# EVALUACIÓN DE HABILIDADES PRACTICAS

## DIPLOMADO DE PROFUNDIZACIÓN CISCO (DISEÑO E IMPLEMENTACIÓN DE SOLUCIONES INTEGRADAS LAN / WAN) (OPCI 203092A_474)

**WALTER LEOPOLD DIAZ PEÑALOZA**
**COD:88249034**

**UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA**
**BOGOTÁ D.C.**
**DICIEMBRE DE 2018**

**EVALUACIÓN DE HABILIDADES PRACTICAS**

**DIPLOMADO DE PROFUNDIZACIÓN CISCO (DISEÑO E IMPLEMENTACIÓN DE SOLUCIONES INTEGRADAS LAN / WAN) (OPCI 203092A_474)**

**TUTOR: ALEJANDRO PEREZ**

**PRESENTADO POR:**

**WALTER LEOPOLD DIAZ PEÑALOZA**
**COD:88249034**

**UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA**
**BOGOTÁ D.C.**
**DICIEMBRE DE 2018**

# Tabla de Contenido

# ABSTRACT

The purpose of this paper is to demonstrate the practical way of knowledge in the CCNA Cisco diploma, conceptualizing about IPV4, IPV6, OSPFv2, DHCP Services, Routing, NAT and ACL access lists

In the course of Cisco CCNA 1 and 2 are shown in the practice of the laboratories to obtain the basic knowledge in the matter to solve them in the practical results in the examination of practical practices, in the forms of configuration of the devices of the network In an adequate manner and Description of each of the points, with the IPV4 and IPV6 addressing specifications, in this practical examination, the VLAN, OSPF, DNS servers and DHCP networks are used, which must have connectivity. Quality verified through the commands, the scenarios shows the software tool for all the devices of the "Cisco Packet Tracer" network.

The knowledge applied in the exam, are those used in LAN and WLAN networks of companies, which always seek to improve connectivity and reduce communication failures between servers with the connection through DHCP and IPV4 addressing. Companies are also looking for ways to better maintain networks in a more practical way.

# 1. Introducción

El presente trabajo tiene como fin evidenciar de manera práctica los conocimientos aprendidos en el diplomado de CCNA Cisco, conceptualizando sobre IPV4, IPV6,OSPFv2,Servicios de DHCP, Enrutamiento, NAT y listas de acceso ACL

Durante el curso de Cisco CCNA 1 y 2 se enfocó en la práctica de laboratorios para obtener los conocimientos funda necesarios para resolver los dos escenarios propuestos en este examen de habilidades prácticas, de esta forma se resuelven configurando los dispositivos de la red de manera adecuada y descrita en cada uno de los puntos, con las especificaciones del direccionamiento IPV4 y IPV6 , en este examen práctico también se aplican las configuraciones de las VLAN, OSPF, La configuración de servidores DNS y DHCP, los cuales deben tener la conectividad la cual es verificada mediante los comandos, los escenarios se desarrollan en la herramienta de software para emular todos los dispositivos de la red “Cisco Packet Tracer”.

Los conocimientos aplicados en el examen, son los que se aplican normalmente en las redes LAN y WLAN de las empresas, las cuales siempre buscan mejorar la conectividad y reducir las fallas de comunicación entre servidores con la conexión mediante DHCP y el direccionamiento IPV4.Actualmente las empresas también buscan la forma de dar un mejor mantenimiento a las redes de forma más práctica.

## 1.1. Justificación

El siguiente informe se presenta apartir del desarrollo del examen de habilidades practricas en el cual se aplican todos los conocimiento y las competencias obtenidas durante el seminario de CCNA Cisco, en el informen se describen los pasos de la solucion de cada uno de los problemas de Networking de los dos escenarios, los comandos para las configuraciones que se realizan en cada uno de los equipos en la tipologia de la red, de la misma forma los comandos para verificar la conectividad.

Se detallan el direcionamiento IP de acuedo a las tablas con las especificaiones, con el fin de que se cumpla la solucion de manera correcta se adjuntan las evidencias mediante las imágenes, del emulador “Cisco Packet Tracer”. En el cual como se ha mecionado anteriormente se desarrolla la solucion de los Escenarios.

En el escenario 1 se derasarrolla con el fin de demostrar las conocimientos de la configuracion de los servidores DHCP, RIPV2 y la Implemantacion NAT, al igual que las capacidades de configurar la tabla de direccionameinto y los enlaces trocales.

En el escenario 2 se desarrolla para demostrar las competacias de las configraciones de enrutamiento por OSPFv2 , habilitar DNS y la configuracion de las VLAN.

# 2. Objetivos

Demostras las competencias y conocimientos obtenidos durante el curso de CISCO CCNA, resolviendo los escenarios con la difentes problematicas que se presentan, realizando el enrutamiento OSPFv2 y configuracion de los servidores DHCP, RIPV2 y la Implemantacion NAT.

## 2.1. Objetivos Generales

Realizar la configuracion de los escenarios 1 y 2 poniendo en practica las basicas de igual forma conficar el enrutamiento entre las VLAN, OSPFv2, DHCP, NAT dinámica / estática.

## 2.2. Objetivos Específicos

- Determinar la conceptualizacion de forma practica en cuanto a la Tipologia de una red y los requisitos para la implementación.
- Realizar las configuraciones basicas de los switch y router propuestos en la actuvidad con IPV4 y los servicios de DHCP
- Realizar el enrutamiento entre las VLAN de cada area y OSPFv2
- Hacer el informe con evidencias donde se aplique y configure una solución práctica descrita en el escenario propuesto en la prueba de habilidades.
- crear los escenarios 1 y 2 de las actividades en la aplicación Packet Tracer
- Realizar las validaciones de l conectividad de los equipos mediante los comando descritos en la evaluación

# 3. Desarrollo de la Actividad Escenario 1

SITUACIÒN: En esta actividad, demostrará y reforzará su capacidad para implementar NAT, servidor de DHCP, RIPV2 y el routing entre VLAN, incluida la configuración de direcciones IP, las VLAN, los enlaces troncales y las subinterfaces. Todas las pruebas de alcance deben realizarse a través de ping únicamente

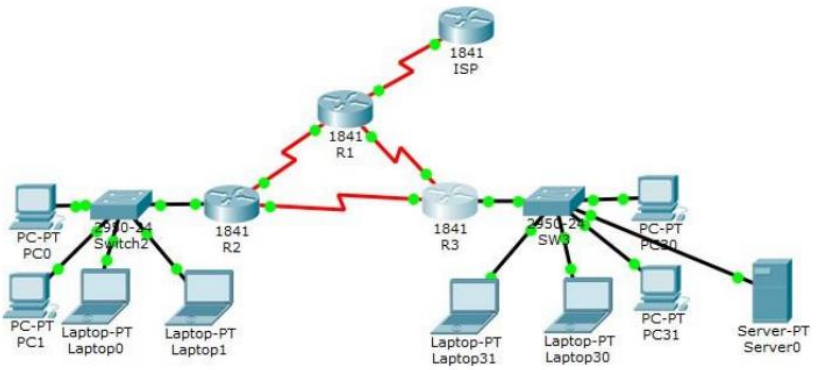



Figura 1: Escenario 1

**Tabla de direccionamiento**

| El administrador | Interfaces | Dirección IP | Máscara de subred | Gateway predeterminado |
|---|---|---|---|---|
| ISP | S0/0/0 | 200.123.211.1 | 255.255.255.0 | N/D |
| R1 | Se0/0/0 | 200.123.211.2 | 255.255.255.0 | N/D |
| | Se0/1/0 | 10.0.0.1 | 255.255.255.252 | N/D |
| | Se0/1/1 | 10.0.0.5 | 255.255.255.252 | N/D |
| R2 | Fa0/0,100 | 192.168.20.1 | 255.255.255.0 | N/D |
| | Fa0/0,200 | 192.168.21.1 | 255.255.255.0 | N/D |
| | Se0/0/0 | 10.0.0.2 | 255.255.255.252 | N/D |
| | Se0/0/1 | 10.0.0.9 | 255.255.255.252 | N/D |
| R3 | Fa0/0 | 192.168.30.1 | 255.255.255.0 | N/D |
| | | 2001:db8:130::9C0:80F:301 | /64 | N/D |
| | Se0/0/0 | 10.0.0.6 | 255.255.255.252 | N/D |
| | Se0/0/1 | 10.0.0.10 | 255.255.255.252 | N/D |
| SW2 | VLAN 100 | N/D | N/D | N/D |
| | VLAN 200 | N/D | N/D | N/D |
| SW3 | VLAN1 | N/D | N/D | N/D |

Figura 2: Tabla de Direccionamiento Escenario 1

**Tabla de asignación de VLAN y de puertos**

| Dispositivo | VLAN | Nombre | Interfaz |
|---|---|---|---|
| SW2 | 100 | LAPTOPS | Fa0/2-3 |
| SW2 | 200 | DESTOPS | Fa0/4-5 |
| SW3 | 1 | - | Todas las interfaces |

**Tabla de enlaces troncales**

| Dispositivo local | Interfaz local | Dispositivo remoto |
|---|---|---|
| SW2 | Fa0/2-3 | 100 |

Figura 3: Tablas de asignación y troncales Escenario 1

## Soluciòn en el Emulador “Cisco Packet Tracer”.

Se realiza la creacion de la red de acuerdo a la tipologia planteada en el escenario1 basados en la tabla de dierccionamiento IP y las trablas de asignacion de puertos troncales.

