SOLUCIÓN DE DOS ESTUDIOS DE CASO SOPORTADOS EN TECNOLOGÍA CISCO

Presentado por:

Eulen Steven Serrato

Informe Técnico

Grupo:

203092_5

Presentado a:

Juan Carlos Vesgas

Unidad Nacional Abierta y a Distancia – UNAD

Escuela de Ingeniería

Bogotá

14 de Diciembre de 2019

Tabla de Contenido

Tabla de Ilustraciones

Índice de Tablas

RESUMEN

El presente trabajo se desarrolló bajo la metodología autónomo donde es necesario utilizar y emplear los medios y mediaciones tecnológicas tanto proporcionados por Cisco a través de la página NetCad, como también los proporcionado por la Universidad UNAD para llevar a cabo la elaboración y el diseño de las redes y subredes virtuales de acuerdo a los escenarios propuestos en la guía de actividad y así el poner en práctica lo aprendido en los demás talleres y al mismo tiempo conocer las herramientas, protocolos y recursos que los elementos Cisco proporciona para la configuración de redes de información. A través de la comprobación total de los dispositivos instalados en las redes virtuales y a su vez la implementación de protocolos de seguridad en dichas dispositivos, se obtuvo un resultado satisfactorio tanto a nivel personal como también profesional.

Palabras Clave: Redes, Cisco, Subredes, Vlan, Router y Switch.

ABSTRACT

The present work was developed under the autonomous methodology where it is necessary to use and use the technological means and mediations provided by Cisco through the NetCad page, as well as those provided by the UNAD University to carry out the development and design of the virtual networks and subnets according to the scenarios proposed in the activity guide and thus put into practice what has been learned in the other workshops and at the same time know the tools, protocols and resources that Cisco provides for the configuration of information networks . Through the total verification of the devices installed in the virtual networks and in turn the implementation of security protocols in said devices, a satisfactory result was obtained both personally and professionally.

INTRODUCCIÓN

La seguridad de la información y de los diferentes equipos de cómputo es algo a tener muy en cuenta hoy día principalmente si somos los encargados de la seguridad de la red en la empresa en la cual laboramos. En muchas casos la puesta en seguridad o bloqueo de algún equipo puede ocasionar el bloqueo masivo de comunicación hacia y desde el mismo por lo que es indispensable contar con herramientas y recursos tecnológico que permitan la administración segura del tráfico en las redes de comunicación y que de igual manera permita su completa comunicación y accesos a los recursos a los cuales requiere dentro de la red, a presente actividad nos permite poner en práctica los conocimientos de redes y diferentes protocolos de enrutamiento y restricción de accesos y permisos a diferentes entornos de la red con lo cual se puede diseñar redes más eficientes y seguras.

OBJETIVOS

Objetivo general

- Conocer las herramientas protocolos y recursos que los elementos cisco proporcionas para la configuración de redes de información.

Objetivo específicos

- Poner en práctica los diferentes sistemas de subredes como el subneteo y redes Vlan
- Configurar accesos mediantes protocolos ACL
- Realizar enrutamientos de los routers
- Crear diferentes servicios en los servidores como WB, DHCL, TFTP etc.
- Realizar configuraciones seguras en los routers

DESCRIPCIÓN DE ESCENARIOS PROPUESTOS PARA LA PRUEBA DE HABILIDADES

1 Escenario 1 Una empresa posee sucursales distribuidas en las ciudades de Bogotá, Medellín y Cali en donde el estudiante será el administrador de la red, el cual deberá configurar e interconectar entre sí cada uno de los dispositivos que forman parte del escenario, acorde con los lineamientos establecidos para el direccionamiento IP, protocolos de enrutamiento y demás aspectos que forman parte de la topología de red. Topología de red Los requerimientos solicitados son los siguientes:

Parte 1: Para el direccionamiento IP debe definirse una dirección de acuerdo con el número de hosts requeridos.

Parte 2: Considerar la asignación de los parámetros básicos y la detección de vecinos directamente conectados.

Parte 3: La red y subred establecidas deberán tener una interconexión total, todos los hosts deberán ser visibles y poder comunicarse entre ellos sin restricciones.

Parte 4: Implementar la seguridad en la red, se debe restringir el acceso y comunicación entre hosts de acuerdo con los requerimientos del administrador de red.

Parte 5: Comprobación total de los dispositivos y su funcionamiento en la red.

Parte 6: Configuración final

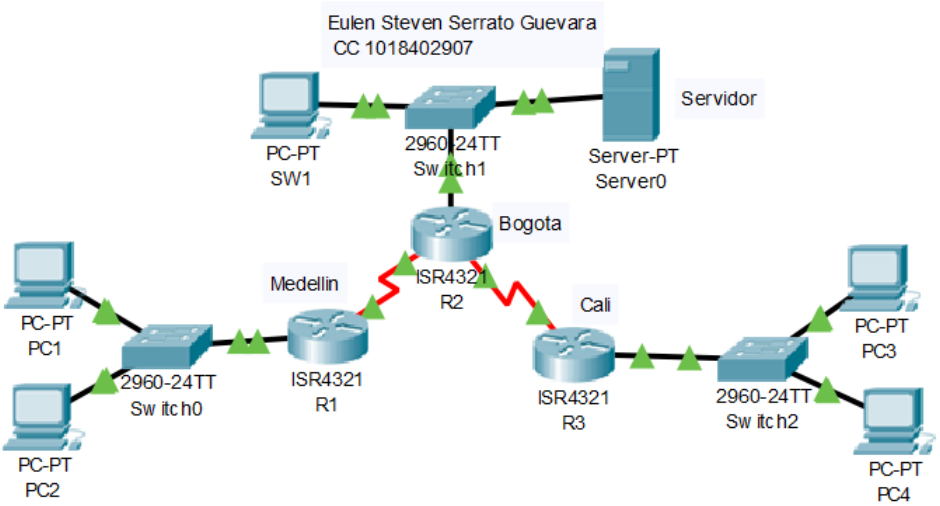


Ilustración 1 Ejemplo Escenario 1

DESARROLLO ESCENARIO 1

Como trabajo inicial se debe realizar lo siguiente.

• Realizar las rutinas de diagnóstico y dejar los equipos listos para su configuración (asignar nombres de equipos, asignar claves de seguridad, etc).

• Realizar la conexión física de los equipos con base en la topología de red Configurar la topología de red, de acuerdo con las siguientes especificaciones.

1.1 Parte 1: Asignación de direcciones IP:
a. Se debe dividir (subnetear)la red creando una segmentación en ocho partes, para permitir su crecimiento futuro de la red corporativa.

$$2^3 = 8$$

Se toman 3 bits de la parte de Hots

La máscara de subred seria 255.255.255.224

b. Asignar una dirección IP a la red.

Las direcciones IP seria las siguientes:

Tabla 1 Tabla de Direccionamiento IP

Red		Direccionamiento IP	
		Binario	Dirección IP
0	Red	11111111.11111111.11111111'.11100000	192.168.1.0
	Primero	11111111.11111111.11111111'.11100001	192.168.1.1
	Ultimo	11111111.11111111.11111111'.11111110	192.168.1.30
	Broadcast	11111111.11111111.11111111'.11111111	192.168.1.31
1	Red	11111111.11111111.11111111'.100000000	192.168.1.32
	Primero	11111111.11111111.11111111'.100000001	192.168.1.33
	Ultimo	11111111.11111111.11111111'.100011110	192.168.1.62
	Broadcast	11111111.11111111.11111111'.100011111	192.168.1.63
2	Red	11111111.11111111.11111111'.100100000	192.168.1.64
	Primero	11111111.11111111.11111111'.100100001	192.168.1.65
	Ultimo	11111111.11111111.11111111'.100111110	192.168.1.94
	Broadcast	11111111.11111111.11111111'.100111111	192.168.1.95
3	Red	11111111.11111111.11111111'.101000000	192.168.1.96
	Primero	11111111.11111111.11111111'.101000001	192.168.1.97
	Ultimo	11111111.11111111.11111111'.101011110	192.168.1.126
	Broadcast	11111111.11111111.11111111'.101011111	192.168.1.127

4	Red	11111111.11111111.11111111'.101100000	192.168.1.128
	Primero	11111111.11111111.11111111'.101100001	192.168.1.129
	Ultimo	11111111.11111111.11111111'.101111110	192.168.1.158
	Broadcast	11111111.11111111.11111111'.101111111	192.168.1.159
5	Red	11111111.11111111.11111111'.110000000	192.168.1.160
	Primero	11111111.11111111.11111111'.110000001	192.168.1.161
	Ultimo	11111111.11111111.11111111'.110011110	192.168.1.190
	Broadcast	11111111.11111111.11111111'.110011111	192.168.1.191
6	Red	11111111.11111111.11111111'.110100000	192.168.1.192
	Primero	11111111.11111111.11111111'.110100001	192.168.1.193
	Ultimo	11111111.11111111.11111111'.110111110	192.168.1.222
	Broadcast	11111111.11111111.11111111'.110111111	192.168.1.223
7	Red	11111111.11111111.11111111'.111000000	192.168.1.224
	Primero	11111111.11111111.11111111'.111000001	192.168.1.225
	Ultimo	11111111.11111111.11111111'.111011110	192.168.1.254
	Broadcast	11111111.11111111.11111111'.111011111	192.168.1.255

1.2 Parte 2: Configuración Básica.

a. Completar la siguiente tabla con la configuración básica de los routers, teniendo en cuenta las subredes diseñadas.

Tabla 2 Configuración Básica de Routers

	R1	R2	R3
Nombre de Host	MEDELLIN	BOGOTA	CALI
Dirección de Ip en interfaz Serial 0/0	162.16.1.1	162.167.1.2	162.167.1.1
Dirección de Ip en interfaz Serial 0/1		162.16.1.2	
Dirección de Ip en interfaz FA 0/0	192.168.1.33	192.168.1.1	192.168.1.65
Protocolo de enrutamiento	Eigrp	Eigrp	Eigrp
Sistema Autónomo	200	200	200
Afirmaciones de red	192.168.1.0	192.168.1.0	192.168.1.0

