PRUEBA DE HABILIDADES PRACTICAS CCNA DIPLOMADO DE PROFUNDIZACIÓN CISCO

JONATHAN FERNEY PERAFAN MORENO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA DIPLOMADO DE PROFUNDIZACIÓN CISCO (DISEÑO E IMPLEMENTACIÓN DE SOLUCIONES INTEGRADAS LAN/WAN)
PASTO
2019

PRUEBA DE HABILIDADES PRACTICAS CCNA DIPLOMADO DE PROFUNDIZACIÓN CISCO

DISEÑO E IMPLEMENTACION DE SOLUCIONES INTEGRADAS LAN / WLAN

TUTOR
Ing. NILSON ALBEIRO FERREIRA MANZANARES

DIRECTOR
Ing. JUAN CARLOS VESGA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA DIPLOMADO DE PROFUNDIZACIÓN CISCO (DISEÑO E IMPLEMENTACIÓN DE SOLUCIONES INTEGRADAS LAN/WAN)
PASTO
2019

Universidad Nacional Abierta y a Distancia

CONTENIDO

Universidad Nacional Abierta y a Distancia

TABLA DE ILUSTRACIONES

RESUMEN

El principal objetivo de este trabajo es la elaboración de dos escenarios propuestos los cuales deberán estar documentados, estos corresponden al registro de la configuración de cada uno de los dispositivos, se realizará una descripción detallada del paso a paso de cada etapa, llevando así un registro de los procesos de verificación de conectividad mediante el uso de comandos.

Para la elaboración del primer escenario propuesto hay que desarrollar una topología en red en donde una empresa posee sucursales distribuidas en las ciudades de Bogotá, Medellín y Cali, la cual deberá ser configurada e interconectar entre si cada uno de los dispositivos que forman parte del escenario, esto acorde con los lineamientos establecidos para el direccionamiento IP, protocolos de enrutamiento y demás aspectos de la topología de red.

En el segundo escenario hay que adaptar una topología de red, para facilitar que los routers y las redes que incluyen puedan conectarse a internet, empleando las direcciones de la red LAN original.

Con estas pruebas se busca identificar el desarrollo de competencias y habilidades que fueron adquiridas a lo largo del diplomado. Es importante poner a prueba los niveles de comprensión y solución de problemas relacionados con aspectos de Networking.

ABSTRACT

The main objective of this work is the elaboration of two proposed scenarios which must be documented, these correspond to the registration of the configuration of each of the devices, a detailed description of the step by step of each stage will be made, thus keeping a record of connectivity verification processes through the use of commands.

To develop the first proposed scenario, a network topology must be developed where a company has branches distributed in the cities of Bogotá, Medellín and Cali, which must be configured and interconnect each of the devices that are part of the scenario. This is in accordance with the guidelines established for IP addressing, routing protocols and other aspects of the network topology.

In the second scenario, a network topology must be adapted, to make it easier for the routers and the networks they include to connect to the internet, using the addresses of the original LAN.

These tests seek to identify the development of skills and abilities that were acquired throughout the diploma. It is important to test the levels of understanding and solution of problems related to aspects of Networking.

INTRODUCCIÓN

El presente trabajo se enfoca en el desarrollo de habilidades para desarrollar, gestionar he implementar redes que cuenten con los estándares de la industria como la autenticación, automatización y contabilización que son elementos fundamentales a la hora de gestionar redes que puedan ser escalables y mantenibles en el tiempo.

Por esta razón se implementan dos escenarios en donde el estudiante de muestra sus capacidades a la hora de implementar y resolver problemas de redes, como el direccionamiento IP, implementación de AAA, gestión de usuarios, configurar listas de acceso, etc.

1. OBJETIVOS

1.1. OBJETIVO GENERAL

El objetivo general del diplomado de profundización en CISCO, es generar en el estudiante la capacidad de crear una red empresarial eficaz y escalable, así como a instalar, configurar, supervisar y solucionar problemas en los equipos pertenecientes a la infraestructura de una red convergente.

1.2. OBJETIVOS ESPECÍFICOS

- Desarrollar en el estudiante las habilidades de implementar una red escalabre y mantenible en el tiempo.
- Impulsar al estudiante a la resolución de problemas comunes en una red empresarial.
- Identificar el grado de desarrollo de competencias en el estudiante.

DESARROLLO DE LOS DOS ESCENARIOS

2. 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.

2.1. Topología de Red

Para el desarrollo de los requerimientos realizaremos las siguientes actividades.

- En el direccionamiento IP se debe definir una dirección de acuerdo con el número de hosts requeridos.
- Se realizará la asignación de los parámetros básicos y la detección de vecinos directamente conectados.
- Las redes y subredes establecidas deberán tener una interconexión total, todos los hosts deberán ser visibles y poder comunicarse entre ellos sin restricciones.
- Se debe restringir el acceso y comunicación entre hosts de acuerdo con los requerimientos del administrador.