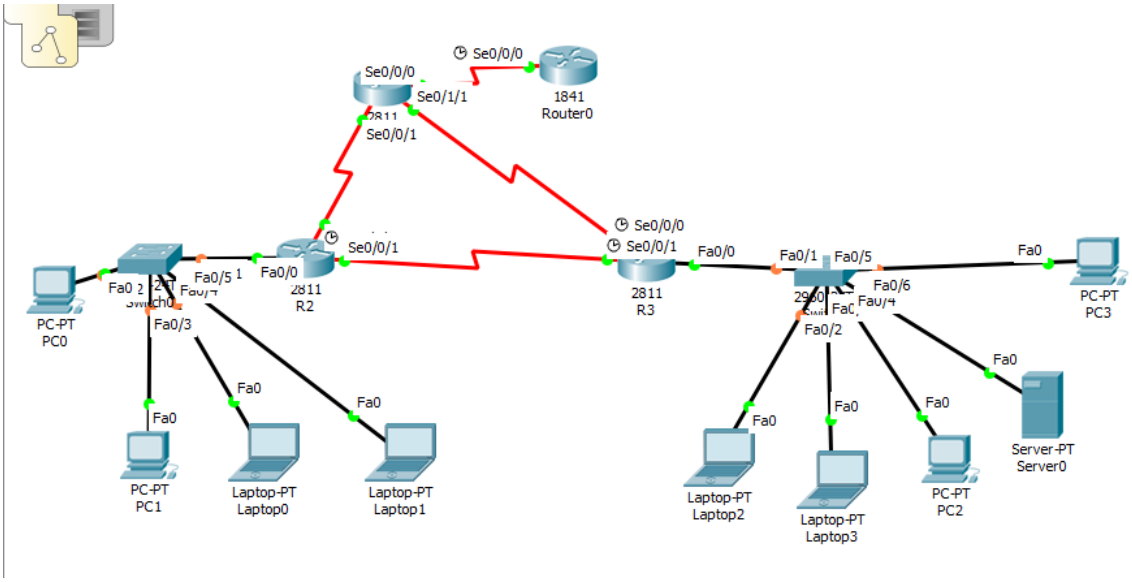



Figura 4: Crear el Escenario 1

A continuación, se detallan los comandos para la configuración básica de la Red descrita en el escenario

**ROUTER ISP**

```
Router>en
Router#config t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname ISP
ISP(config)#enable secret class
ISP(config)#line con 0
ISP(config-line)#pass cisco
ISP(config-line)#login
ISP(config-line)#line vty 0 4
ISP(config-line)#login
% Login disabled on line 194, until 'password' is set
% Login disabled on line 195, until 'password' is set
% Login disabled on line 196, until 'password' is set
% Login disabled on line 197, until 'password' is set
% Login disabled on line 198, until 'password' is set
ISP(config-line)#service password-encryption
ISP(config)#banner motd $solo acceso Autorizado$
%SYS-5-CONFIG_I: Configured from console by console
```

**ROUTER R1**

```
en
config t
Enter configuration commands, one per line. End with CNTL/Z.
hostname R1
enable secret class
line con 0
pass cisco
login
line vty 0 4
login
service password-encryption
banner motd $solo acceso Autorizado$
```

**ROUTER R2**

```
Router#config t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname R2
R2(config)#enable secret class
R2(config)#line con 0
R2(config-line)#pass cisco
R2(config-line)#login
R2(config-line)#line vty 0 4
R2(config-line)#login
% Login disabled on line 322, until 'password' is set
% Login disabled on line 323, until 'password' is set
% Login disabled on line 324, until 'password' is set
% Login disabled on line 325, until 'password' is set
% Login disabled on line 326, until 'password' is set
R2(config-line)#service password-encryption
```

## 3.1. SW1 VLAN y las asignaciones de puertos de VLAN.

A continuación, se muestran los comandos que se ejecutan mediante el (CLI) Command Line Comand Interface en el SW 1

```
Switch>en
Switch #configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch (config)#vlan 100
Switch (config-vlan)#name LAPTOPS
Switch (config-vlan)#exit
Switch (config)#vlan 200
Switch (config-vlan)#name DESKTOPS
Switch (config-vlan)#exit
Switch (config)#interface range fa0/2 - 3
Switch (config-if-range)# switchport mode trunk
Switch (config-if-range)#switchport trunk native vlan 100
Switch (config-if-range)#no sh
```

Switch (config-if-range)#exit
Switch (config)#interface range fa0/4 – 5
Switch (config-if-range)#port access vlan 200
Switch (config-if-range)#no sh
Switch (config-if-range)#exit

Asignación de enlace troncal en fa0/1 Se habilita el Puerto fa0/1 como troncal para que permita la transmisión de datos de las VLANS

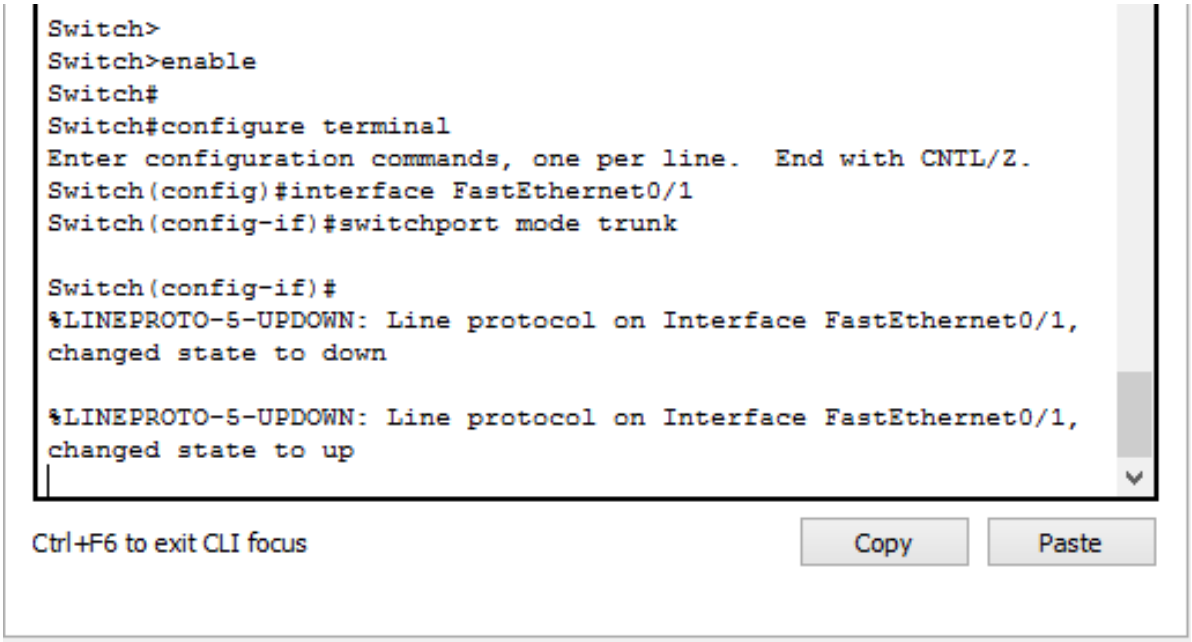


Figura 5: Asignación de Enlace Troncal

Switch (config)#interface fa0/1
Switch (config-if)#switchport mode trunk

## 3.2. Configuración Los puertos de red que no se utilizan se deben deshabilitar.

Se selecciona el rango de las fastethernet que no son utilizadas y se ejecuta el comando Shutdown para deshabilitarlas estos puertos no interfieren en la conectividad