Configuración R1

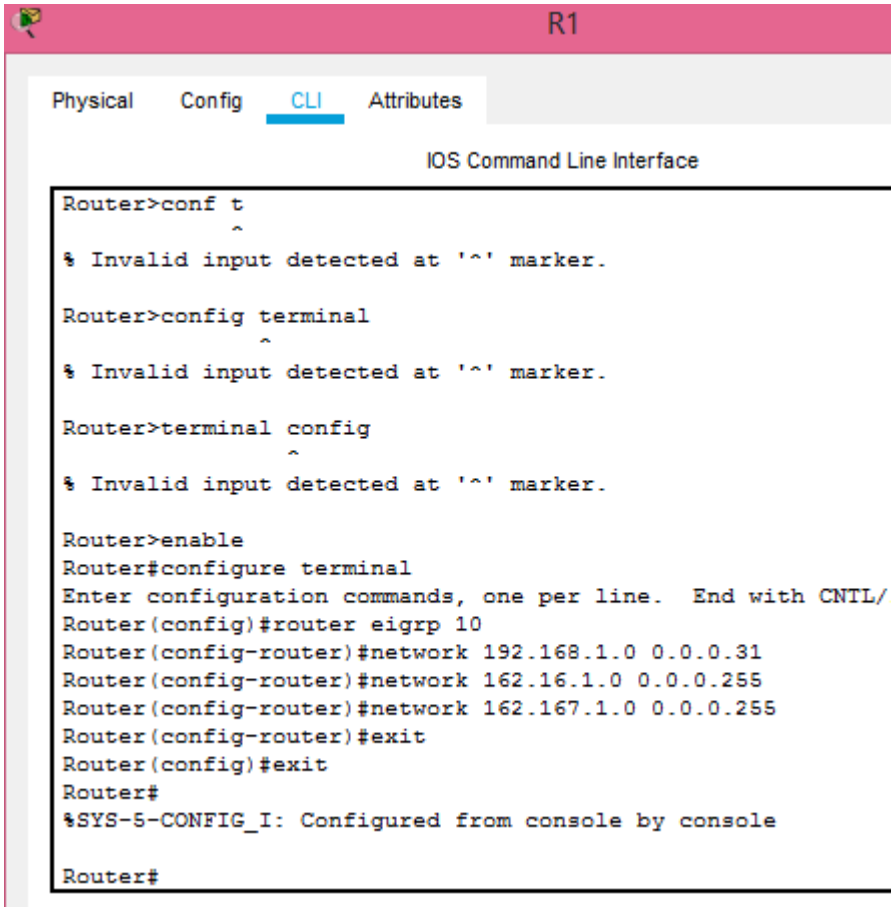


Ilustración 2 Configuración R1 Paso 1

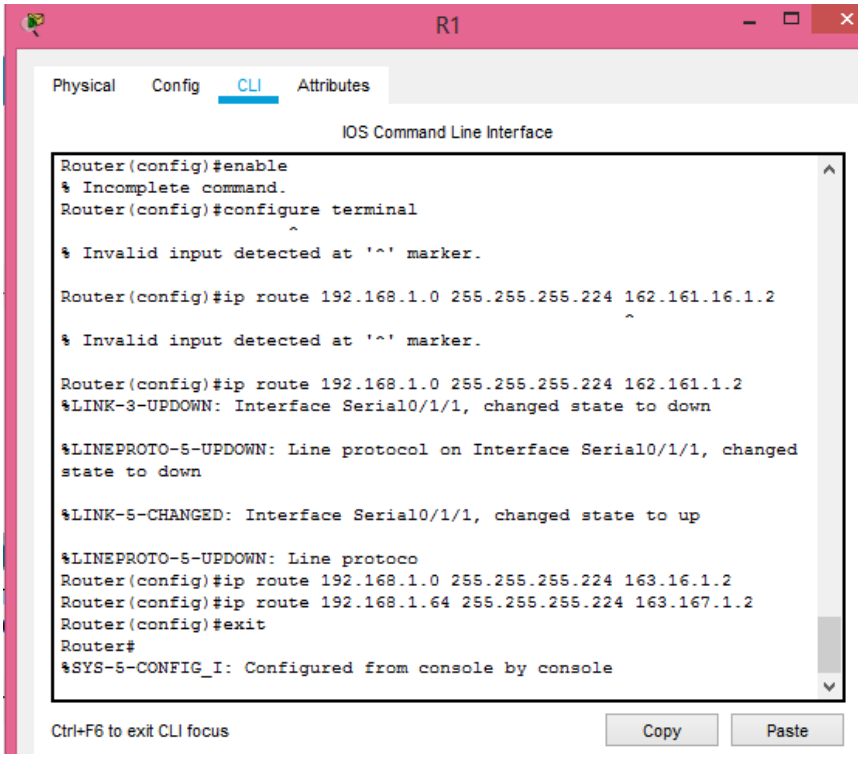


Ilustración 3 Configuración R1 Paso 2

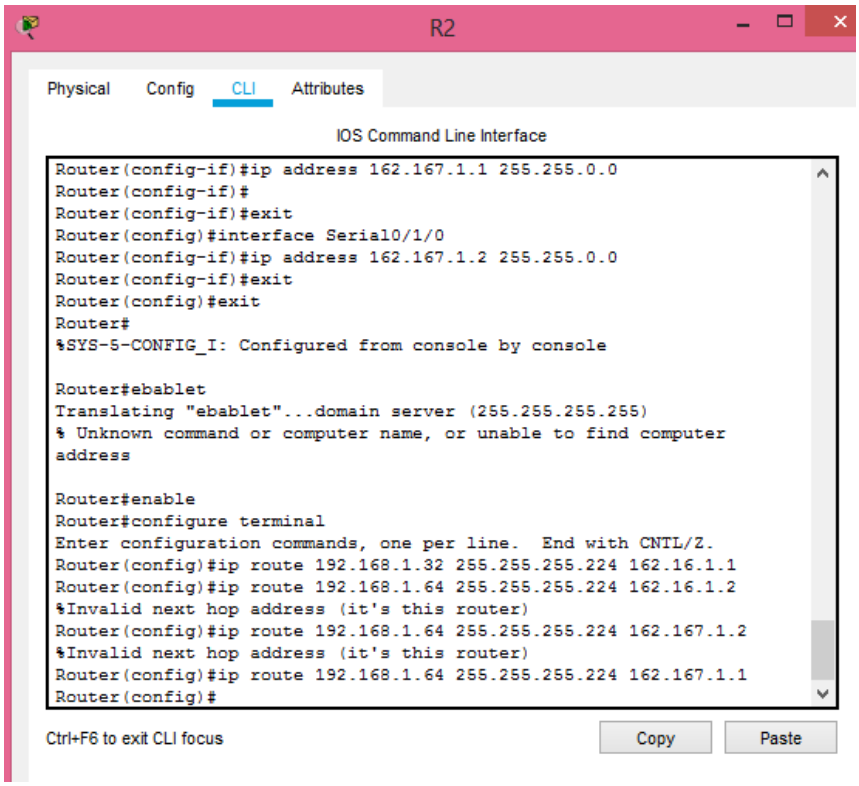


Ilustración 4 Configuración R2

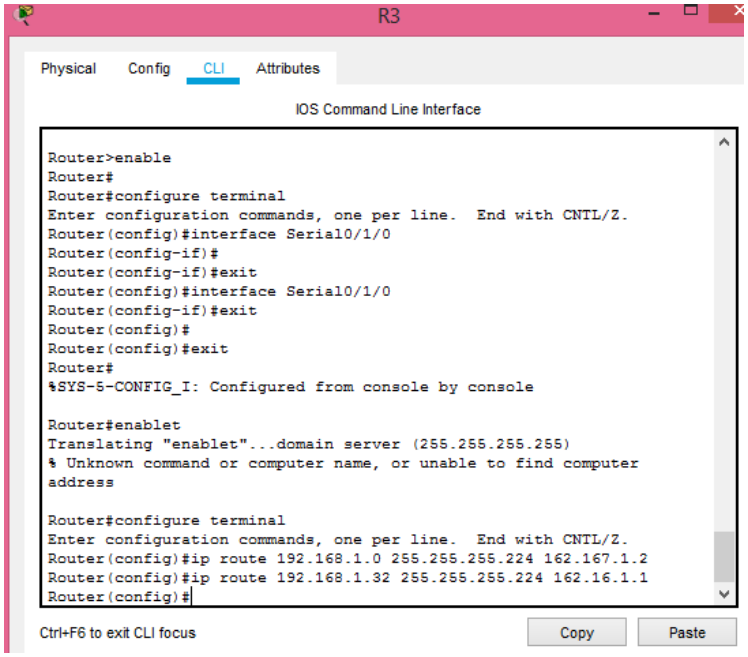


Ilustración 5 Configuración R3

b. Después de cargada la configuración en los dispositivos, verificar la tabla de enrutamiento en cada uno de los routers para comprobar las redes y sus rutas.

Tabla 3 Tabla de Enrutamiento R1

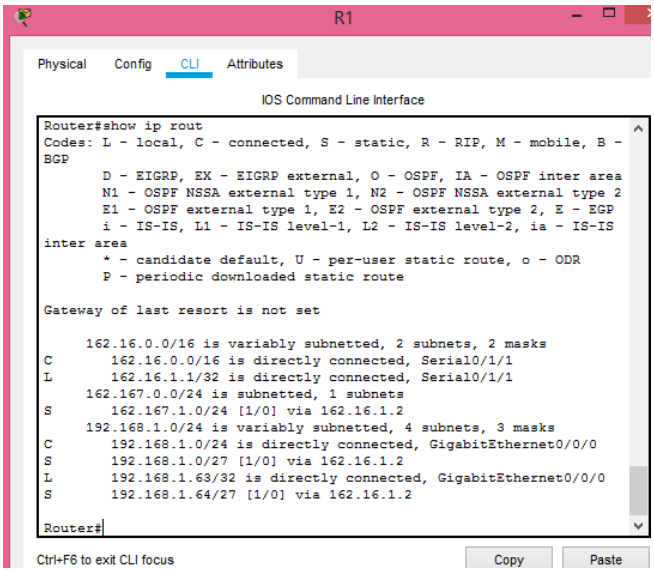


Tabla 4 Tabla de enrutamiento R2

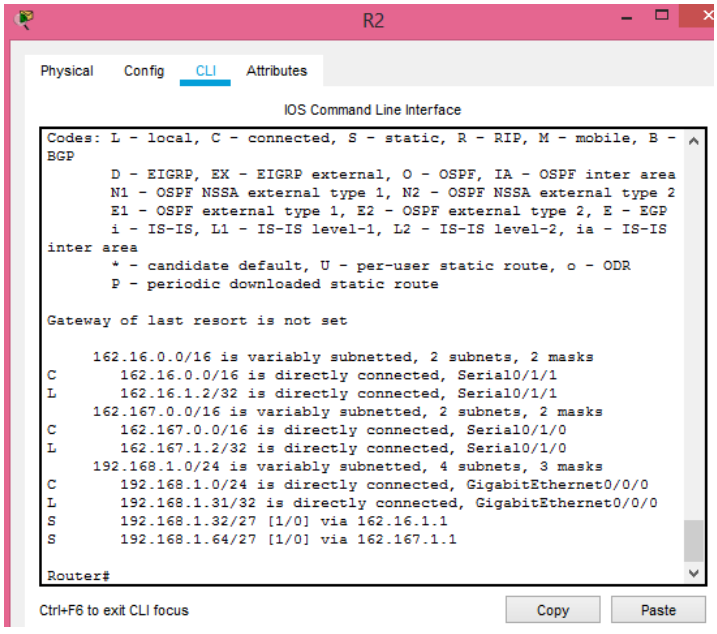
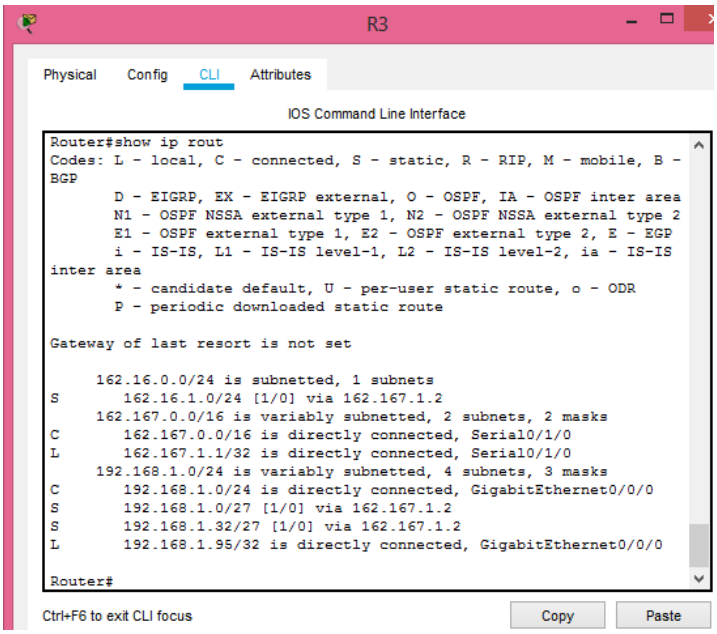


Tabla 5 Tabla de enrutamiento R3



c. Verificar el balanceo de carga que presentan los routers.

Verificamos la métrica utilizada

```
Router#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B -
BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS
inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     162.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
C       162.16.0.0/16 is directly connected, Serial0/1/1
L       162.16.1.1/32 is directly connected, Serial0/1/1
     162.167.0.0/24 is subnetted, 1 subnets
S       162.167.1.0/24 [1/0] via 162.16.1.2
     192.168.1.0/24 is variably subnetted, 4 subnets, 3 masks
C       192.168.1.0/24 is directly connected, GigabitEthernet0/0/0
S       192.168.1.0/27 [1/0] via 162.16.1.2
L       192.168.1.63/32 is directly connected, GigabitEthernet0/0/0
S       192.168.1.64/27 [1/0] via 162.16.1.2

Router#
```

Ilustración 6 Verificación Métrica

Notamos que es la misma

d. Realizar un diagnóstico de vecinos usando el comando cdp.

Diagnóstico De Vecinos R1

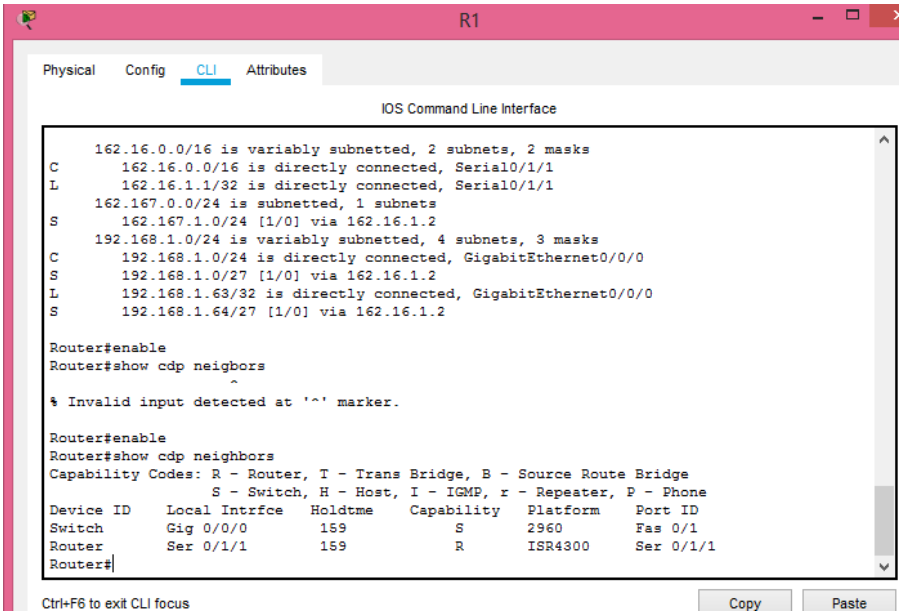


Ilustración 7 Diagnósticos R1

Diagnóstico De Vecinos R2

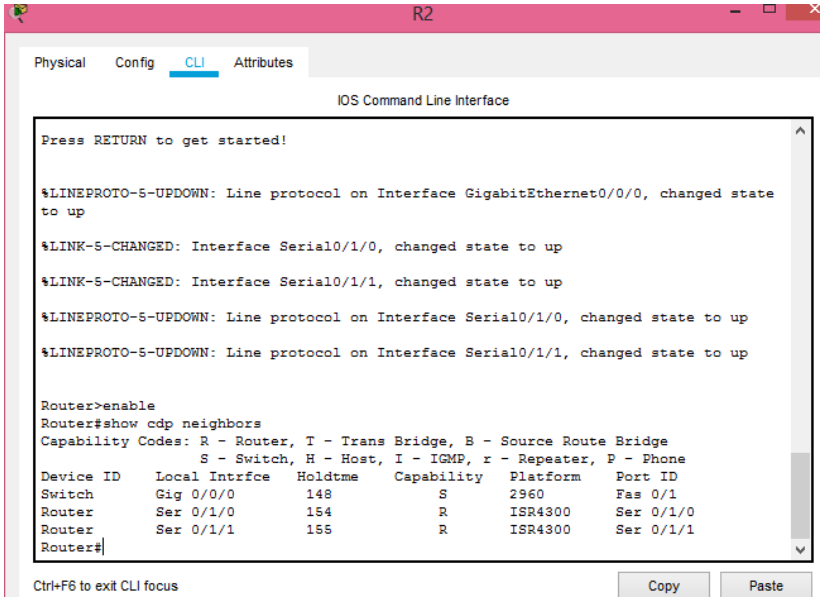


Ilustración 8 Diagnóstico R2

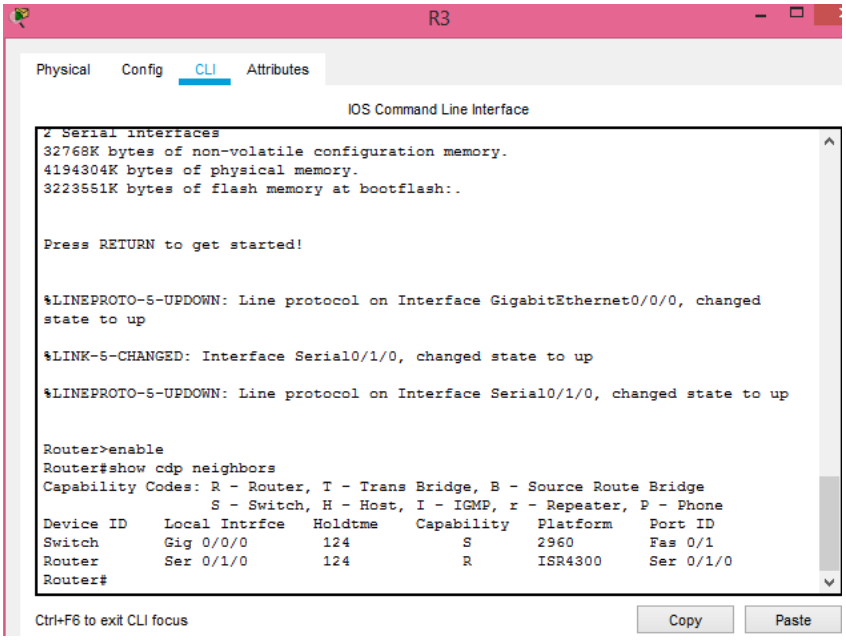


Ilustración 9 Diagnóstico R3

e. Realizar una prueba de conectividad en cada tramo de la ruta usando Ping.