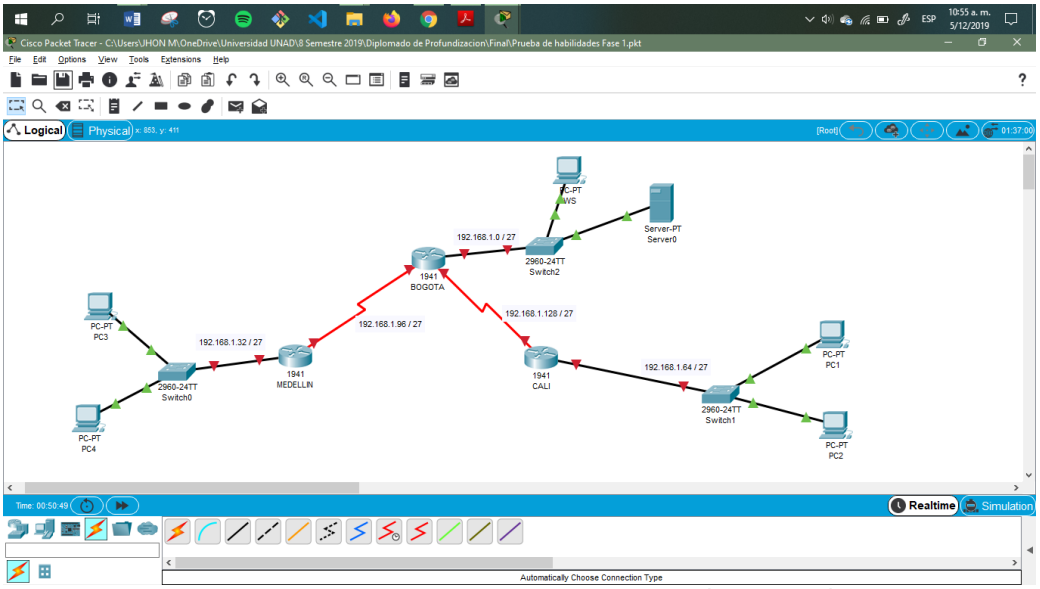


Ilustración 1 Topología de Red (2019). Escenario 1

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).

CONFIGURACION ROUTER BOGOTA.

>enable
#conf t
#hostname BOGOTA
#no ip domain-lookup
#enable secret cisco
#service password-encryption
#banner motd "Acceso no autorizado."
#line vty 0 15
#password class
#login
#exit
#line con 0
#password class
#login
#loggin synchronous
#end

CONFIGURACION ROUTER MEDELLIN

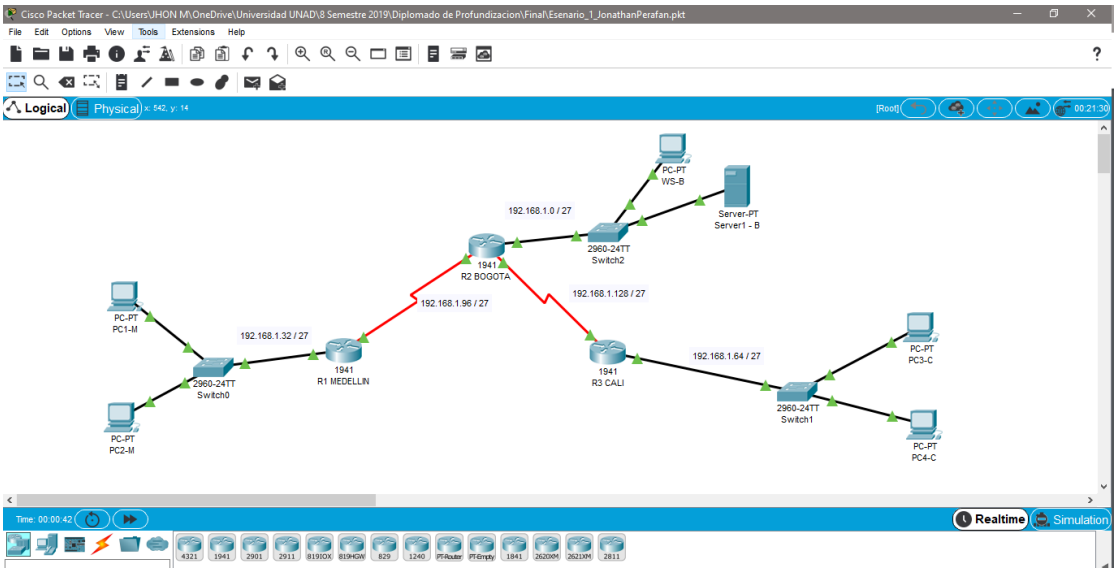
>enable
#conf t
#hostname MEDELLIN
#no ip domain-lookup
#enable secret cisco
#service password-encryption
#banner motd "Acceso no autorizado."
#line vty 0 15
#password class
#login
#exit
#line con 0
#password class
#login
#loggin synchronous
#end

CONFIGURACION ROUTER CALI

>enable
#conf t

#hostname CALI
#no ip domain-lookup
#enable secret cisco
#service password-encryption
#banner motd “Acceso no autorizado.”
#line vty 0 15
#password class
#login
#exit
#line con 0
#password class
#login
#loggin synchronous
#end

- Realizar la conexión física de los equipos con base en la topología de red



2.2. Parte 1: Asignación de direcciones IP:

a. SE DEBE DIVIDIR (SUBNETEAR) LA RED CREANDO UNA SEGMENTACIÓN EN OCHO PARTES, PARA PERMITIR CRECIMIENTO FUTURO DE LA RED CORPORATIVA.

Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway predeterminado
BOGOTA	G0/0	192.168.1.1	255.255.255.224	N/A
	S0/0/0	192.168.1.98	255.255.255.224	N/A
	S0/0/1	192.168.1.130	255.255.255.224	N/A
MEDELLIN	G0/0	192.168.1.33	255.255.255.224	N/A
	S0/0/0	192.168.1.99	255.255.255.224	N/A
	S0/0/1	192.168.1.160	255.255.255.224	N/A
CALI	G0/0	192.168.1.65	255.255.255.224	N/A
	S0/0/0	192.168.1.131	255.255.255.224	N/A
	S0/0/1	192.168.1.192	255.255.255.224	N/A
PC1-M	NIC	192.168.1.34	255.255.255.224	192.168.1.33
PC2-M	NIC	192.168.1.35	255.255.255.224	192.168.1.33
PC3-C	NIC	192.168.1.66	255.255.255.224	192.168.1.65
PC4-C	NIC	192.168.1.67	255.255.255.224	192.168.1.65
WS-B	NIC	192.168.1.2	255.255.255.224	192.168.1.1
Server1-B	NIC	192.168.1.3	255.255.255.224	192.168.1.1

b. REALIZAMOS LA ASIGNACIÓN DE UNA DIRECCIÓN IP A LA RED .

Asignar dirección IP router: Para asignar una dirección IP al router ingresamos al CLI y ingresamos los siguientes comandos.

ROUTER BOGOTA

#int fastEthernet 0/0
#ip address 192.168.1.1 255.255.255.224
#no shutdown

#int serial 0/0/0
#ip address 192.168.1.98 255.255.255.254
#no shutdown

#int serial 0/0/1
#ip address 192.168.1.130 255.255.255.254
#no shutdown

ROUTER MEDELLIN

#int fastEthernet 0/0
#ip address 192.168.1.33 255.255.255.224
#no shutdown

#int serial 0/0/0
#ip address 192.168.1.99 255.255.255.254
#no shutdown

ROUTER CALI

#int fastEthernet 0/0
#ip address 192.168.1.65 255.255.255.224
#no shutdown

#int serial 0/0/0
#ip address 192.168.1.131 255.255.255.254
#no shutdown

Asignar direccion IP PC: Para asignar una dirección IP al PC ingresamos a IP Configuration seleccionamos la FastEthernet y ingresamos la siguiente información.

$IP\ Address = 192.168.1.34$
$Subnet\ Mask = 255.255.255.0$
$Default\ Gateway = 192.168.1.33$

Asignar dirección IP Servidor: Para asignar una dirección IP al Servidor ingresamos a IP Configuration ingresamos la siguiente información.

$IP\ Address = 192.168.1.3$
$Subnet\ Mask = 255.255.255.0$
$Default\ Gateway = 192.168.1.1$

2.3. Parte 2: Configuración Básica.

a. COMPLETAR LA SIGUIENTE TABLA CON LA CONFIGURACIÓN BÁSICA DE LOS ROUTERS, TENIENDO EN CUENTA LAS SUBREDES DISEÑADAS.

	R1	R2	R3
Nombre de Host	**MEDELLIN**	**BOGOTA**	**CALI**
Dirección de Ip en interfaz Serial 0/0	192.168.1.99	192.168.1.98	192.168.1.131
Dirección de Ip en interfaz Serial	192.168.1.160	192.168.1.130	192.168.1.192

0/1			
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

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.

Para verificar la tabla de enrutamiento en el Router utilizamos el siguiente comando **show ip route,** en donde el Router nos muestra las redes conectadas.