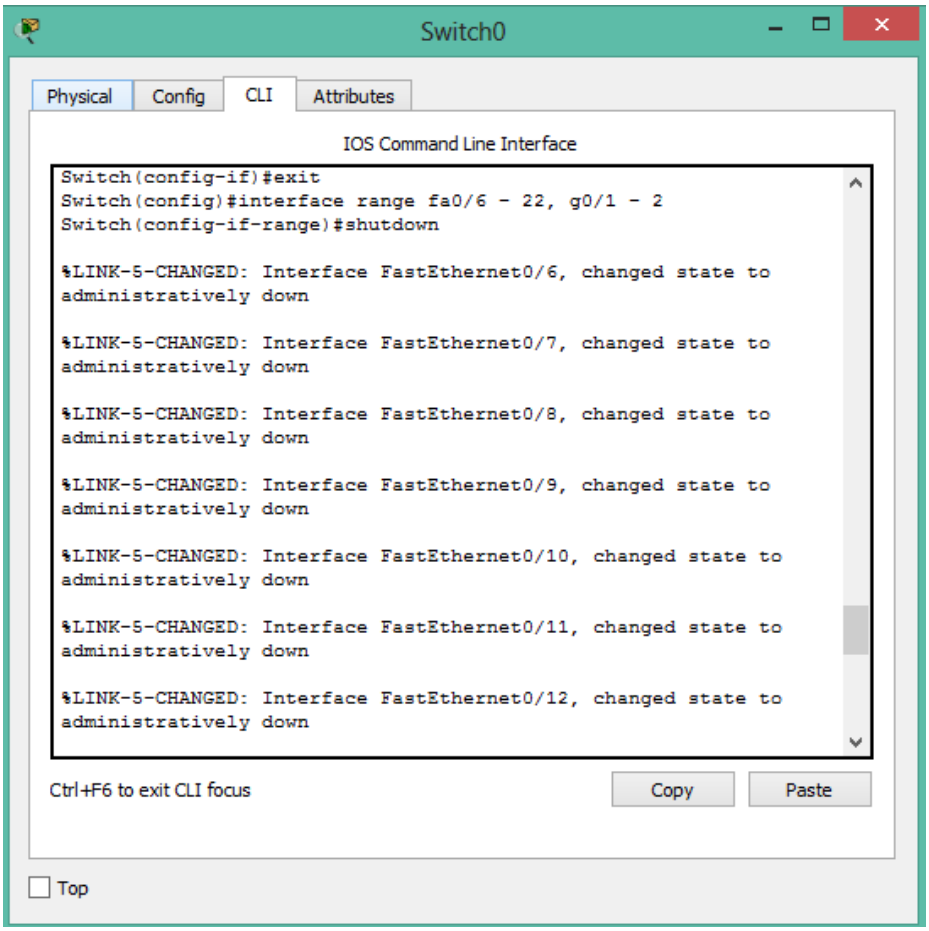



Figura 6: Deshabilitar Puertos Escenario 1

## 3.3. La información de dirección IP R1, R2 y R3 debe cumplir con la tabla 1.

**ROUTER ISP**

ISP(config)#int s0/0/0
ISP(config-if)#ip add 200.123.211.1 255.255.255.0
ISP(config-if)#clock rate 128000
ISP(config-if)#no sh
ISP#

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

**ROUTER R1**

int s0/0/0

clock rate 128000

ip add 200.123.211.2 255.255.255.0

clock rate 128000

int s0/1/0

clock rate 128000

ip add 10.0.0.1 255.255.255.252

clock rate 128000

int s0/1/1

clock rate 128000

ip add 10.0.0.5 255.255.255.252

clock rate 128000

no sh

**ROUTER R2**

R2(config)#int f0/0.100

R2(config-subif)#ip add 192.168.20.1 255.255.255.0

## 3.4. Laptop20, Laptop21, PC20, PC21, Laptop30, Laptop31, PC30 y PC31 deben obtener información IPv4 del servidor DHCP.

## 3.5. R1 debe realizar una NAT con sobrecarga sobre una dirección IPv4 pública. Asegúrese de que todos los terminales pueden comunicarse con Internet pública (haga ping a la dirección ISP) y la lista de acceso estándar se llama INSIDE-DEVS.

Se realizan los siguientes comandos de configuración en R1 para realizar la NAT

R1#config t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#ip nat pool NAT-POOL2 10.0.0.2 10.0.0.40 netmask 255.255.255.192

Se ejecuta el comando de ACL la lista de control para permitir el acceso de las IP anteriores

R1(config)#access-list 1 permit 192.168.0.0 0.0.255.255
R1(config)#ip nat inside source list 1 pool NAT-POOL2 overload
R1(config)#int s0/1/1
R1(config-if)#ip nat outside
R1(config-if)#int s0/0/0
R1(config-if)#ip nat inside

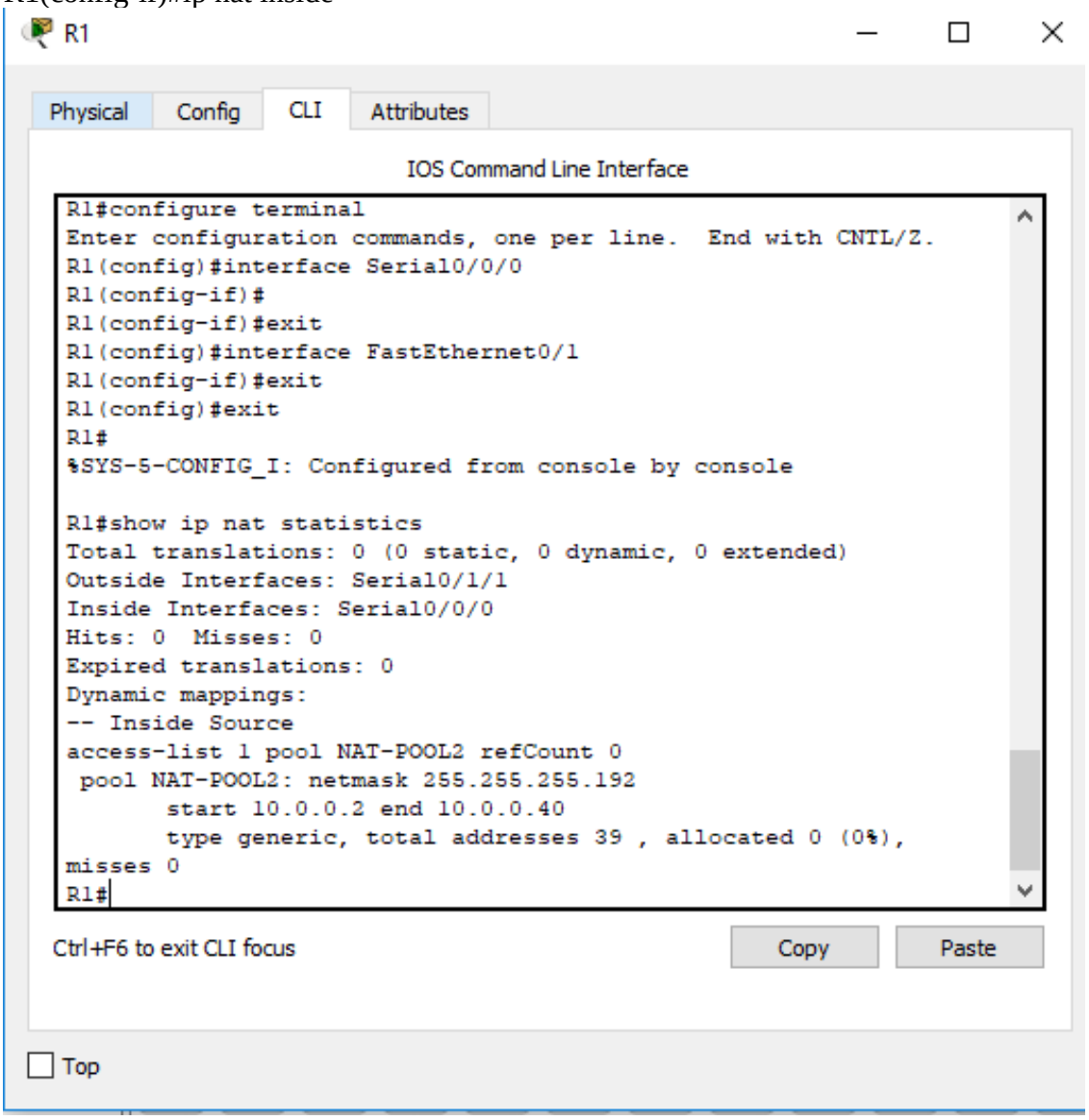



Figura 7: NAT Y Lista De Control De Acceso

## 3.6. R1 debe tener una ruta estática predeterminada al ISP que se configuró y que incluye esa ruta en el dominio RIPv2.

