

PRUEBA DE HABILIDADES PRACTICAS CCNA

PRESENTADO POR:

ROBERTO ROGER REYES JOJOA

TUTOR:

DIEGO EDINSON RAMIREZ

**UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD
ESCUELA DE CIENCIAS BÁSICAS DE TECNOLOGÍA E INGENIERÍA -
ECBTI
PROGRAMA DE INGENIERÍA DE SISTEMAS
MAYO DE 2019**

Resumen

Entender el papel tan importante que desempeñan las redes y el uso de las tecnologías que aplican al mundo de las redes a nivel mundial y que en nuestro país ha tenido un gran desarrollo durante los últimos 10 años con una amplia cobertura del internet en Colombia, alcanzando coberturas en la mayoría de la población. EL uso de todo tipo de topologías y redes de ha convertido en una necesidad muy importante en las instituciones educativas como colegios, universidades, empresas, hospitales, empresas públicas y privadas las cuales necesitan optimizar su desempeño y gestiones.

Razón por la cual este curso de CISCO para soluciones integradas LAN/WAN pone a prueba todas las habilidades y conocimientos previos los cuales mediante un estudio y análisis previo se han llevado a una construcción y diseño mediante ayuda del programa PACKET TRACER en cual es una simulación real a casos prácticos y comunes que incluye todas las herramientas necesarias para ejecutar diferentes requerimientos , es así que en el estudio del curso se aplico los conocimientos de los dos módulos tanto del modulo CCNA 1 R&S y el modulo CCNA 2 R&S en convenio con CISCO Networking Academy el cual mediante un trabajo paralelo y la plataforma de la universidad nacional abierta y a distancia UNAD se logro llevar un trabajo continuo y de mucho apoyo.

Abstract

Understand the important role that networks play and the use of technologies that apply to the world of networks worldwide and that in our country has had a great development during the last 10 years with a wide coverage of the internet in Colombia, reaching coverage in the majority of the population. The use of all types of topologies and networks has become a very important need in educational institutions such as schools, universities, companies, hospitals, public and private companies which need to optimize their performance and management.

Reason why this course of CISCO for integrated solutions LAN / WAN tests all the previous skills and knowledge which through a previous study and analysis have led to a construction and design by means of the PACKET TRACER program in which is a simulation Real to practical and common cases that includes all the necessary tools to execute different requirements, it is so in the study of the course I applied the knowledge of the two modules of the module CCNA 1 R & S and the module CCNA 2 R & S in agreement with CISCO Networking Academy which through a parallel work and the platform of the national university open and distance UNAD was able to carry a continuous work and a lot of support.

Tabla de contenido

PRUEBA DE HABILIDADES PRACTICAS CCNA.....	1
1. ESCENARIO 1.....	8
1.1 creando los dispositivos de la red.....	8
1.2 Encendiendo los puertos	9
1.3 Configuración de usuario y contraseña.....	11
1.4 Verificación de usuario y contraseña.....	12
1.5 Configurando enrutamiento ripv2.....	12
1.6 Verificando el correcto funcionamiento de la red.....	14
1.7 Verificación de la tabla de direccionamiento	15
1.7 Revisando el balanceo de carga	21
1.8 Configurando interfaces pasivas.....	23
1.9. Verificando interfaz pasiva.....	24
1.9 Verificando funcionalidad general después de la implementación de la interfases pasivas	25
1.10 Configuración de encapsulación ppp	26
1.11 AUTENTICACION MEDIANTE pap	27
1.12 AUTENTICACION MEDIANTE CHAT	29
1.13 CONFIGURACION PAT	30

1.14 Configuración de DHCP	35
Escenario 2	39
2.1 Implementando los dispositivos de la red	40
2.2 configuración vlan	41
2.3 enrutamiento ospf	47
2.4 Configuración inter-vlan	51
2.5 Desactivar las dns	57
2.6 Configuración nat	59
2.7 Listas de acceso estándar	66

INTRODUCCION

A lo largo de los dos cursos tanto como del CCNA-1 y CCNA-2 se han venido desarrollando una cantidad importante de actividades , así como de evaluaciones de los 21 capítulos que contienen los dos cursos , simultáneamente se han venido trabajando un número significativo de ejercicios prácticos en la plataforma de la UNAD los cuales han sido en su totalidad prácticos y colaborativos , en conjunto con las dos plataformas tanto de CISCO NETCAP como la de la universidad nacional abierta y a distancia se lograron varias metas que son de suprema importancia en el campo profesional en la implementación de soluciones de redes LAN y WAN con un amplio sentido teórico y práctico en participación y apoyo de grupos de trabajo .

Razón por la cual en esta práctica de habilidades se pondrá todo nuestro conocimiento aprendido durante las dos partes del curso y a su vez fortalecerá la versatilidad y desempeño como futuros profesionales.

Objetivos

General

Implementar las destrezas , habilidades y conocimientos en el area de redes que permitan evidenciar el desempeño aprendido durante las dos unidades del curso CISCO que conlleven a crear soluciones practicas y reales a cada uno de los ambientes propuestos .

Especificos

Identificar la topologia mediante un analisis general para luego aplicar los dispositivos mas acordes al escenario planteado

Configurar dispositivos de comunicacion como: servidores, Routers y Switch.

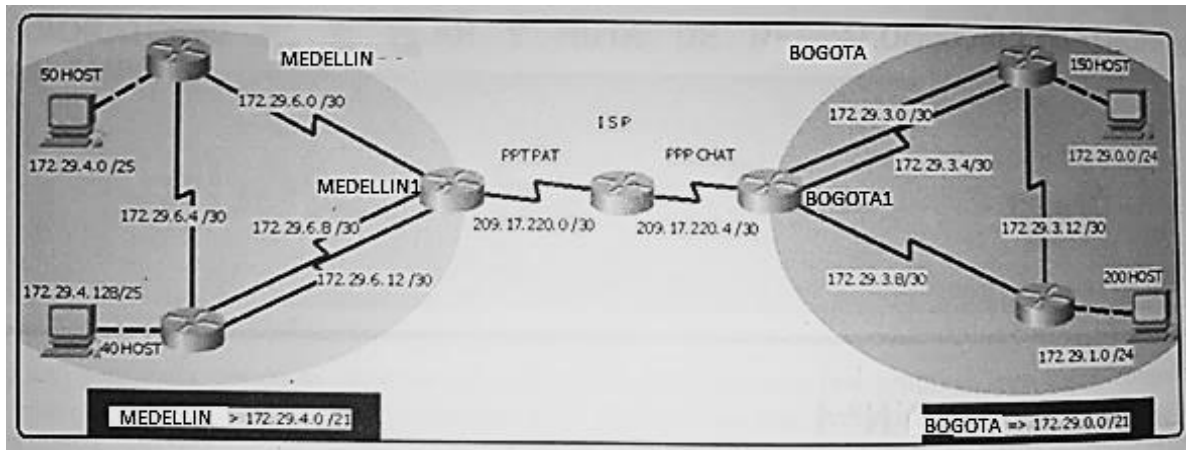
Implementar los protocolos necesarios para que las redes tengan una seguridad confiable

aplicar el protocolo DHCP y NAT en dispositivos de comunicaci3n.

Revizar la conectividad entre los dispositivos realizada a los dos escenarios que fueron propuestos para el desarrollo de la actividad.

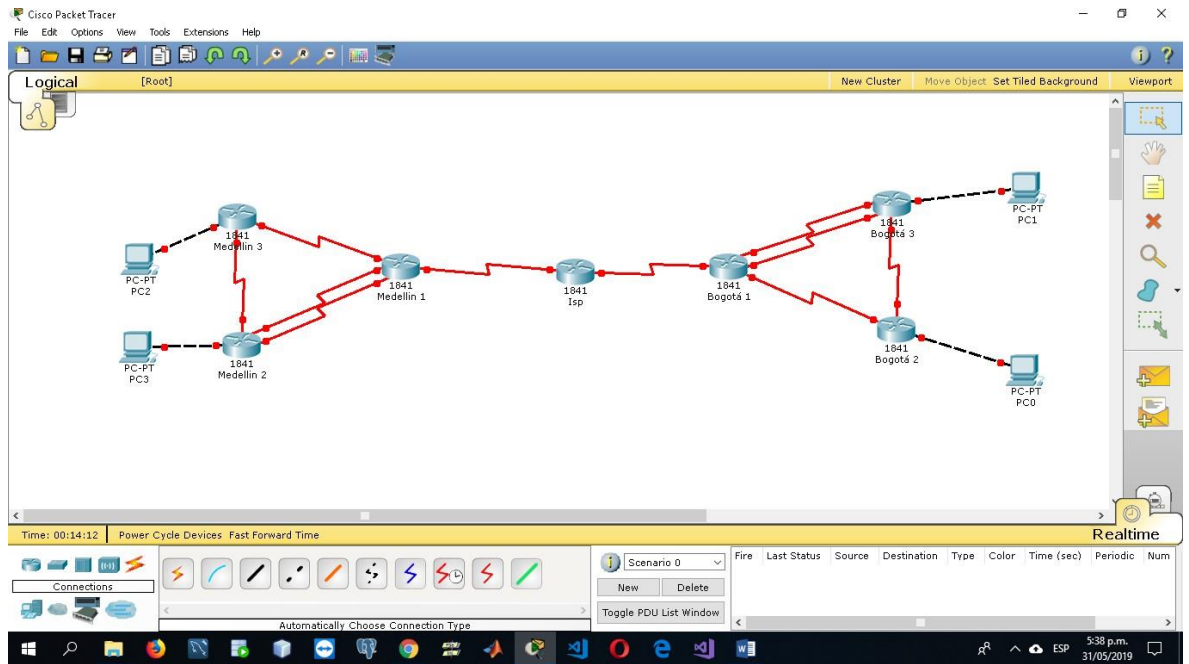
1. ESCENARIO 1

Una empresa posee sucursales distribuidas en las ciudades de Bogotá y Medellín, 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.



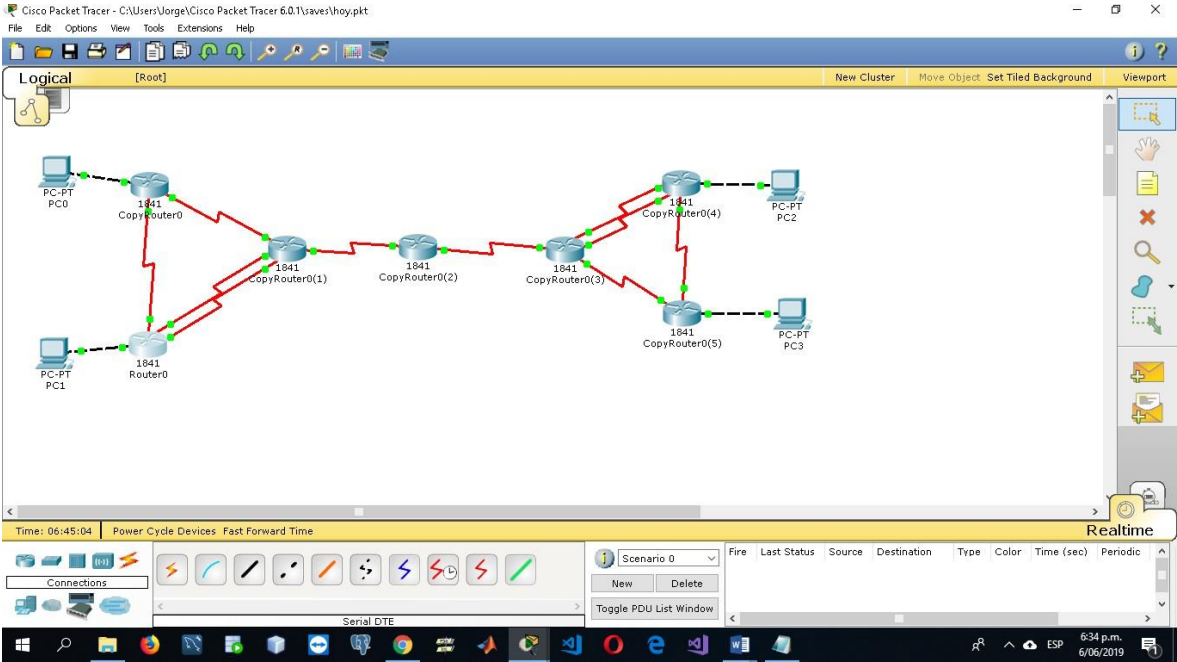
1.1 creando los dispositivos de la red

Para comenzar el desarrollo del Escenario 1, implementamos los dispositivos de red en la simulación.



1.2 Encendiendo los puertos

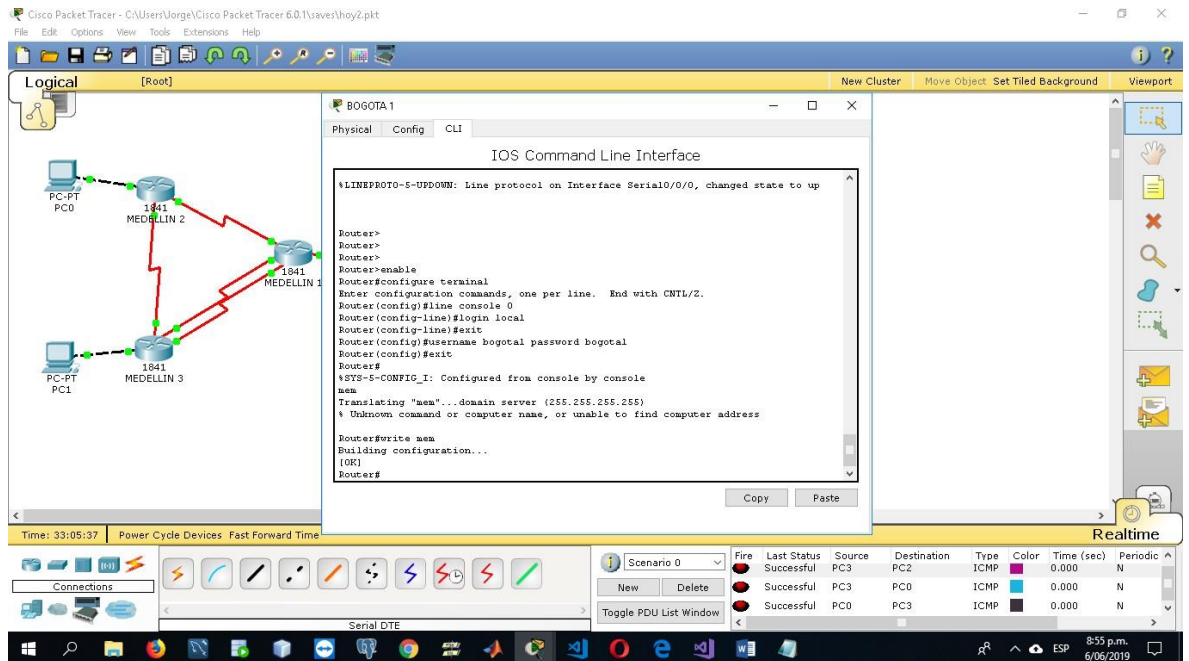
Procedemos a encender los puertos de cada uno de los routers. Podemos verificarlo visualmente con la forma de un led encendido de color verde en las conexiones de los routers



1.3 Configuración de usuario y contraseña

Realizamos la configuración del usuario y la contraseña para cada uno de los routers, donde utilizamos el mismo nombre de las etiquetas del router como usuario y contraseña.

Ej: El router bogota1, tendrá como usuario: bogota1 y contraseña bogota1



The screenshot shows the Cisco Packet Tracer interface. On the left, a network diagram displays three routers labeled 'MEDELLIN 2', 'MEDELLIN 1', and 'MEDELLIN 3', along with two PCs labeled 'PC-PT PC0' and 'PC-PT PC1'. The main window shows the CLI for 'BOGOTA 1' with the following configuration commands:

```

Router>
Router>
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#line console 0
Router(config-line)#login local
Router(config-line)#exit
Router(config)#username bogota1 password bogota1
Router(config)#exit
Router#
*SYS-5-CONFIG_I: Configured from console by console
*
*
Translating "aaa"...domain server (255.255.255.255)
* Unknown command or computer name, or unable to find computer address

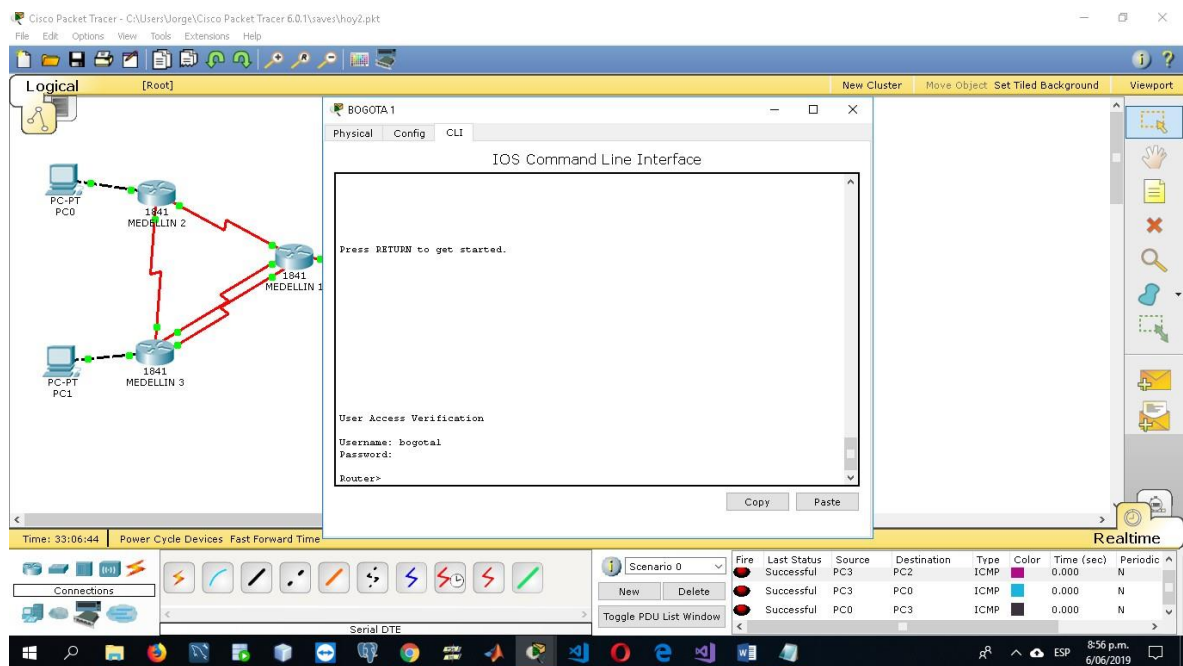
Router#write mem
Building configuration...
[OK]
Router#
  
```

The bottom of the interface shows a 'Realtime' table with the following data:

Fire	Last Status	Source	Destination	Type	Color	Time (sec)	Periodic
●	Successful	PC3	PC2	ICMP		0.000	N
●	Successful	PC3	PC0	ICMP		0.000	N
●	Successful	PC0	PC3	ICMP		0.000	N

1.4 Verificación de usuario y contraseña

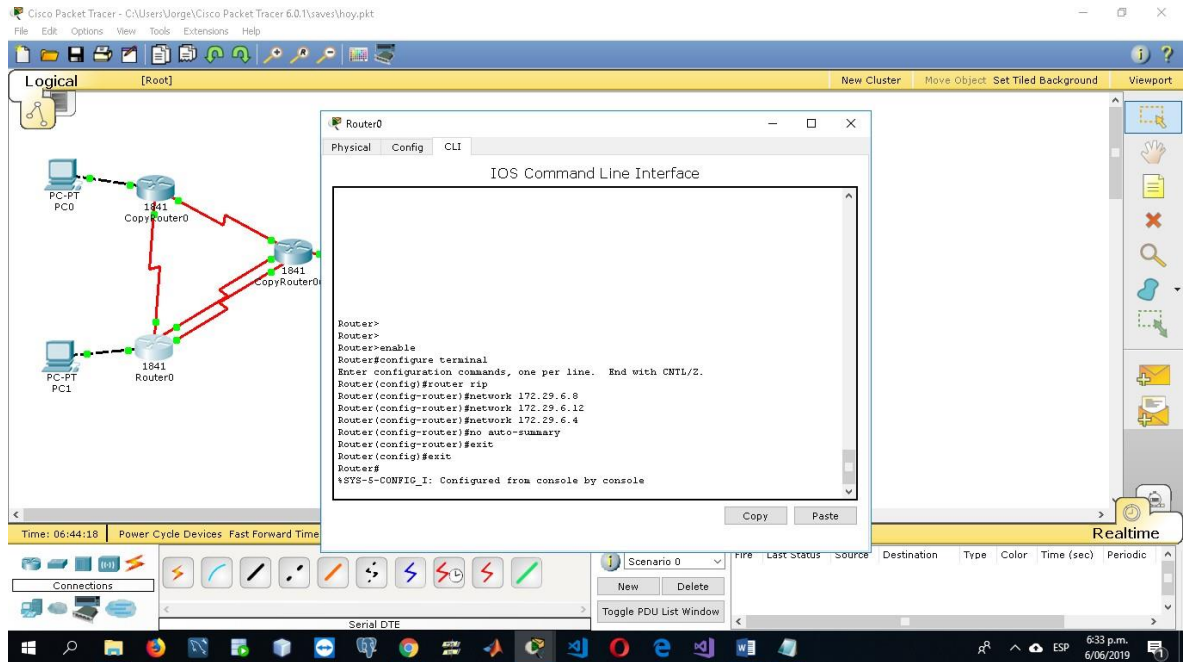
Una vez realizada la configuración de seguridad de los routers mediante usuario y contraseña, procedemos a verificar su funcionamiento, ingresando a la terminal con el usuario y la contraseña configurados previamente.