$> enable$
$\#show\ ip\ route$

MEDELLIN

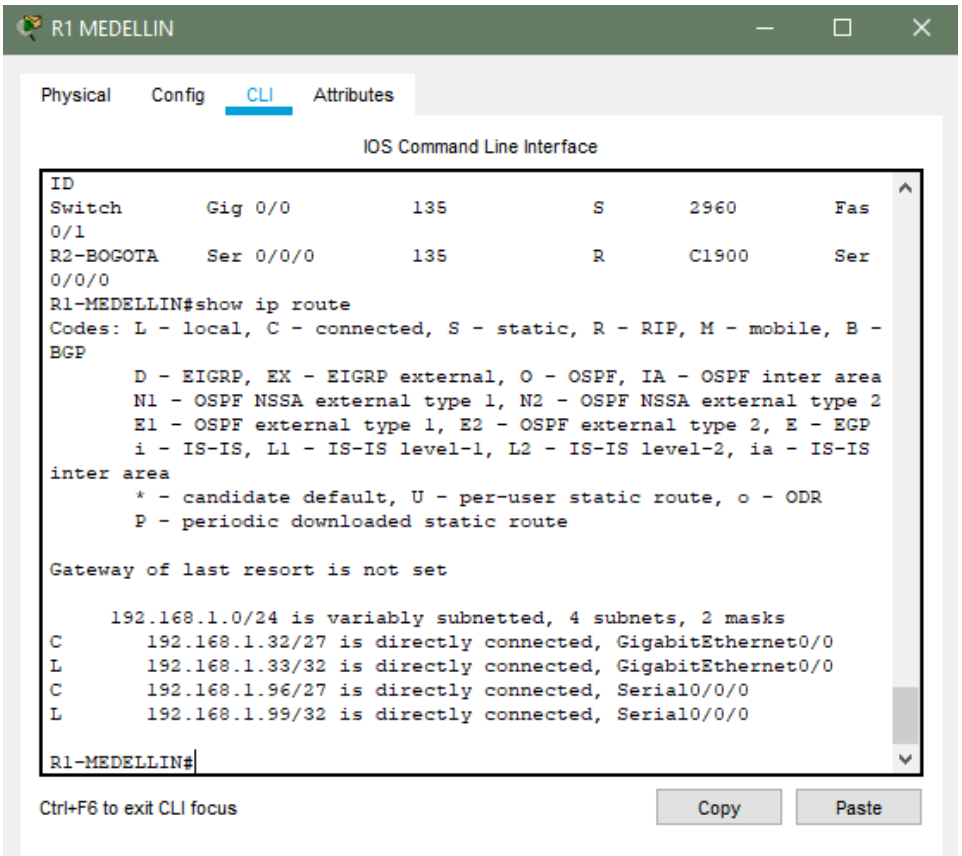


Ilustración 2 Tabla de enrutamiento (2019). Escenario 1

BOGOTA

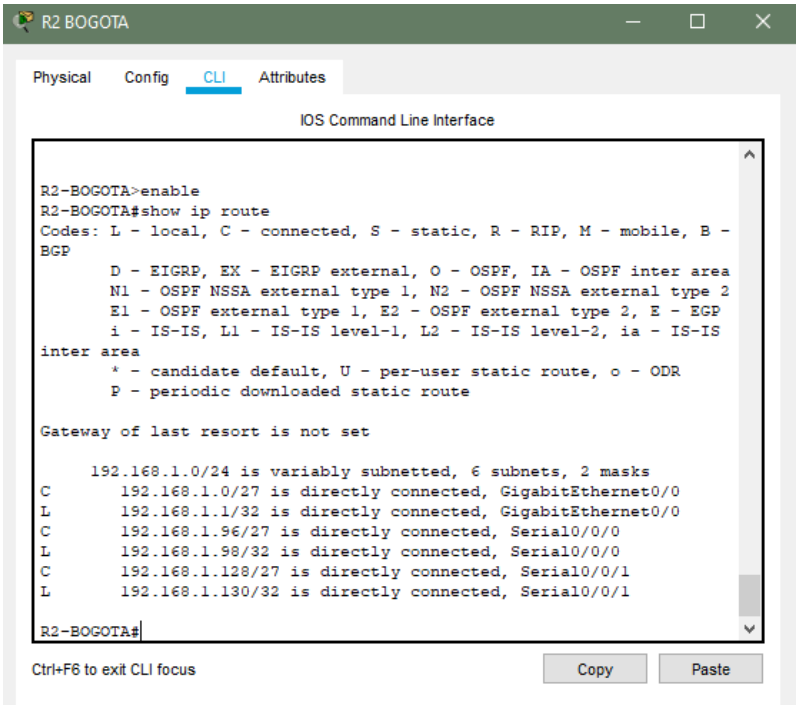


Ilustración 3 Tabla de enrutamiento (2019). Escenario 1

CALI

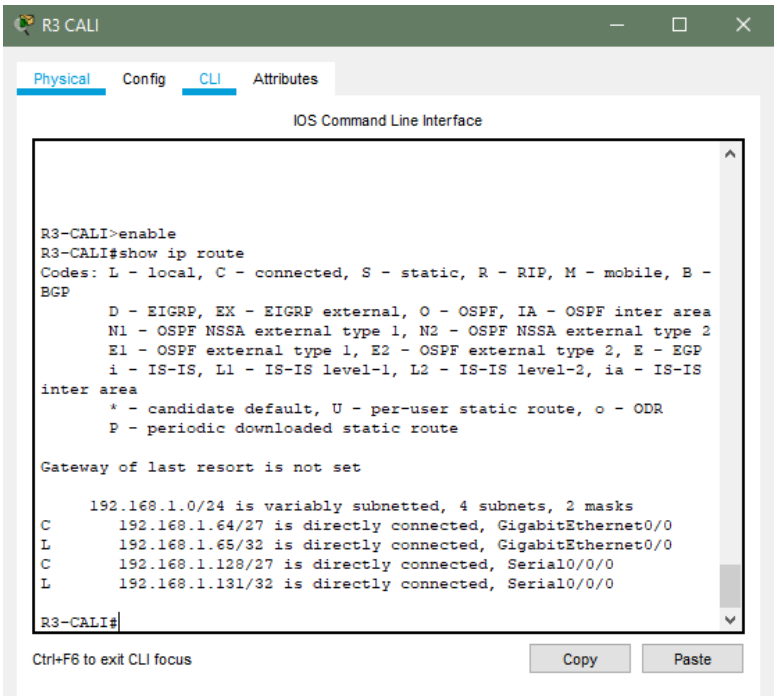


Ilustración 4 Tabla de enrutamiento (2019). Escenario 1

c. REALIZAR UN DIAGNÓSTICO DE VECINOS UANDO EL COMANDO CDP.

El protocolo CDP es un protocolo de capa 2 que conecta los medios físicos inferiores con los protocolos de red de las capas superiores. Para CDP utilizamos el comando show cdp neighbors. El cual nos arroja el siguiente resultado para nuestra red.