Para la configuración se utiliza el comando passive-interface. Para la configuración de la ruta

```
R1(config-router)#passive-interface S0/0/0
R1(config-router)#network 200.123.211.2
```

## 3.7. R2 es un servidor de DHCP para los dispositivos conectados al puerto FastEthernet0/0.

Se realiza la configuración en R2 DHCP para asignar el conjunto de direcciones mediante le comando IP DHCP POOL

```
R2(config)#ip dhcp pool DHCP_P1
R2(dhcp-config)#network 192.168.0.0 255.255.255.255
R2(dhcp-config)#default-router 192.168.0.0 255.255.255.255
R2(dhcp-config)#dns-server 192.168.30.6
R2(dhcp-config)#exit
```

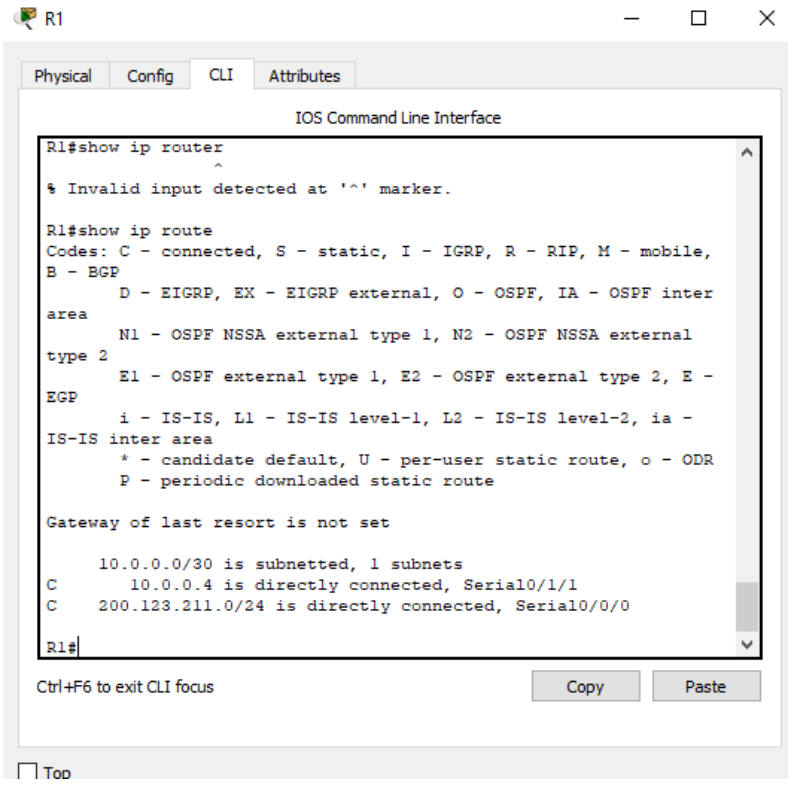



Figura 8: configuración servidor DHCP

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

```
R2#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#int vlan 100
R2(config-if)#ip address 192.168.20.1 255.255.255.0
% 192.168.20.0 overlaps with FastEthernet0/0.100
R2(config-if)#exit
R2(config)#int vlan 200
R2(config-if)#ip address 192.168.21.1 255.255.255.0
% 192.168.21.0 overlaps with FastEthernet0/0.200
25
R2(config-if)#exit
R2(config)#end
```

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

```
R3(config-if)#ipv6 dhcp pool CISCO
R3(config-dhcpv6)#prefix-delegation pool LOCAL-HOSTS
R3(config-dhcpv6)#dns-server AAAA:BBBB:CCCC:DDDD::FFFF
R3(config-dhcpv6)#domain-name cisco.com
R3(config-dhcpv6)#ipv6 local pool LOCAL-HOSTS 2001:A:A:A::/64 64
% Pool is reserved by IPv6 Localpool
R3(config)#interface FastEthernet0/0
R3(config-if)#no ip address
R3(config-if)#duplex auto
R3(config-if)#speed auto
R3(config-if)#ipv6 address FE80::1 link-local
R3(config-if)#ipv6 address 2001:A:A:A::1/64
R3(config-if)#ipv6 nd managed-config-flag
R3(config-if)#ipv6 dhcp server CISCO
```

3.10. La NIC instalado en direcciones IPv4 e IPv6 de Laptop30, de Laptop31, de PC30 y obligación de configurados PC31 simultáneas (dual-stack). Las direcciones se deben configurar mediante DHCP y DHCPv6.

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

```
R2>enable
R2#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#ip dhcp excluded-address 10.0.0.2 10.0.0.9
R2(config)#ip dhcp pool INSIDE-DEVS
R2(dhcp-config)#network 192.168.20.1 255.255.255.0
R2(dhcp-config)#network 192.168.21.1 255.255.255.0
R2(dhcp-config)#default-router 192.168.1.1
R2(dhcp-config)#dns-server 0.0.0.0
R2(dhcp-config)#exit
R2(config)#exit
```

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

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

```
Configuración para R1
R1>enable
R1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#router rip
R1(config-router)#version 2
R1(config-router)#network 10.0.0.0
R1(config-router)#network 10.0.0.4
R1(config-router)#end
R1#
%SYS-5-CONFIG_I: Configured from console by console
R1#wr
Building configuration...
Configuración para R2
R2>enable
R2#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
```

```
R2(config)#router rip
R2(config-router)#version 2
R2(config-router)#network 10.0.0.0
R2(config-router)#network 10.0.0.8
R2(config-router)#end
R2#
```

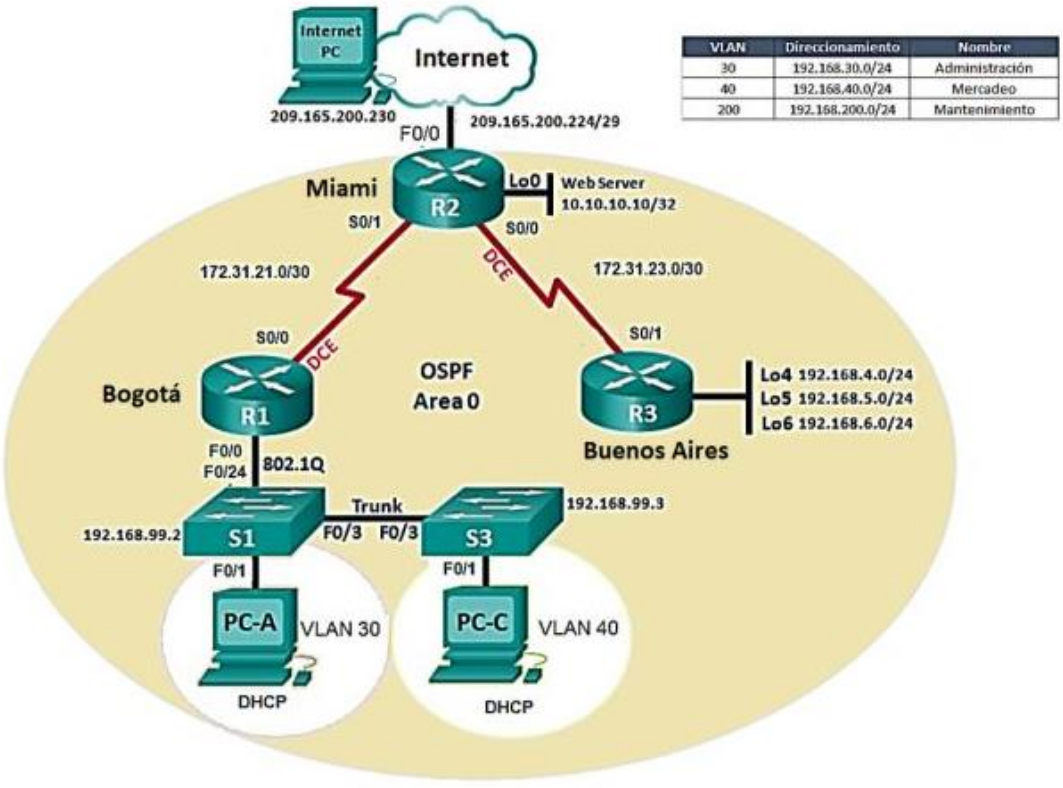
Configuración para R3

```
R3>enable
R3#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#router rip
R3(config-router)#version 2
R3(config-router)#network 10.0.0.0
R3(config-router)#network 10.0.0.8
R3(config-router)#end
```