1.5 Configurando enrutamiento ripv2

Debido a que en el escenario se nos presentan múltiples routers que deben comunicarse entre sí, es necesario que en ellos se configure un protocolo de enrutamiento, en este caso rip 2, para ello en modo de configuración de consola del router, escribimos el comando - router rip con el cual estamos determinando que el enrutamiento se hará por el protocolo rip, y también ingresamos a la configuración del mismo, como él tiene dos versiones es necesario escribir el comando -version 2 para configurar la versión 2, luego de esto

pasamos a configurar las diferentes redes con las que deseamos que nuestro router se conecte mediante el comando `-network` más la dirección de red.



The screenshot displays the Cisco Packet Tracer interface. On the left, a network diagram shows a central router labeled 'Router0' connected to two other routers labeled 'CopyRouter0'. Two PCs, 'PC-PT PC0' and 'PC-PT PC1', are connected to the central router. The network is shown in a 'Logical' view. On the right, a terminal window titled 'Router0' shows the following configuration commands:

```
Router>
Router>
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#router rip
Router(config-router)#network 172.29.6.8
Router(config-router)#network 172.29.6.12
Router(config-router)#network 172.29.6.4
Router(config-router)#no auto-summary
Router(config-router)#exit
Router#
Router#
*SYS-5-CONFIG_I: Configured from console by console
```

The bottom of the interface shows a taskbar with various icons and a system tray indicating the time as 6:33 p.m. on 6/06/2019.

1.6 Verificando el correcto funcionamiento de la red

Una vez realizadas las configuraciones de enrutamiento mediante rip, procedemos a verificar que estas estén bien realizadas, por lo cual hacemos varios ping con host ubicados en distintas redes.

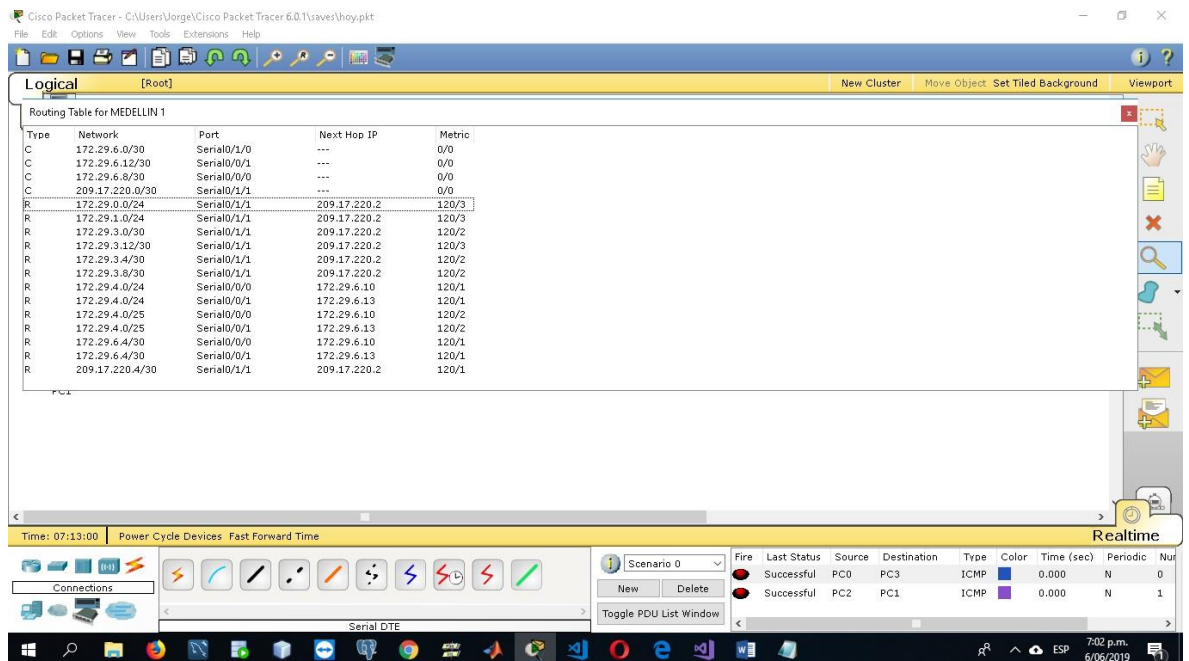
The screenshot shows the Cisco Packet Tracer interface. The main workspace displays a network topology with several routers and PCs. The routers are labeled: 1841 MEDELLIN 2, 1841 MEDELLIN 1, 1841 CopyRouter0(2), 1841 BOGOTA 1, 1841 BOGOTA 2, and 1841 BOGOTA 3. The PCs are labeled: PC-PT PC0, PC-PT PC1, PC-PT PC2, and PC-PT PC3. The network is connected via red lines representing links. The interface includes a menu bar, a toolbar, and a Realtime console window at the bottom. The Realtime console shows the following table:

Fire	Last Status	Source	Destination	Type	Color	Time (sec)	Periodic	Nut
●	Successful	PC0	PC3	ICMP	Blue	0.000	N	0
●	Successful	PC2	PC1	ICMP	Purple	0.000	N	1

1.7 Verificación de la tabla de direccionamiento

Mediante la herramienta de inspeccionar identificada con el icono de la lupa, ubicada en el panel derecho del programa, podemos verificar la direcciones a las que podría acceder un router, al hacer clic en él y seleccionar en el menú contextual la opción de tabla de enrutamiento.

Tabla de enrutamiento de Medellín 1



The screenshot shows the 'Logical' view of a Cisco Packet Tracer network. The routing table for 'MEDELLIN 1' is displayed, showing the following entries:

Type	Network	Port	Next Hop IP	Metric
C	172.29.6.0/30	Serial0/1/0	---	0/0
C	172.29.6.12/30	Serial0/0/1	---	0/0
C	172.29.6.8/30	Serial0/0/0	---	0/0
C	209.17.220.0/30	Serial0/1/1	---	0/0
R	172.29.0.0/24	Serial0/1/1	209.17.220.2	120/3
R	172.29.1.0/24	Serial0/1/1	209.17.220.2	120/3
R	172.29.3.0/30	Serial0/1/1	209.17.220.2	120/2
R	172.29.3.12/30	Serial0/1/1	209.17.220.2	120/3
R	172.29.3.4/30	Serial0/1/1	209.17.220.2	120/2
R	172.29.3.8/30	Serial0/1/1	209.17.220.2	120/2
R	172.29.4.0/24	Serial0/0/0	172.29.6.10	120/1
R	172.29.4.0/24	Serial0/0/1	172.29.6.13	120/1
R	172.29.4.0/25	Serial0/0/0	172.29.6.10	120/2
R	172.29.4.0/25	Serial0/0/1	172.29.6.13	120/2
R	172.29.6.4/30	Serial0/0/0	172.29.6.10	120/1
R	172.29.6.4/30	Serial0/0/1	172.29.6.13	120/1
R	209.17.220.4/30	Serial0/1/1	209.17.220.2	120/1

Como podemos observar la red LAN Medellín 1 se conecta directamente con las redes LAN 172.29.6.12/30, 172.29.8.12/30 y 209.27.220.0/30. Mediante enrutamiento dinámico a las otras redes que conforman nuestra red WAN

Tabla de enrutamiento de Medellín 2

Routing Table for MEDELLIN 2

Type	Network	Port	Next Hop IP	Metric
C	172.29.4.0/25	FastEthernet0/0	---	0/0
C	172.29.6.0/27	Serial0/0/1	---	0/0
C	192.29.6.0/30	Serial0/0/0	---	0/0
R	172.29.0.0/24	Serial0/0/1	172.29.6.6	120/5
R	172.29.1.0/24	Serial0/0/1	172.29.6.6	120/5
R	172.29.3.0/30	Serial0/0/1	172.29.6.6	120/4
R	172.29.3.12/30	Serial0/0/1	172.29.6.6	120/5
R	172.29.3.4/30	Serial0/0/1	172.29.6.6	120/4
R	172.29.3.8/30	Serial0/0/1	172.29.6.6	120/4
R	172.29.4.0/24	Serial0/0/1	172.29.6.6	120/1
R	172.29.6.0/30	Serial0/0/1	172.29.6.6	120/2
R	172.29.6.12/30	Serial0/0/1	172.29.6.6	120/1
R	172.29.6.8/30	Serial0/0/1	172.29.6.6	120/1
R	209.17.220.0/30	Serial0/0/1	172.29.6.6	120/2
R	209.17.220.4/30	Serial0/0/1	172.29.6.6	120/3

Time: 07:13:56 Power Cycle Devices Fast Forward Time

Realtime

Fire	Last Status	Source	Destination	Type	Color	Time (sec)	Periodic	Num
●	Successful	PC0	PC3	ICMP	Blue	0.000	N	0
●	Successful	PC2	PC1	ICMP	Purple	0.000	N	1

Como podemos observar la red LAN Medellín 2 se conecta directamente con las redes LAN 172.29.4.0/25, 172.29.6.0/30 y 172.279.6.4/30. Mediante enrutamiento dinámico a las otras redes que conforman nuestra red WAN.

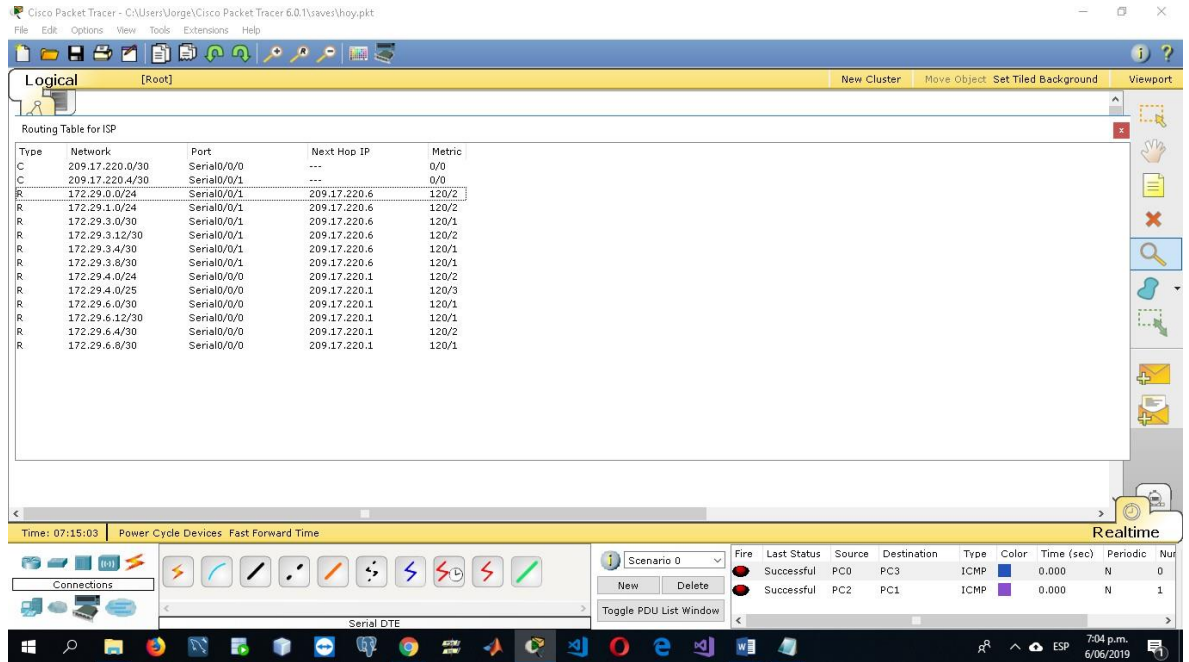
Tabla de enrutamiento de Medellín 3

Routing Table for MEDELLIN 3

Type	Network	Port	Next Hop IP	Metric
C	172.29.4.0/24	FastEthernet0/0	---	0/0
C	172.29.6.12/30	Serial0/0/1	---	0/0
C	172.29.6.4/30	Serial0/1/0	---	0/0
C	172.29.6.8/30	Serial0/0/0	---	0/0
R	172.29.0.0/24	Serial0/0/0	172.29.6.9	120/4
R	172.29.0.0/24	Serial0/0/1	172.29.6.14	120/4
R	172.29.1.0/24	Serial0/0/0	172.29.6.9	120/4
R	172.29.1.0/24	Serial0/0/1	172.29.6.14	120/4
R	172.29.3.0/30	Serial0/0/0	172.29.6.9	120/3
R	172.29.3.0/30	Serial0/0/1	172.29.6.14	120/3
R	172.29.3.12/30	Serial0/0/0	172.29.6.9	120/4
R	172.29.3.12/30	Serial0/0/1	172.29.6.14	120/4
R	172.29.3.4/30	Serial0/0/0	172.29.6.9	120/3
R	172.29.3.4/30	Serial0/0/1	172.29.6.14	120/3
R	172.29.3.8/30	Serial0/0/0	172.29.6.9	120/3
R	172.29.3.8/30	Serial0/0/1	172.29.6.14	120/3
R	172.29.4.0/25	Serial0/1/0	172.29.6.5	120/1
R	172.29.6.0/30	Serial0/0/0	172.29.6.9	120/1
R	172.29.6.0/30	Serial0/0/1	172.29.6.14	120/1
R	209.17.220.0/30	Serial0/0/0	172.29.6.9	120/1
R	209.17.220.0/30	Serial0/0/1	172.29.6.14	120/1
R	209.17.220.4/30	Serial0/0/0	172.29.6.9	120/2
R	209.17.220.4/30	Serial0/0/1	172.29.6.14	120/2

Como podemos observar la red LAN Medellín 3 se conecta directamente con las redes LAN 172.29.4.0/24, 172.29.6.12/30, 172.279.6.4/30 y 172.279.6.8/30. Mediante enrutamiento dinámico a las otras redes que conforman nuestra red WAN.

Tabla enrutamiento ISP



Routing Table for ISP

Type	Network	Port	Next Hop IP	Metric
C	209.17.220.0/30	Serial0/0/0	---	0/0
C	209.17.220.4/30	Serial0/0/1	---	0/0
R	172.29.0.0/24	Serial0/0/1	209.17.220.6	120/2
R	172.29.1.0/24	Serial0/0/1	209.17.220.6	120/2
R	172.29.3.0/30	Serial0/0/1	209.17.220.6	120/1
R	172.29.3.12/30	Serial0/0/1	209.17.220.6	120/2
R	172.29.3.4/30	Serial0/0/1	209.17.220.6	120/1
R	172.29.3.8/30	Serial0/0/1	209.17.220.6	120/1
R	172.29.4.0/24	Serial0/0/0	209.17.220.1	120/2
R	172.29.4.0/25	Serial0/0/0	209.17.220.1	120/3
R	172.29.6.0/30	Serial0/0/0	209.17.220.1	120/1
R	172.29.6.12/30	Serial0/0/0	209.17.220.1	120/1
R	172.29.6.4/30	Serial0/0/0	209.17.220.1	120/2
R	172.29.6.8/30	Serial0/0/0	209.17.220.1	120/1

Como podemos observar la red LAN ISP se conecta directamente con las redes LAN 209.17.220.0 y 209.17.220.4/30. Mediante enrutamiento dinámico a las otras redes que conforman nuestra red WAN.

Tabla de enrutamiento Bogota 1

Routing Table for BOGOTA 1

Type	Network	Port	Next Hop IP	Metric
C	172.29.3.0/30	Serial0/1/0	---	0/0
C	172.29.3.4/30	Serial0/0/1	---	0/0
C	172.29.3.8/30	Serial0/1/1	---	0/0
C	209.17.220.4/30	Serial0/0/0	---	0/0
R	172.29.0.0/24	Serial0/0/1	172.29.3.6	120/1
R	172.29.0.0/24	Serial0/1/0	172.29.3.2	120/1
R	172.29.1.0/24	Serial0/1/1	172.29.3.10	120/1
R	172.29.3.12/30	Serial0/0/1	172.29.3.6	120/1
R	172.29.3.12/30	Serial0/1/0	172.29.3.2	120/1
R	172.29.3.12/30	Serial0/1/1	172.29.3.10	120/16
R	172.29.4.0/24	Serial0/0/0	209.17.220.5	120/3
R	172.29.4.0/25	Serial0/0/0	209.17.220.5	120/4
R	172.29.6.0/30	Serial0/0/0	209.17.220.5	120/2
R	172.29.6.12/30	Serial0/0/0	209.17.220.5	120/2
R	172.29.6.4/30	Serial0/0/0	209.17.220.5	120/3
R	172.29.6.8/30	Serial0/0/0	209.17.220.5	120/2
R	209.17.220.0/30	Serial0/0/0	209.17.220.5	120/1

Time: 07:15:27 Power Cycle Devices Fast Forward Time

Scenario 0

Fire	Last Status	Source	Destination	Type	Color	Time (sec)	Periodic	Num
●	Successful	PC0	PC3	ICMP	Blue	0.000	N	0
●	Successful	PC2	PC1	ICMP	Purple	0.000	N	1

Serial DTE

7:05 p.m. 6/06/2019

Como podemos observar la red LAN Bogota 1 se conecta directamente con las redes LAN 209.17.220.4/30, 172.29.3.0/30, 172.29.3.4/30. Y 172.29.3.8/30. Mediante enrutamiento dinámico a las otras redes que conforman nuestra red WAN.

Lista de enrutamiento Bogota 2

Cisco Packet Tracer - C:\Users\Uorge\Documents\Cisco Packet Tracer 6.0.1\save\hoy.pkt

File Edit Options View Tools Extensions Help

Logical [Root] New Cluster Move Object Set Tiled Background Viewport

Routing Table for BOGOTA 2

Type	Network	Port	Next Hop IP	Metric
C	172.29.0.0/24	FastEthernet0/0	---	0/0
C	172.29.3.0/30	Serial0/0/1	---	0/0
C	172.29.3.12/30	Serial0/1/0	---	0/0
C	172.29.3.4/30	Serial0/0/0	---	0/0
R	172.29.1.0/24	Serial0/1/0	172.29.3.14	120/1
R	172.29.3.8/30	Serial0/0/0	172.29.3.5	120/1
R	172.29.3.8/30	Serial0/0/1	172.29.3.1	120/1
R	172.29.3.8/30	Serial0/1/0	172.29.3.14	120/1
R	172.29.4.0/24	Serial0/0/0	172.29.3.5	120/4
R	172.29.4.0/24	Serial0/0/1	172.29.3.1	120/4
R	172.29.4.0/25	Serial0/0/0	172.29.3.5	120/5
R	172.29.4.0/25	Serial0/0/1	172.29.3.1	120/5
R	172.29.6.0/30	Serial0/0/0	172.29.3.5	120/3
R	172.29.6.0/30	Serial0/0/1	172.29.3.1	120/3
R	172.29.6.12/30	Serial0/0/0	172.29.3.5	120/3
R	172.29.6.12/30	Serial0/0/1	172.29.3.1	120/3
R	172.29.6.4/30	Serial0/0/0	172.29.3.5	120/4
R	172.29.6.4/30	Serial0/0/1	172.29.3.1	120/4
R	172.29.6.8/30	Serial0/0/0	172.29.3.5	120/3
R	172.29.6.8/30	Serial0/0/1	172.29.3.1	120/3
R	209.17.220.0/30	Serial0/0/0	172.29.3.5	120/2
R	209.17.220.0/30	Serial0/0/1	172.29.3.1	120/2
R	209.17.220.4/30	Serial0/0/0	172.29.3.5	120/1
R	209.17.220.4/30	Serial0/0/1	172.29.3.1	120/1

Time: 07:15:54 Power Cycle Devices Fast Forward Time

Connections

Serial DTE

Scenario 0

Fire	Last Status	Source	Destination	Type	Color	Time (sec)	Periodic	Num
●	Successful	PC0	PC3	ICMP	Blue	0.000	N	0
●	Successful	PC2	PC1	ICMP	Purple	0.000	N	1

Toggle PDU List Window

7:05 p.m. 6/06/2019

Como podemos observar la red LAN Bogota 2 se conecta directamente con las redes LAN 172.29.0.0/24, 172.29.3.12/30, 172.29.3.0/30, y 172.29.3.4/30. Mediante enrutamiento dinámico a las otras redes que conforman nuestra red WAN.