Pin desde SW1

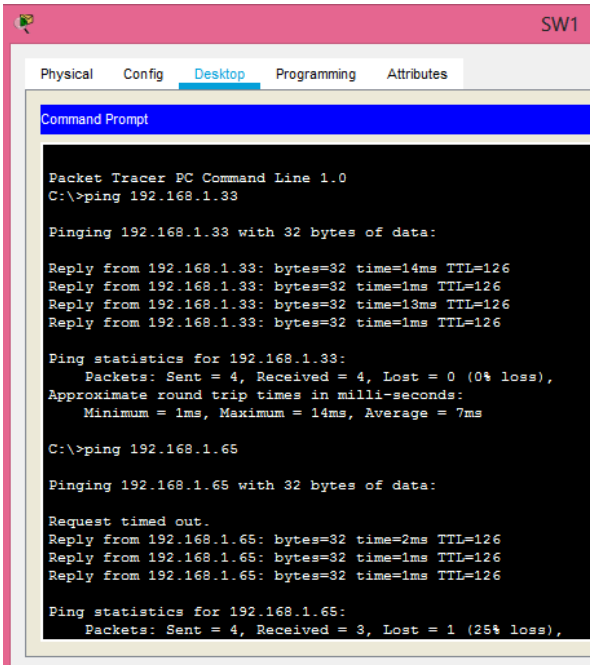


Ilustración 10 Prueba de Conectividad desde SW1

Pin desde PC1

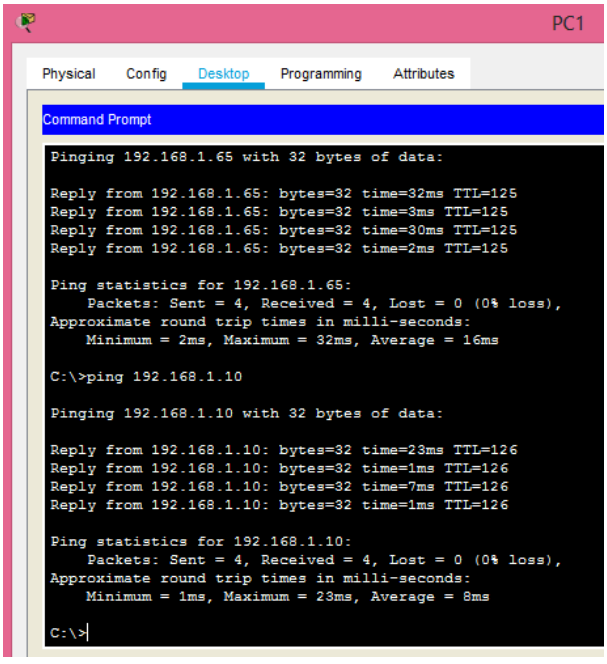


Ilustración 11 Prueba Conectividad desde PC1

Pin desde PC2

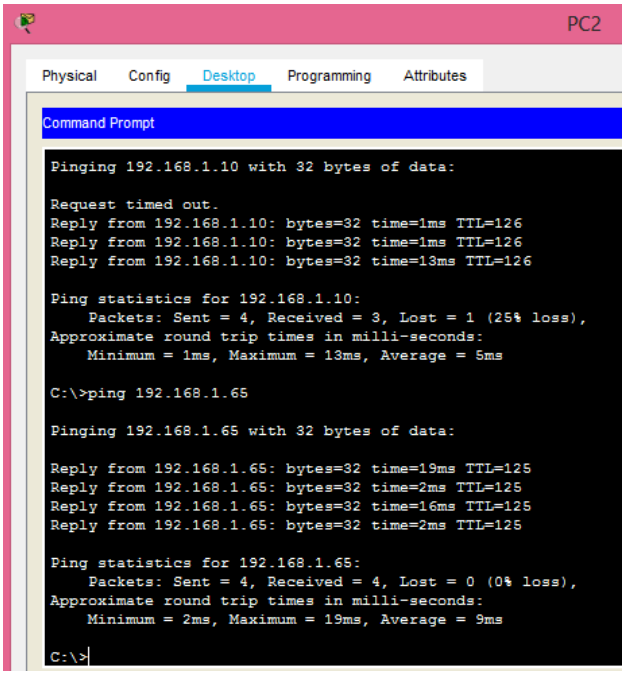


Ilustración 12 Prueba de Conectividad desde PC2

Pin desde PC3

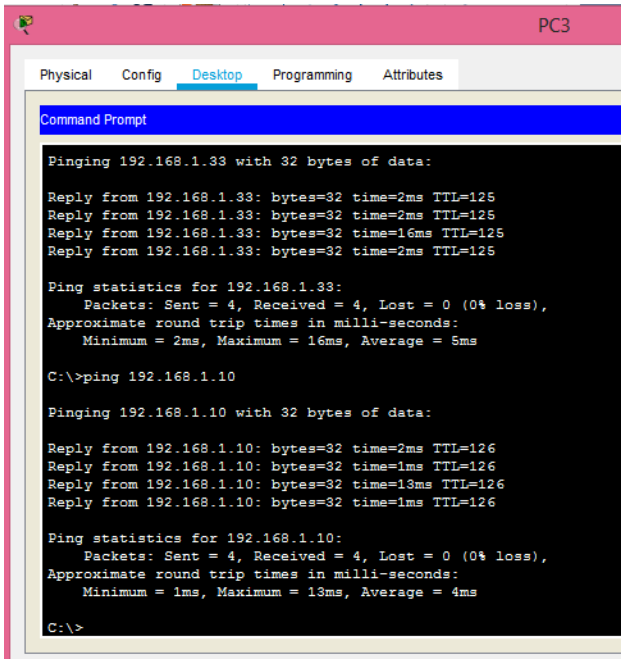


Ilustración 13 Prueba de Conectividad desde PC3

Pin desde PC4

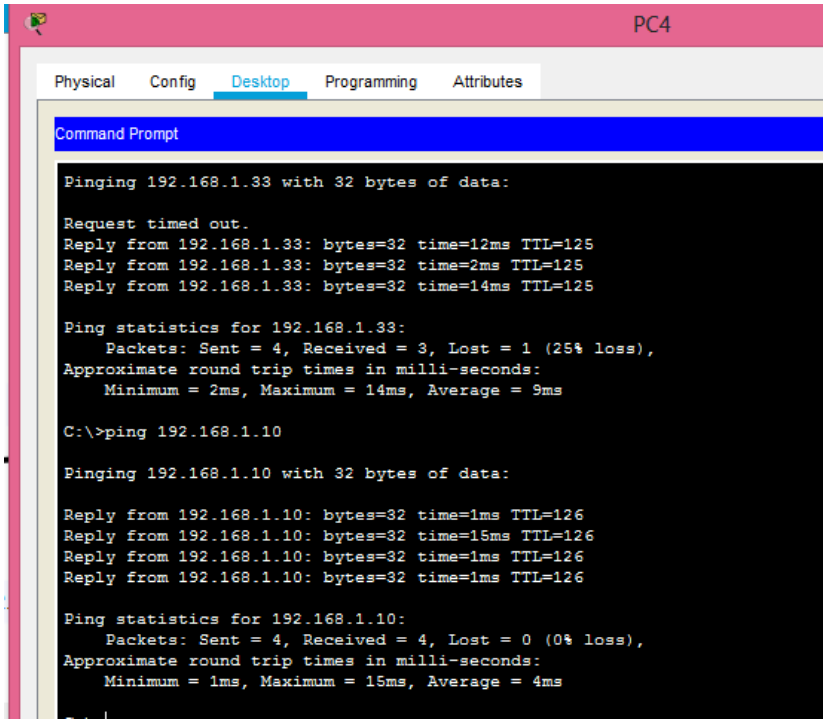


Ilustración 14 Prueba de Conectividad desde PC4

1.3 Parte 3: Configuración de Enrutamiento.

a. Asignar el protocolo de enrutamiento EIGRP a los routers considerando el direccionamiento diseñado.

Router R1

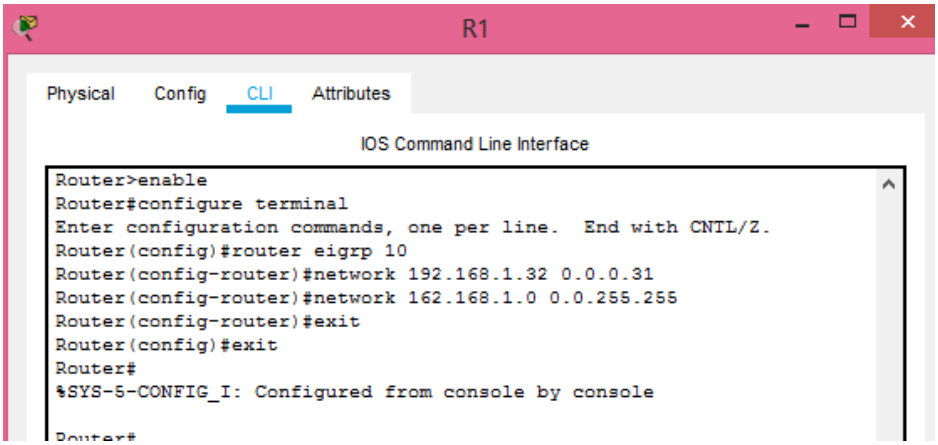


Ilustración 15 Configuración Router R1

Router R2

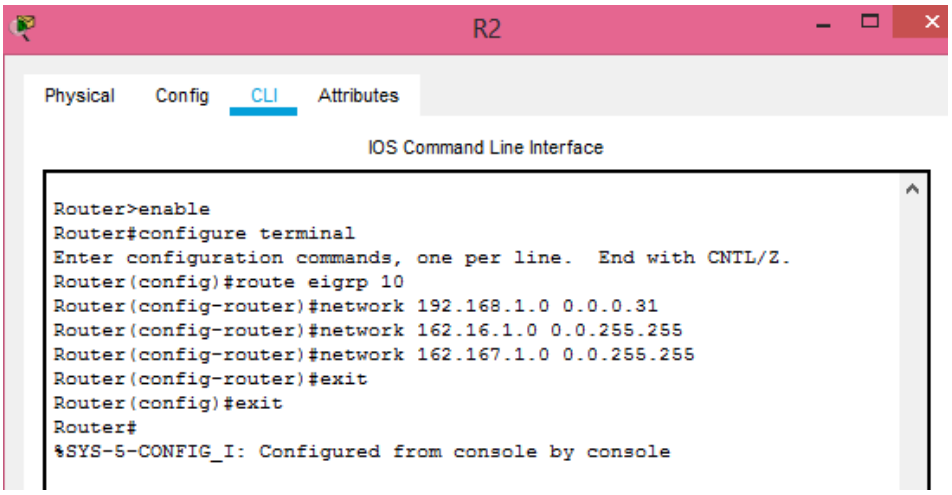


Ilustración 16 Configuración Router R2

Router R3

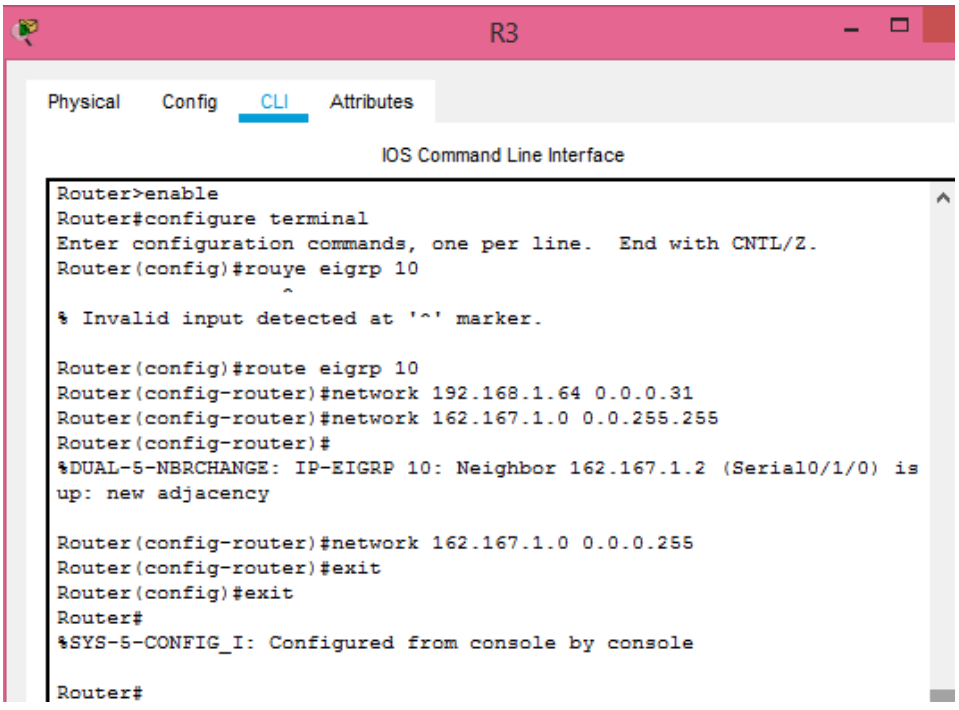


Ilustración 17 Configuración Router R3

b. Verificar si existe vecindad con los routers configurados con EIGRP.

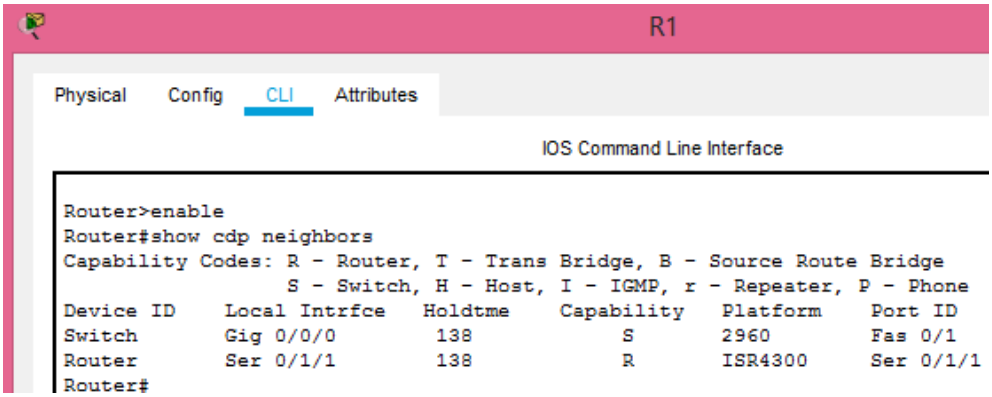


Ilustración 18 R1 configurados con EIGRP

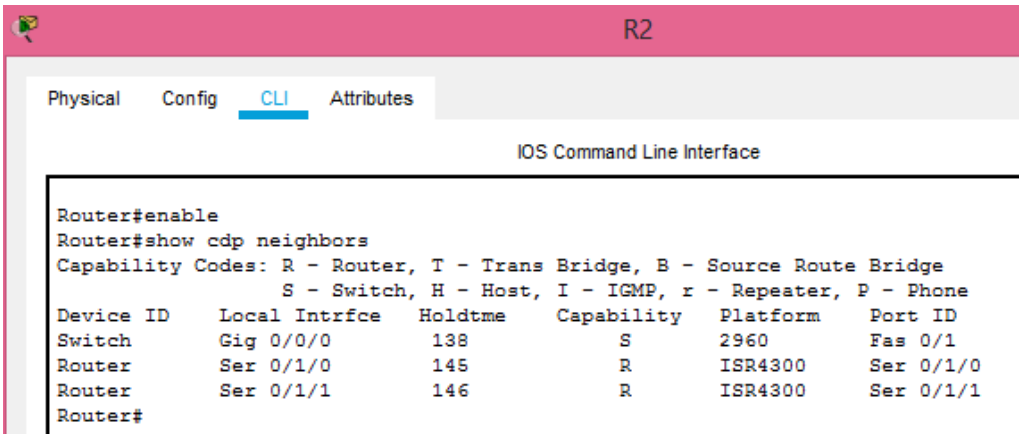


Ilustración 19 R2 configurados con EIGRP

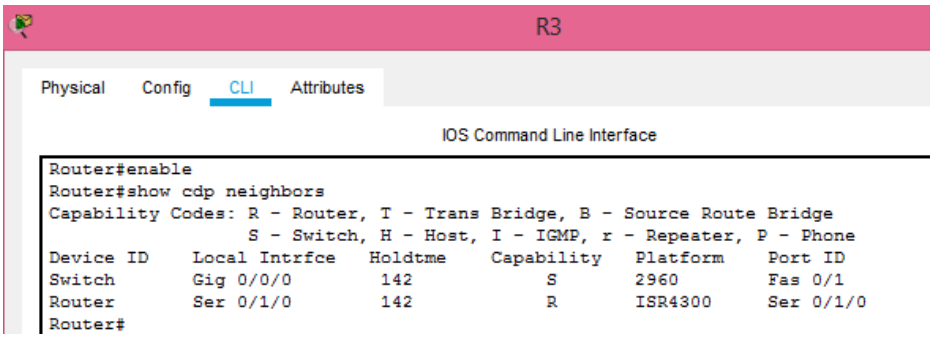


Ilustración 20 R3 configurados con EIGRP

c. Realizar la comprobación de las tablas de enrutamiento en cada uno de los routers para verificar cada una de las rutas establecidas.