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

## 4. Desarrollo de la Actividad Escenario 2

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




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

## 4.1. Tipología Escenario 2

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

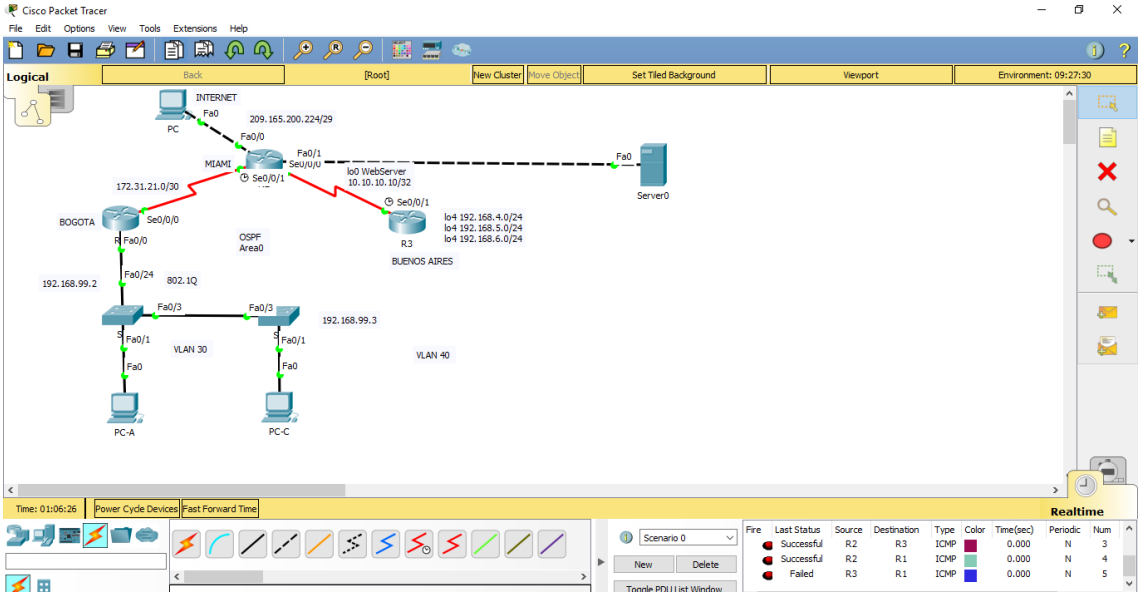



Figura 9: Creacion de la tipologia Escenario 2

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

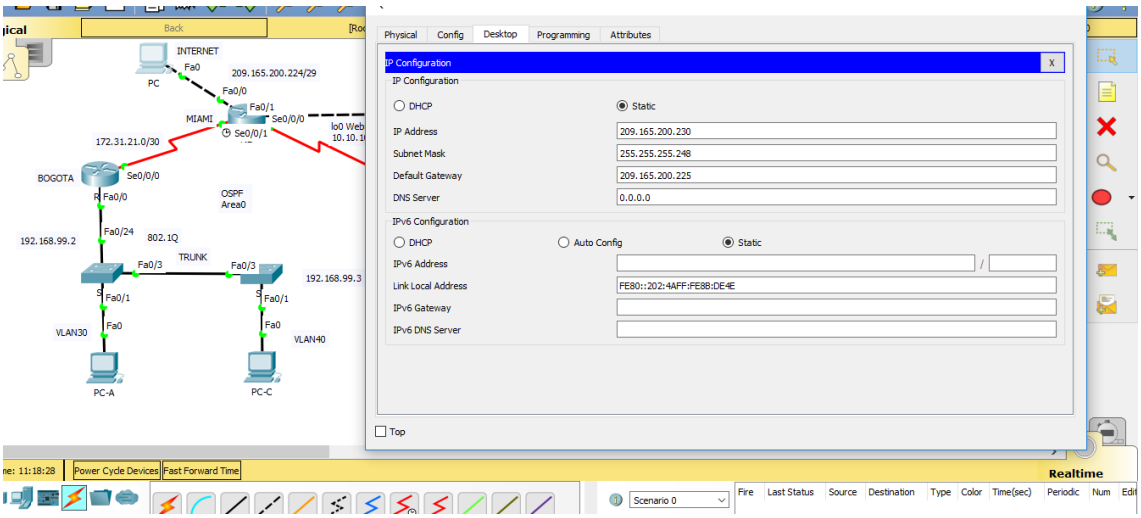



Figura 9: Configuración de las IP de acuerdo a la Tipologia

## 4.3. Configurar el protocolo de enrutamiento

Enrutamiento RIPV2

```
R1# config t
R1(config)# router rip
R1(config-router)# version 2
R1(config-router)# passive-interface g0/1
R1(config-router)# network 172.30.0.0
R1(config-router)# network 10.0.0.0
```