Lista de enrutamiento Bogota 3

Routing Table for BOGOTA 3

Type	Network	Port	Next Hop IP	Metric
C	172.29.1.0/24	FastEthernet0/0	---	0/0
C	172.29.3.12/30	Serial0/0/1	---	0/0
C	172.29.3.8/30	Serial0/0/0	---	0/0
R	172.29.0.0/24	Serial0/0/1	172.29.3.13	120/1
R	172.29.3.0/30	Serial0/0/0	172.29.3.9	120/1
R	172.29.3.0/30	Serial0/0/1	172.29.3.13	120/1
R	172.29.3.4/30	Serial0/0/0	172.29.3.9	120/1
R	172.29.3.4/30	Serial0/0/1	172.29.3.13	120/1
R	172.29.4.0/24	Serial0/0/0	172.29.3.9	120/4
R	172.29.4.0/25	Serial0/0/0	172.29.3.9	120/5
R	172.29.6.0/30	Serial0/0/0	172.29.3.9	120/3
R	172.29.6.12/30	Serial0/0/0	172.29.3.9	120/3
R	172.29.6.4/30	Serial0/0/0	172.29.3.9	120/4
R	172.29.6.8/30	Serial0/0/0	172.29.3.9	120/3
R	209.17.220.0/30	Serial0/0/0	172.29.3.9	120/2
R	209.17.220.4/30	Serial0/0/0	172.29.3.9	120/1

Como podemos observar la red LAN Bogota 3 se conecta directamente con las redes LAN 172.29.1.0/24, 172.29.3.12/30 y 172.29.3.8/30. Mediante enrutamiento dinámico a las otras redes que conforman nuestra red WAN.

1.7 Revisando el balanceo de carga

Cuando un router detecta varias rutas a una red específica a través de varios procesos de ruteo (o protocolos de ruteo, como RIP, RIPv2, IGRP, EIGRP y OSPF), instala la ruta con la mínima distancia administrativa en la tabla de ruteo. Esto lo podemos ver ingresando al terminal del router deseado y digitando el comando

—show ip route mas la dirección a la cual queremos ver la ruta más corta

Cisco Packet Tracer - C:\Users\yorge\Cisco Packet Tracer 6.0.1\saves\hoy.pkt

File Edit Options View Tools Extensions Help

Logical [Root] New Cluster Move Object Set Titled Background Viewport

```

    graph TD
      PC0[PC-PT PC0] --- R2[1841 MEDELLIN 2]
      PC1[PC-PT PC1] --- R3[1841 MEDELLIN 3]
      R2 --- R4[1841 MEDELLIN 4]
      R3 --- R4
  
```

BOGOTA 3

Physical Config CLI

IOS Command Line Interface

Press RETURN to get started.

```

Router>
Router>show ip route 172.29.4.2
Routing entry for 172.29.4.0/25
  Known via "rip", distance 120, metric 5
  Redistributing via rip
  Last update from 172.29.3.9 on Serial0/0/0, 00:00:27 ago
  Routing Descriptor Blocks:
    * 172.29.3.9, from 172.29.3.9, 00:00:27 ago, via Serial0/0/0
      Route metric is 5, traffic share count is 1
Router>
          
```

Copy Paste

Time: 07:21:12 Power Cycle Devices Fast Forward Time

Connections

Serial DTE

Scenario 0

Fire	Last Status	Source	Destination	Type	Color	Time (sec)	Periodic	Nur
●	Successful	PC0	PC3	ICMP	Blue	0.000	N	0
●	Successful	PC2	PC1	ICMP	Purple	0.000	N	1

Toggle PDU List Window

Realtime

7:10 p.m. 6/06/2019

1.8 Configurando interfaces pasivas

Debido a que el protocolo de red rip 2 envía actualizaciones cada 30 segundos a todos los dispositivos de la red para actualizar sus tablas de enrutamiento, se hace necesario el poder desactivar estas actualización donde no sea coherente tenerlas, debido a que provocan varios problemas, entre ellos el desperdicio de ancho de banda al recibir paquetes que no cumplen ninguna función en ese segmento de red, desperdicio de recursos debido a que los equipo de la red LAN van a trabajar innecesariamente procesando paquetes sin ningún fin, fallas de seguridad porque alguien podría analizar el tráfico de los datos de la red LAN leer la configuración de las tablas de enrutamiento y reenviar datos para falsear las configuraciones reales.

En este escenario teniendo en cuenta lo anteriormente mencionado, debemos cambiar a modo pasivas las interfeces fa0/0 que son las que conectan con los hots en los routers Medellin 2, Medellin 3, Bogota 2 y Bogota 3

The screenshot shows a Cisco Packet Tracer interface with a network topology on the left and a terminal window for router MEDELLIN 2 on the right. The topology includes several 1841 routers (MEDELLIN 1, 2, 3, ISP, BOGOT) and two PCs (PC0, PC1). The terminal window shows the following commands and output:

```

IOS Command Line Interface

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to do
wn
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up

Router>
Router>
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#router rip
Router(config-router)#version 2
Router(config-router)#passive-interface fa0/0
^
% Invalid input detected at '^' marker.
Router(config-router)#passive-interface fa0/0
Router(config-router)#end
Router#
*SYS-5-COMFIG_I: Configured from console by console

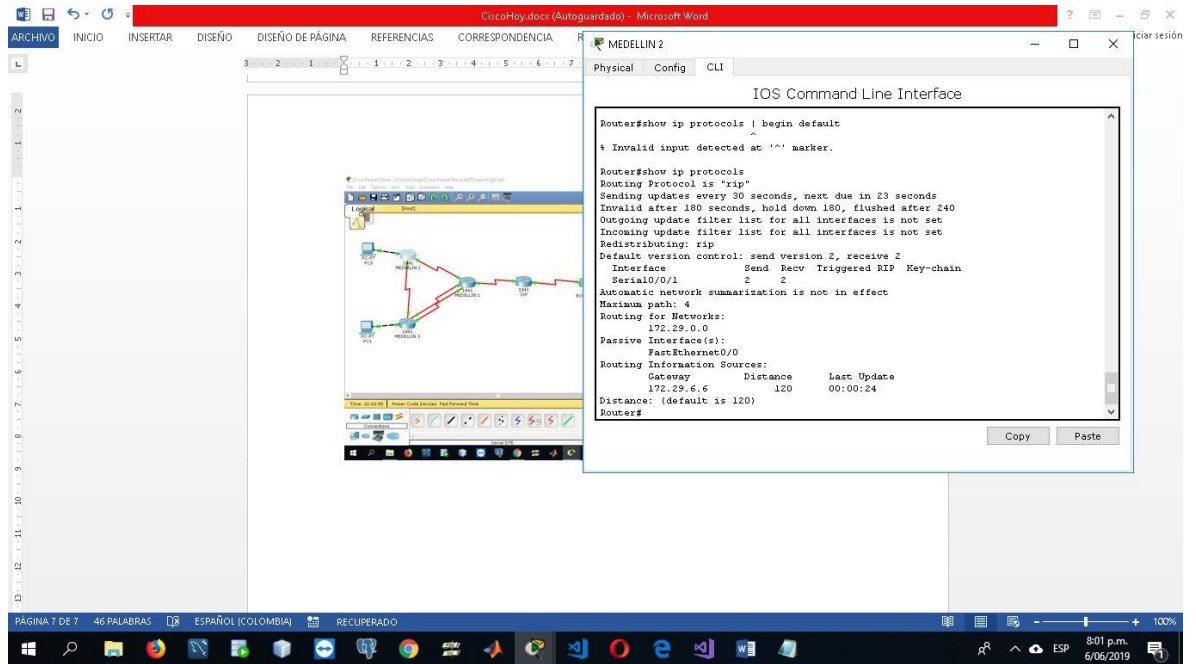
```

At the bottom of the interface, there is a table for Scenario 0:

Fire	Last Status	Source	Destination	Type	Color	Time (sec)	Periodic	Nur
●	Successful	PC0	PC3	ICMP	Blue	0.000	N	0
●	Successful	PC2	PC1	ICMP	Purple	0.000	N	1

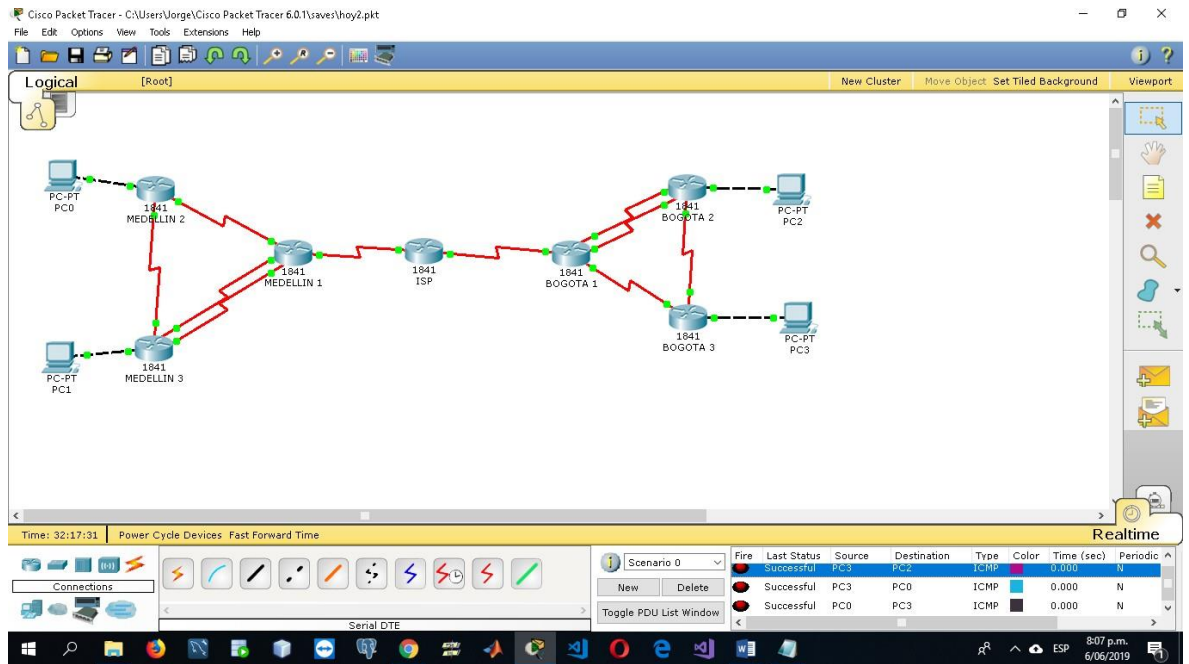
1.9. Verificando interfaz pasiva

Ingresando al router mediante el comando –show ip protocols, podemos observar una tabla con la información del protocolo configurado en la terminal, allí en la sección “passive interface” vemos las interfaces que se han configurado en modo pasivo



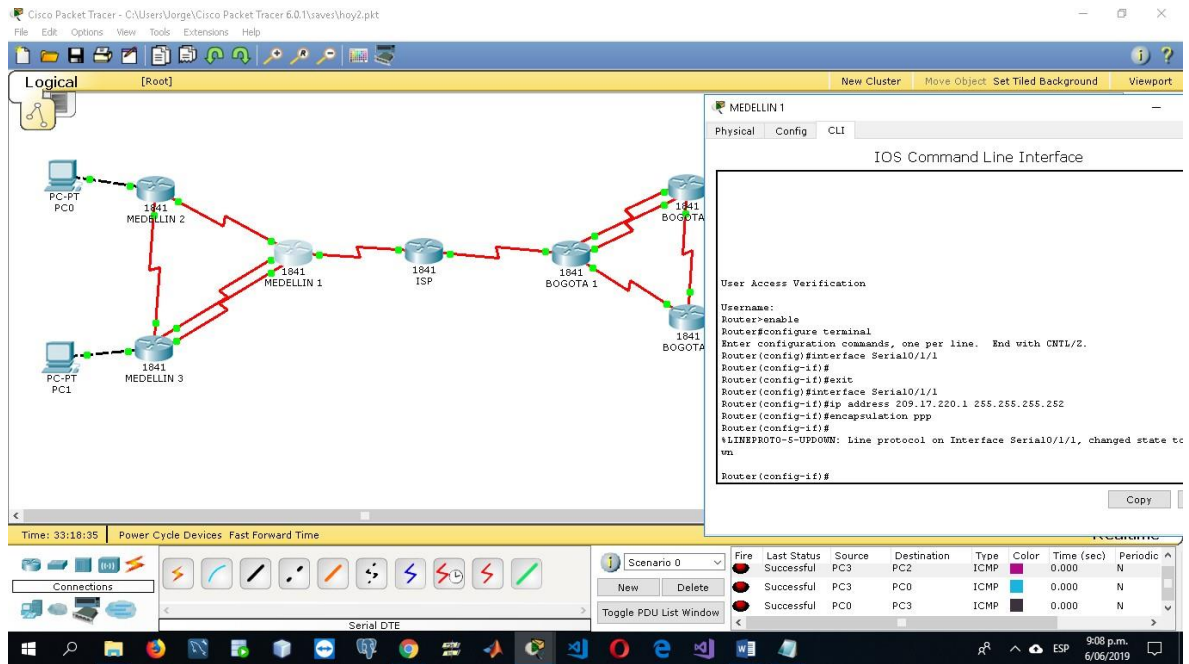
1.9 Verificando funcionalidad general después de la implementación de las interfaces pasivas

Luego de varias modificaciones a la red es necesario hacer un test, realizando pines en toda la red para constatar el correcto funcionamiento de la red



1.10 Configuración de encapsulación ppp

PPP es un protocolo que permite la conexión directa entre nodos de una red, puede contener autenticación mediante PAP o CHAP. Para configurar este protocolo en un router es necesario entrar al modo privilegiado de la terminal, e ingresar a la interfaz a la cual se le desea agregar, con el comando `-interface interfaz deseada`, luego de eso ingresamos `-ip address la dirección ip y mascara de subred`, y finalmente ingresamos en el comando `-encapsulation ppp`



1.11 AUTENTICACION MEDIANTE pap

Como se había mencionado anteriormente en este documento el protocolo PPP permite la autenticación mediante PAP, el cual aumenta la seguridad de la conexión al darnos la opción de agregar un usuario y contraseña al proceso de conexión, para ello en el modo de configuración de la terminal agregamos el comando `–username nombre de usuario password contraseña`, seguidamente entramos a la configuración de la interfaz con el comando `–interface interfaz objetivo`, allí escribimos `–encapsulation ppp authentication pap` y con esto solo nos restaría hacer la misma configuración en el otro extremo de la conexión para finalizar el proceso.

MEDELLIN 1

IOS Command Line Interface

```

Router#configure terminal
Router(config)#interface Serial0/1/1
Router(config-if)#
Router(config-if)#exit
Router(config)#interface Serial0/1/1
Router(config-if)#ip address 209.17.220.1 255.255.255.252
Router(config-if)#encapsulation ppp
Router(config-if)#
!LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/1/1, changed state to do
wn
Router(config-if)#
!LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/1/1, changed state to up
Router(config-if)#
Router(config-if)#exit
Router(config)#username medellin1 password medellin1
Router(config)#interface serial 0/1/1
Router(config-if)#ppp authentication pap
Router(config-if)#
!LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/1/1, changed state to do
wn
    
```

Fire	Last Status	Source	Destination	Type	Color	Time (sec)	Periodic
●	Successful	PC3	PC2	ICMP	■	0.000	N
●	Successful	PC3	PC0	ICMP	■	0.000	N
●	Successful	PC0	PC3	ICMP	■	0.000	N

ISP

IOS Command Line Interface

```

Router#configure terminal
Router(config)#interface Serial0/0/0
Router(config-if)#ip address
! Incomplete command.
Router(config-if)#exit
Router(config)#interface Serial0/0/0
Router(config-if)#ip address 209.17.220.2 255.255.255.252
Router(config-if)#encapsulation ppp
Router(config-if)#
!LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up
Router(config-if)#
!LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to do
wn
Router(config-if)#
Router(config-if)#exit
Router(config)#interface serial 0/0/0
Router(config-if)#ppp pap sent-username medellin1 password medellin1
Router(config-if)#
!LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up
    
```

Fire	Last Status	Source	Destination	Type	Color	Time (sec)	Periodic
●	Successful	PC3	PC2	ICMP	■	0.000	N
●	Successful	PC3	PC0	ICMP	■	0.000	N
●	Successful	PC0	PC3	ICMP	■	0.000	N

1.12 AUTENTICACION MEDIANTE CHAT

El protocolo PPP con autenticación CHAT permite elevar la seguridad al encriptar la contraseña y el usuario mediante md5. Para implementar este tipo de autenticación el proceso es casi el mismo que autenticación por PAP, solamente hay que cambiar el comando `-encapsulation ppp authentication pap` por `-encapsulation ppp authentication chat`.

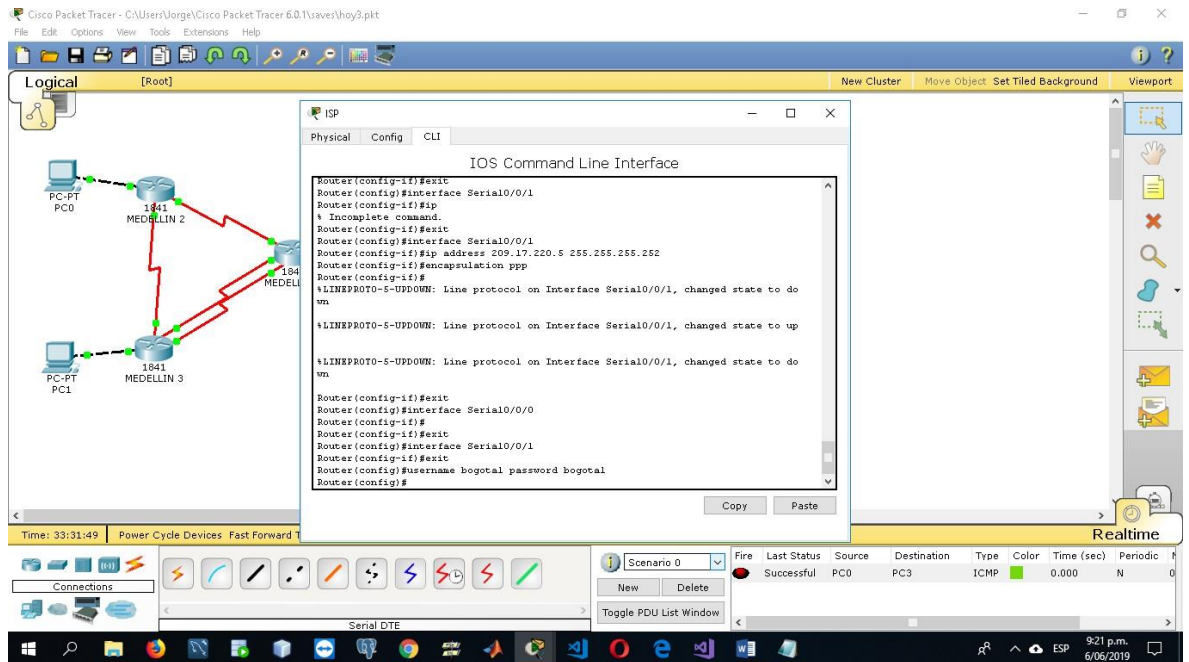
The screenshot displays the Cisco Packet Tracer interface. On the left, a network diagram shows three routers (MEDELLIN 1, 2, and 3) and an ISP router, all connected via serial links. Two PCs (PC1 and PC2) are connected to MEDELLIN 2 and MEDELLIN 3 respectively. The main window shows the CLI for router BOGOTA 1, where the following configuration commands have been entered:

```

Router>enable
Router(config)#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#interface Serial0/0/0
Router(config-if)#ip address
!LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to do
wn
% Incomplete command.
Router(config)#interface Serial0/0/0
Router(config-if)#ip address 209.17.220.6 255.255.255.252
Router(config-if)#encapsulation ppp
Router(config-if)#
!LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to do
wn

Router(config-if)#exit
Router(config)#
Router(config)#interface Serial0/0/0
Router(config-if)#ppp authentication chap
Router(config-if)#
!LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to do
wn
  
```

The bottom status bar shows the network is in 'Realtime' mode, with a successful connection between PC0 and PC3, and an ICMP ping of 0.000 seconds.



1.13 CONFIGURACION PAT

La configuración PAT es un algoritmo de traducción de direcciones IPV4, que permite a un proveedor de internet mapear múltiples ip privadas mediante una ip publica, lo que quiere decir que aunque en nuestro hogar tengamos 10 dispositivos, el isp puede ahorrarse 9 direcciones publicas mediante la traducción de ip privadas.