MEDELLIN

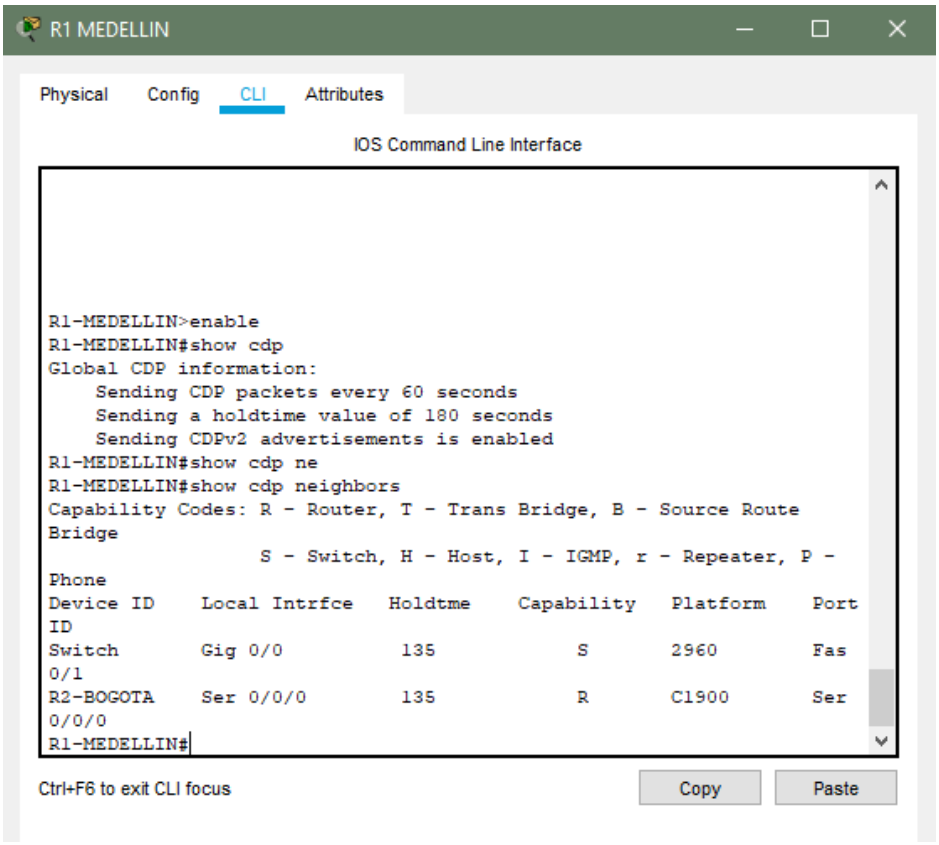


Ilustración 5 Diagnostico de vecinos (2019). Escenario 1

BOGOTA

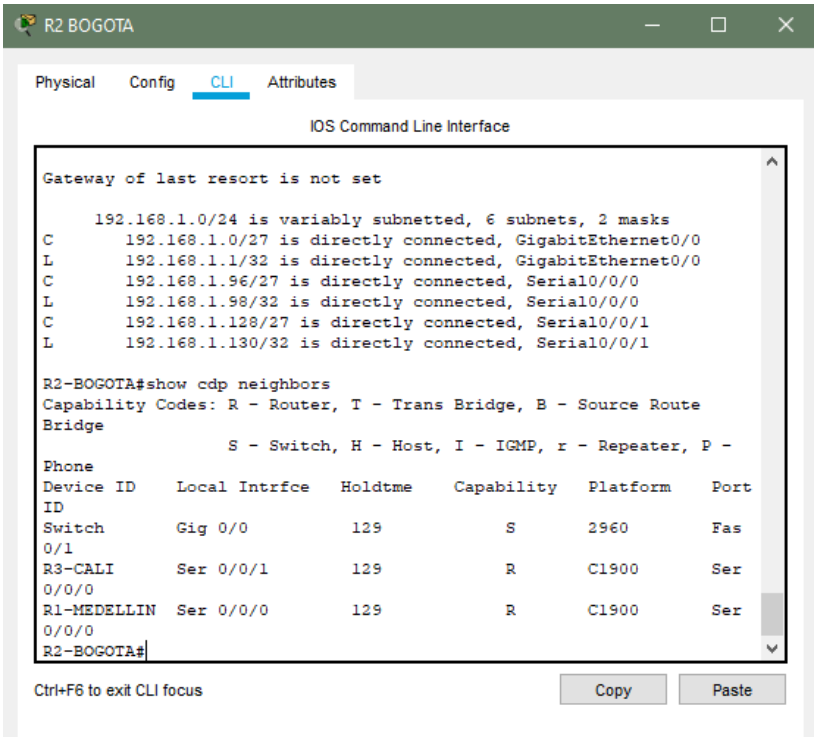


Ilustración 6 Diagnostico de vecinos (2019). Escenario 1

CALI

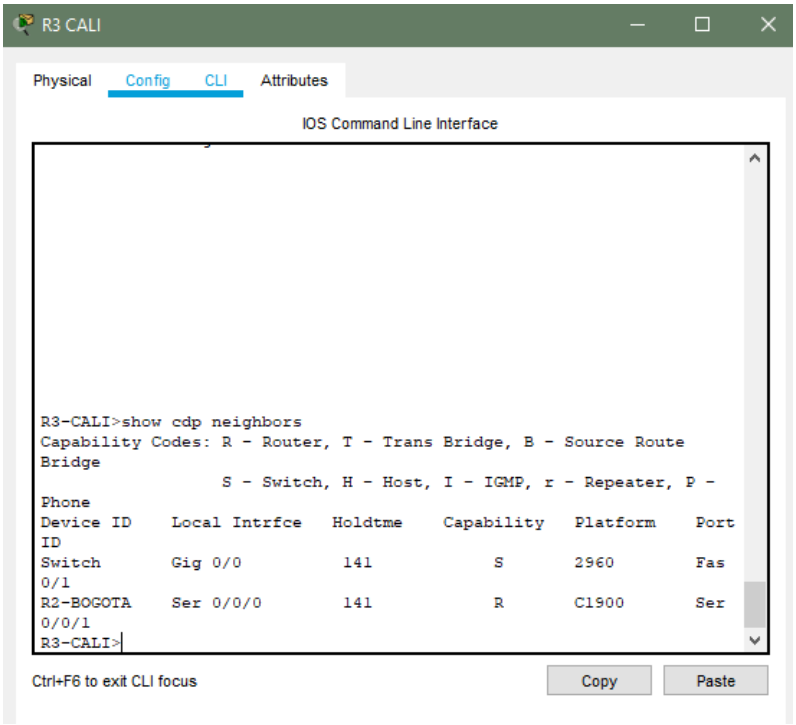


Ilustración 7 Diagnostico de vecinos (2019). Escenario 1

d. REALIZAR UNA PRUEBA DE CONECTIVIDAD EN CADA TRAMO DE LA RUTA USANDO PING.