## 4.4. Visualizar tablas de enrutamiento y routers conectados por OSPFv2

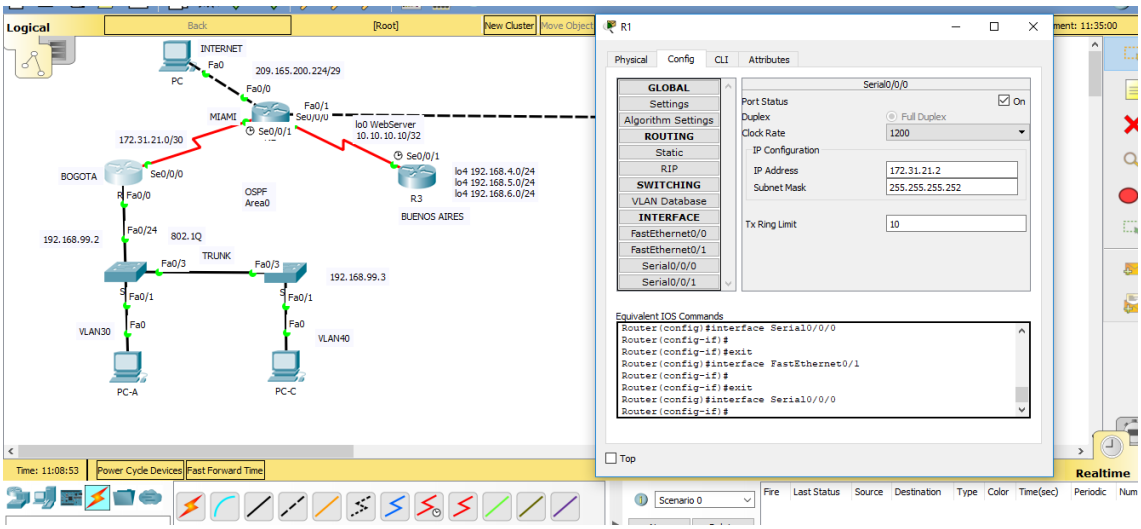



Figura 10: Configuración de las VLAN R1

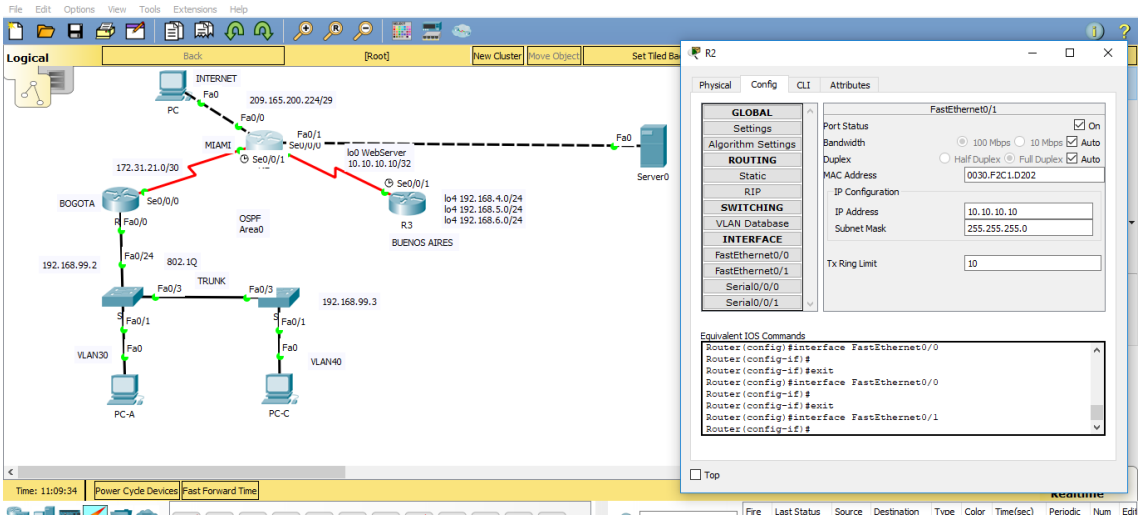



Figura 11: Configuración de las VLAN R2

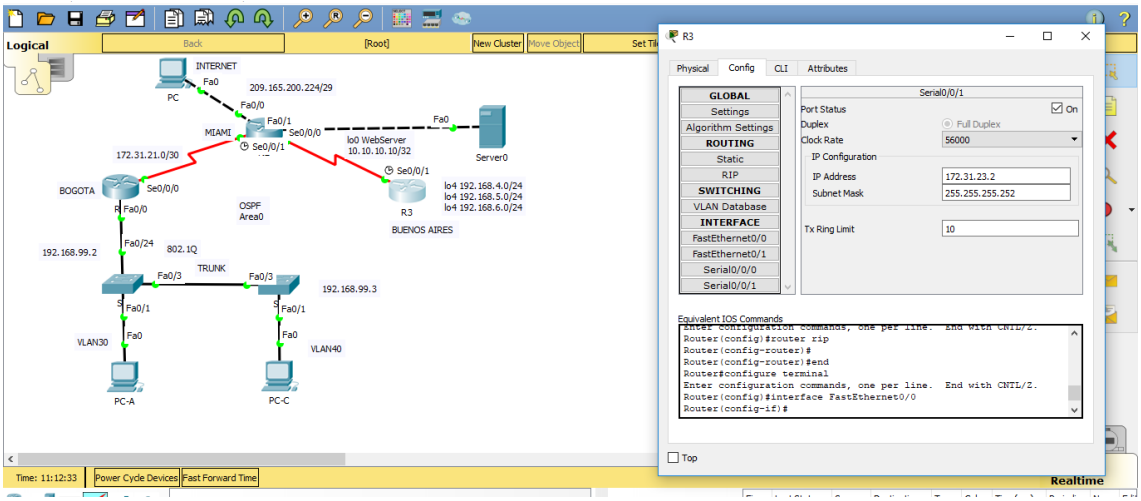
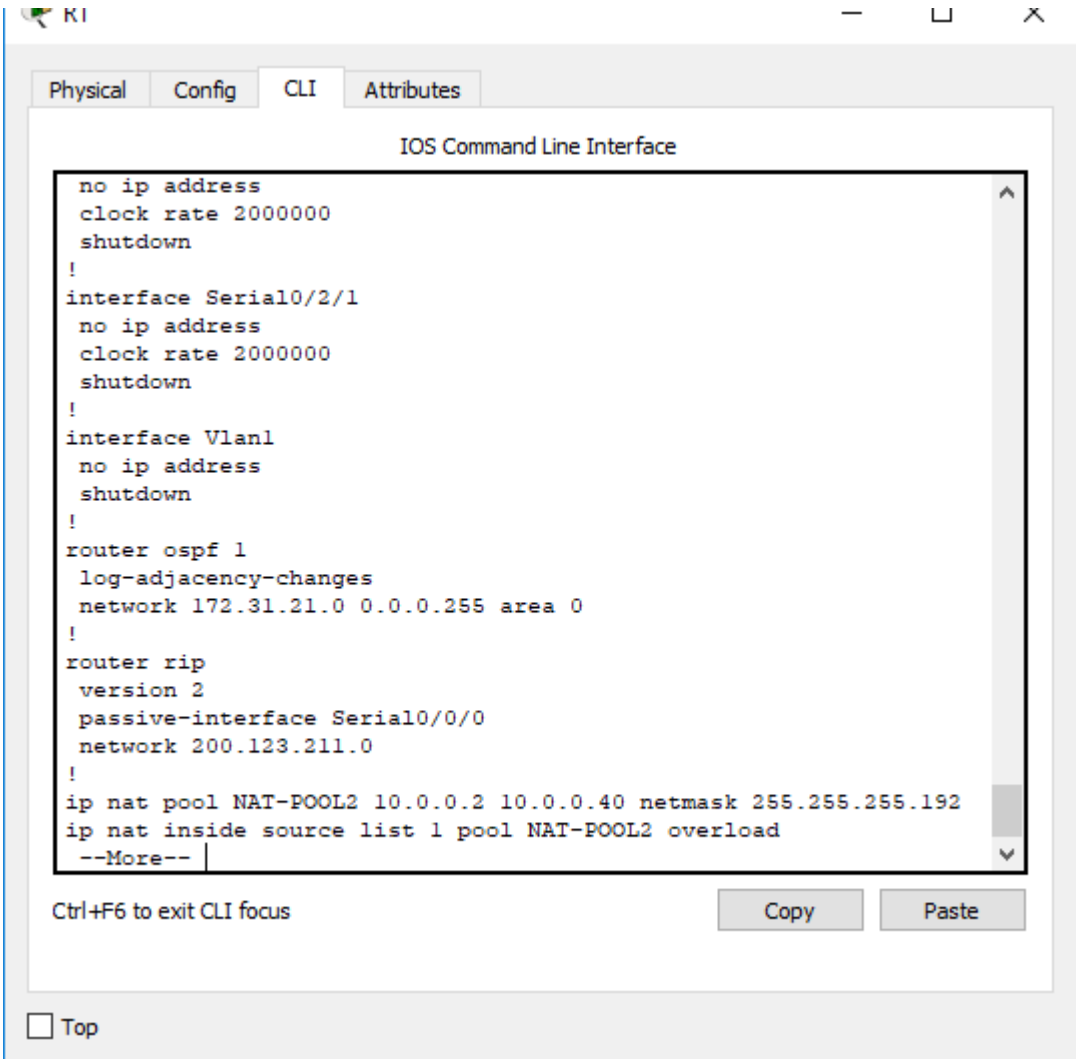



Figura 12: Configuración de las VLAN R3

## 4.5. Visualizar lista resumida de interfaces por OSPF en donde se ilustre el costo de cada interface

Se ejecuta el comando para ver la configuración OSPF




Se visualizar que la interfaz S0/0/0 quedo con la configuración del protocolo de enrutamiento OSPF1, esta acción se repite en los Routers