Como se solicita en el Escenario se realiza la configuración NAT en los routers Bogota 1 y Medellin 1

The screenshot displays the Cisco Packet Tracer interface. On the left, a network diagram shows three routers labeled MEDELLIN 1, MEDELLIN 2, and MEDELLIN 3, each with IP address 1841. MEDELLIN 1 is connected to MEDELLIN 2 and MEDELLIN 3. Two PCs, PC0 and PC1, are connected to MEDELLIN 2 and MEDELLIN 3 respectively. The main window shows the CLI for MEDELLIN 1 with the following configuration:

```

IOS Command Line Interface

Username: medellin1
Password:

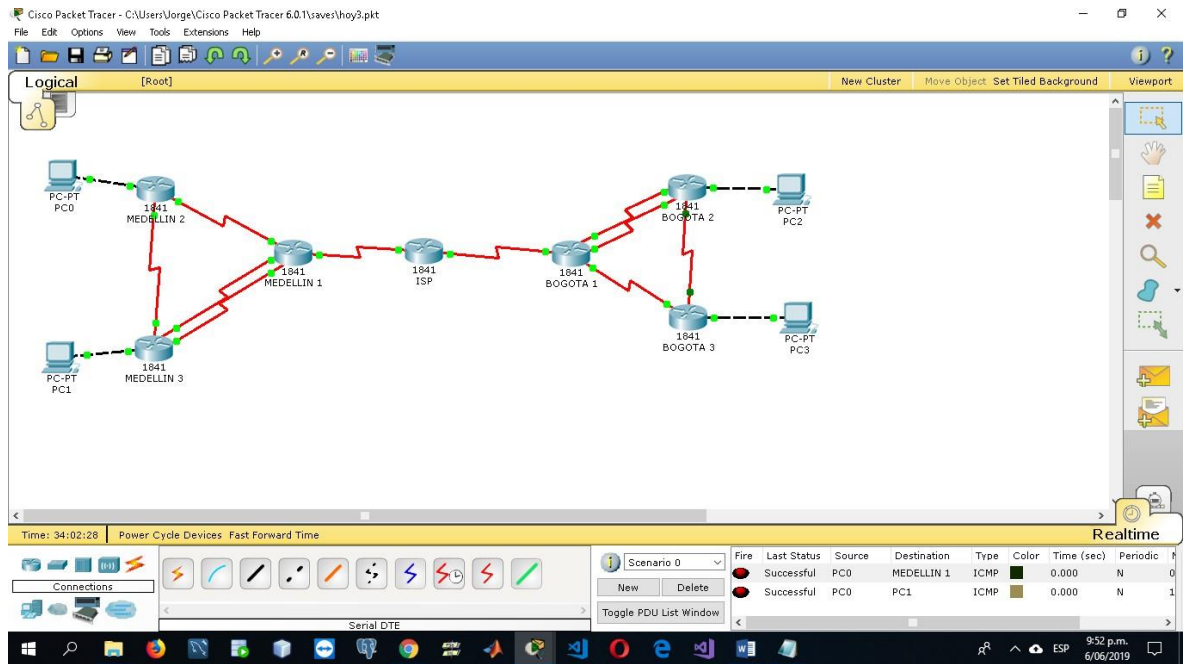
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#access-list 1 permit 209.17.220.0 0.0.0.3
Router(config)#ip nat inside source list 1 interface se 0/1/1 overload
Router(config)#interface se 0/1/1
Router(config-if)#ip nat outside
Router(config-if)#exit
^
Invalid input detected at '^' marker.
Router(config-if)#exit
Router(config)#interface se 0/1/0
Router(config-if)#ip nat inside
Router(config-if)#exit
Router(config)#interface se 0/0/0
Router(config-if)#ip nat inside
Router(config-if)#exit
Router(config)#interface se 0/0/1
Router(config-if)#ip nat inside
Router(config-if)#exit
Router(config)#

```

At the bottom right, a Realtime traffic table is visible:

Fire	Last Status	Source	Destination	Type	Color	Time (sec)	Periodic
●	Successful	PC0	PC3	ICMP	Green	0.000	N
●	Successful	PC0	MEDELLIN 1	ICMP	Blue	0.000	N
●	Failed	PC0	PC3	ICMP	Brown	0.000	N

Se realizan las pruebas de conexión entre el router Medellin 1 y las sucursales Medellin 2 y Medellin 3.



Las fallas de conexión entre los host de Medellín y Bogotá.

Cisco Packet Tracer - C:\Users\Uorge\Cisco Packet Tracer 6.0.1\save\Uoy3.pkt

File Edit Options View Tools Extensions Help

Logical [Root] New Cluster Move Object Set Tiled Background Viewport

Time: 34:03:05 Power Cycle Devices Fast Forward Time

Realtime

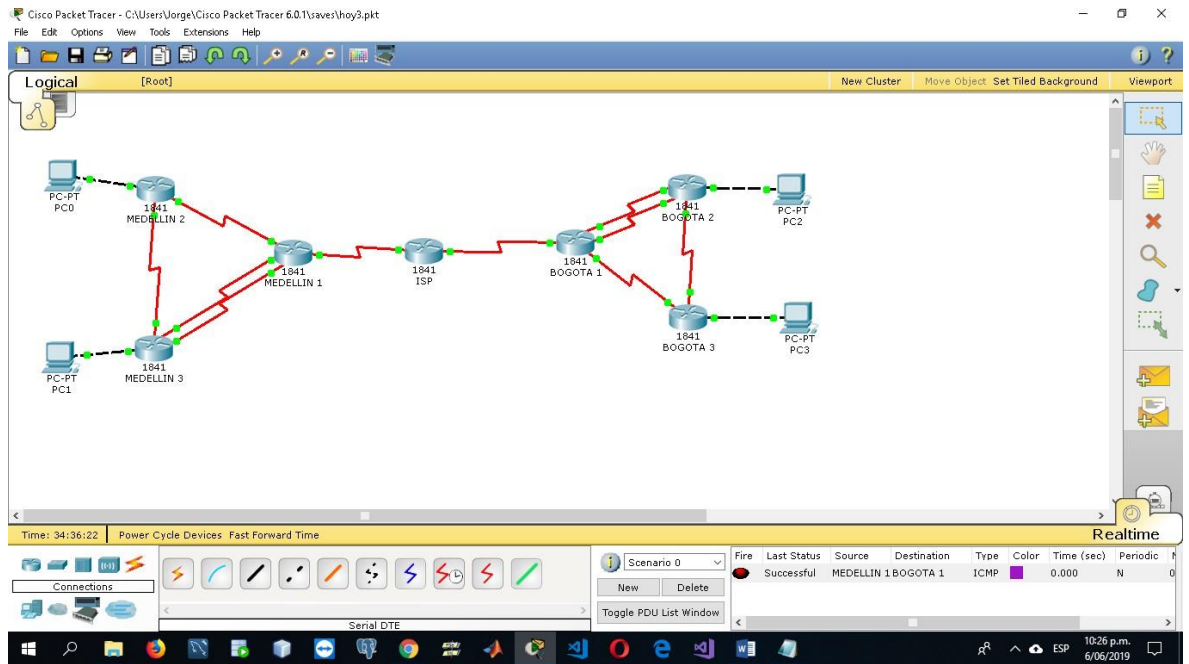
Fire	Last Status	Source	Destination	Type	Color	Time (sec)	Periodic	
●	Failed	PC0	PC2	ICMP	■	0.000	N	0
●	Failed	PC1	PC3	ICMP	■	0.000	N	1

Serial DTE

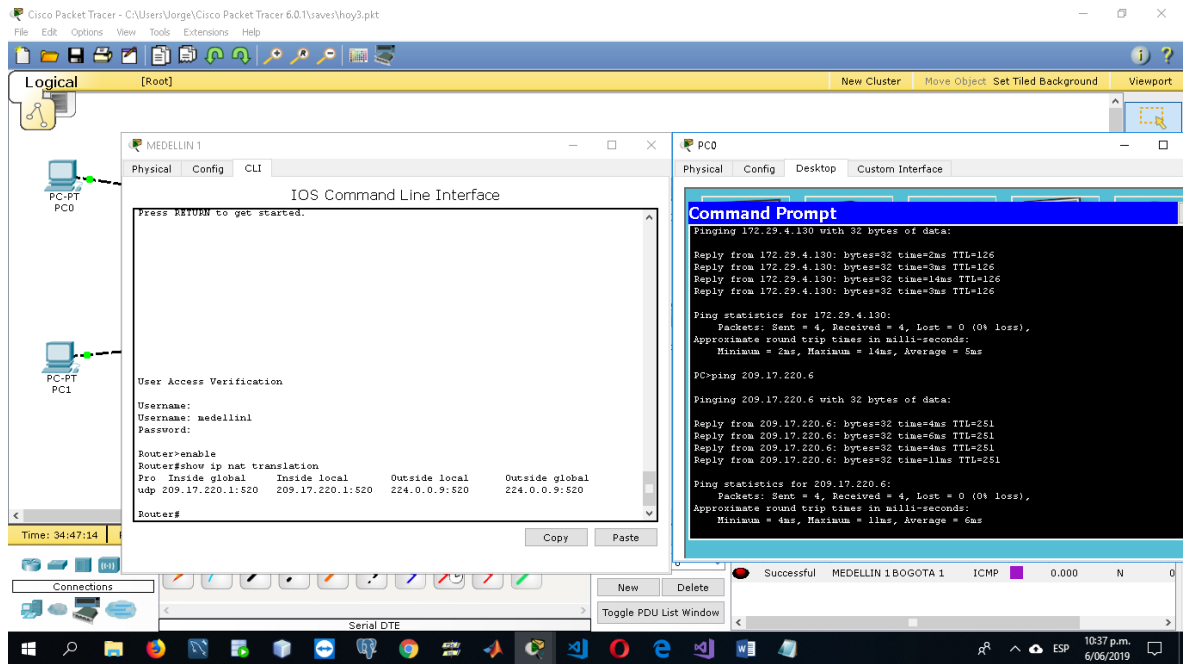
Toggle PDU List Window

9:53 p.m. 6/06/2019

Conexión entre bogota1, isp y medellin1.



Para verificar la nat podemos utilizar el comando `-show ip nat translation`.



1.14 Configuración de DHCP

Para la configuración de las ip privadas es conveniente utilizar DHCP, debido a que presenta múltiples ventajas entre ellas ahorro significativo en el tiempo requerido de la implementación de la red, debido a que si por ejemplo necesitáramos conectar 1, 1000 o n host el DHCP le asigna direcciones ip automáticas, que de otra forma deberíamos ir equipo por equipo a agregar cada una de las ip. También nos provee mayor seguridad porque al ser las direcciones ip dinámicas, estas están en constante cambio lo que dificulta el rastreo del equipo de origen. Para asignar direcciones ip mediante DHCP podemos hacerlo mediante switch capa 3, servidor DHCP y Routers, en este caso lo haremos por medio del router, para ello necesitamos crear un pool de direcciones las cuales asignaría el router a los host que se vayan agregando a la red, el comando es el siguiente: -ip dhcp pool + nombre de

identificación del pool, luego asignamos el rango de direcciones que está determinado por la ip y la máscara de subred con el siguiente comando: `-network +ip+mascara` de subred, se asigna la puerta de enlace predeterminada `-default-router+puerta de enlace` predeterminada, y finalmente se agrega la dirección del servidor dns `-dns-server + direccion servidor dns`.

The screenshot displays the Cisco Packet Tracer interface. On the left, a network topology is visible with four routers: MEDELLIN 2, MEDELLIN 1, ISP, and BOGOTA 1. Two PCs, PC0 and PC1, are connected to MEDELLIN 2 and MEDELLIN 3 respectively. The main window shows the CLI for MEDELLIN 2 with the following configuration:

```

IOS Command Line Interface

User Access Verification
Username:
Username: medellin2
Password:

Router>enable
Router#ip dhcp pool RED1
% Invalid input detected at '^' marker.

Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#ip dhcp pool red1
Router(dhcp-config)#network 172.29.4.0 255.255.255.128
% Invalid input detected at '^' marker.

Router(dhcp-config)#network 172.29.4.0 255.255.255.128
Router(dhcp-config)#default-router 172.29.4.1
Router(dhcp-config)#dns-server 8.8.8.8
Router(dhcp-config)#exit
Router(config)#
  
```

At the bottom of the interface, a table shows the status of DHCP leases:

Device	IP	MAC	Lease Time	Expires	Status
MEDELLIN 1	BOGOTA 1	ICMP	0.000	N	Successful
BOGOTA 1	MEDELLIN 1	ICMP	0.000	N	Successful

Para verificar que los host estén recibiendo las direcciones DHCP ingresamos a su configuración ip y cambiamos la opción que por defecto esta en static, por DHCP, esperamos un momento y si todo está correcto debería mostrarnos la dirección ip, puerta de enlace, máscara de subred y dirección dns, obtenida automáticamente desde el router, si no funciona la interfaz nos mostrara un mensaje indicándonos el error.

Cisco Packet Tracer - C:\Users\Jorge\Cisco Packet Tracer 6.0.1\save\hoy5.pkt

File Edit Options View Tools Extensions Help

Logical [Root] New Cluster Move Object Set Tiled Background Viewport

PC0

IP Configuration

IP Configuration
 DHCP Static DHCP request successful.

IP Address: 172.29.4.2
 Subnet Mask: 255.255.255.128
 Default Gateway: 172.29.4.1
 DNS Server: 8.8.8.8

IPv6 Configuration
 DHCP Auto Config Static

IPv6 Address:
 Link Local Address: FE80::260:3EFF:FE2:CA00
 IPv6 Gateway:
 IPv6 DNS Server:

Time: 35:07:42 Power Cycle Devices Fast Forward Time

Fire	Last Status	Source	Destination	Type	Color	Time (sec)	Periodic
	Successful	MEDELLIN 1	BOGOTA 1	ICMP		0.000	N
	Successful	MEDELLIN 1	BOGOTA 1	ICMP		0.000	N

10:58 p.m. 6/06/2019

Cisco Packet Tracer - C:\Users\Jorge\Cisco Packet Tracer 6.0.1\save\hoy5.pkt

File Edit Options View Tools Extensions Help

Logical [Root] New Cluster Move Object Set Tiled Background Viewport

PC1

IP Configuration

IP Configuration
 DHCP Static DHCP request successful.

IP Address: 172.29.4.131
 Subnet Mask: 255.255.255.128
 Default Gateway: 172.29.4.129
 DNS Server: 8.8.8.8

IPv6 Configuration
 DHCP Auto Config Static

IPv6 Address:
 Link Local Address: FE80::201:96FF:FE03:62A1
 IPv6 Gateway:
 IPv6 DNS Server:

Time: 35:20:25 Power Cycle Devices Fast Forward Time

Fire	Last Status	Source	Destination	Type	Color	Time (sec)	Periodic
	Successful	MEDELLIN 1	BOGOTA 1	ICMP		0.000	N
	Successful	MEDELLIN 1	BOGOTA 1	ICMP		0.000	N
	Successful	BOGOTA 1	MEDELLIN 1	ICMP		0.000	N

Serial DTE

11:11 p.m. 6/06/2019

The screenshot displays the Cisco Packet Tracer 6.0.1 interface. The main window shows a network diagram with two routers, BOGOTA 2 and BOGOTA 3, connected to four PCs: PC0, PC1, PC2, and PC3. The IP configuration window for PC2 is open, showing the following settings:

IP Configuration

- DHCP Static DHCP request successful.
- IP Address: 172.29.0.4
- Subnet Mask: 255.255.255.0
- Default Gateway: 172.29.0.1
- DNS Server: 8.8.8.8

IPv6 Configuration

- DHCP Auto Config Static
- IPv6 Address: [empty]
- Link Local Address: FE80::205:5EFF:FE55:CEC2
- IPv6 Gateway: [empty]
- IPv6 DNS Server: [empty]

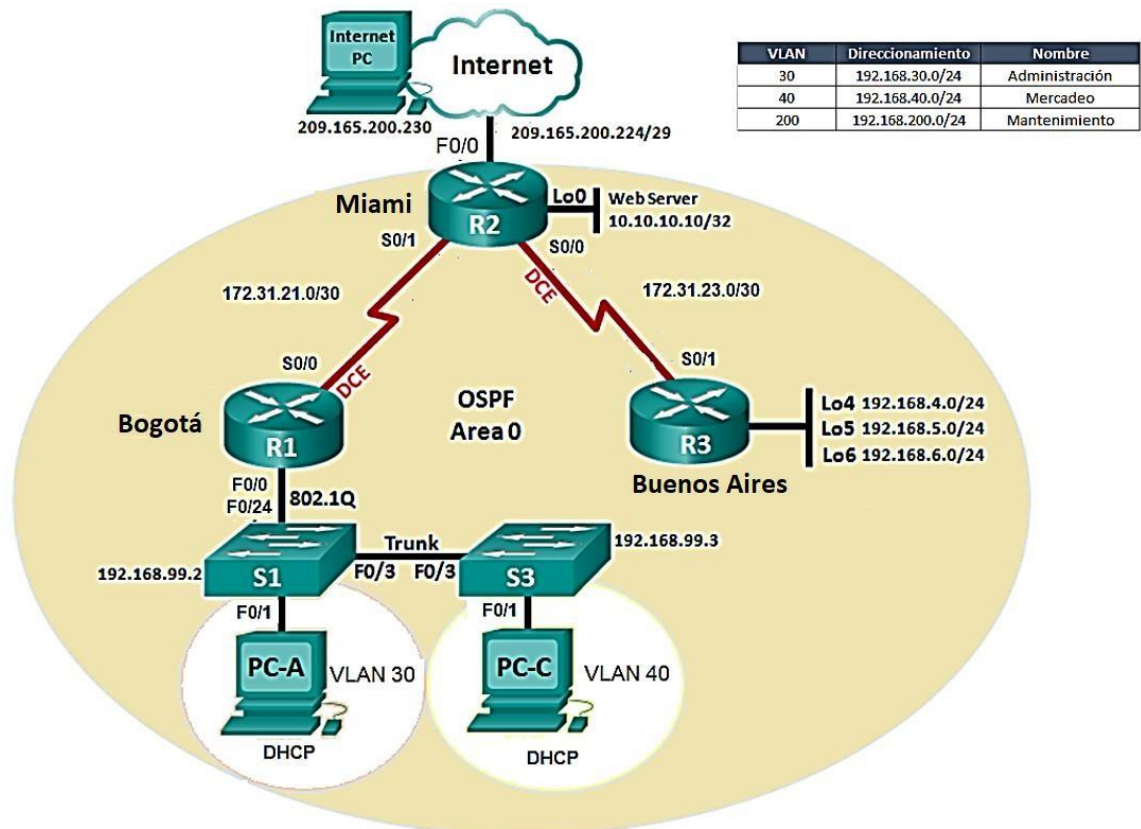
The interface also includes a toolbar at the top, a 'Logical' panel on the left, and a 'Realtime' panel at the bottom right showing a packet capture table:

Fire	Last Status	Source	Destination	Type	Color	Time (sec)	Periodic
<input checked="" type="checkbox"/>	Successful	PC2	PC0	ICMP	Light Blue	0.000	N

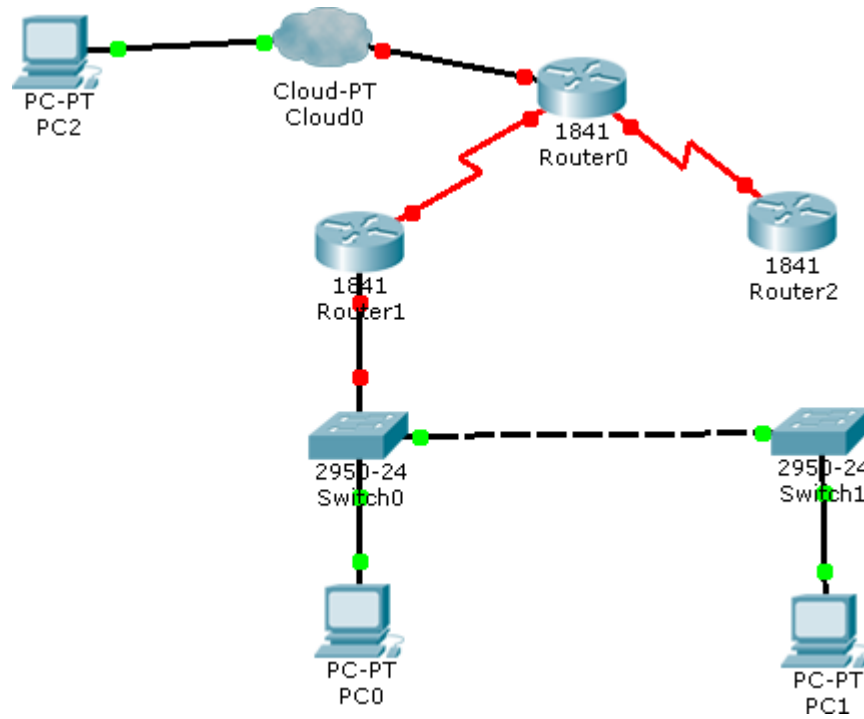
The system tray at the bottom right shows the time as 11:22 p.m. on 6/06/2019.

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.