Tabla 6 Comprobación Tabla de Enrutamiento R1

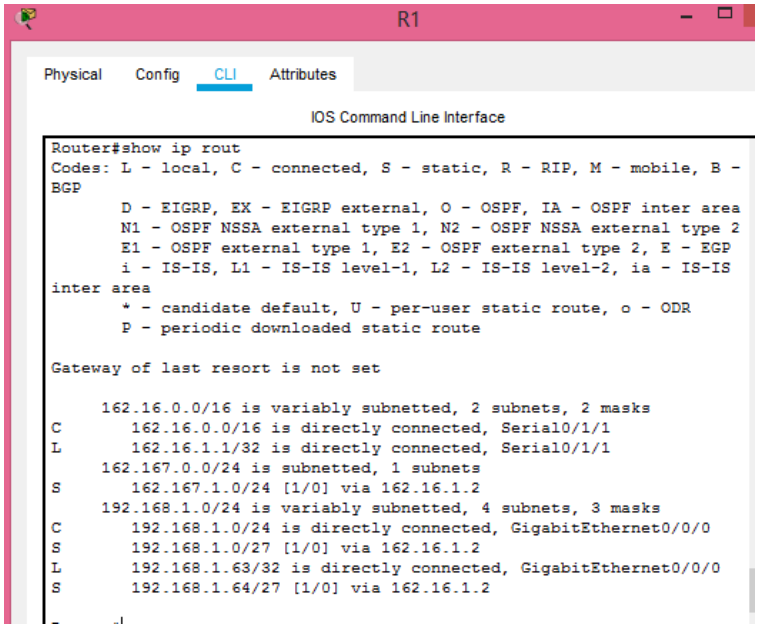


Tabla 7 Comprobación Tabla de Enrutamiento R2

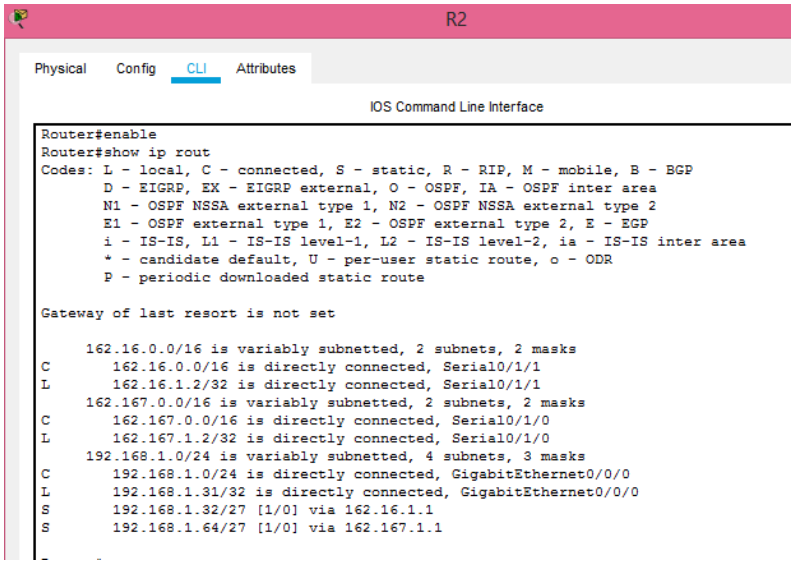
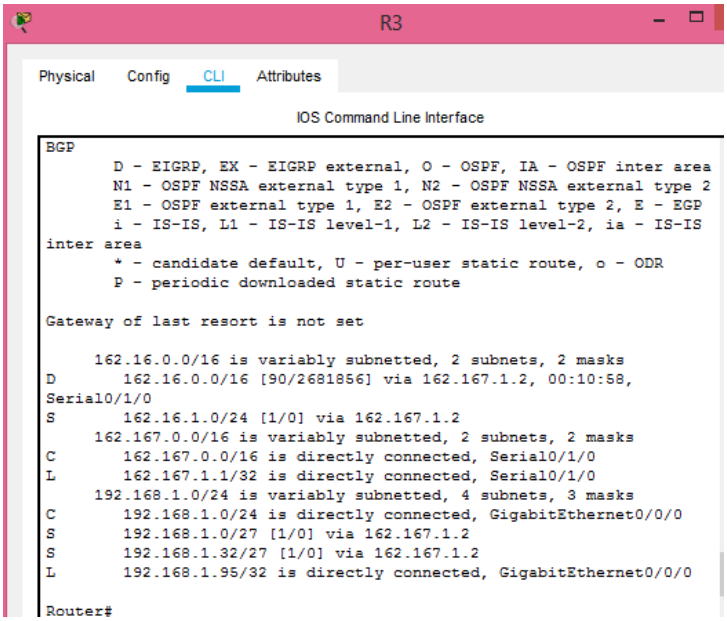


Tabla 8 Comprobación Tabla de Enrutamiento R3



d. Realizar un diagnóstico para comprobar que cada uno de los puntos de la red se puedan ver y tengan conectividad entre sí. Realizar esta prueba desde un host de la red LAN del router CALI, primero a la red de MEDELLIN y luego al servidor.

Prueba de conexión lan Cali a Host PC1 Medellín

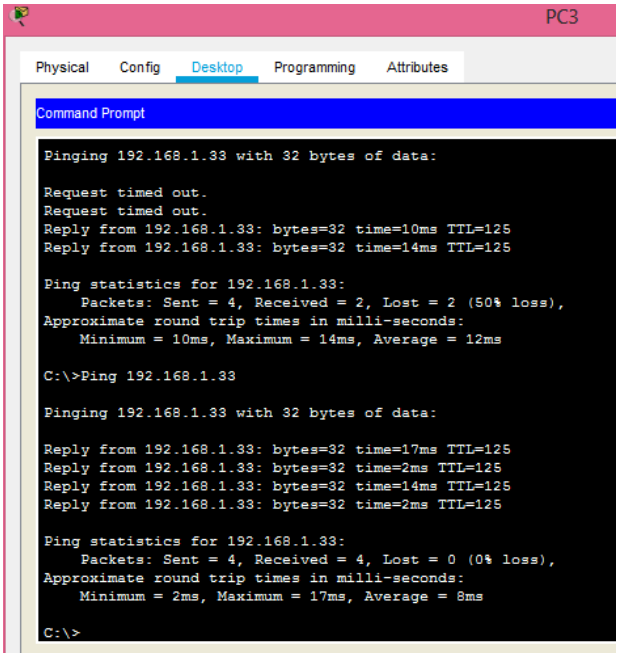


Ilustración 21 Prueba de Conexión Lan Calia Host PC1 Medellín

Prueba de Conexión al servidor

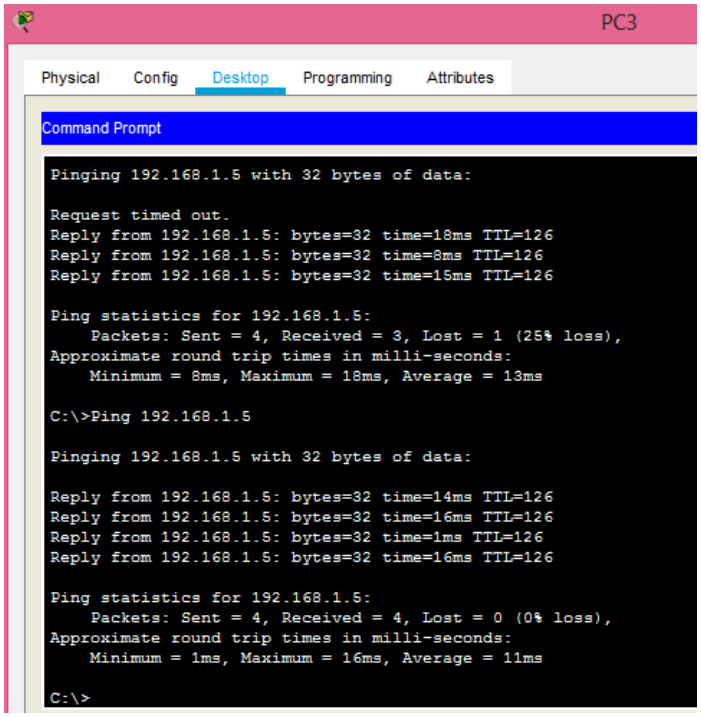


Ilustración 22 Prueba de Conexión al Servidor

1.4 Parte 4: Configuración de las listas de Control de Acceso.

En este momento cualquier usuario de la red tiene acceso a todos sus dispositivos y estaciones de trabajo.

El jefe de redes le solicita implementar seguridad en la red. Para esta labor se decide configurar listas de control de acceso (ACL) a los routers.

Las condiciones para crear las ACL son las siguientes:

a. Cada router debe estar habilitado para establecer conexiones Telnet con los demás routers y tener acceso a cualquier dispositivo en la red.

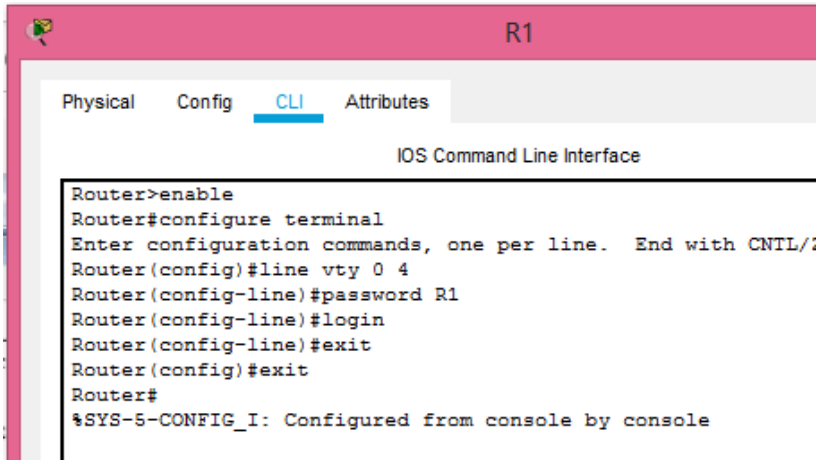


Ilustración 23 Establecer Conexión Telnet R1

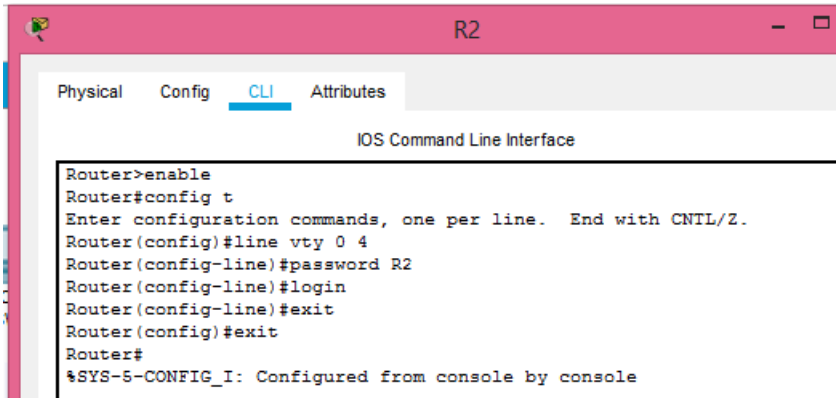


Ilustración 24 Establecer Conexión Telnet R2

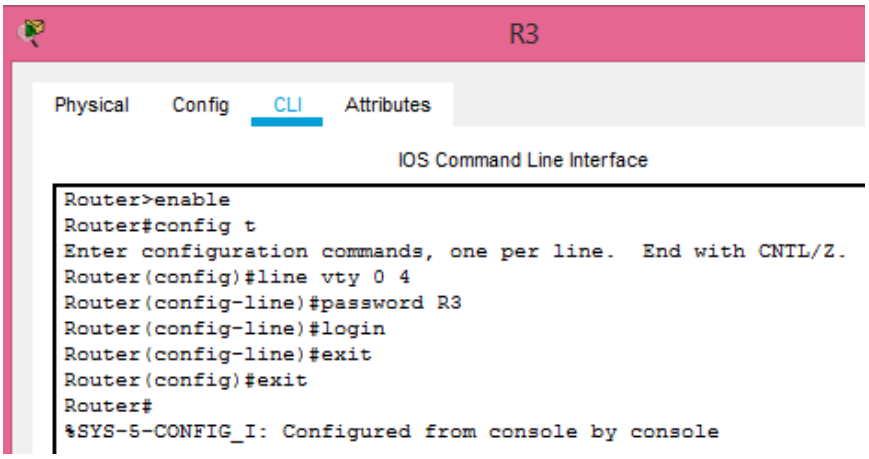


Ilustración 25 Establecer Conexión Telnet R3

Prueba de acceso

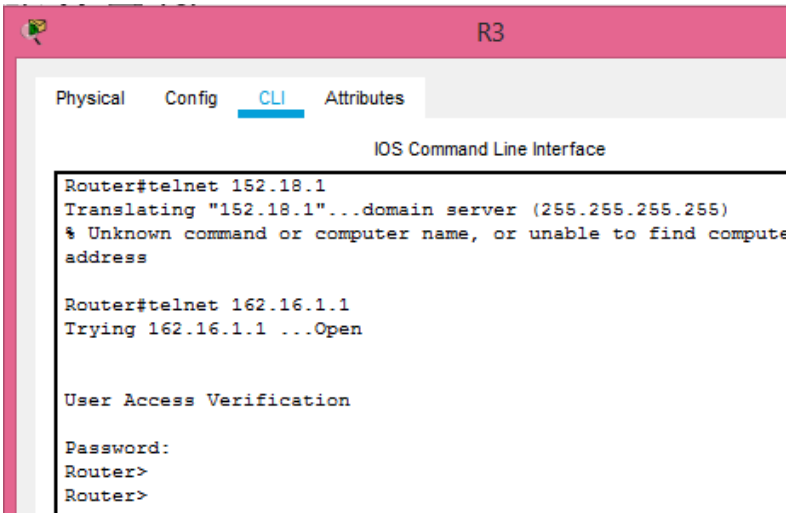


Ilustración 26 Prueba de Acceso R3

b. El equipo WS1 y el servidor se encuentran en la subred de administración. Solo el servidor de la subred de administración debe tener acceso a cualquier otro dispositivo en cualquier parte de la red.