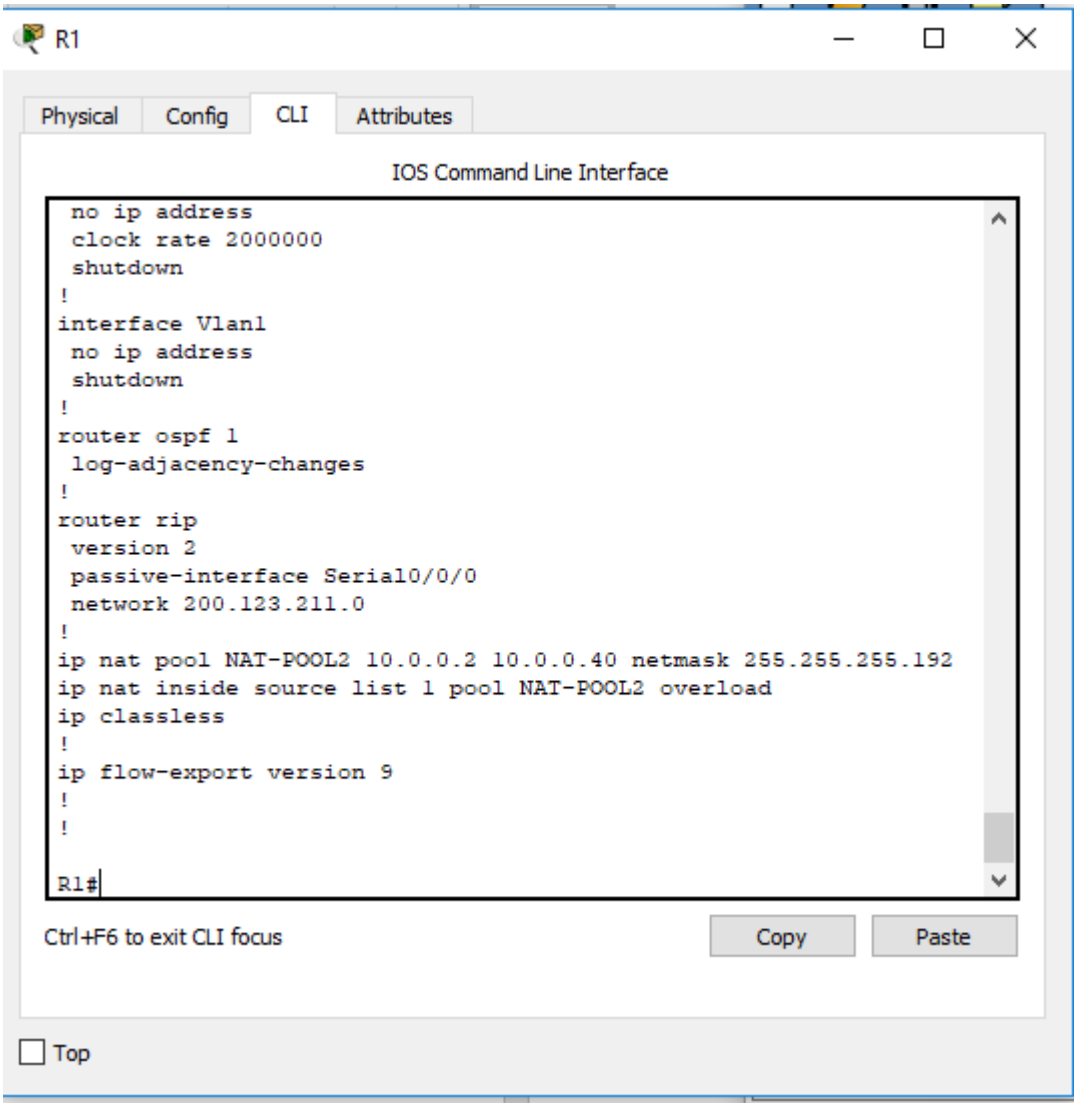



Figura 13: visualización de la configuración OSPF

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

R1(config)#route ospf 1

R1(config-route)#network 172.31.21.0.0.0.255 area 0

R1(config-route)#router-id 1.1.1.1

R1(config)#route ospf 1

R1(config-route)#passive-interfase g0/0

R2(config)#route ospf 1

R2(config-route)#network 172.31.21.0.0.0.0 area 0

R2(config-route)#network 172.31.23.0.0.0.0 area 0

R2(config-route)#router-id 2.2.2.2

R2(config)#route ospf 1

R2(config-route)#passive-interface g0/0

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

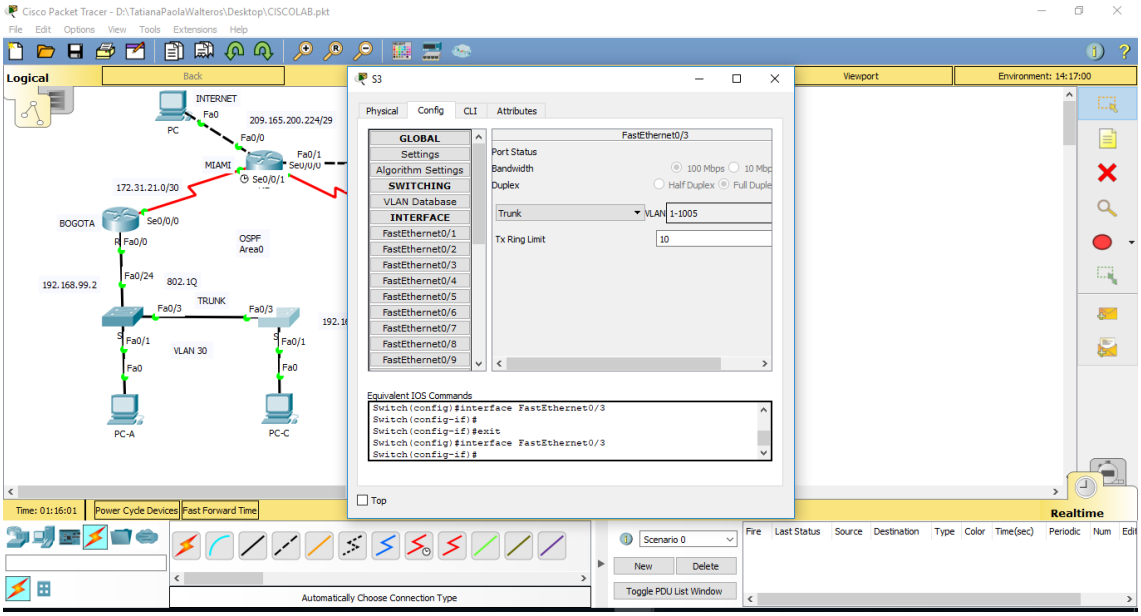



Figura 14: Configuración de las VLAN

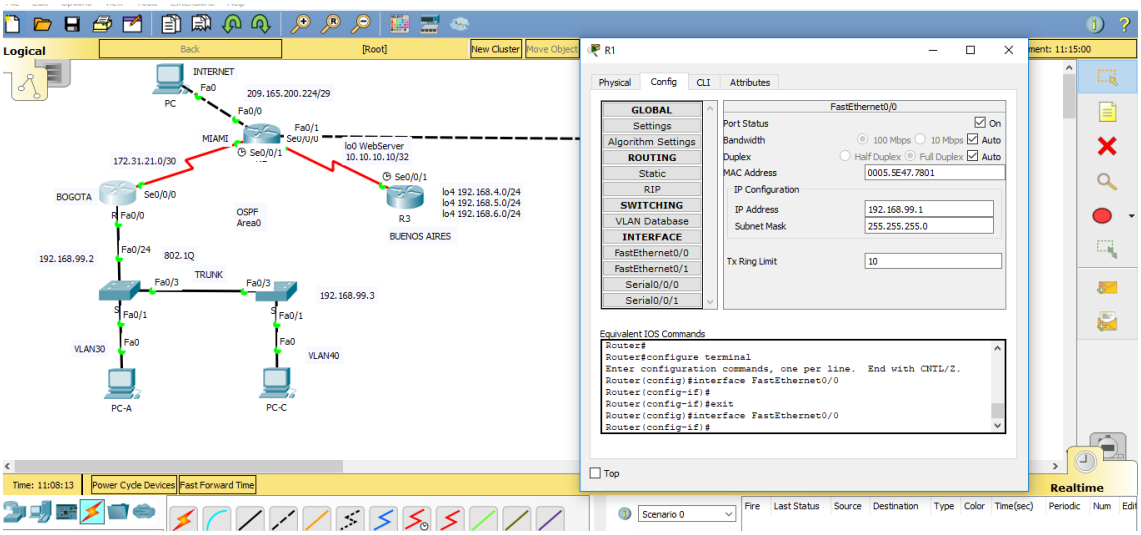
R1(config)#route ospf 1

R1(config-route)#network 172.31.21.0.0.0.3 area 0

R1(config-route)#router-id 1.1.1.1

R1(config)#route ospf 1

R1(config-route)#passive-interfase g0/0




## 4.8. Deshabilitar Domain Lookup

Se ejecuta el comando para deshabilitar en R3 el Domain

R3(config)#no ip domain-lookup
R3(config)

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

Se ejecutan los comandos de control de listas de acceso para permitir la salida desde R2

R2(config)#access-list 10 PERMIT 172.31.0. 0.0.0.0.255
R2(config)#int s0/0/1
R2(config-if)#ip access-group 10
R2(config-if)#ip access-group 10 in
R2(config-if)#
R2#
%SYS-5-CONFIG_I: Configured from console by console

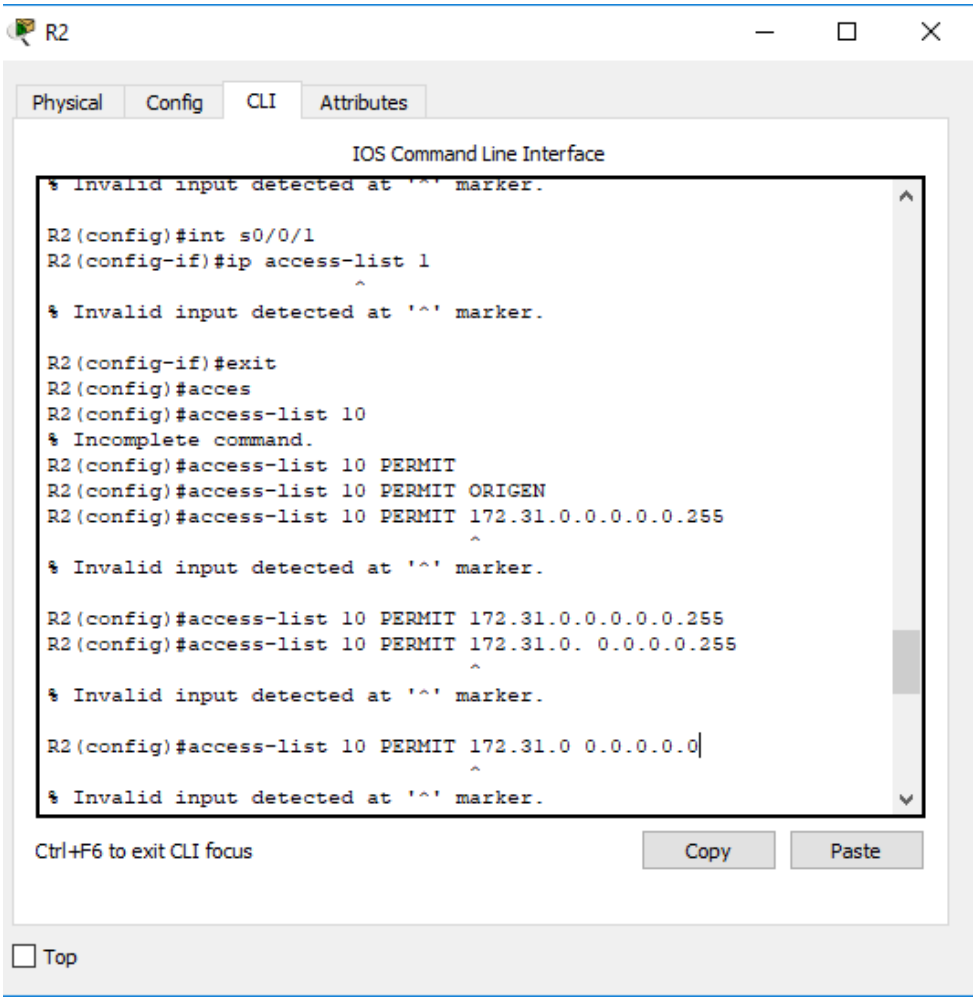



Figura 15: se crea la Access list estándar numero de identificación 10 para el Router R2 con Ip 172.31.0.0 con wildcard 0.0.0.255 y se le asigna a la interfaz s0/0/1 para que permita la salida de internet