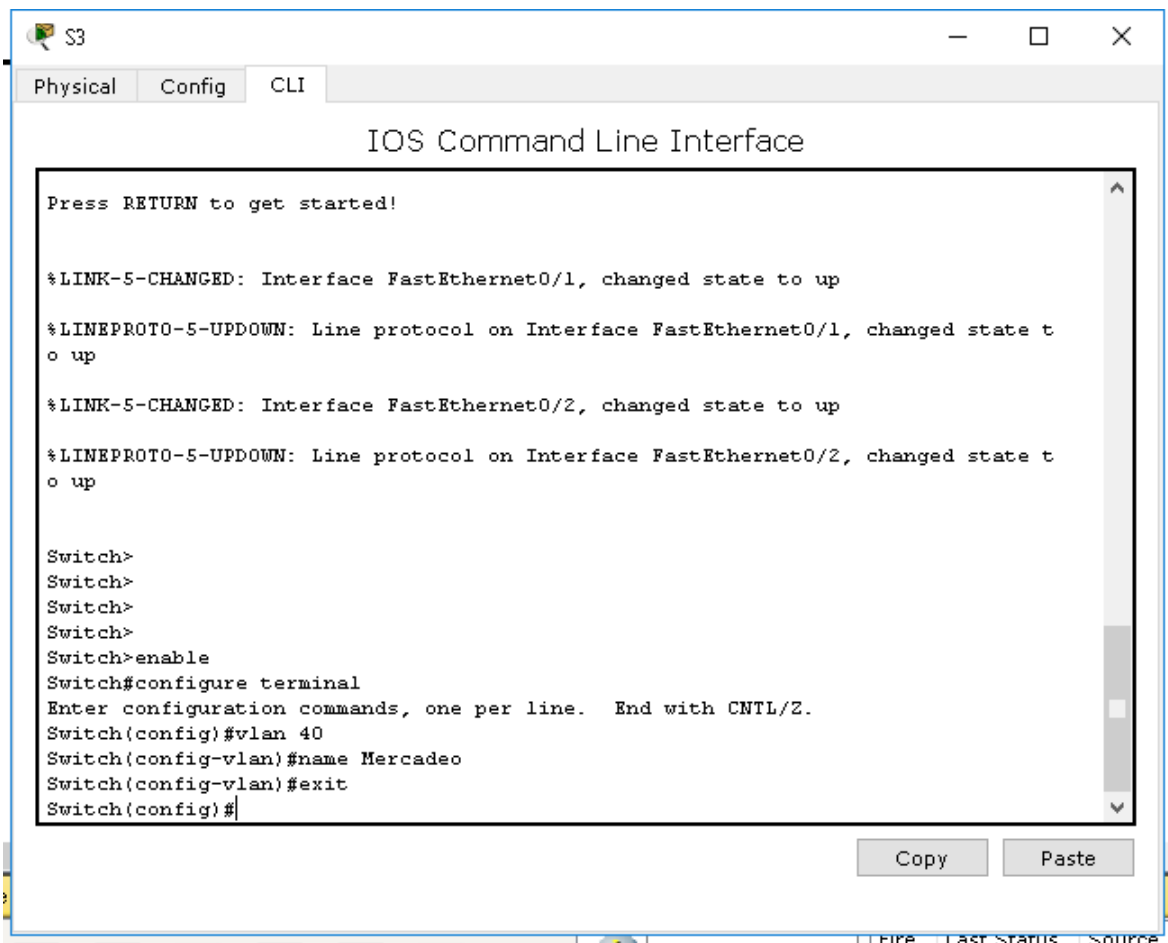
2.1 Implementando los dispositivos de la red



2.2 configuracion vlan

Las vlan nos proveen múltiples beneficios, entre ellos su principal objetivo es aislar lógicamente segmentos de red para proteger los equipos de un determinado grupo.

En el escenario se nos solicita crear 3 vlan, en este caso la primera que creamos fue al vlan 40.



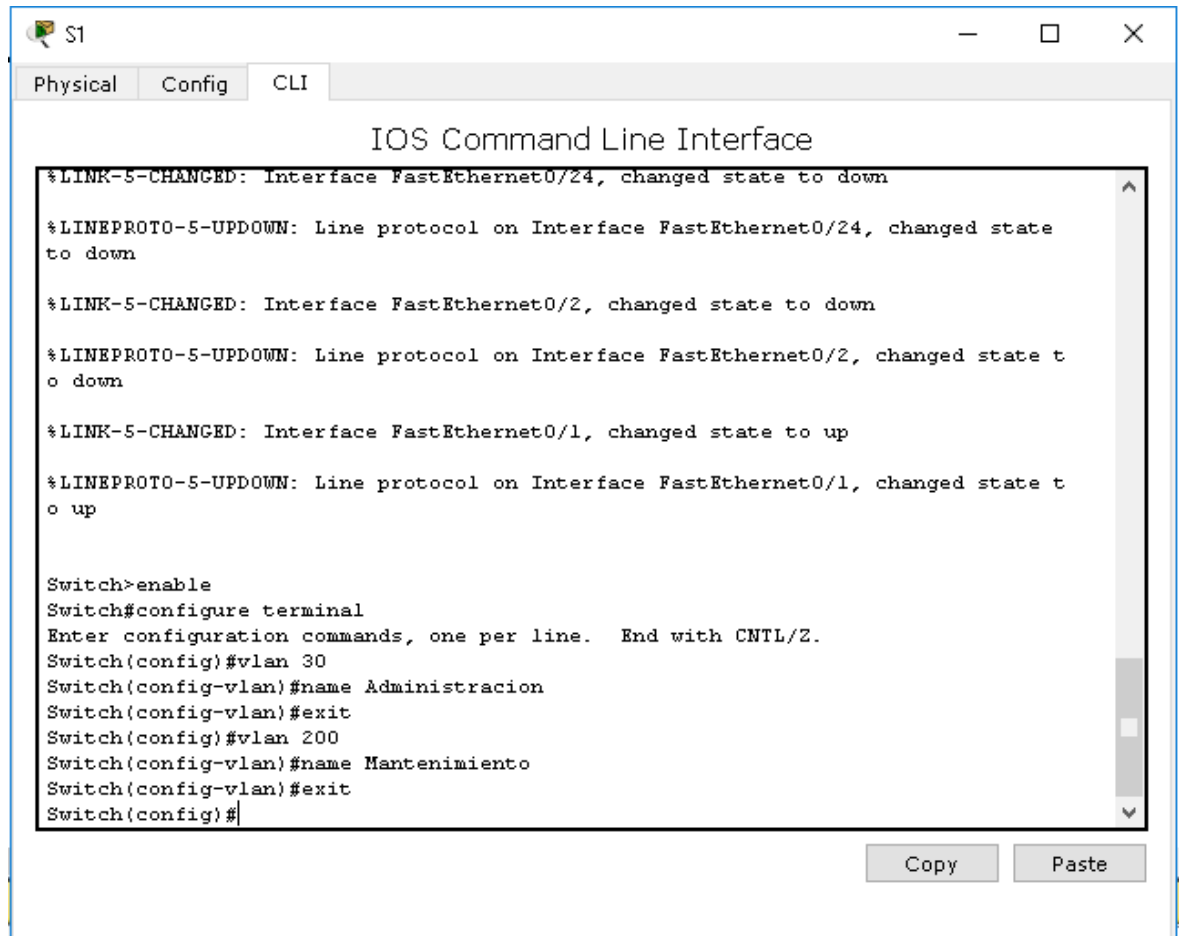
```
S3
Physical Config CLI
IOS Command Line Interface
Press RETURN to get started!

%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up
%LINK-5-CHANGED: Interface FastEthernet0/2, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state to up

Switch>
Switch>
Switch>
Switch>
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#vlan 40
Switch(config-vlan)#name Mercadeo
Switch(config-vlan)#exit
Switch(config)#
```

Copy Paste

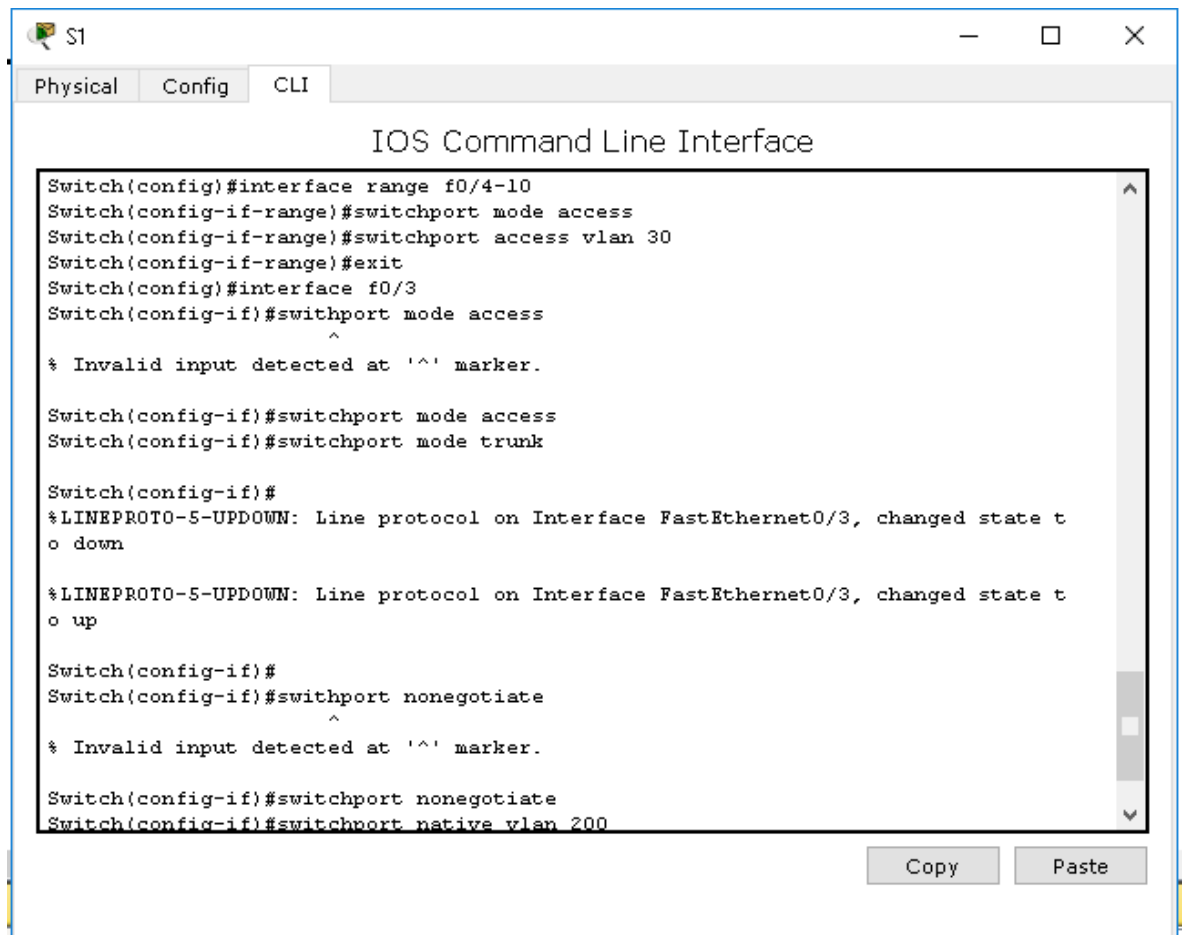
La segunda fue la vlan 30 y finalmente la vlan 200



The screenshot shows a network switch CLI interface with the following text:

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#vlan 30
Switch(config-vlan)#name Administracion
Switch(config-vlan)#exit
Switch(config)#vlan 200
Switch(config-vlan)#name Mantenimiento
Switch(config-vlan)#exit
Switch(config)#
```

Below the terminal output, there are two buttons: "Copy" and "Paste".



The screenshot shows a network switch CLI interface with the following text:

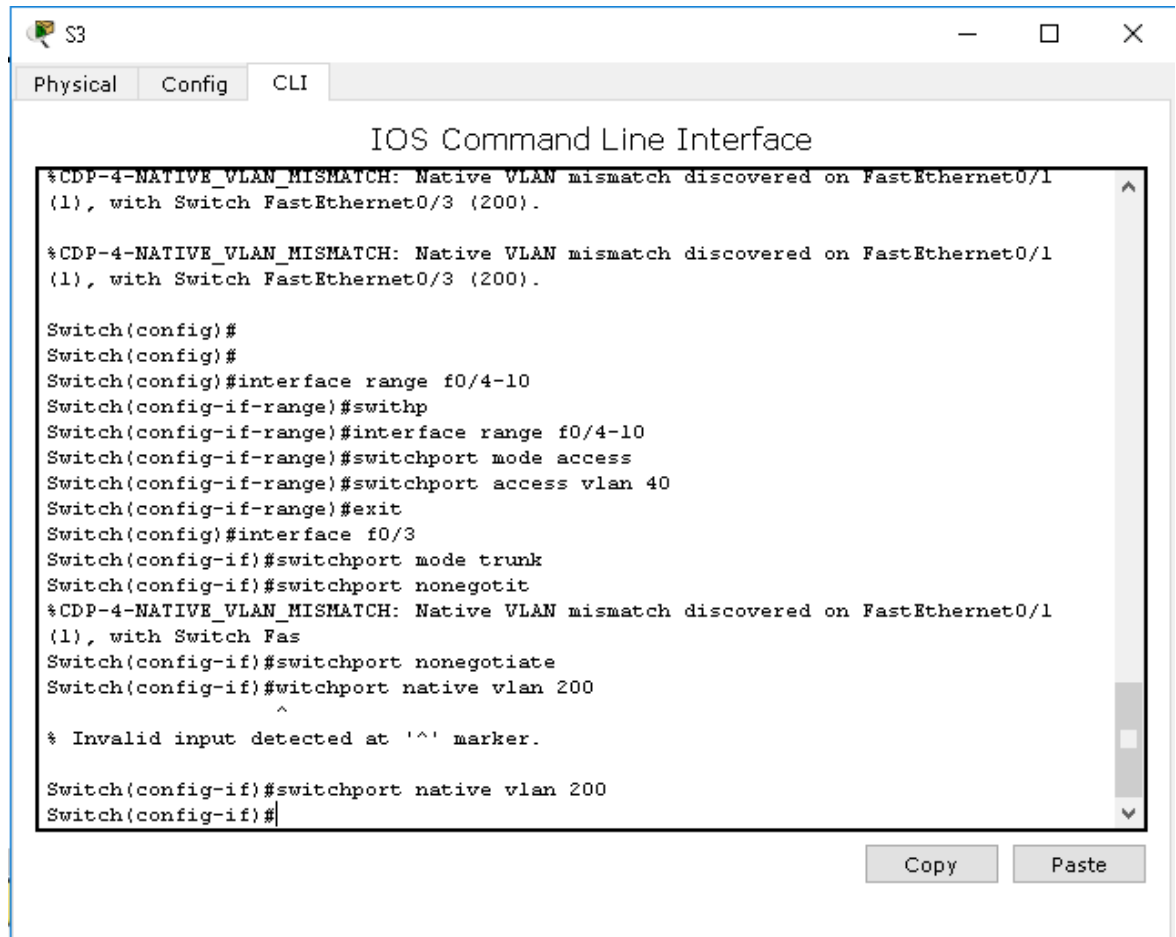
```
Switch(config)#interface range f0/4-10
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 30
Switch(config-if-range)#exit
Switch(config)#interface f0/3
Switch(config-if)#switchport mode access
Switch(config-if)#switchport mode trunk

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

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to up

Switch(config-if)#
Switch(config-if)#switchport nonegotiate
Switch(config-if)#switchport nonegotiate
Switch(config-if)#switchport native vlan 200
```

At the bottom right of the CLI window, there are two buttons: "Copy" and "Paste".



The screenshot shows a window titled "S3" with tabs for "Physical", "Config", and "CLI". The main content is the "IOS Command Line Interface" terminal. The terminal output shows the following sequence of commands and messages:

```
%CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on FastEthernet0/1
(1), with Switch FastEthernet0/3 (200).

%CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on FastEthernet0/1
(1), with Switch FastEthernet0/3 (200).

Switch(config)#
Switch(config)#
Switch(config)#interface range f0/4-10
Switch(config-if-range)#switchp
Switch(config-if-range)#interface range f0/4-10
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 40
Switch(config-if-range)#exit
Switch(config)#interface f0/3
Switch(config-if)#switchport mode trunk
Switch(config-if)#switchport nonegotit
%CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on FastEthernet0/1
(1), with Switch Fas
Switch(config-if)#switchport nonegotiate
Switch(config-if)#witchport native vlan 200
      ^
% Invalid input detected at '^' marker.

Switch(config-if)#switchport native vlan 200
Switch(config-if)#
```

At the bottom right of the terminal window, there are two buttons: "Copy" and "Paste".


```

R2
Physical Config CLI
IOS Command Line Interface
%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
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up
00:00:10: %OSPF-5-ADJCHG: Process 10, Nbr 1.1.1.1 on Serial0/0/1 from LOADING to FULL, Loading Done
00:00:10: %OSPF-5-ADJCHG: Process 10, Nbr 8.8.8.8 on Serial0/0/0 from LOADING to FULL, Loading Done

Router>enable
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#interface Serial0/0/0
Router(config-if)#ip ospf cost 9500
Router(config-if)#bandwidth 256
^
% Invalid input detected at '^' marker.

Router(config-if)#bandwidth 256
Router(config-if)#

```

Copy Paste

2.3 enrutamiento ospf

Ospf es un protocolo de enrutamiento que no solo tiene en cuenta la cantidad de saltos al elegir la ruta adecuada para enviar un paquete, si no que evalúa aspectos como ancho de banda y congestión del enlace para establecer el costo del enlace, lo que le permite elegir no solo la ruta más corta sino la ruta con el menor costo que determine su algoritmo.

Para realizar enrutamiento ospf se debe entrar al modo de configuración privilegiado y escribir los siguientes comandos:

-router ospf xx donde xx es el numero de identificación.

-router-id x.x.x.x donde x.x.x.x es una direccion de identificación que le asignaremos al router.

-network x.x.x.x wilcar área xx donde x.x.x.x es la ruta que estará enlazada mediante ospf, la wilcar es la cantidad de host que permite esa red y xx es un numero identificador del área asignada al protocolo de enrutamiento.

Una vez realizadas las configuraciones requeridas podemos revisar en la tabla de enrutamiento

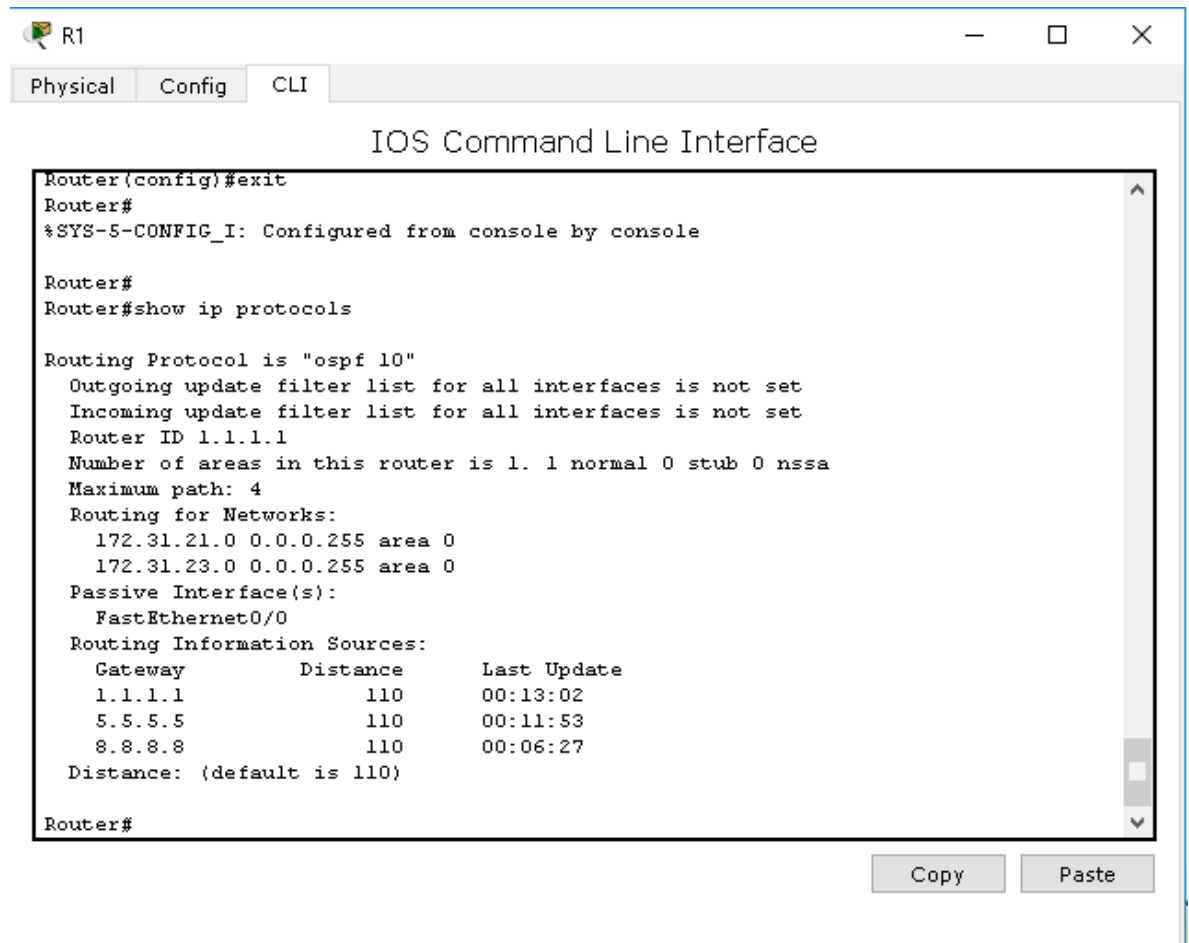
Routing Table for R1

Type	Network	Port	Next Hop IP	Metric
C	172.31.21.0/30	Serial0/0/0	---	0/0
C	192.168.99.0/24	FastEthernet0/0	---	0/0
O	172.31.23.0/30	Serial0/0/0	172.31.21.2	110/19000

Routing Table for R3

Type	Network	Port	Next Hop IP	Metric
C	172.31.23.0/30	Serial0/0/0	---	0/0
O	172.31.21.0/30	Serial0/0/0	172.31.23.2	110/9564

Y mediante el comando `show ip protocols`, cual nos da un gran resumen de las rutas agregadas por el protocolo configurado en este caso ospf, los router-id además de las interfaces pasivas



Router (config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console

Router#
Router#show ip protocols

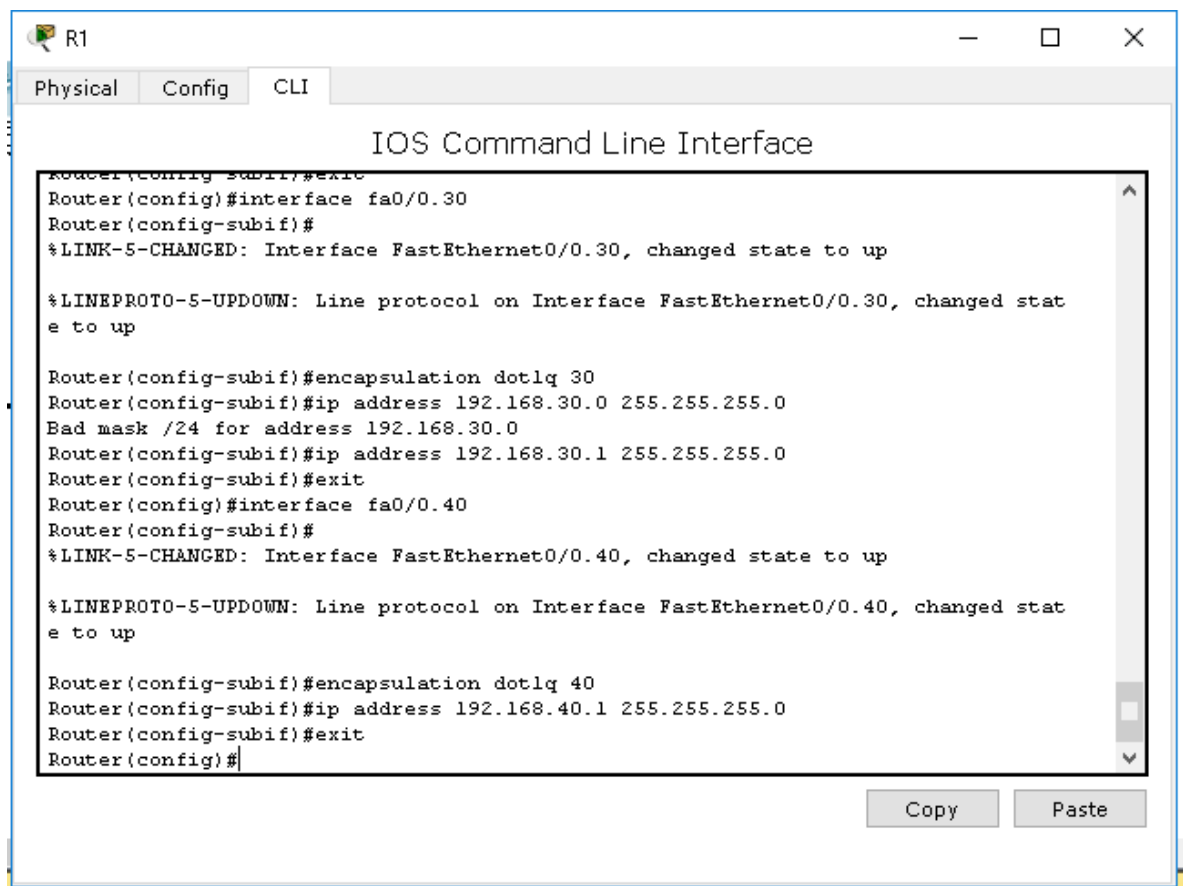
Routing Protocol is "ospf 10"
Outgoing update filter list for all interfaces is not set
Incoming update filter list for all interfaces is not set
Router ID 1.1.1.1
Number of areas in this router is 1. 1 normal 0 stub 0 nssa
Maximum path: 4
Routing for Networks:
 172.31.21.0 0.0.0.255 area 0
 172.31.23.0 0.0.0.255 area 0
Passive Interface(s):
 FastEthernet0/0
Routing Information Sources:
 Gateway Distance Last Update
 1.1.1.1 110 00:13:02
 5.5.5.5 110 00:11:53
 8.8.8.8 110 00:06:27
Distance: (default is 110)

Router#

Copy Paste

2.4 Configuración inter-vlan

Para la configuración inter-vlan, primero debemos haber configurado nuestras vlan, luego de esto ingresamos al router al cual se conectarán, e ingresamos a la interfaz de enlace para configurar las subinterfaces. Esto se logra mediante el siguiente comando: - **interface fa0/0.30** con él hemos creado nuestra subinterfaz, ahora debemos agregarle la encapsulación con el siguiente comando: **-encapsulation dot1q 30**, finalmente debemos agrégale su respectiva dirección ip y máscara de su red esto lo realizamos mediante la siguiente sentencia **-ip address 192.168.30.1 255.255.255.0**