Prueba de conectividad PC1-M ping a R1 MEDELLIN.

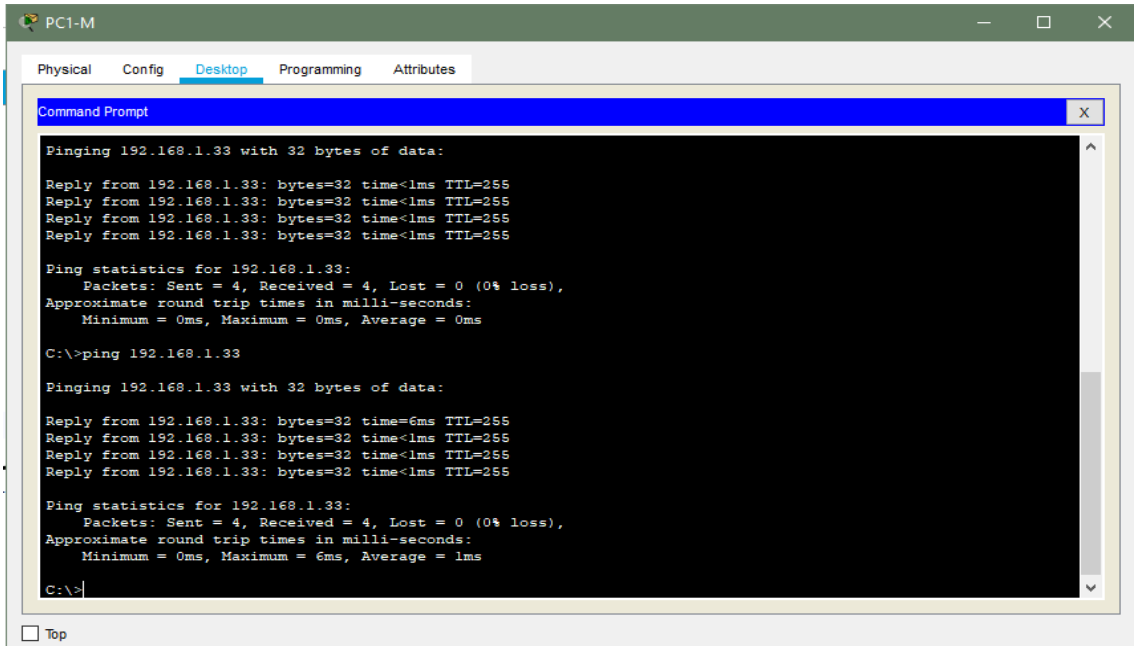


Ilustración 8 ping a R1(2019). Escenario 1

Prueba de conectividad PC2-M ping a R1 MEDELLIN.

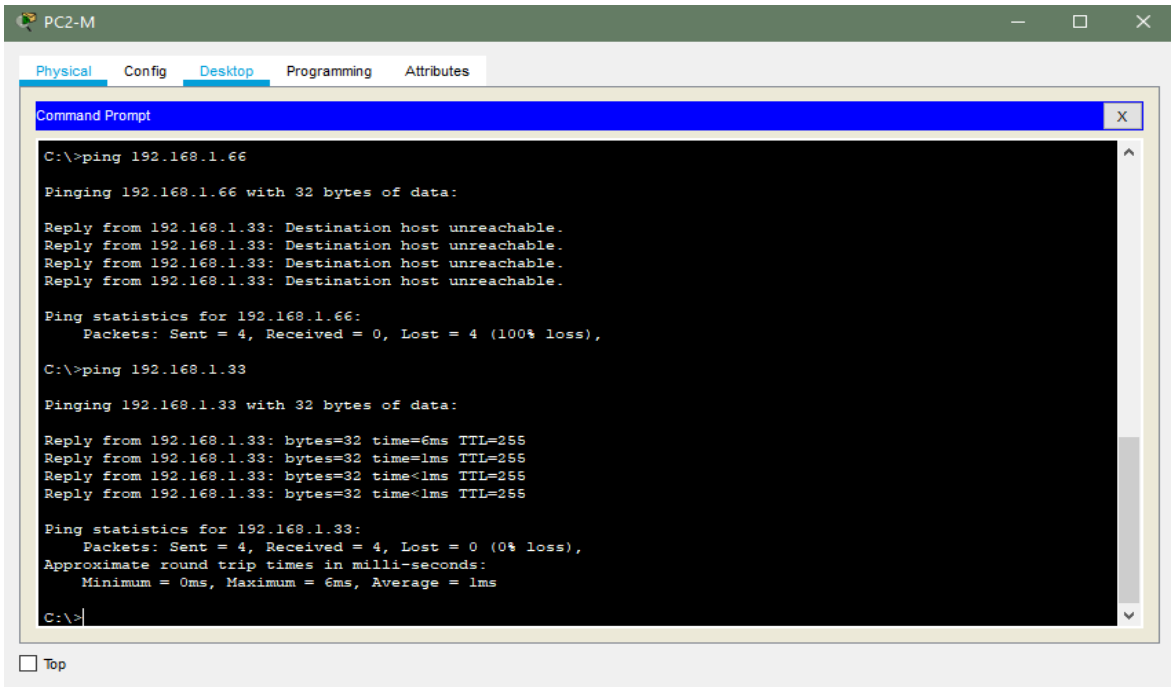


Ilustración 9 ping a R1(2019). Escenario 1

Prueba de conectividad PC1-M ping a PC2-M.

