNET desde el ROUTER R1 este es satisfactorio, si lo hacemos desde cualquier otro equipo este no puede ser posible.

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





TELNET desde un equipo de cualquiera de las VLAN.



hacemos TELNET desde R3.

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

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

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

VALIDACION EN ICMP EN R2

Access-list 101 permit tcp any host 209.165.229.230 eq www

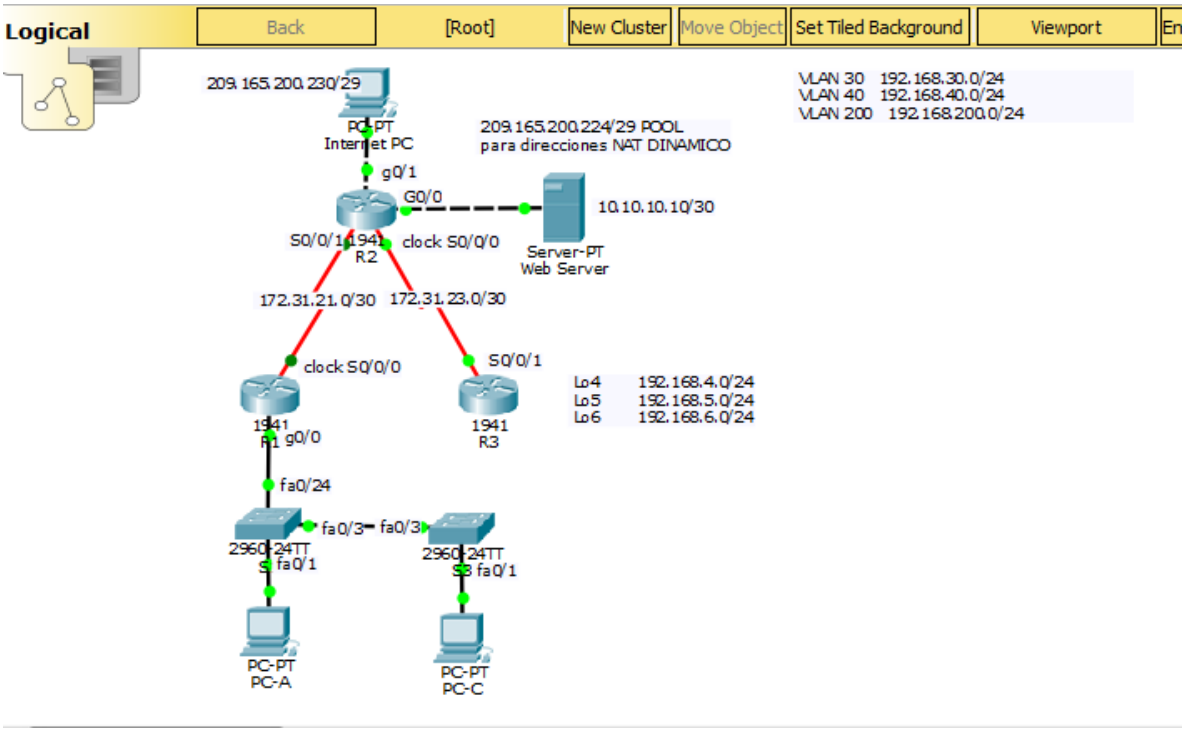
Evitar el tráfico desde INTERNET que no puedan hacer PING a la red interna