```
Router(config-subif)#exit
Router(config)#interface fa0/0.30
Router(config-subif)#
%LINK-5-CHANGED: Interface FastEthernet0/0.30, changed state to up

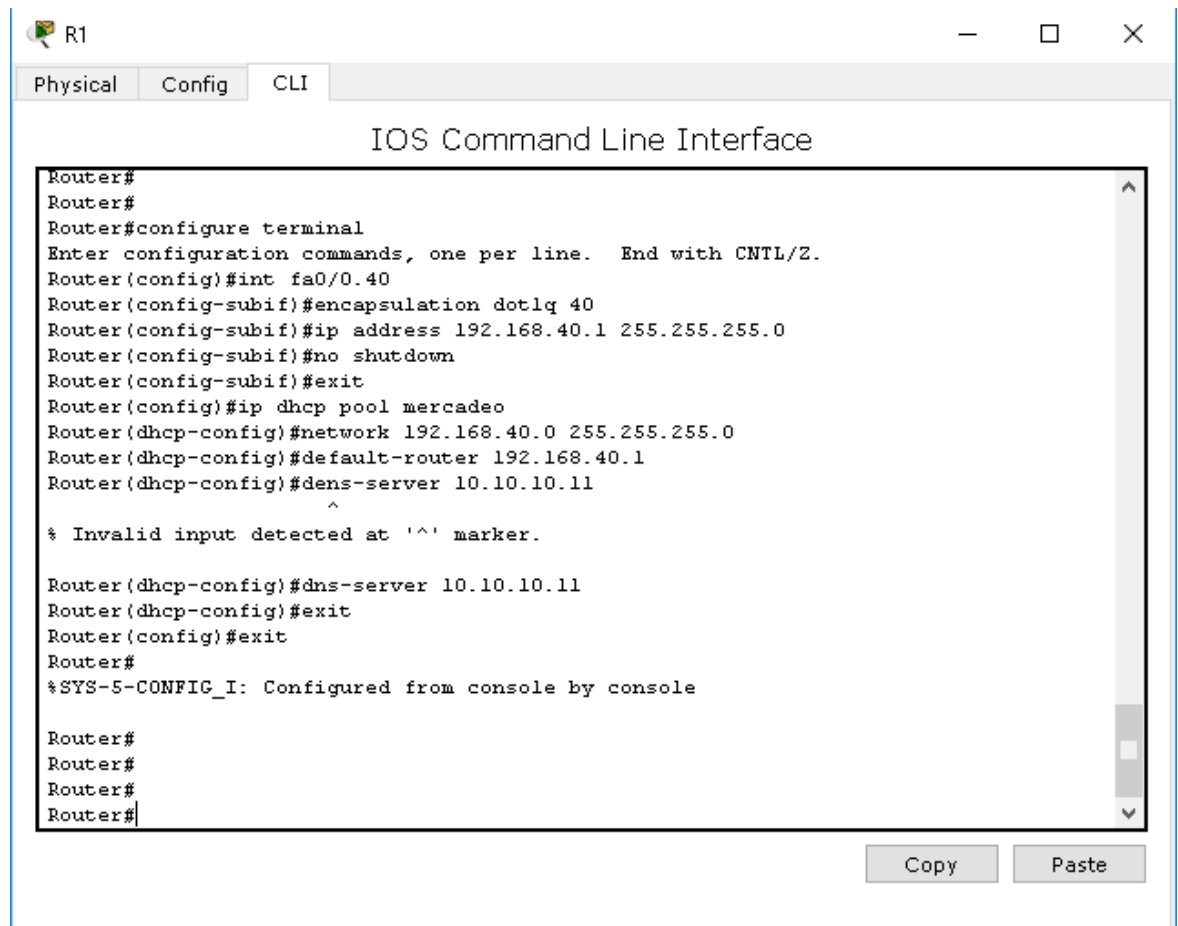
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0.30, changed state to up

Router(config-subif)#encapsulation dot1q 30
Router(config-subif)#ip address 192.168.30.0 255.255.255.0
Bad mask /24 for address 192.168.30.0
Router(config-subif)#ip address 192.168.30.1 255.255.255.0
Router(config-subif)#exit
Router(config)#interface fa0/0.40
Router(config-subif)#
%LINK-5-CHANGED: Interface FastEthernet0/0.40, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0.40, changed state to up

Router(config-subif)#encapsulation dot1q 40
Router(config-subif)#ip address 192.168.40.1 255.255.255.0
Router(config-subif)#exit
Router(config)#
```

Una vez configuradas las subinterfaces debemos agregar el pool de direcciones que le asignaremos a nuestras subinterfaces



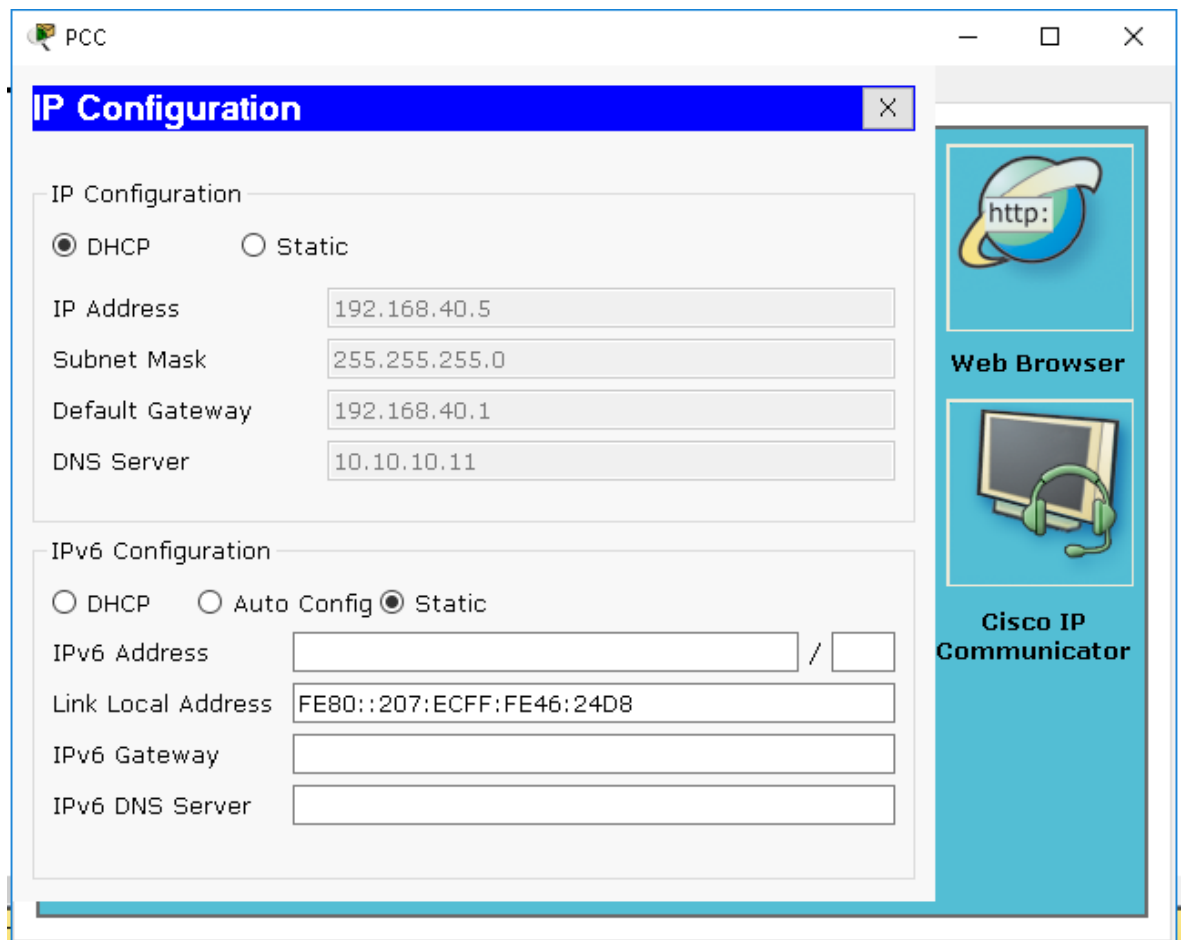
```
Router#
Router#
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#int fa0/0.40
Router(config-subif)#encapsulation dot1q 40
Router(config-subif)#ip address 192.168.40.1 255.255.255.0
Router(config-subif)#no shutdown
Router(config-subif)#exit
Router(config)#ip dhcp pool mercadeo
Router(dhcp-config)#network 192.168.40.0 255.255.255.0
Router(dhcp-config)#default-router 192.168.40.1
Router(dhcp-config)#dens-server 10.10.10.11
^
% Invalid input detected at '^' marker.

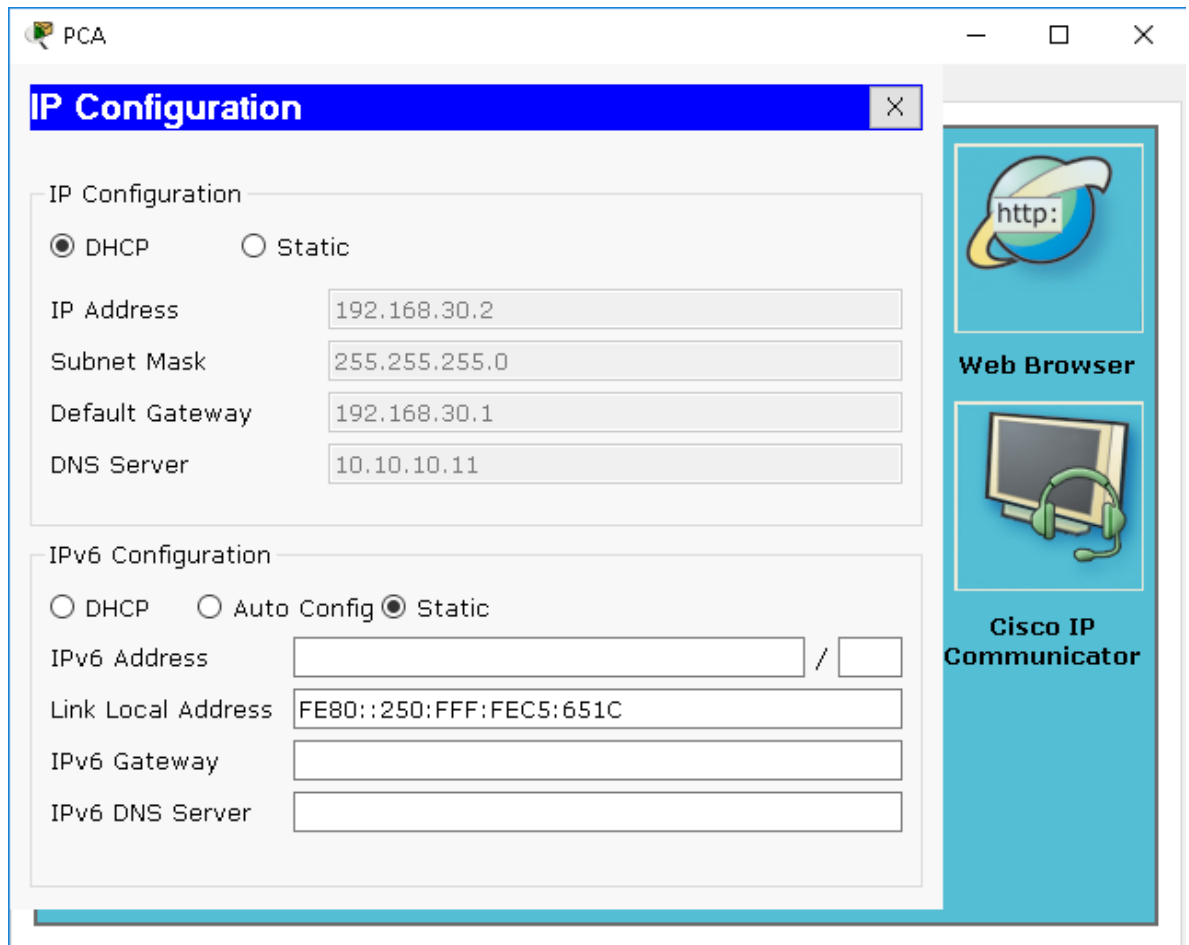
Router(dhcp-config)#dns-server 10.10.10.11
Router(dhcp-config)#exit
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console

Router#
Router#
Router#
Router#
```

Copy Paste

Luego de la configuración DHCP en el router nos dirigimos hacia nuestros host a verificar, haciendo click en la pestaña de desktop, en la opción de ip configuration cambiamos la ip de static a DHCP





En el escenario se nos pide que reservemos las primeras 30 direcciones de las subinterfaces.

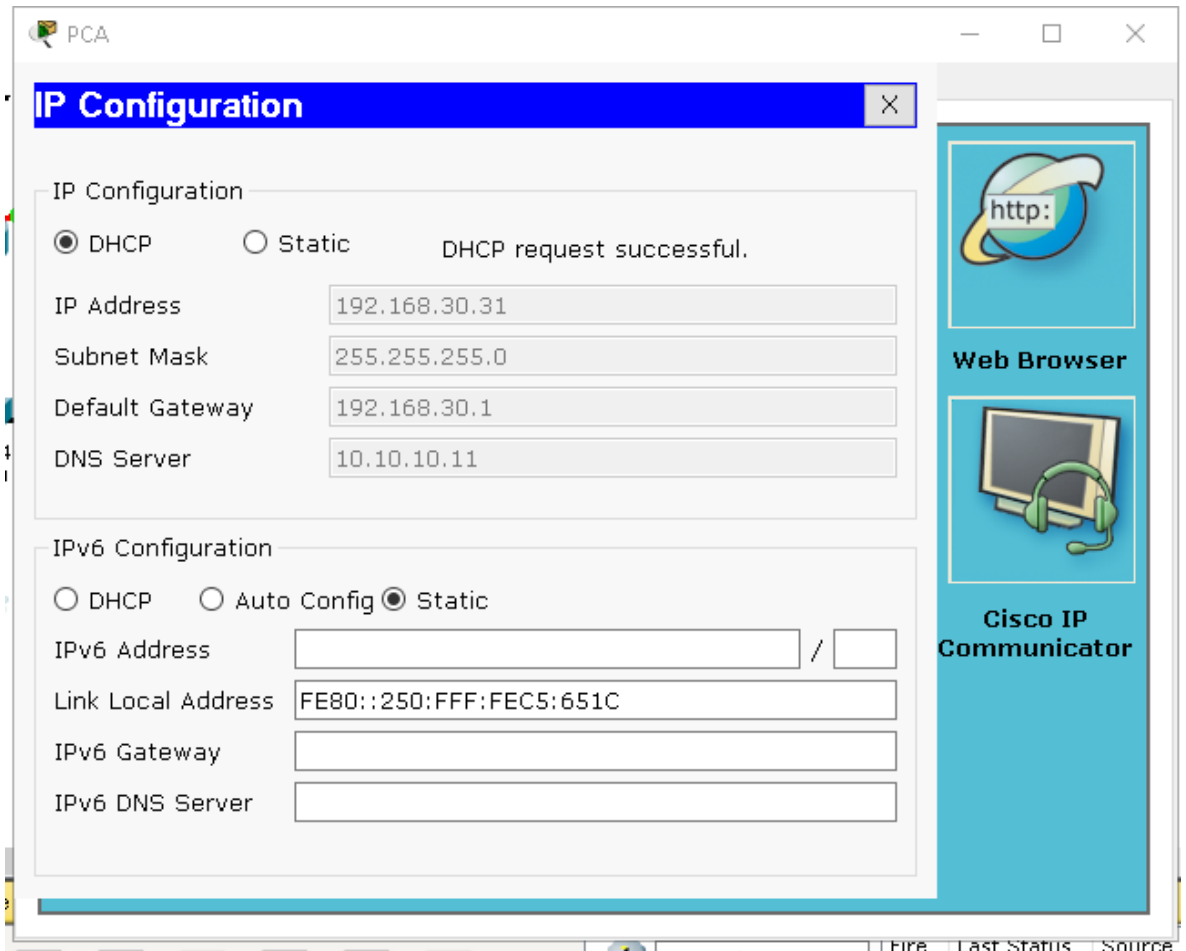
```
R1
Physical Config CLI
IOS Command Line Interface