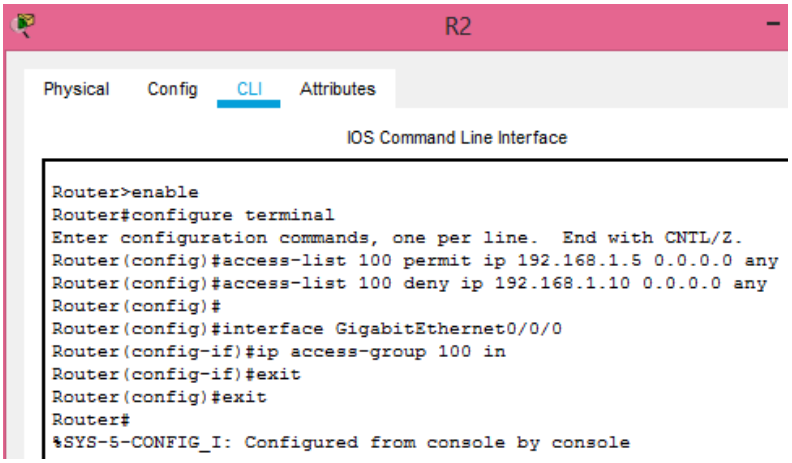


Ilustración 27 Prueba de Acceso R2

c. Las estaciones de trabajo en las LAN de MEDELLIN y CALI no deben tener acceso a ningún dispositivo fuera de su subred, excepto para interconectar con el servidor.

Configuración

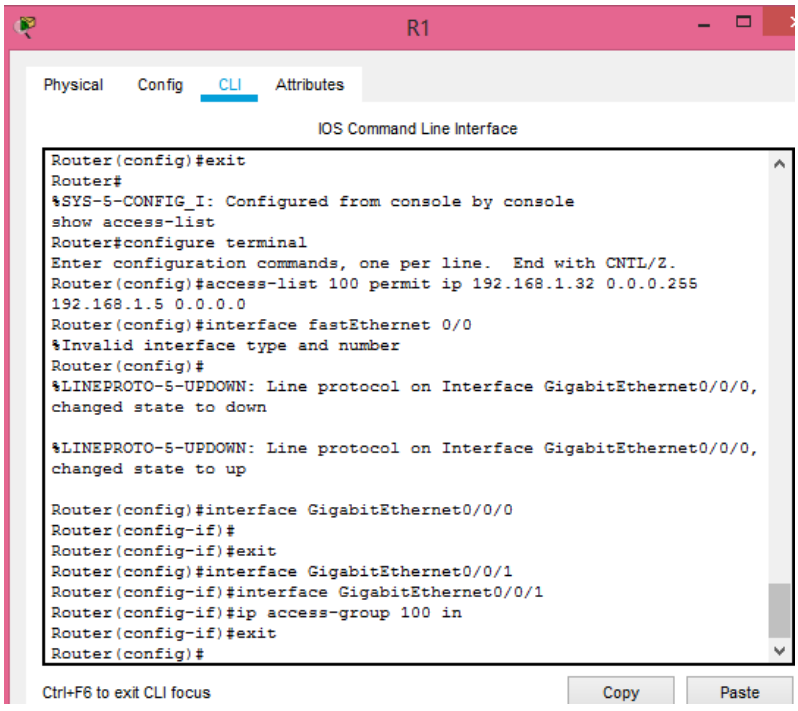


Ilustración 28 Configuración Access Group R1

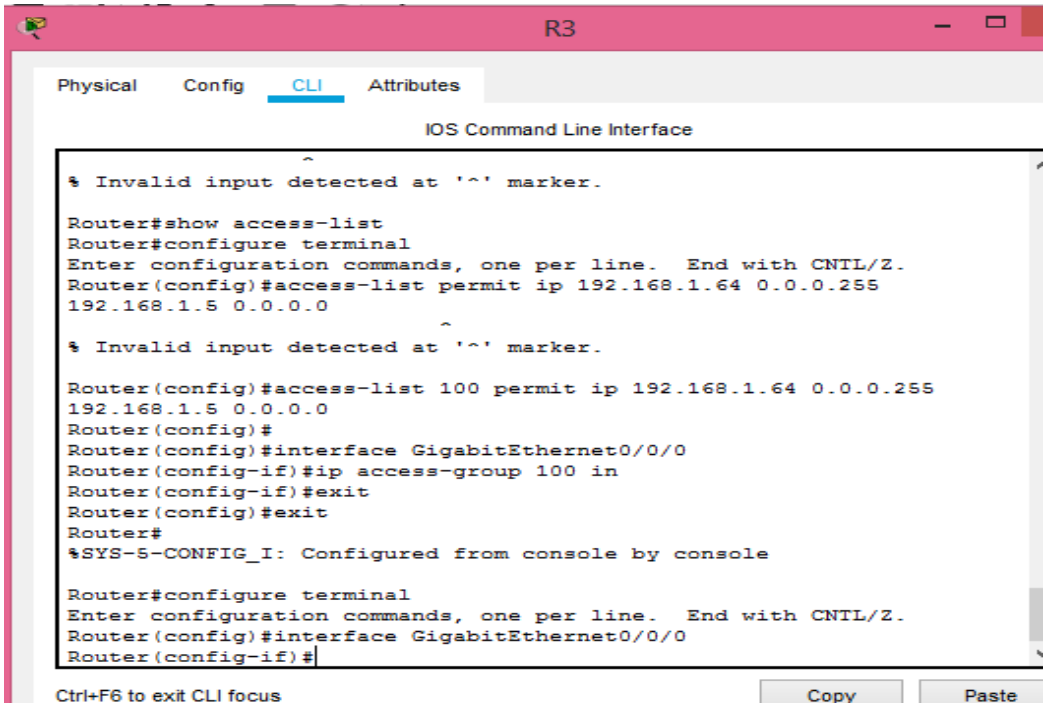


Ilustración 29 Configuración Access Group R3

1.5 Parte 5: Comprobación de la red instalada.

Se debe probar que la configuración de las listas de acceso fue exitosa.

Comprobación acceso de la Red Medellin a el servidor y negación de accesos a la red Cali

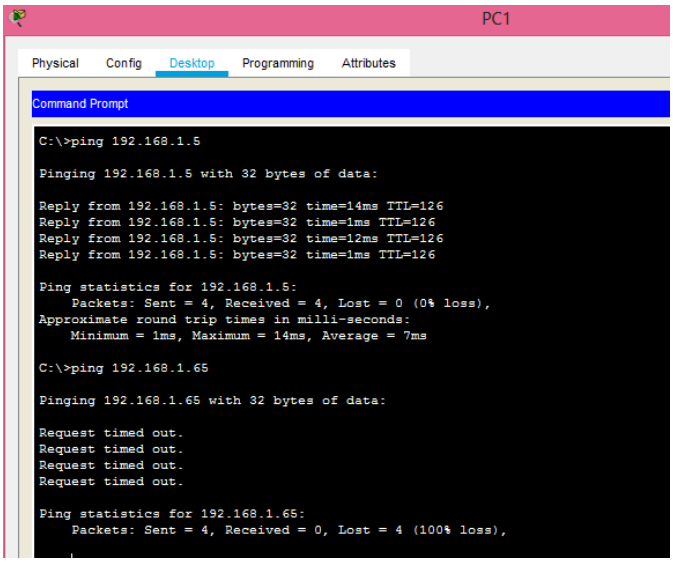


Ilustración 30 Comprobación Red Instalada PC1

Comprobación acceso de la Red Cali a el servidor y negación de accesos a la red Medellin

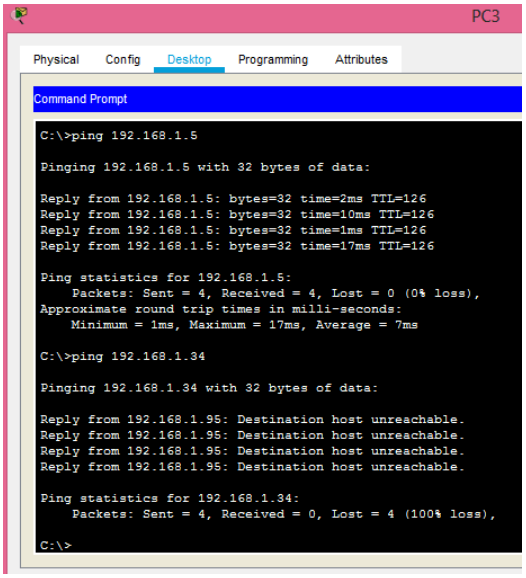


Ilustración 31 Comprobación Red Instalada PC3

Comprobación acceso de la host SW1 a el servidor y negación de accesos a la redes Medellin y Cali

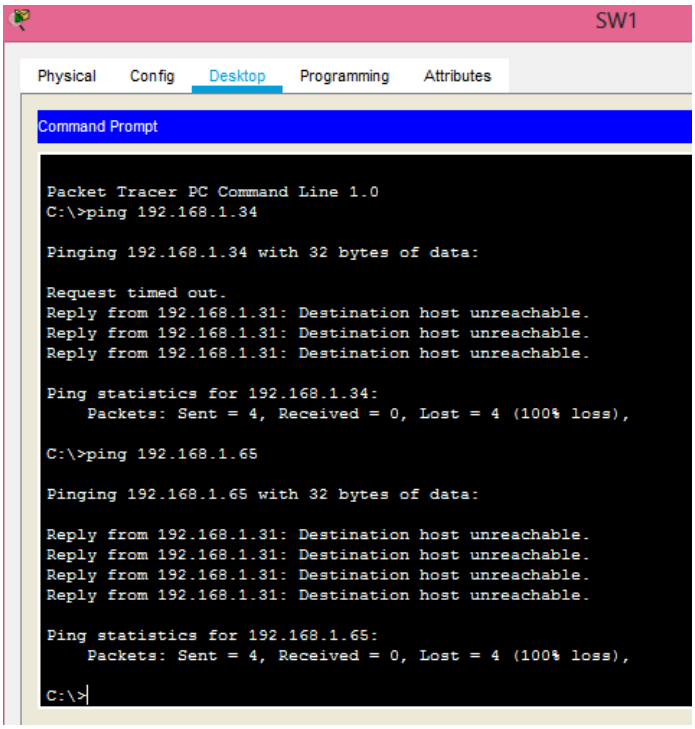


Ilustración 32 Comprobación Acceso de la Host SW1

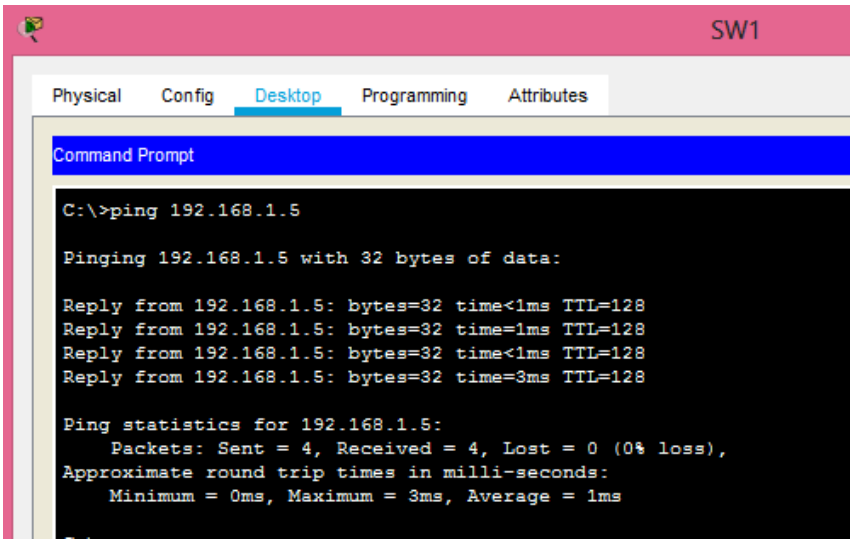


Ilustración 33 Comprobación Acceso de la Host SW1

Prueba de conexión del Servidor

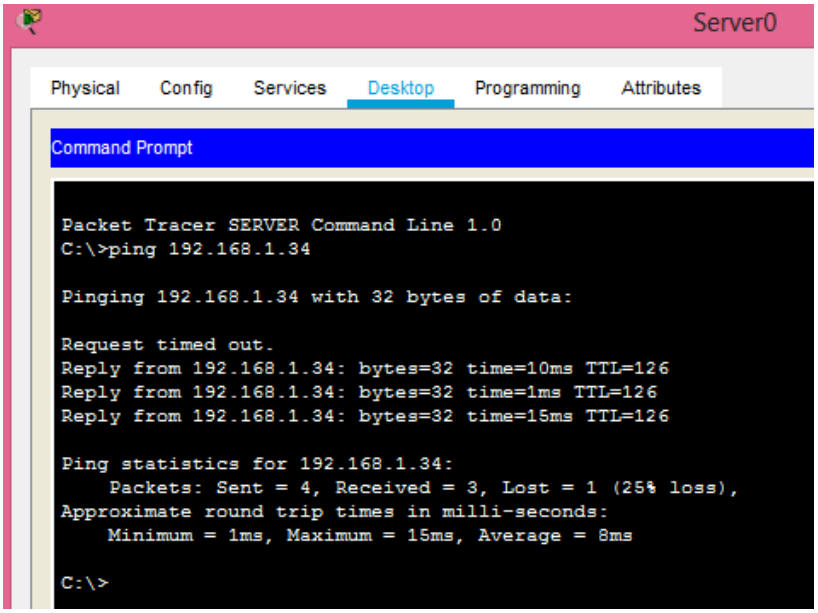


Ilustración 34 Prueba Conexión Servidor Server0

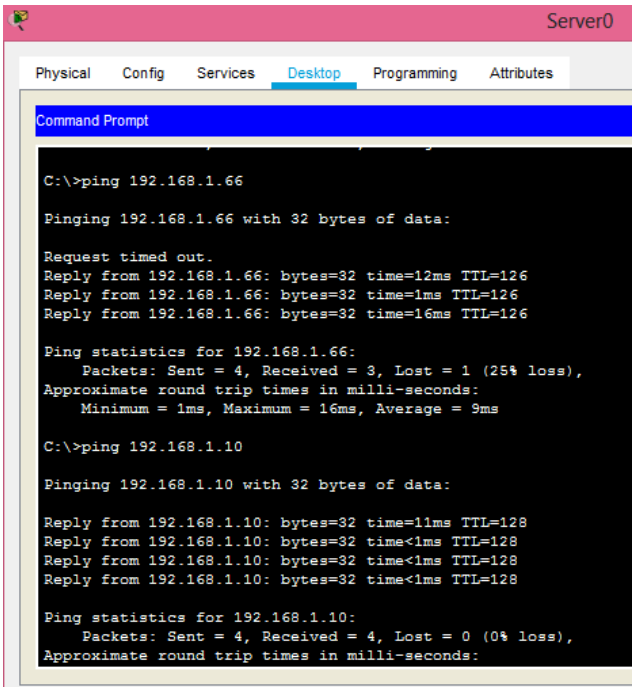


Ilustración 35 Prueba Conexión Servidor Server0

b. Comprobar y Completar la siguiente tabla de condiciones de prueba para confirmar el óptimo funcionamiento de la red e