Access-list 101 permit icmp any any echo-reply

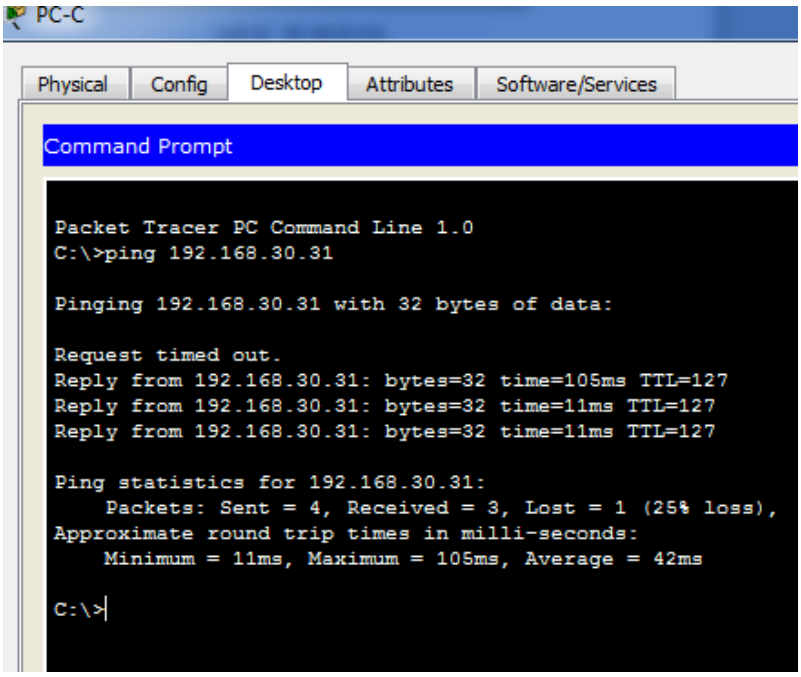
aplicar las ACL a las interfaces adecuadas.