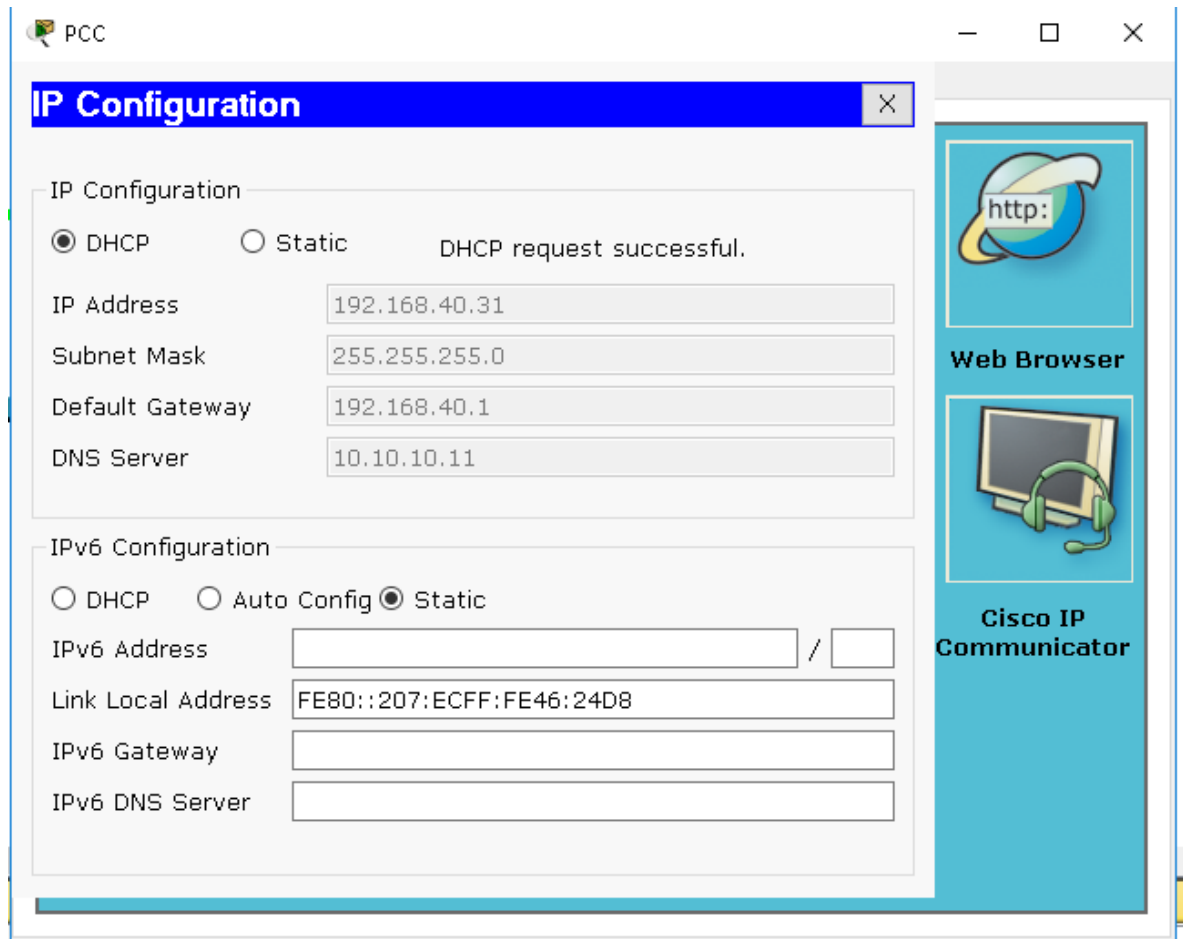
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to do
wn
10:13:44: %OSPF-5-ADJCHG: Process 10, Nbr 5.5.5.5 on Serial0/0/0 from FULL to DO
WN, Neighbor Down: Interface down or detached
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up
10:13:54: %OSPF-5-ADJCHG: Process 10, Nbr 5.5.5.5 on Serial0/0/0 from LOADING to
FULL, Loading Done

Router>
Router>
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#ip dhcp excluded-address 192.168.30.1 192.168.30.30
Router(config)#ip dhcp excluded-address 192.168.40.1 192.168.40.30
Router(config)#
```

Copy Paste

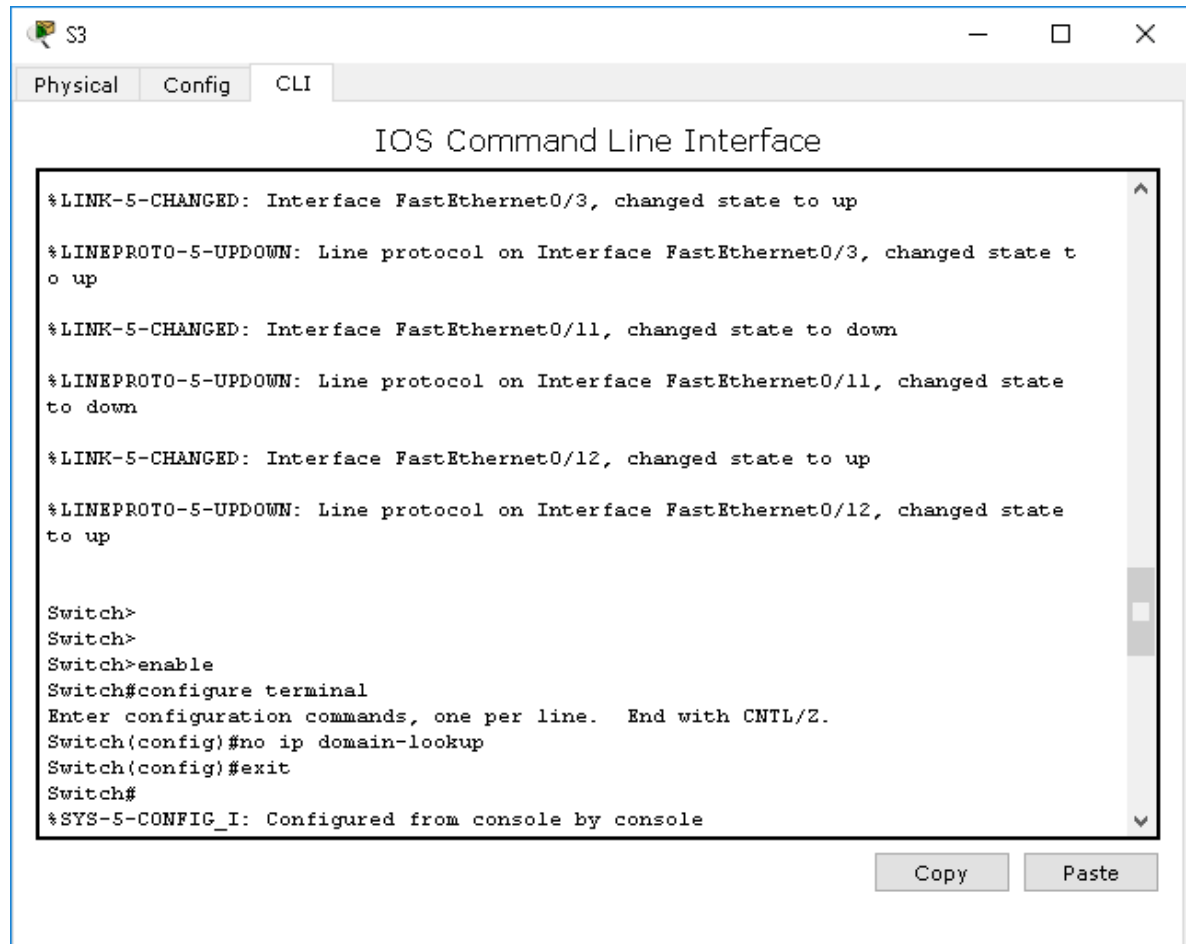
Hecha las configuraciones entramos a la configuracion ip de los hosts para verificar el resultado





2.5 Deshabilitar las dns

Para deshabilitar las dns, ejecutamos el siguiente comando en el sw

-no ip domain-lookup

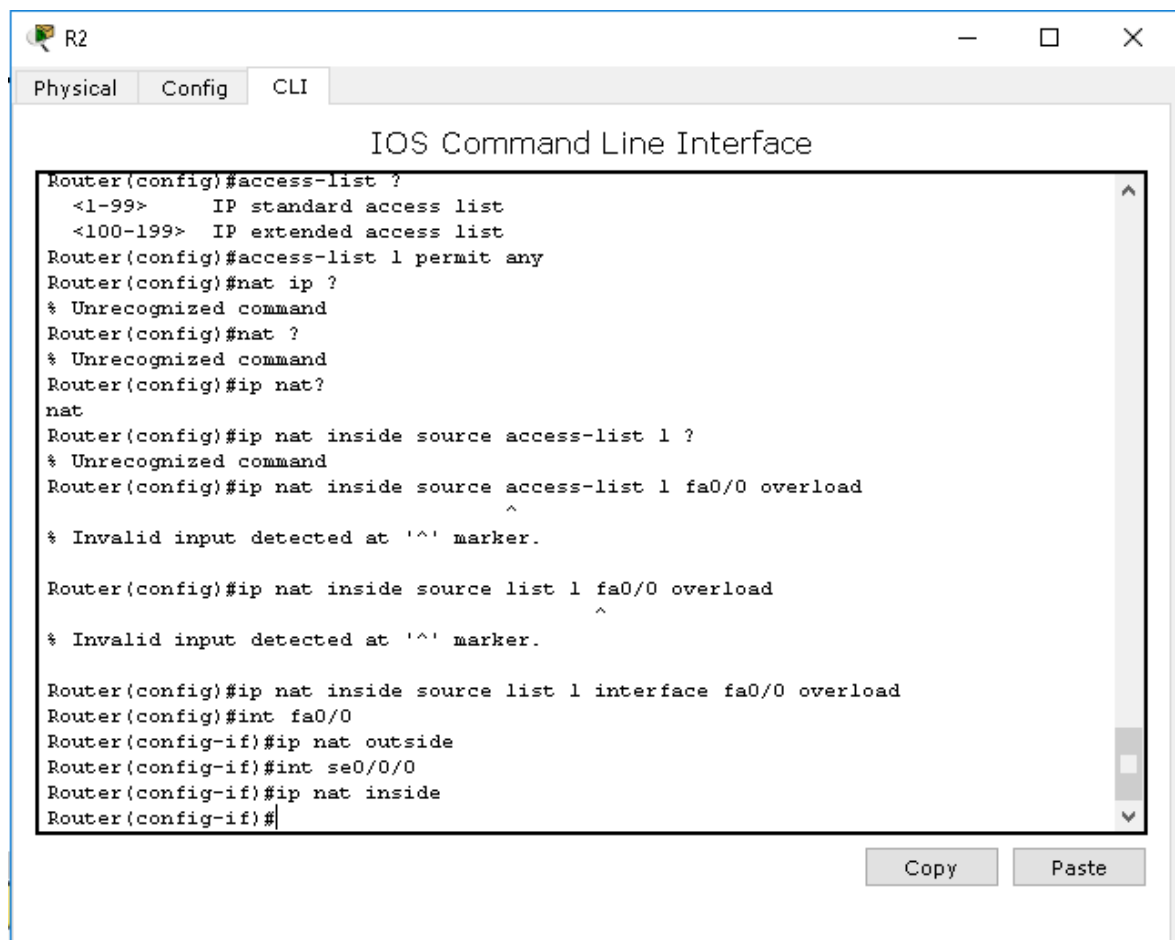
The screenshot shows a window titled "S3" with tabs for "Physical", "Config", and "CLI". The main content is the "IOS Command Line Interface" terminal. The terminal output shows status messages for three interfaces (FastEthernet0/3, 0/11, and 0/12) changing their link and line protocol states. It then shows the user entering the command "no ip domain-lookup" in configuration mode. The terminal ends with a system message: "%SYS-5-CONFIG_I: Configured from console by console".

```
Switch>
Switch>
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#no ip domain-lookup
Switch(config)#exit
Switch#
%LINK-5-CHANGED: Interface FastEthernet0/3, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to up
%LINK-5-CHANGED: Interface FastEthernet0/11, changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/11, changed state to down
%LINK-5-CHANGED: Interface FastEthernet0/12, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/12, changed state to up

Switch#
%SYS-5-CONFIG_I: Configured from console by console
```

2.6 Configuración nat

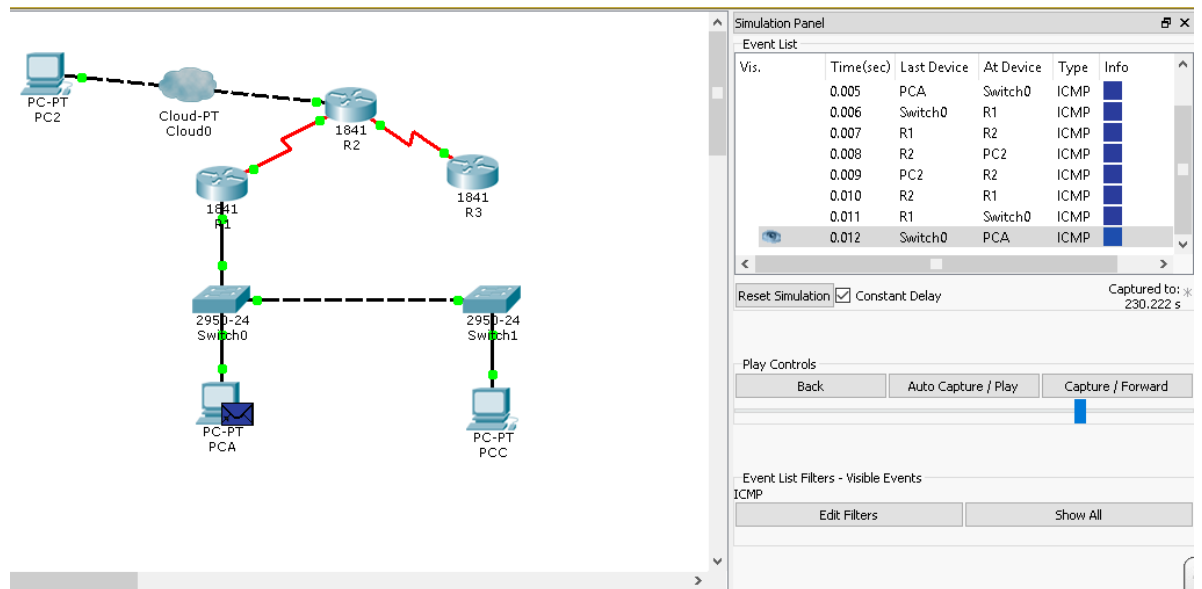
El algoritmo nat nació debido a la falta de direcciones ipv4 y lo que hace principalmente es permitir que varios equipos se conecten mediante una sola ip con el objetivo claro de ahorrarlas. Para esto, existen direcciones ip privadas que son las que tenemos en nuestros hogares las cuales existen pero solo en nuestro entorno local y direcciones públicas que son las reales las cuales debemos limitar su uso para evitar su agotamiento



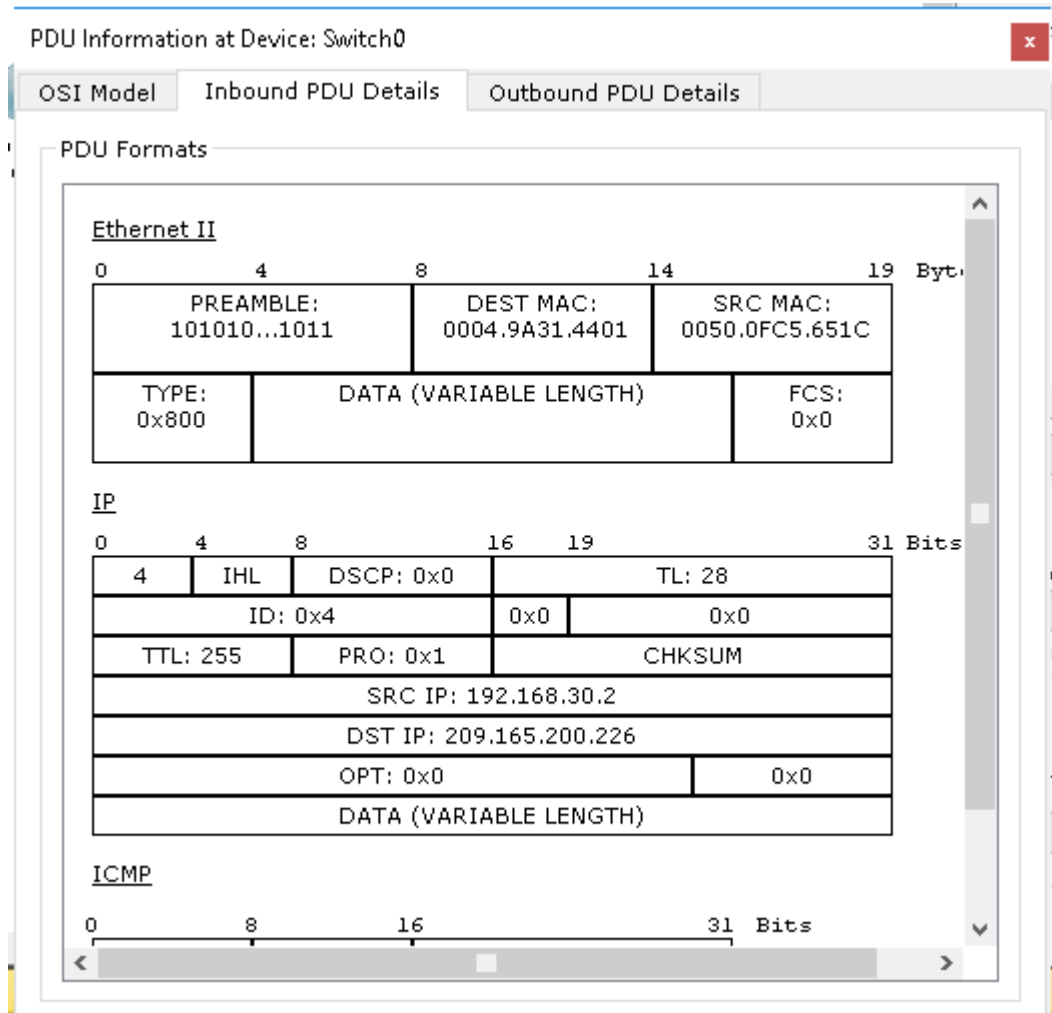
```
R2
Physical Config CLI
IOS Command Line Interface
Router(config)#access-list ?
<1-99> IP standard access list
<100-199> IP extended access list
Router(config)#access-list 1 permit any
Router(config)#nat ip ?
% Unrecognized command
Router(config)#nat ?
% Unrecognized command
Router(config)#ip nat?
nat
Router(config)#ip nat inside source access-list 1 ?
% Unrecognized command
Router(config)#ip nat inside source access-list 1 fa0/0 overload
^
% Invalid input detected at '^' marker.
Router(config)#ip nat inside source list 1 fa0/0 overload
^
% Invalid input detected at '^' marker.
Router(config)#ip nat inside source list 1 interface fa0/0 overload
Router(config)#int fa0/0
Router(config-if)#ip nat outside
Router(config-if)#int se0/0/0
Router(config-if)#ip nat inside
Router(config-if)#
```

Copy Paste

Una vez realizada la configuración NAT procedemos a su verificación para ello ingresamos al modo de simula y enviamos un mensaje, el cual estaremos verificando su ip de origen e ip de destino para este ejercicio.



En el primer paso del pc al sw vemos que la direccion de origen es las 192.168.30.2



Y la dirección es la 209.165.200.226 la cual pertenece al computador que está en internet según la configuración de nuestro escenario.

Luego vemos el siguiente paso del sw al router en el cual no deberíamos notar ningún cambio.

PDU Information at Device: R1

OSI Model Inbound PDU Details Outbound PDU Details

PDU Formats

Ethernet 802.1q

0		4		7		8		14		19		Byt
PREAMBLE: 1010 1010				S	DEST ADDR: 0004.9A31.4401				SRC ADDR: 0050.0FC5.651C			
7	8	F	D	DATA (VARIABLE LENGTH)				FCS: 0x0				
TPID: 0x810		TCI: 0x1e		TYPE: 0x1								

IP

0		4		8		16		19		31		Bits
4		IHL		DSCP: 0x0		TL: 28						
ID: 0x4				0x0		0x0						
TTL: 255		PRO: 0x1		CHKSUM								
SRC IP: 192.168.30.2												
DST IP: 209.165.200.226												
OPT: 0x0								0x0				
DATA (VARIABLE LENGTH)												

ICMP

0		8		16		31		Bits
TYPE: 0x8		CODE: 0x0		CHECKSUM				
ID: 0x2				SEQ NUMBER: 1				

PDU Information at Device: R2

OSI Model Inbound PDU Details Outbound PDU Details

PDU Formats

HDLC

0	8	16	32	32+x	48+x	56+
FLG: 0111 1110	ADR: 0x8f	CONTROL: 0x0	DATA: (VARIABLE LENGTH)		FCS: 0x0	FLG: 0111 1110

IP

0	4	8	16	19	31 Bits
4	IHL	DSCP: 0x0	TL: 28		
ID: 0x4		0x0	0x0		
TTL: 254	PRO: 0x1	CHKSUM			
SRC IP: 192.168.30.2					
DST IP: 209.165.200.226					
OPT: 0x0				0x0	
DATA (VARIABLE LENGTH)					

ICMP

0	8	16	31 Bits
TYPE: 0x8	CODE: 0x0	CHECKSUM	
ID: 0x2		SEQ NUMBER: 1	

En el paso del router1 al router2 tampoco deberían registrarse cambios

Finalmente en el paso del router2 al pc en internet es donde deberíamos observar, la traducción nat, al cambiar la direccion ip fuente, por la ip publica configurada en nuestro router, con lo cual verificamos que se ha configurado correctamente

PDU Information at Device: PC2

OSI Model Inbound PDU Details Outbound PDU Details

PDU Formats

Ethernet II

0	4	8	14	19	Byt.
PREAMBLE: 101010...1011		DEST MAC: 000C.8571.7417		SRC MAC: 0030.A378.B701	
TYPE: 0x800	DATA (VARIABLE LENGTH)			FCS: 0x0	

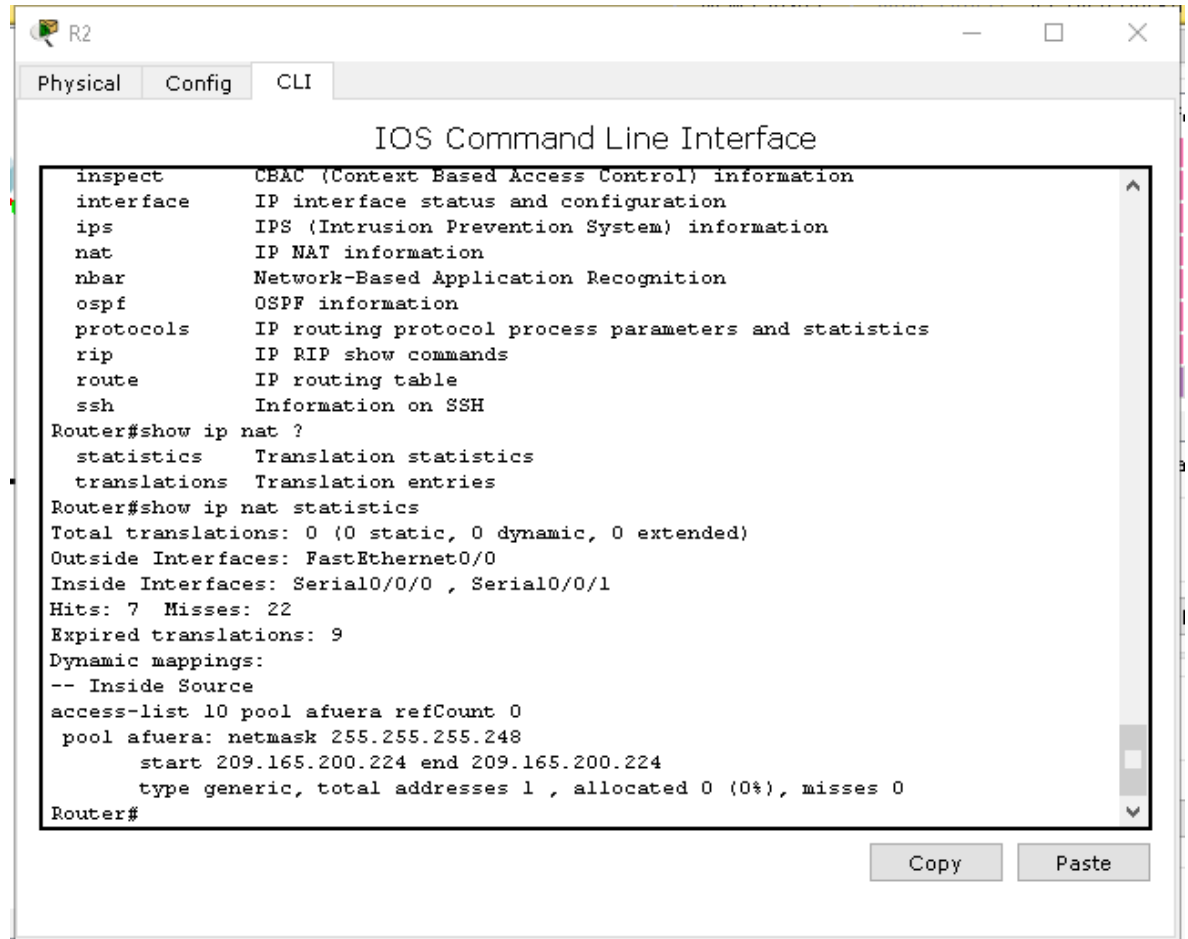
IP

0	4	8	16	19	31	Bits
4	IHL	DSCP: 0x0		TL: 28		
ID: 0x4			0x0	0x0		
TTL: 253		PRO: 0x1	CHKSUM			
SRC IP: 209.165.200.225						
DST IP: 209.165.200.226						
OPT: 0x0					0x0	
DATA (VARIABLE LENGTH)						

ICMP

0	8	16	31	Bits
TYPE: 0x8	CODE: 0x0	CHECKSUM		
ID: 0x2		SEQ NUMBER: 1		

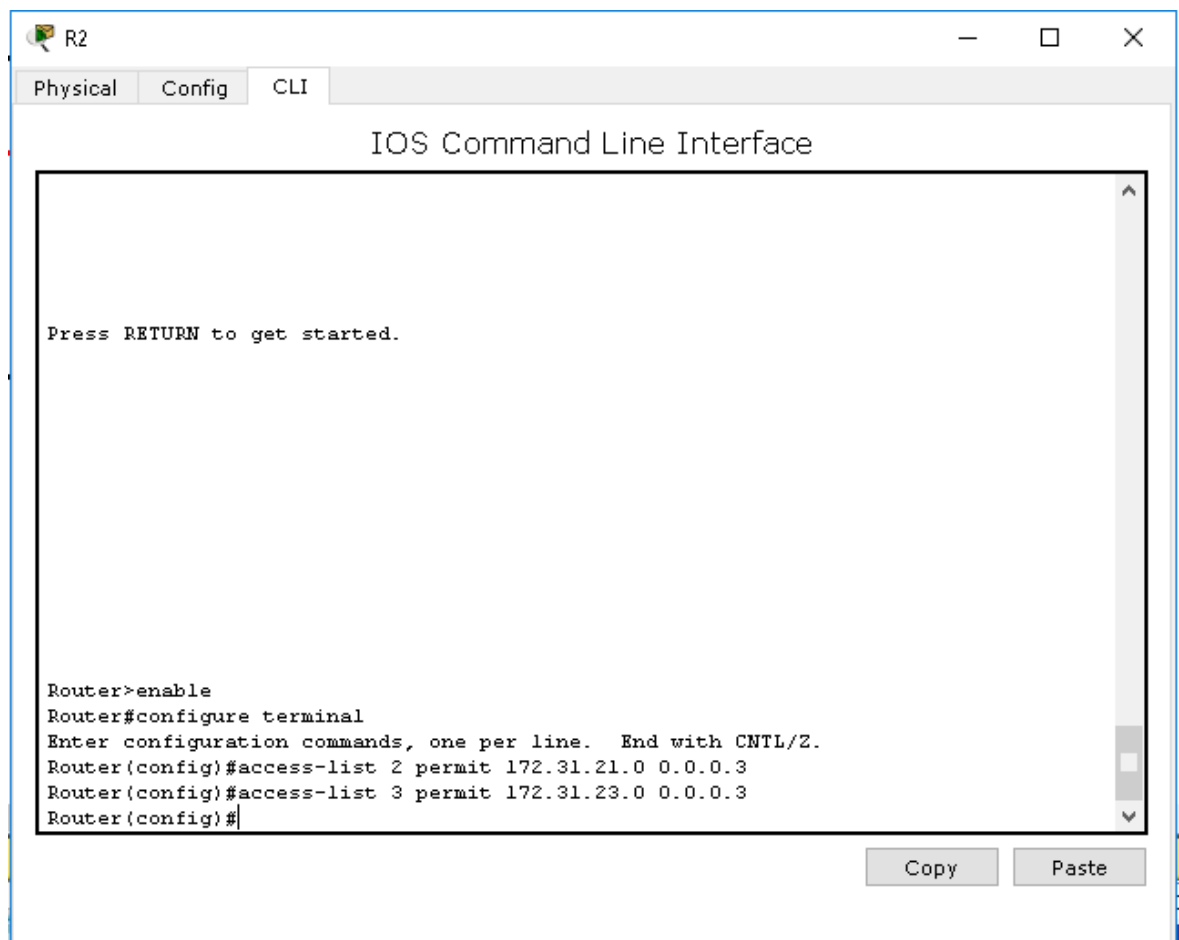
También podemos observar la configuración mediante el comando `show ip nat translations` o `statistics` dependiendo de la configuración.