1.6 Parte 6: Configuración Final.

Tabla 9 Tabla de Condiciones de Prueba

	ORIGEN	DESTINO	RESULTADO
TELNET	Router MEDELLIN	Router CALI	permitido
	WS_1 Router	BOGOTA	permitido
	Servidor	Router CALI	permitido
	Servidor	Router MEDELLIN	permitido
TELNET	LAN del Router	MEDELLIN Router CALI	permitido
	LAN del Router CALI	Router CALI	permitido
	LAN del Router MEDELLIN	Router MEDELLIN	permitido
	LAN del Router CALI	Router MEDELLIN	permitido
PING	LAN del Router CALI	WS_1	Denegado
	LAN del Router MEDELLIN	WS_1	Denegado
	LAN del Router MEDELLIN	LAN del Router CALI	Denegado
PING	LAN del Router CALI	Servidor	permitido
	LAN del Router MEDELLIN	Servidor	permitido
	Servidor	LAN del Router MEDELLIN	permitido
	Servidor	LAN del Router CALI	permitido
	Router CALI	LAN del Router MEDELLIN	Denegado
	Router MEDELLIN	LAN del Router CALI	Denegado

Escenario 2

Una empresa tiene la conexión a internet en una red Ethernet, lo cual deben adaptarlo para facilitar que sus routers y las redes que incluyen puedan, por esa vía, conectarse a internet, pero empleando las direcciones de la red LAN original.

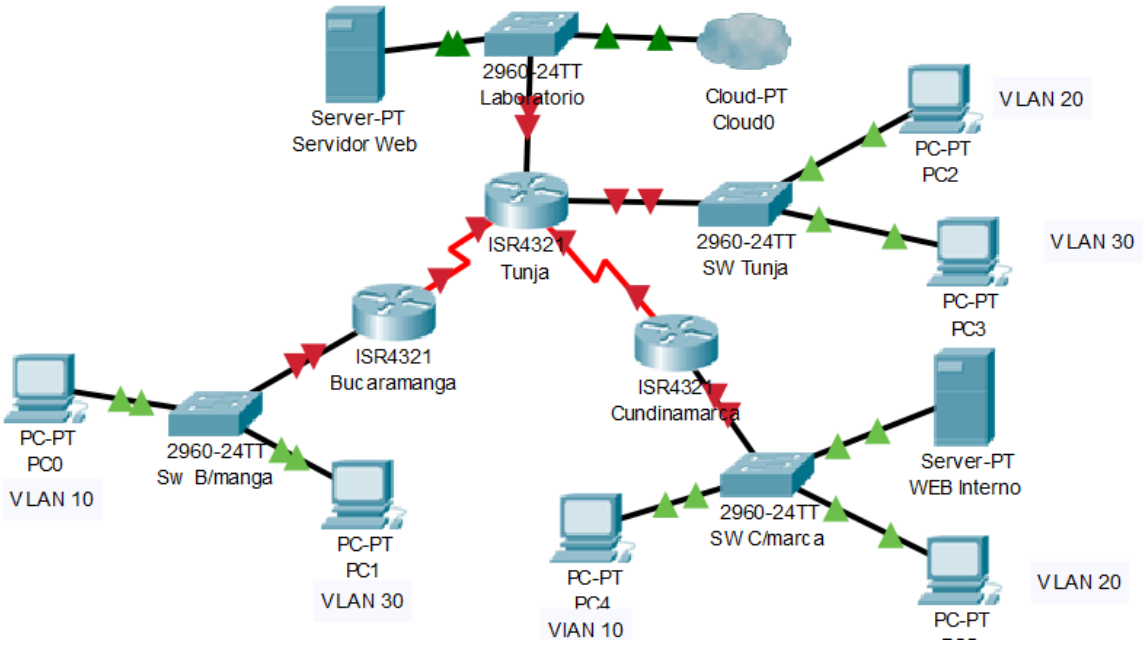


Ilustración 36 Ejemplo de Escenario 2

Desarrollo Escenario 2

Los siguientes son los requerimientos necesarios:

1. Todos los routers deberán tener los siguiente:

• Configuración básica.

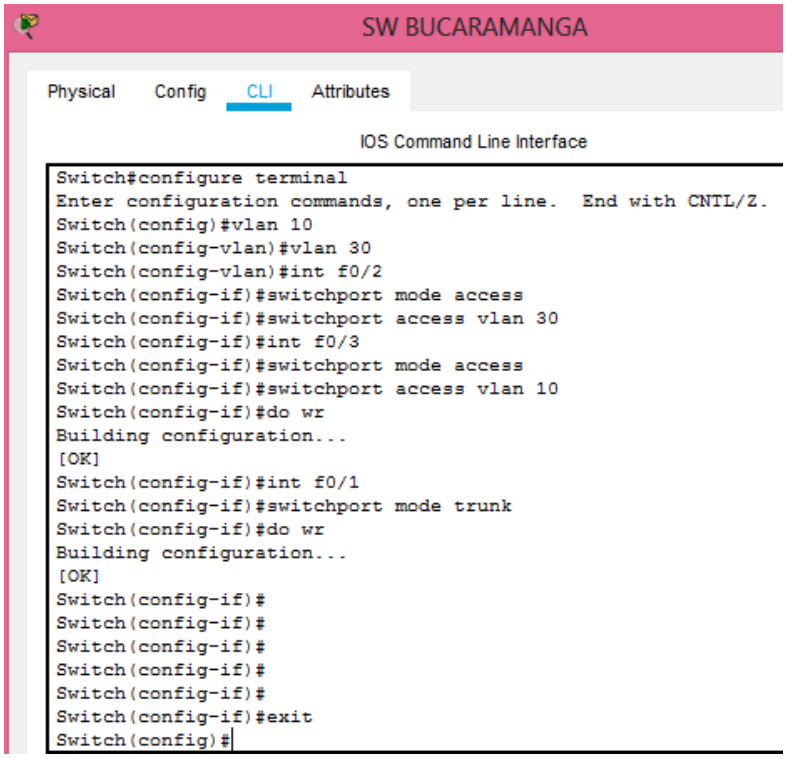


Ilustración 37 Configuración Básica SW Bucaramanga

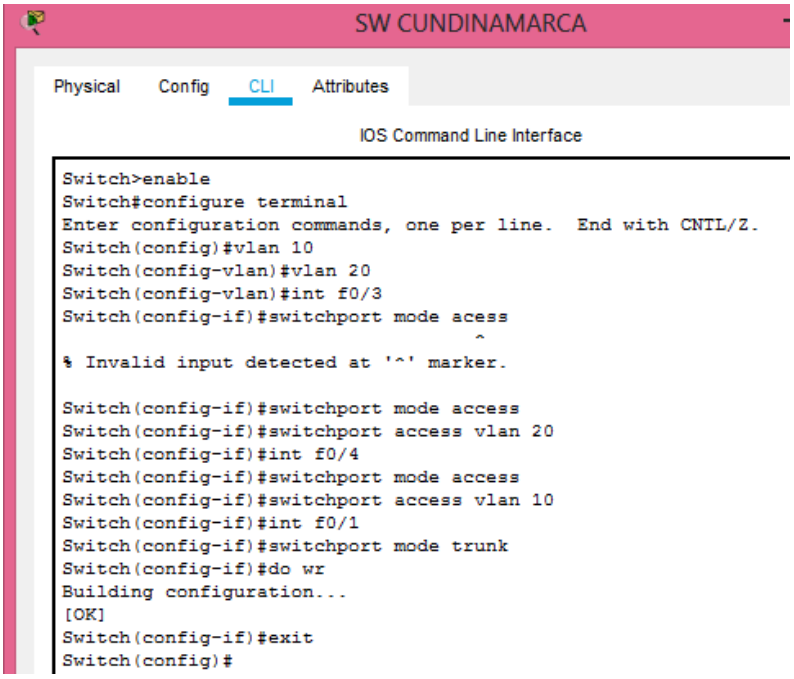


Ilustración 38 Configuración Básica SW Cundinamarca

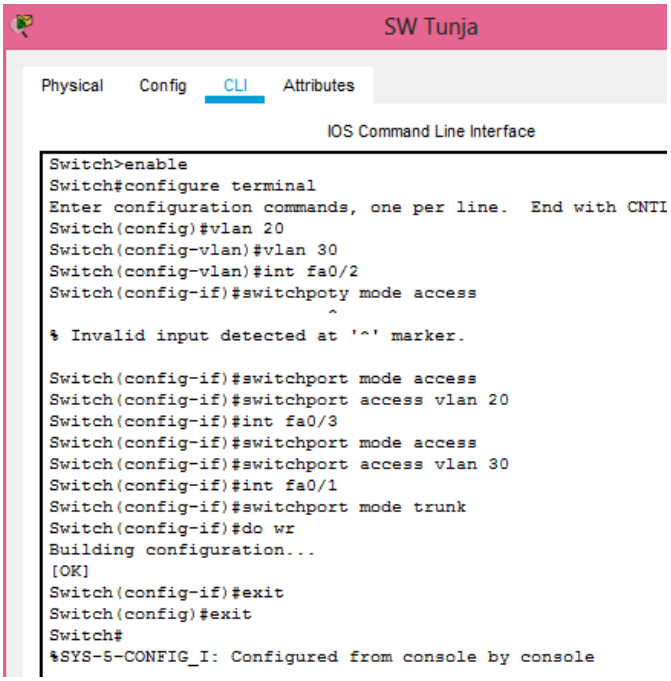


Ilustración 39 Configuración Básica SW Tunja

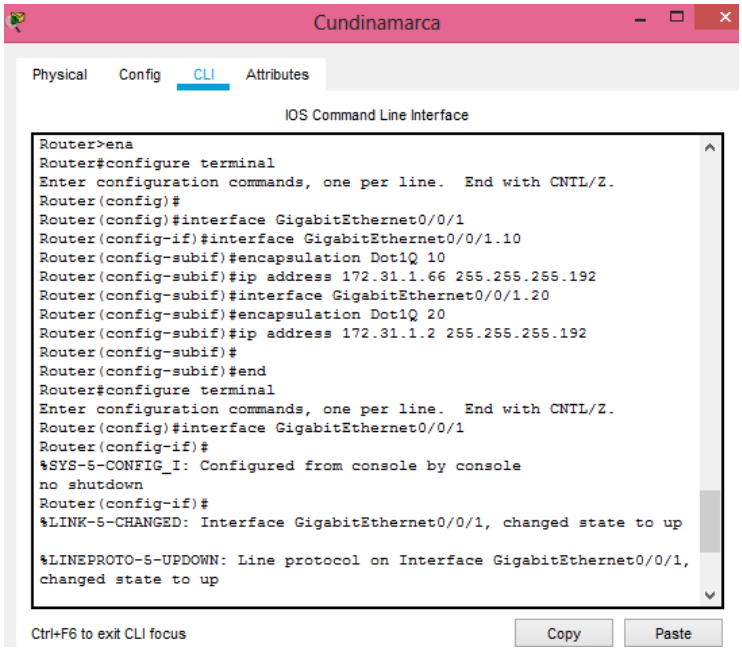


Ilustración 40 Configuración Básica SW Cundinamarca

• Autenticación local con AAA.

• Cifrado de contraseñas.

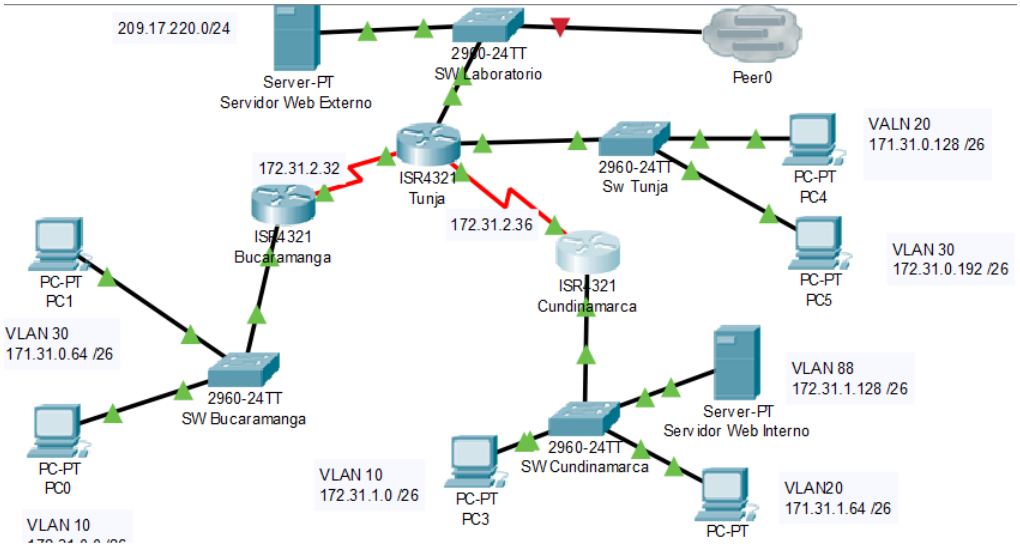


Ilustración 41 Ejemplo de Escenario 2

• Un máximo de internos para acceder al router.

• Máximo tiempo de acceso al detectar ataques.

• Establezca un servidor TFTP y almacene todos los archivos necesarios de los routers.