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

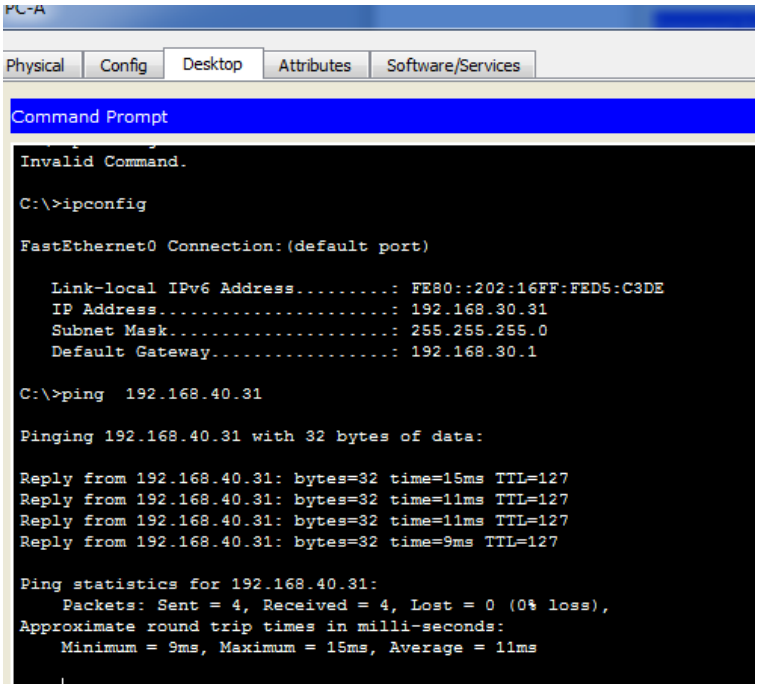
RESUMEN FINAL DE LA TOPOLOGIA



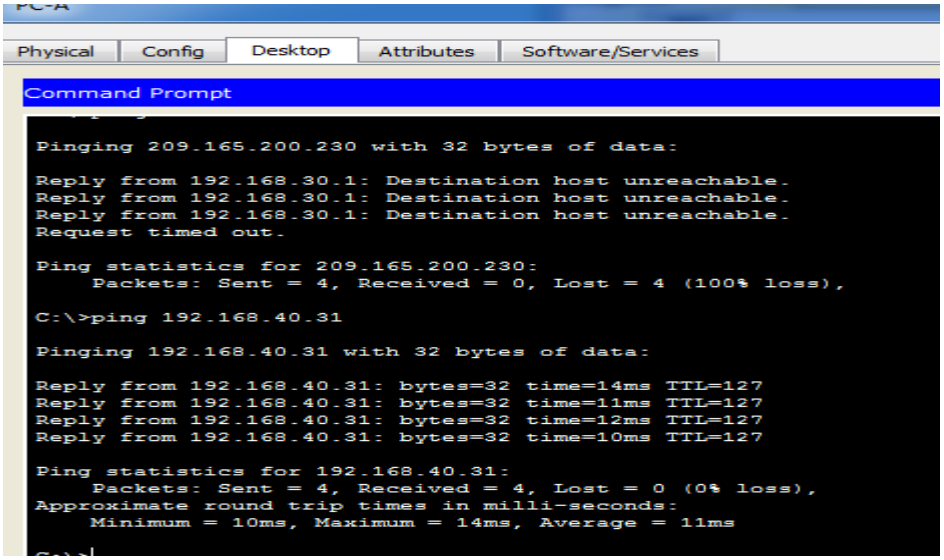
Pig PC C A PC A



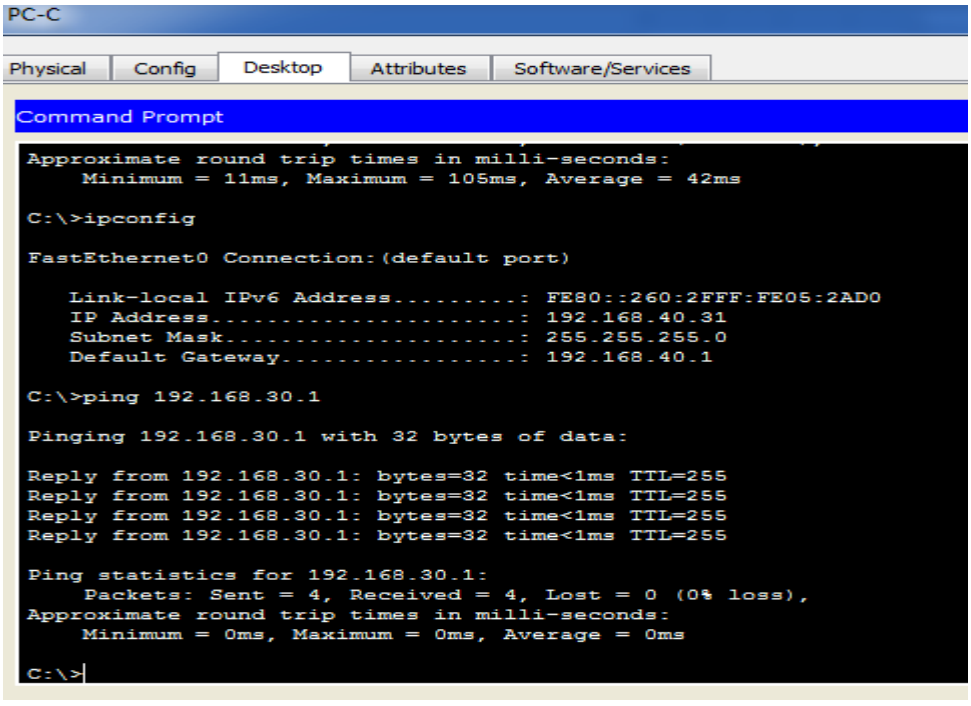
PING PC A PC C



PING PC A PC C



PING PC PC A



CONCLUCIONES

- Se realiza una configuración exitosa de los dispositivos para esta practica
- Se instaló con éxito la red de manera óptima.
- Los dispositivos con funciones con configuración OSPF V2 se enrutaron con éxito.
- Se realizó un modelo mixto de manera exitosa, se hace entrega del prototipo funcional.

BIBLIOGRAFIA

CISCO. (2014). Introducción a redes conmutadas. Principios de Enrutamiento y Conmutación. Recuperado de:https://static-course assets.s3.amazonaws.com/RSE50ES/module1/index.html#1.0.1.1

CISCO. (2014). Configuración y conceptos básicos de Switching. Principios de Enrutamiento y Conmutación. Recuperado de: https://static-course-assets.s3.amazonaws.com/RSE50ES/module2/index.html#2.0.1.1

CISCO. (2014). VLANs. Principios de Enrutamiento y Conmutación. Recuperado de: https://static-course-assets.s3.amazonaws.com/RSE50ES/module3/index.html#3.0.1.1

CISCO. (2014). Conceptos de Routing. Principios de Enrutamiento y Conmutación. Recuperado de: https://static-course-assets.s3.amazonaws.com/RSE50ES/module4/index.html#4.0.1.1

CISCO. (2014). Enrutamiento entre VLANs. Principios de Enrutamiento y Conmutación. Recuperado de: https://static-course-assets.s3.amazonaws.com/RSE50ES/module5/index.html#5.0.1.1

CISCO. (2014). Enrutamiento Estático. Principios de Enrutamiento y Conmutación. Recuperado de: https://static-course-assets.s3.amazonaws.com/RSE50ES/module6/index.html#6.0.1.1