```
inspect      CBAC (Context Based Access Control) information
interface   IP interface status and configuration
ips         IPS (Intrusion Prevention System) information
nat         IP NAT information
nbar        Network-Based Application Recognition
ospf        OSPF information
protocols   IP routing protocol process parameters and statistics
rip         IP RIP show commands
route       IP routing table
ssh         Information on SSH
Router#show ip nat ?
  statistics  Translation statistics
  translations Translation entries
Router#show ip nat statistics
Total translations: 0 (0 static, 0 dynamic, 0 extended)
Outside Interfaces: FastEthernet0/0
Inside Interfaces: Serial0/0/0 , Serial0/0/1
Hits: 7 Misses: 22
Expired translations: 9
Dynamic mappings:
-- Inside Source
access-list 10 pool afuera refCount 0
 pool afuera: netmask 255.255.255.248
               start 209.165.200.224 end 209.165.200.224
               type generic, total addresses 1 , allocated 0 (0%), misses 0
Router#
```

2.7 Listas de acceso estándar

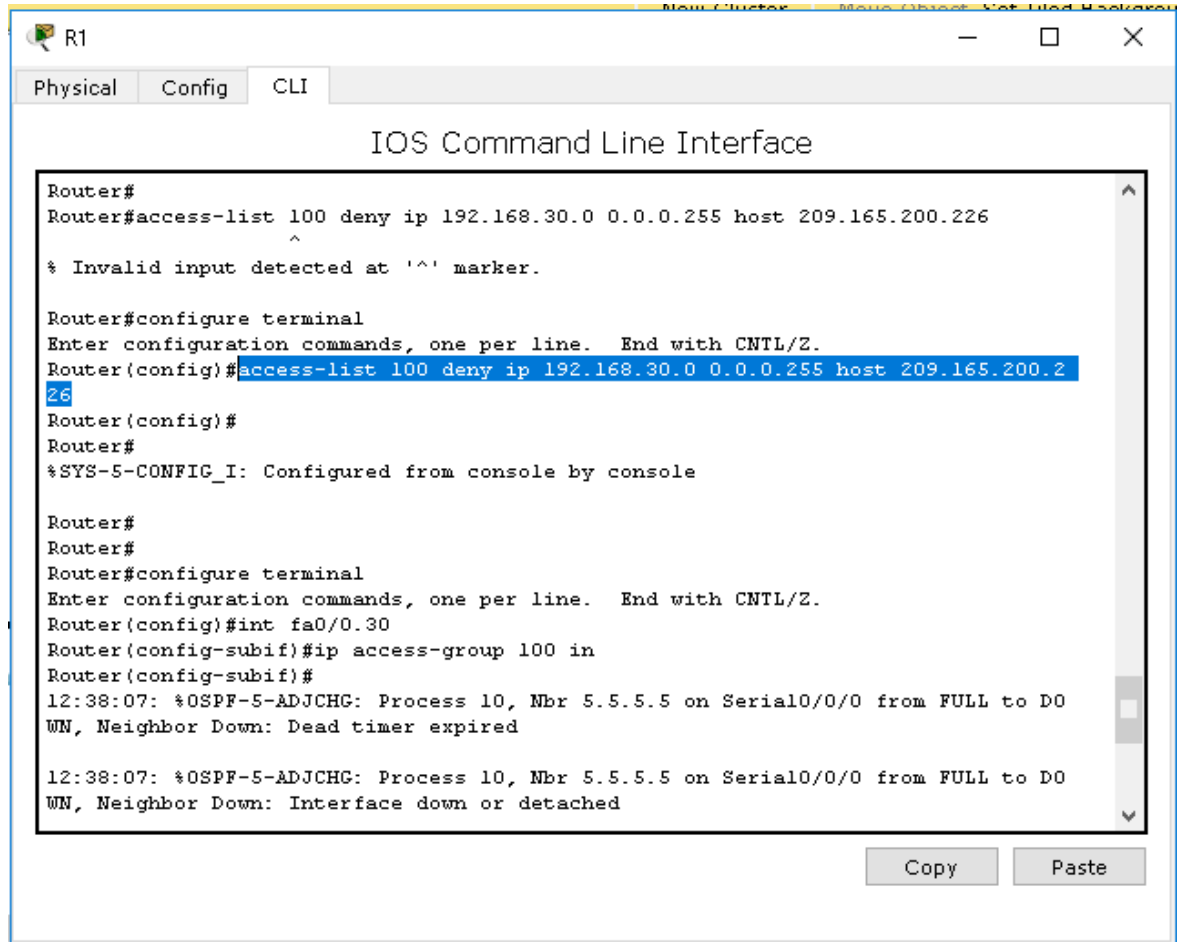
Configuramos listas de acceso básicas en donde permitimos pasar todo el tráfico ip de las redes 192.168.30.0 255.255.255.0 y 192.168.40.0 255.255.255.0



```
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#access-list 2 permit 172.31.21.0 0.0.0.3
Router(config)#access-list 3 permit 172.31.23.0 0.0.0.3
Router(config)#
```

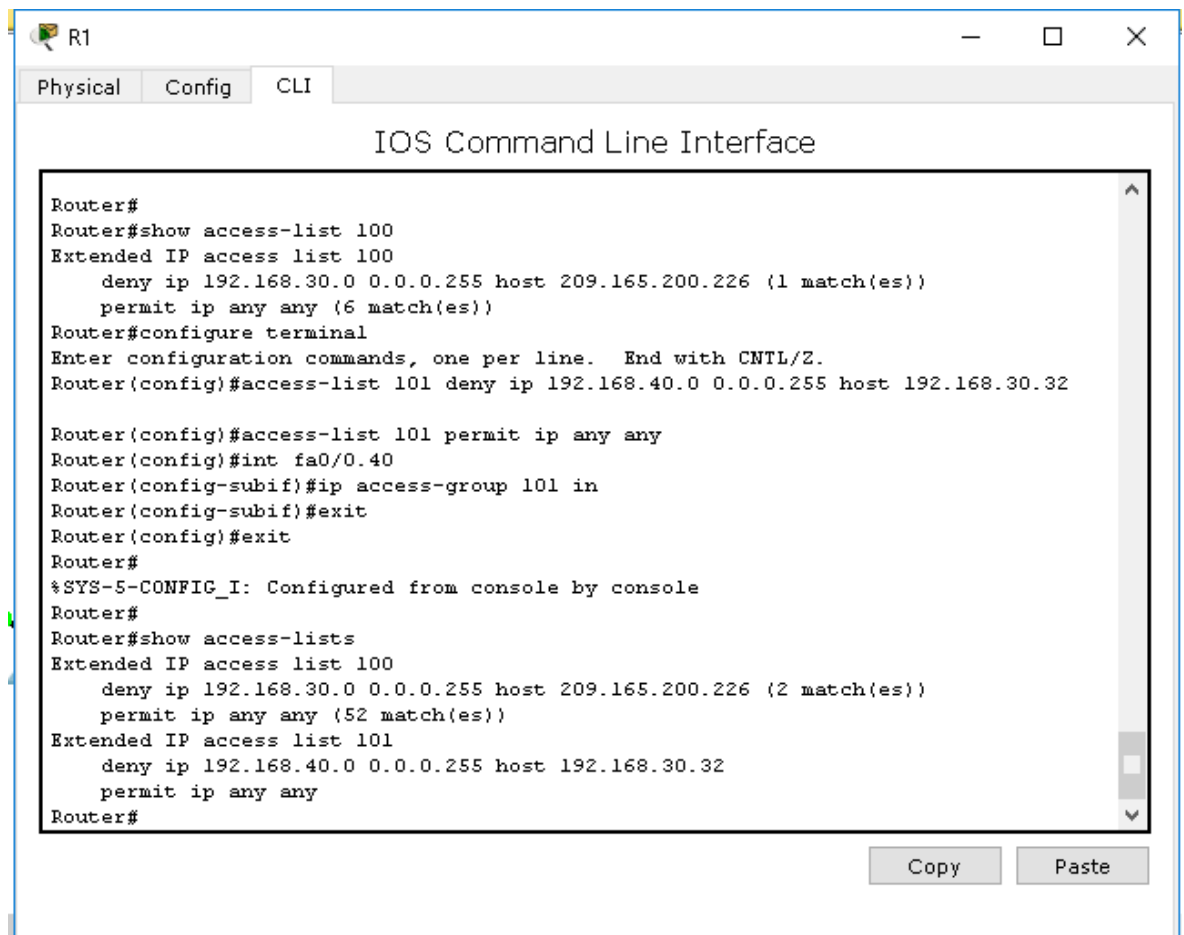
Lista de acceso extendida

En la lista de acceso extendida 100 bloquea la ip 209.165.200.226 en la red 192.168.30.0



```
R1
Physical Config CLI
IOS Command Line Interface
Router#
Router#access-list 100 deny ip 192.168.30.0 0.0.0.255 host 209.165.200.226
^
% Invalid input detected at '^' marker.
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#access-list 100 deny ip 192.168.30.0 0.0.0.255 host 209.165.200.226
Router(config)#
Router#
%SYS-5-CONFIG_I: Configured from console by console
Router#
Router#
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#int fa0/0.30
Router(config-subif)#ip access-group 100 in
Router(config-subif)#
12:38:07: %OSPF-5-ADJCHG: Process 10, Nbr 5.5.5.5 on Serial0/0/0 from FULL to DO
WN, Neighbor Down: Dead timer expired
12:38:07: %OSPF-5-ADJCHG: Process 10, Nbr 5.5.5.5 on Serial0/0/0 from FULL to DO
WN, Neighbor Down: Interface down or detached
Copy Paste
```

En la lista de acceso extendida 101 bloquea la ip 192.168.30.32 en la red 192.168.40.0



```
Router#
Router#show access-list 100
Extended IP access list 100
  deny ip 192.168.30.0 0.0.0.255 host 209.165.200.226 (1 match(es))
  permit ip any any (6 match(es))
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#access-list 101 deny ip 192.168.40.0 0.0.0.255 host 192.168.30.32

Router(config)#access-list 101 permit ip any any
Router(config)#int fa0/0.40
Router(config-subif)#ip access-group 101 in
Router(config-subif)#exit
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console
Router#
Router#show access-lists
Extended IP access list 100
  deny ip 192.168.30.0 0.0.0.255 host 209.165.200.226 (2 match(es))
  permit ip any any (52 match(es))
Extended IP access list 101
  deny ip 192.168.40.0 0.0.0.255 host 192.168.30.32
  permit ip any any
Router#
```

CONCLUSIONES

- Por medio de los dos cursos se logró aplicar conocimientos en el área de redes por medio del curso de formación CISCO NETCAP que abordó capítulos para ser aplicados a escenarios reales como los cuales se desarrolló en esta práctica, también con ayuda del programa PACKET TRACER el cual nos fue de mucha ayuda para la creación de varias topologías y variedad de computadoras, servidores, cables de red, routers, switches y demás elementos básicos para la creación de redes y sus configuraciones.
- En los dos escenarios se aplicaron la mayoría de protocolos, comandos que fueron vistos a lo largo de los dos módulos del curso CISCO los cuales resultaron útiles para la creación de topologías y configuraciones en cada uno de los pasos planteados para la práctica.
- En este trabajo se consolidan las actividades prácticas finales en el desarrollo de cada unidad de acuerdo a los casos de estudio dados, se ha aplicado los conocimientos proporcionados en el material de apoyo emanado por la empresa CISCO en el desarrollo del aprendizaje autónomo promovido para este tipo de ambientes virtuales.
- Se logró una satisfactoria conexión, configuración y simulación de los dispositivos de las redes en los correspondientes casos de estudio.
- Se repasaron todos los conceptos aprendidos en los módulos enfocando todo a los diseños de las redes solicitadas.

Bibliografía

I'm Learning - Networking Academy. [en línea], [sin fecha]. [Consulta: 21 mayo 2019].
Disponible en: <https://www.netacad.com/es/group/landing/v2/learn/>.

RON WELLMAN, [sin fecha]. *Passive Interfaces* [en línea]. Disponible en:
<https://www.youtube.com/watch?v=Kk2ONxdYb7Y>.

OFIMATICA EASY, [sin fecha]. *CONFIGURACIÓN NAT | PACKET TRACER | TUTORIAL 10* [en línea]. Disponible en:
<https://www.youtube.com/watch?v=544AdGEkL2c>.

MASTERHEHEGAR, [sin fecha]. *09 - VLSM con Enrutamiento RIP Versión 2 en Packet Tracer (CYERD)* [en línea]. Disponible en:
<https://www.youtube.com/watch?v=7oNQFRaS6xQ&t=533s>.

HAROLD CASTAÑO GIRALDO, [sin fecha]. *Configuración de la subred y del router* [en línea]. Disponible en: <https://www.youtube.com/watch?v=CsMWRDBMapk>.

BYRON CUMBAL, [sin fecha]. *Ruta por defecto en redes cisco* [en línea]. Disponible en:
<https://www.youtube.com/watch?v=ABmjwSS4npg>.

ARUMADIGITAL, [sin fecha]. *Redes 134 WAN PPP Autenticacion PAP y CHAP* [en línea]. Disponible en: <https://www.youtube.com/watch?v=IvxzG15wm4I>.