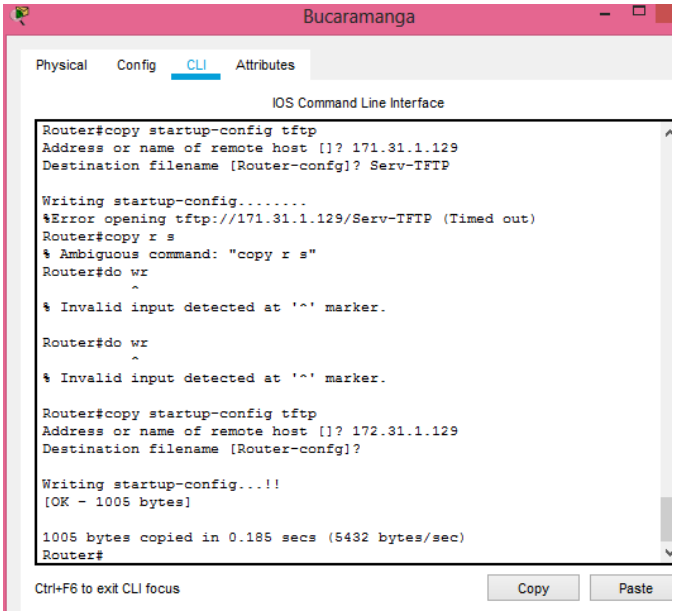


Ilustración 42 Establecer Servidor TFTP

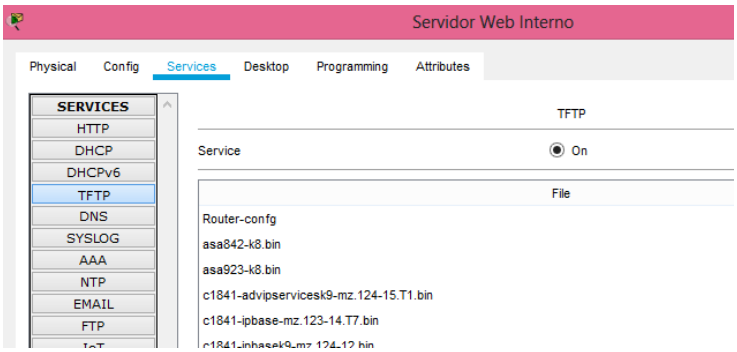


Ilustración 43 Servidor Web Interno

2. El DHCP deberá proporcionar solo direcciones a los hosts de Bucaramanga y Cundinamarca

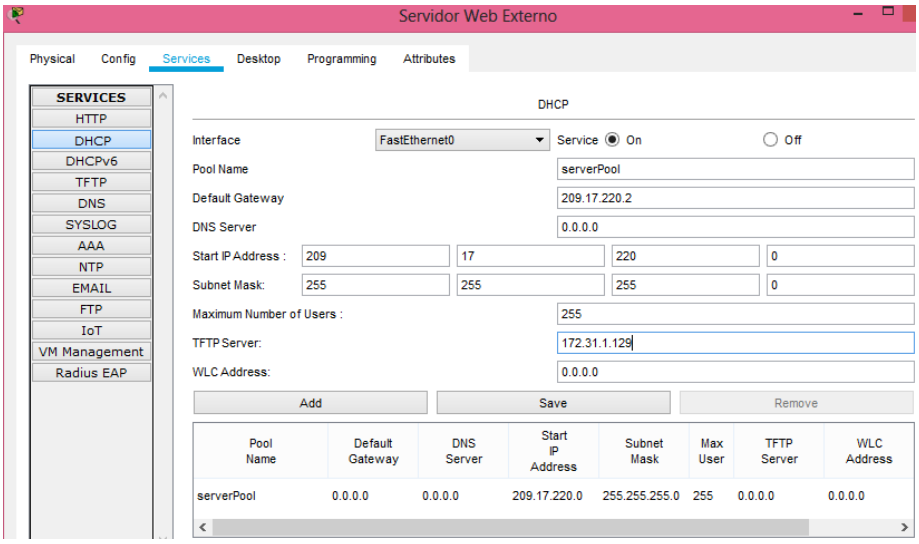


Ilustración 44 DHCP Servidor Web Externo

3. El web server deberá tener NAT estático y el resto de los equipos de la topología emplearan NAT de sobrecarga (PAT).

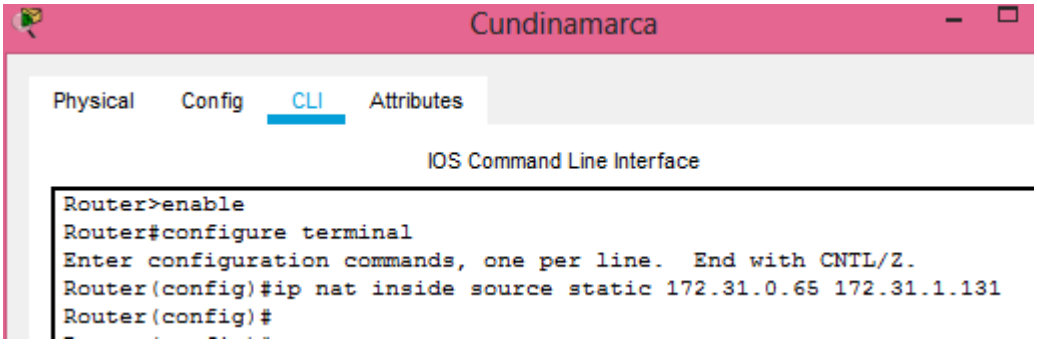


Ilustración 45 NAT Estático

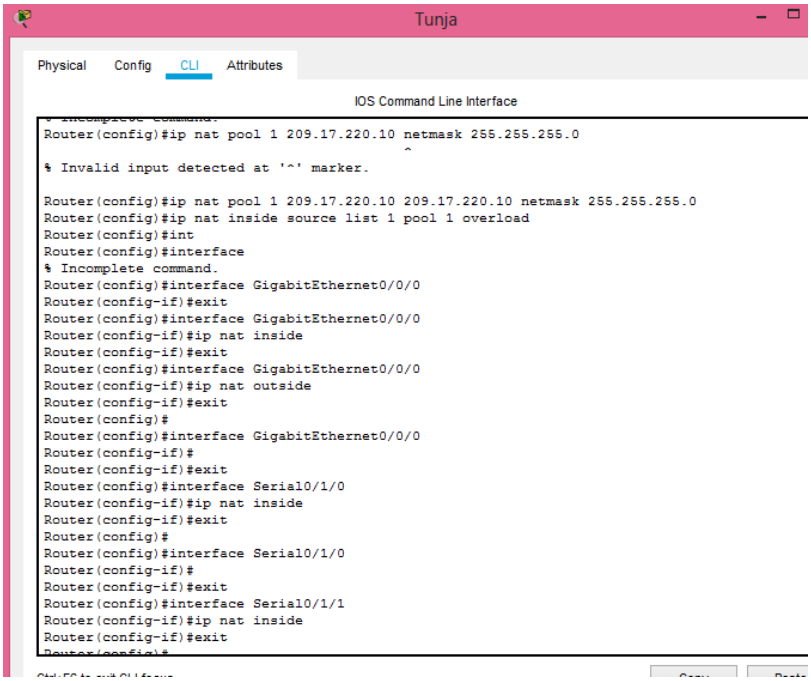


Ilustración 46 NAT Estático

4. El enrutamiento deberá tener autenticación.

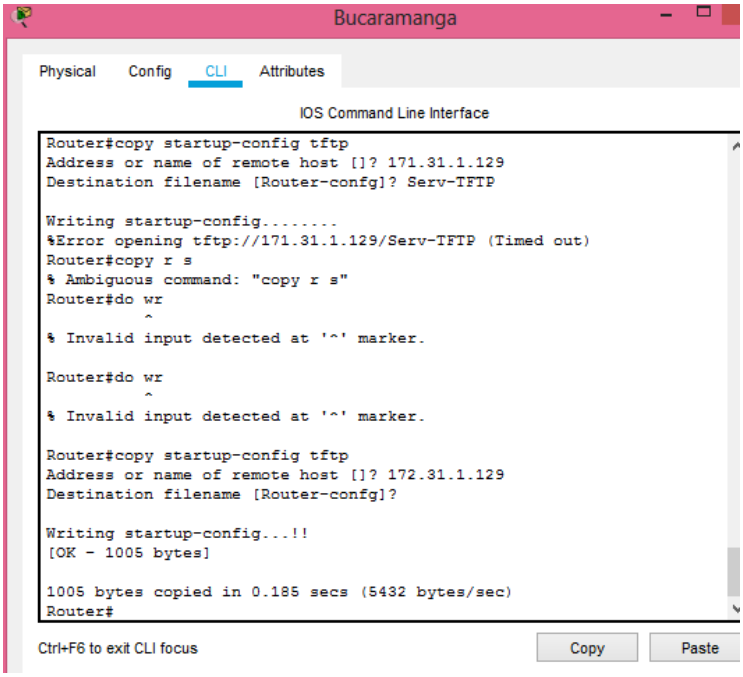


Ilustración 47 Autenticación del Router Bucaramanga

5. Listas de control de acceso:

• Los hosts de VLAN 20 en Cundinamarca no acceden a internet, solo a la red interna de Tunja.

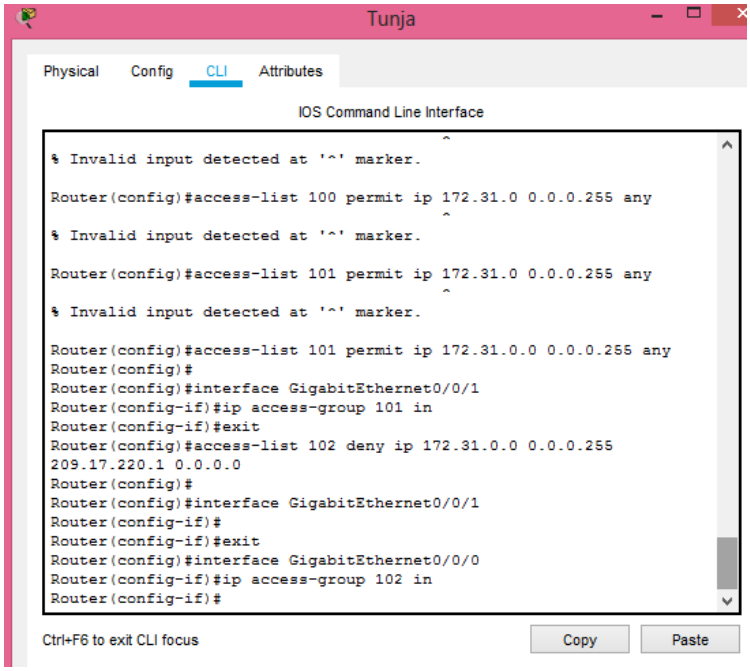


Ilustración 48 Configuración Vlan20 Router Tunja

• Los hosts de VLAN 10 en Cundinamarca si acceden a internet y no a la red interna de Tunja.

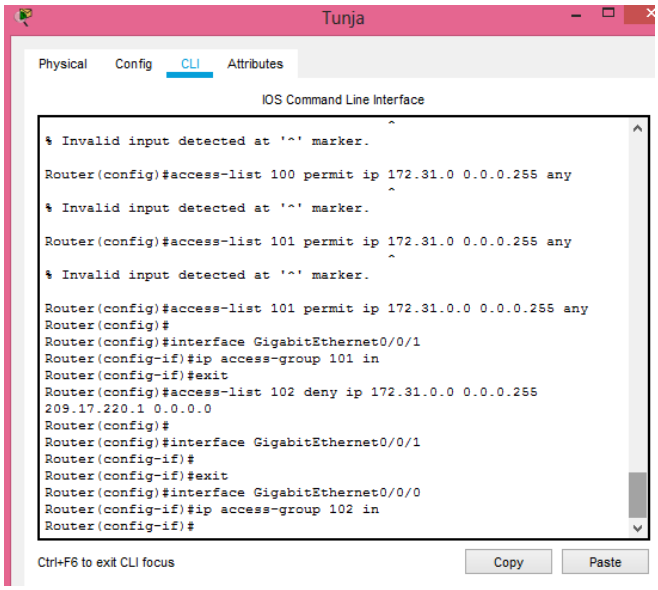


Ilustración 49 Configuración Vlan10 Router Tunja

• Los hosts de VLAN 30 en Tunja solo acceden a servidores web y ftp de internet.

• Los hosts de VLAN 20 en Tunja solo acceden a la VLAN 20 de Cundinamarca y VLAN 10 de Bucaramanga.

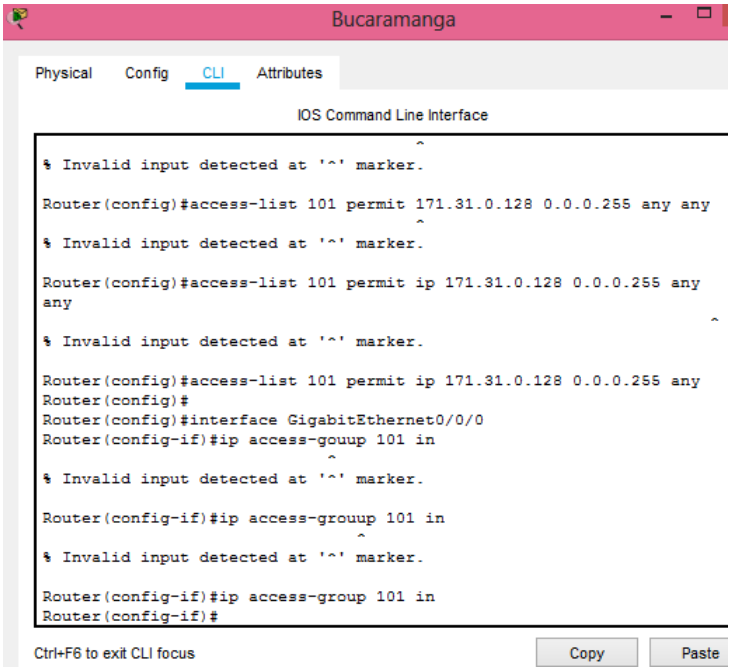


Ilustración 50 Hosts de VLAN 20

```
Router(config)#acccess-list 102 permit ip 172.31.0.128 0.0.0.255
172.31.1.64 0.0.0.255
                ^
Router(config)#
```

Ilustración 51 Hosts de VLAN 20 Parte 2

Aspectos a tener en cuenta

- Habilitar VLAN en cada switch y permitir su enrutamiento.
- Enrutamiento OSPF con autenticación en cada router.