## 4.10. Configurar al menos dos listas de acceso de tipo estándar a su criterio en para restringir o permitir tráfico desde R1 o R3 hacia R2.

```
R1(config-if)#
%LINK-5-CHANGED: Interface Serial0/0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1, changed state to up
no ip address
R1(config-if)#ip address
% Incomplete command.
R1(config-if)#ip address 10.0.0.10 255.255.255.252
R1(config-if)#ip address 10.0.0.10 255.255.255.252
R1(config-if)#clock rate 64000
This command applies only to DCE interfaces
R1(config-if)#
```

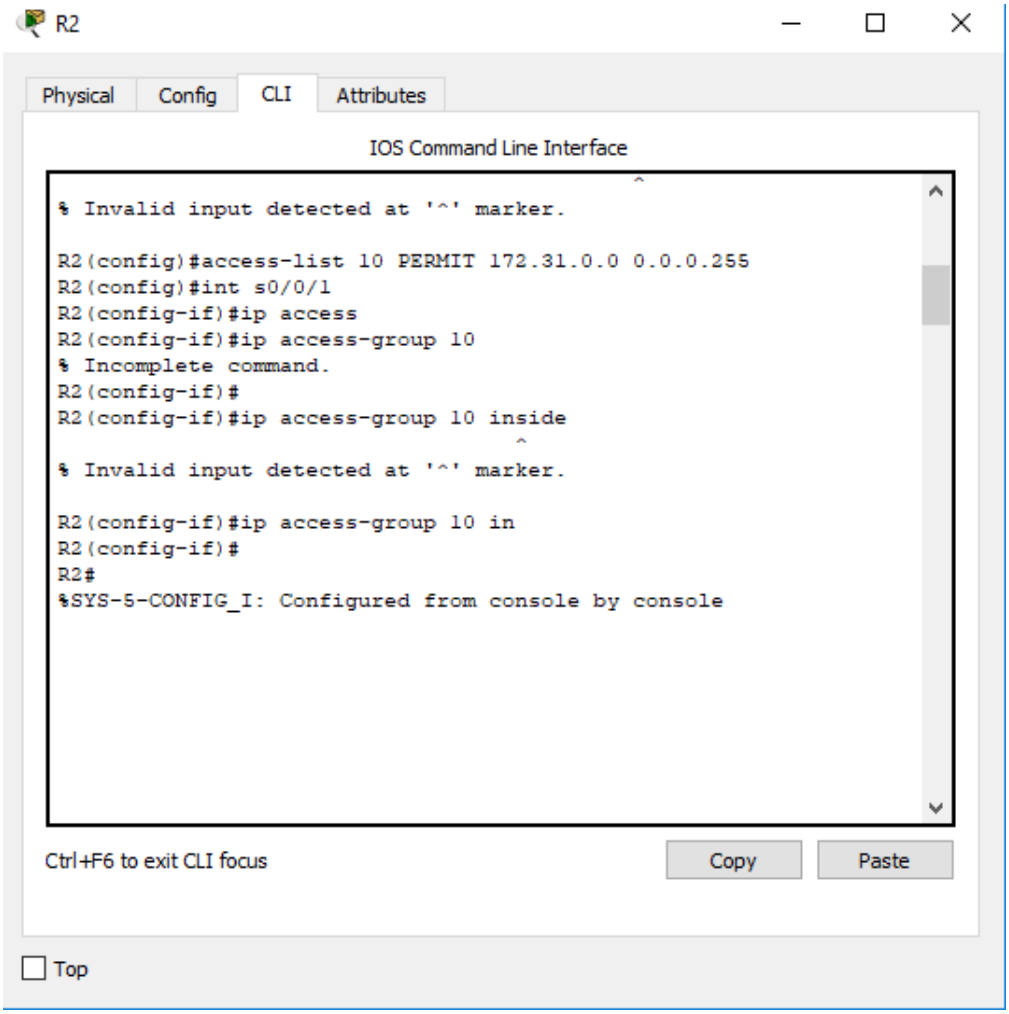



Figura 16: Configuración de las listas de acceso en R2

4.11. Configurar al menos dos listas de acceso de tipo extendido o nombradas a su criterio en para restringir o permitir tráfico desde R1 o R3 hacia R2.

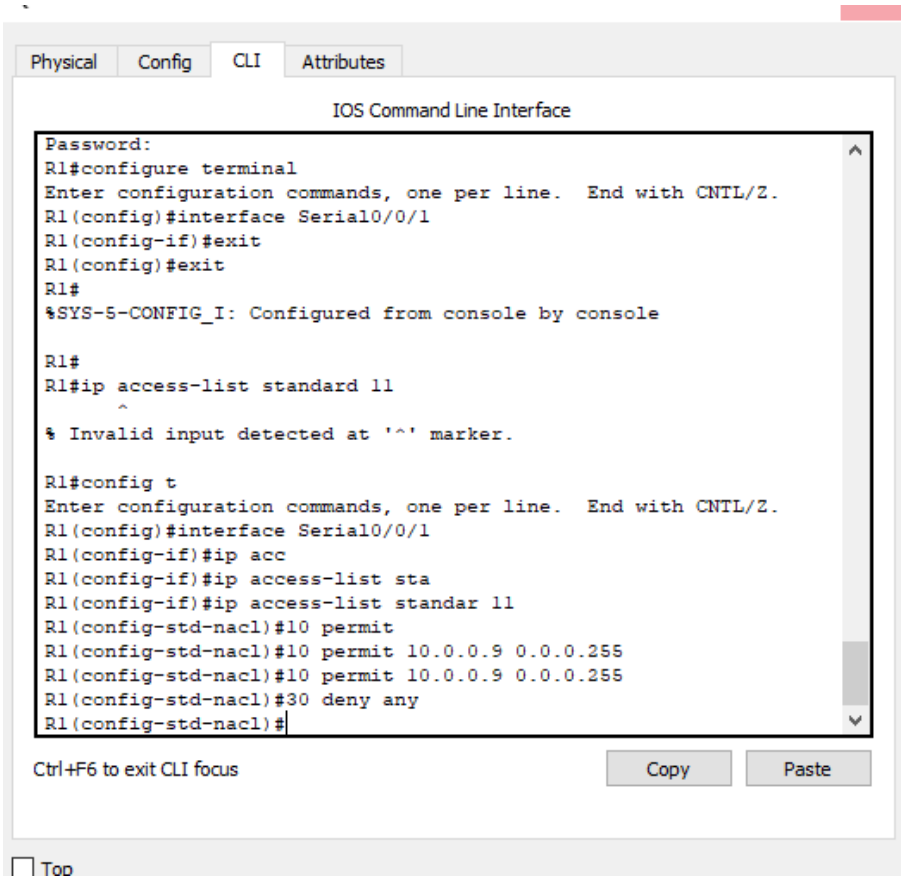



Figura 12: Configuración de las listas de acceso R1

# 5. Conclusiones

- las VLAN: (Red de área local virtual). son Mecanismo para crear redes lógicamente independientes, pero dentro de una misma red física. Las LAN virtuales permiten agrupar a los usuarios por departamento u equipo y la única forma de lograr comunicación entre ellas es por medio de un enrutador.
- Los SWITCH: generalmente de capa 2, pero hay algunos de capa 3. Toman decisiones de envió con base a las direcciones MAC que van de las tramas que envían los dispositivos.
- Las listas de control de acceso se utilizan como medida de seguridad lógica, ya que su cometido siempre es controlar el acceso a los recursos o activos del sistema.
- El servicio DHCP del Servidor que les proporciona a los clientes de una red IP la configuración necesaria para que puedan tener acceso a ella. Algunos de los parámetros que suministra el DHCP son la máscara de subred, la puerta de enlace, la dirección IP. Este protocolo facilita la administración de la red.
- El ISP es la empresa que le provee acceso a Internet. Por lo general, este servicio se realiza a través de una línea telefónica con un enlace dial up, o bien mediante enlaces dedicados que funcionan a altas velocidades.

# 6. Bibliografía


- CISCO. (2014). OSPF de una sola área. Principios de Enrutamiento y Conmutación. Recuperado de:https://static-course-assets.s3.amazonaws.com/RSE50ES/module8/index.html#8.0.1.1
- CISCO. (2014). Enrutamiento Dinámico. Principios de Enrutamiento y Conmutación. Recuperado de: https://static-course-assets.s3.amazonaws.com/RSE50ES/module7/index.html#7.0.1.1
- CISCO. (2014). Listas de control de acceso. Principios de Enrutamiento y Conmutación. Recuperado de:
- https://static-course-assets.s3.amazonaws.com/RSE50ES/module9/index.html#9.0.1.1
- CISCO. (2014). DHCP. Principios de Enrutamiento y Conmutación. Recuperado de: https://static-course-
- assets.s3.amazonaws.com/RSE50ES/module10/index.html#10.0.1.1
- CISCO. (2014). Traducción de direcciones IP para IPv4. Principios de Enrutamiento y Conmutación. Recuperado
- de: https://static-course-assets.s3.amazonaws.com/RSE50ES/module11/index.html#11.0.1.1