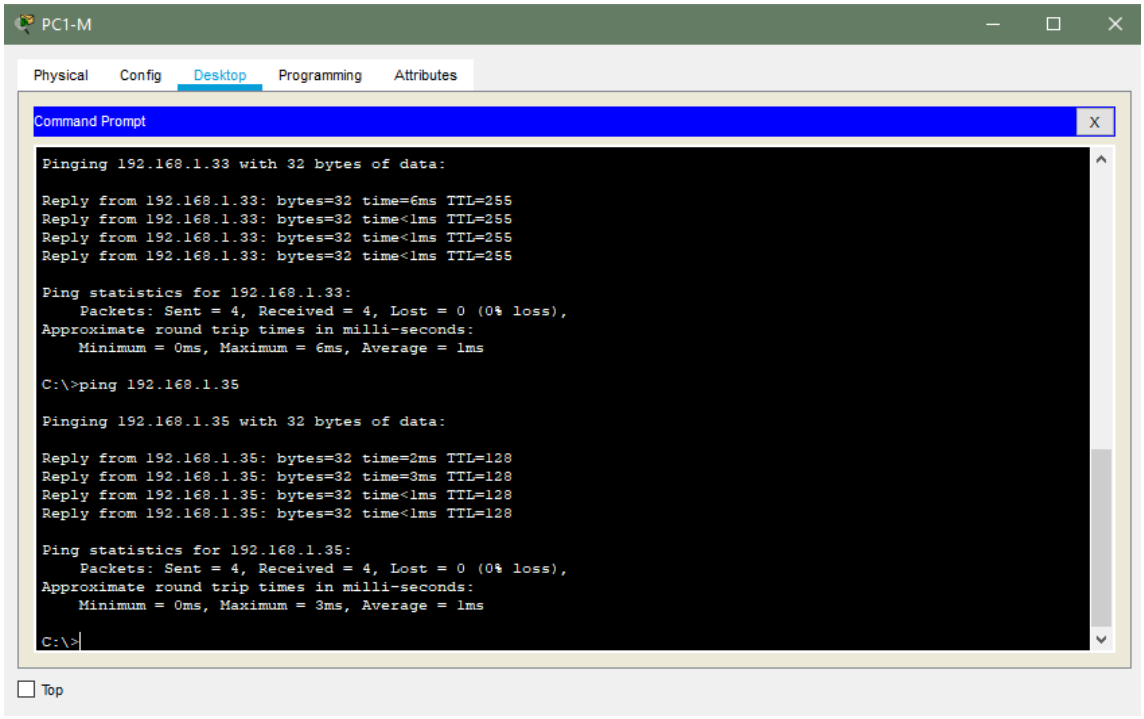


Ilustración 10 ping a PC2 (2019). Escenario 1

Prueba de conectividad PC1-M ping a WS-B.

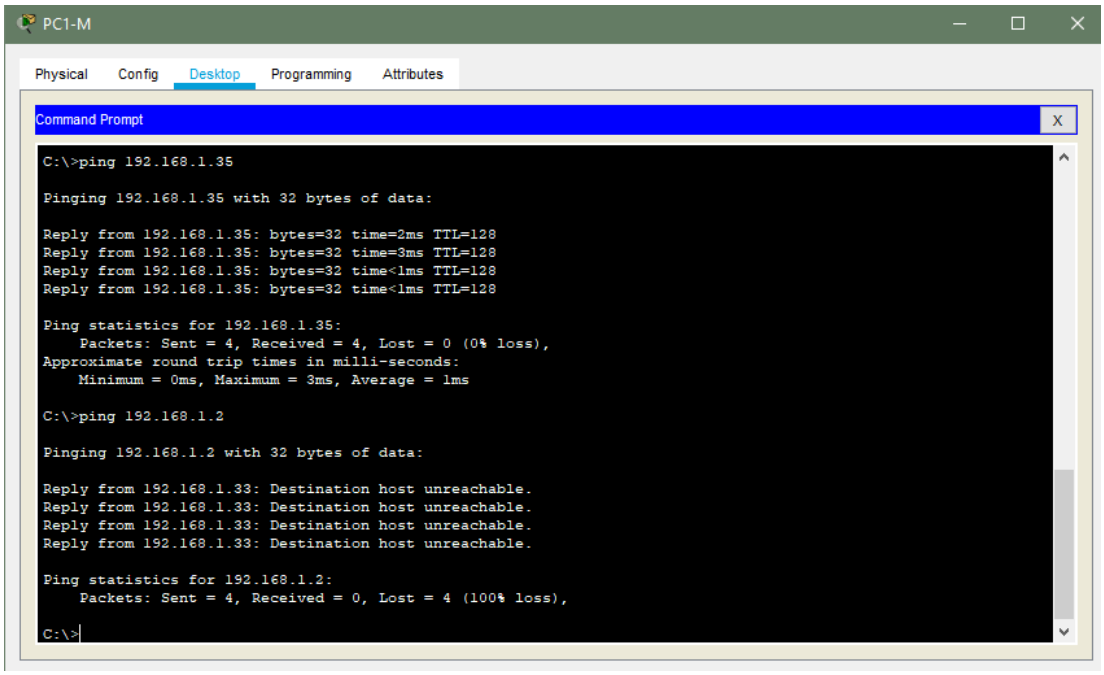


Ilustración 11 ping a WS-B(2019). Escenario 1

Prueba de conectividad PC2-M ping a PC4-C.