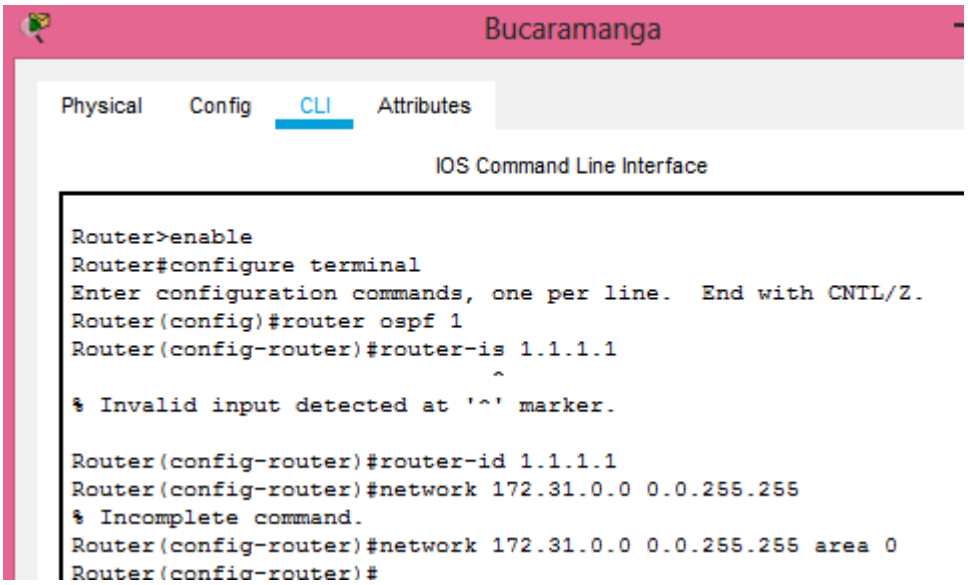


Ilustración 52 Hosts de VLAN 20 Parte 3

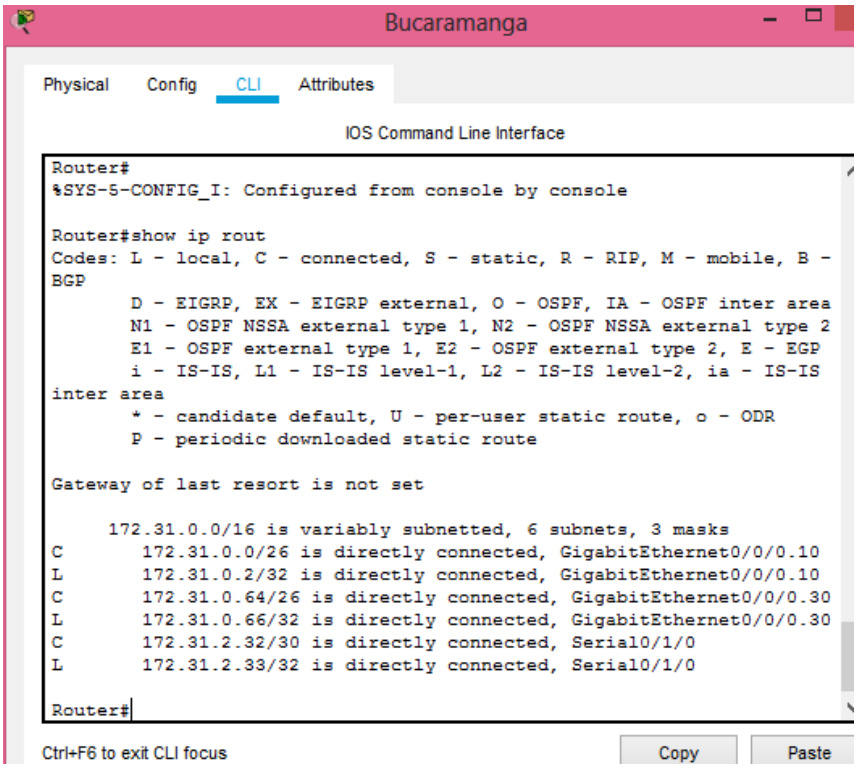


Ilustración 53 Hosts de VLAN 20 Parte 4

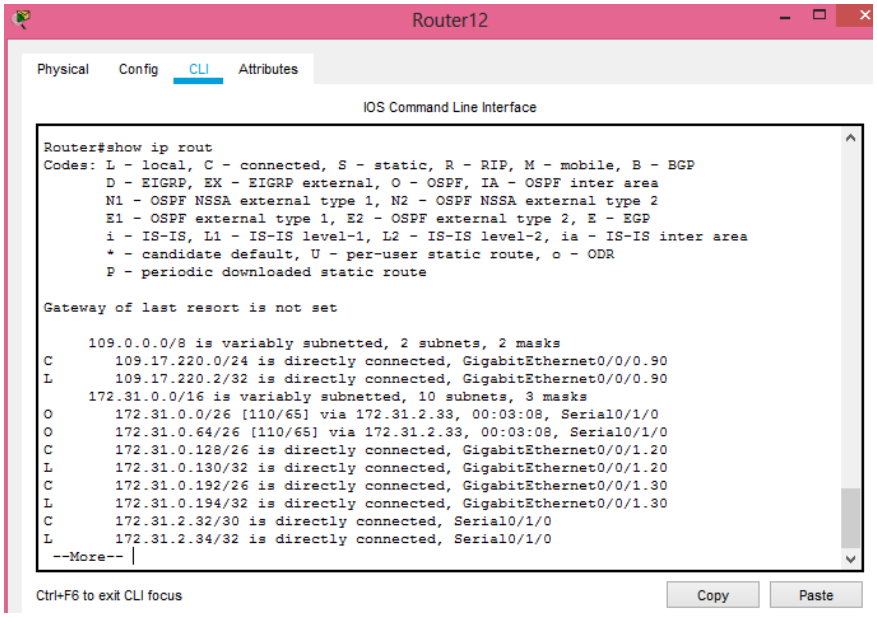


Ilustración 54 Router 12

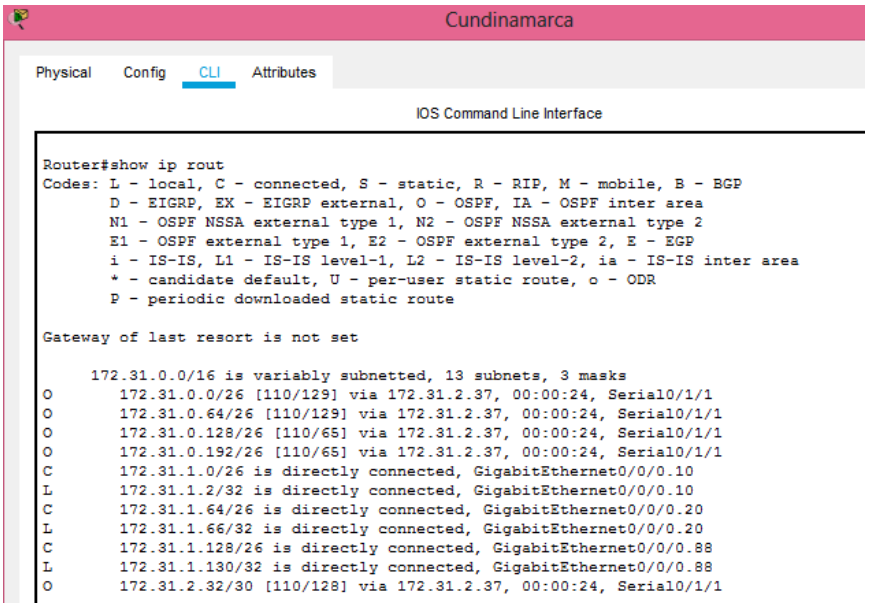


Ilustración 55 Router Cundinamarca

• Servicio DHCP en el router Tunja, mediante el helper address, para los routers Bucaramanga y Cundinamarca.

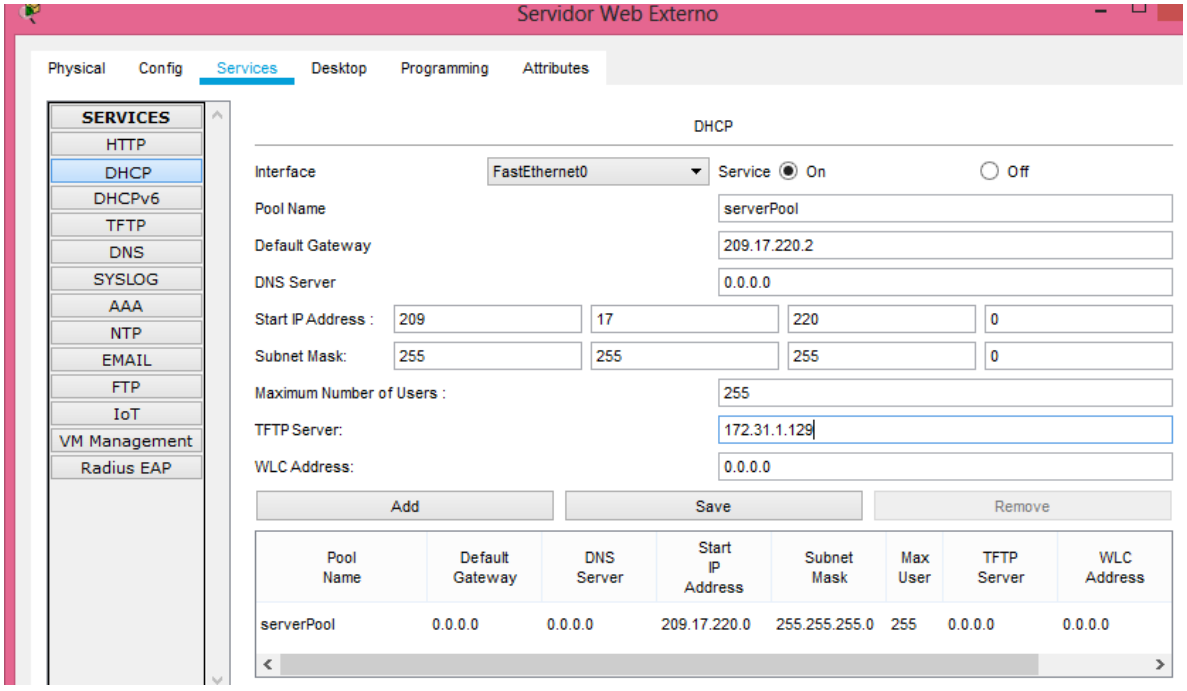


Ilustración 56 Servidor Web Externo

• Configuración de NAT estático y de sobrecarga.

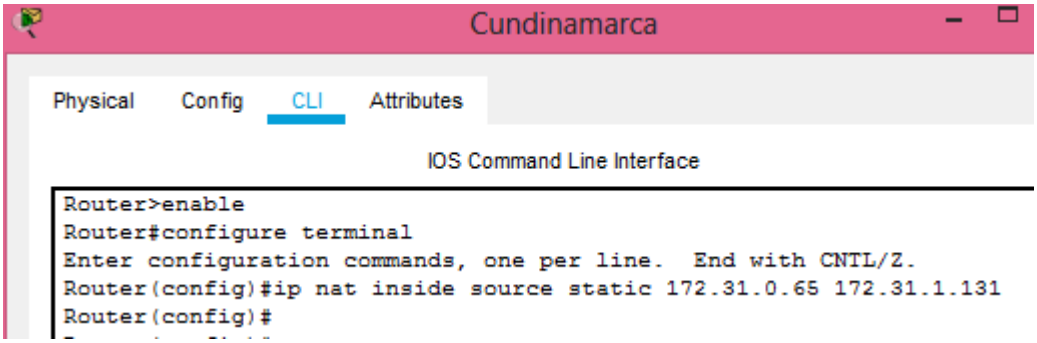


Ilustración 57 Configuración de NAT Estático y de Sobrecarga Router Cundinamarca

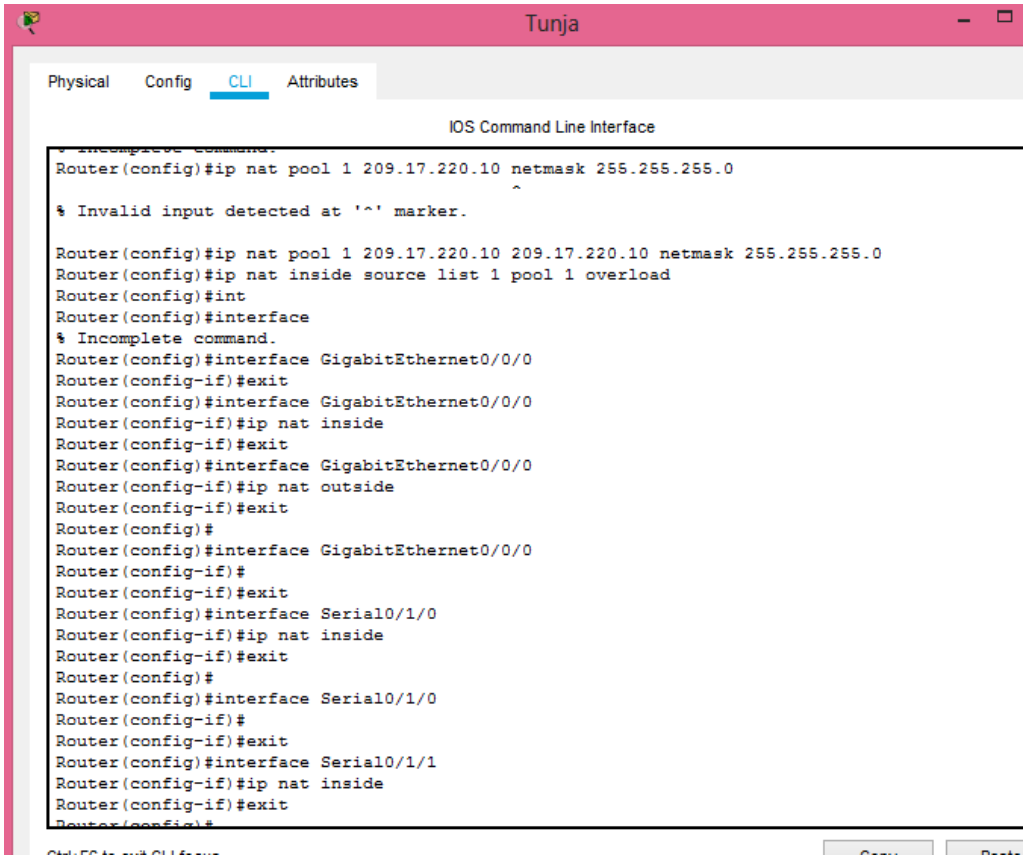


Ilustración 58 Configuración de NAT Estático y de Sobrecarga Router Tunja

Conclusión

Por medio de la elaboración del presente trabajo se pudo comprobar a importancia de las subredes en un entorno de trabajo o red de información, de igual manera se entendió la importancia en la seguridad de las mismas, por lo que se pudo poner en práctica los conocimientos adquiridos en el curso de redes de CISCO.

Se pudo realizar redes virtuales con sus respectivos protocolos de comunicación y de seguridad, tanto propios de CISCO como los externos, para obtener un óptimo rendimiento de la red.

Estos conocimientos son de gran importancia ya que nos toparemos con problemas como los presentados en el presente trabajo en el campo laboral.

Bibliografía

Anonimo. (s.f.). *REDES.* Obtenido de https://sites.google.com/site/redessenagloria/subne

CISCO. (s.f.). *Módulos de servicio Cisco Enhanced EtherSwitch para routers Cisco.* Obtenido de https://www.cisco.com/c/dam/global/es_mx/assets/docs/pdf/Request_0004_Etherswitch_data_sheet_c78-553980_Ready_to_translate.pdf

CISCO. (s.f.). *Principios básicos de enrutamiento y switching.* Obtenido de https://juliorestrepo.files.wordpress.com/2015/03/pdf_ccna1_v5.pdf