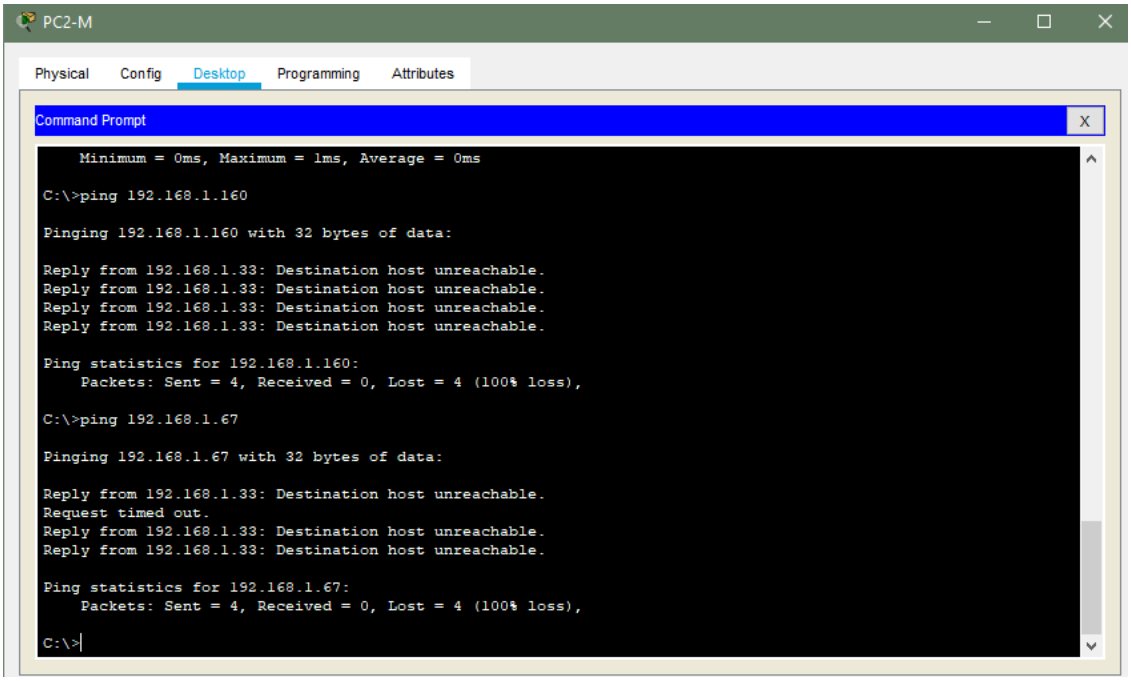


Ilustración 12 ping a PC4-C(2019). Escenario 1

Prueba de conectividad WS-B ping a Server1-B.

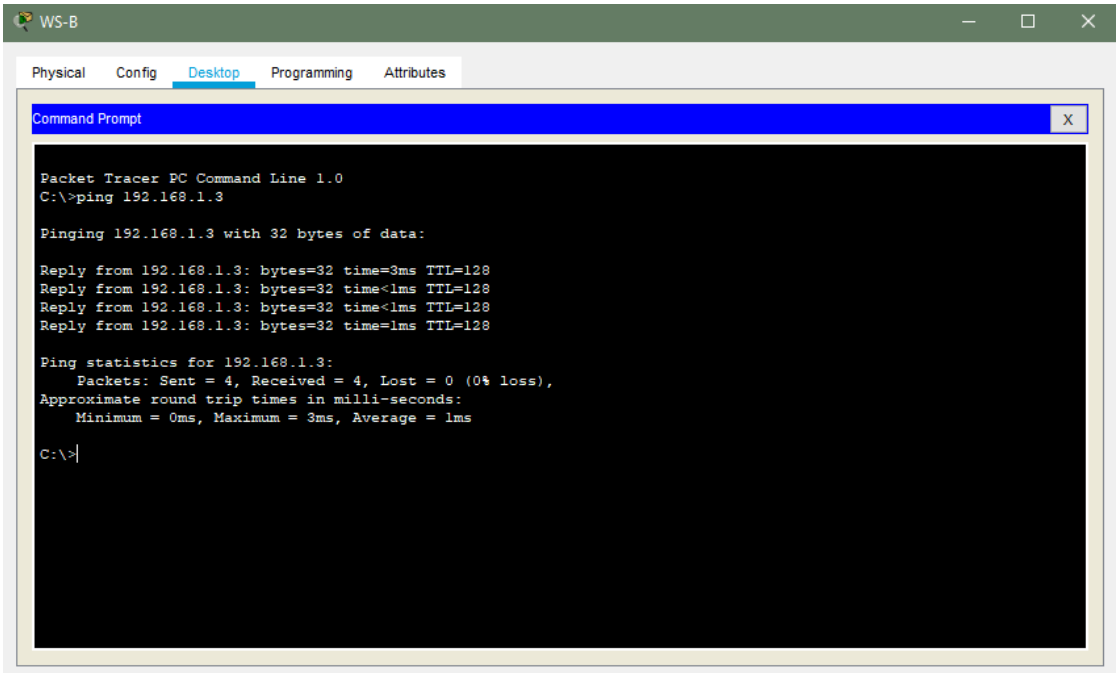


Ilustración 13 ping a Server1-B (2019). Escenario 1

Prueba de conectividad PC3-C ping a PC4-C.

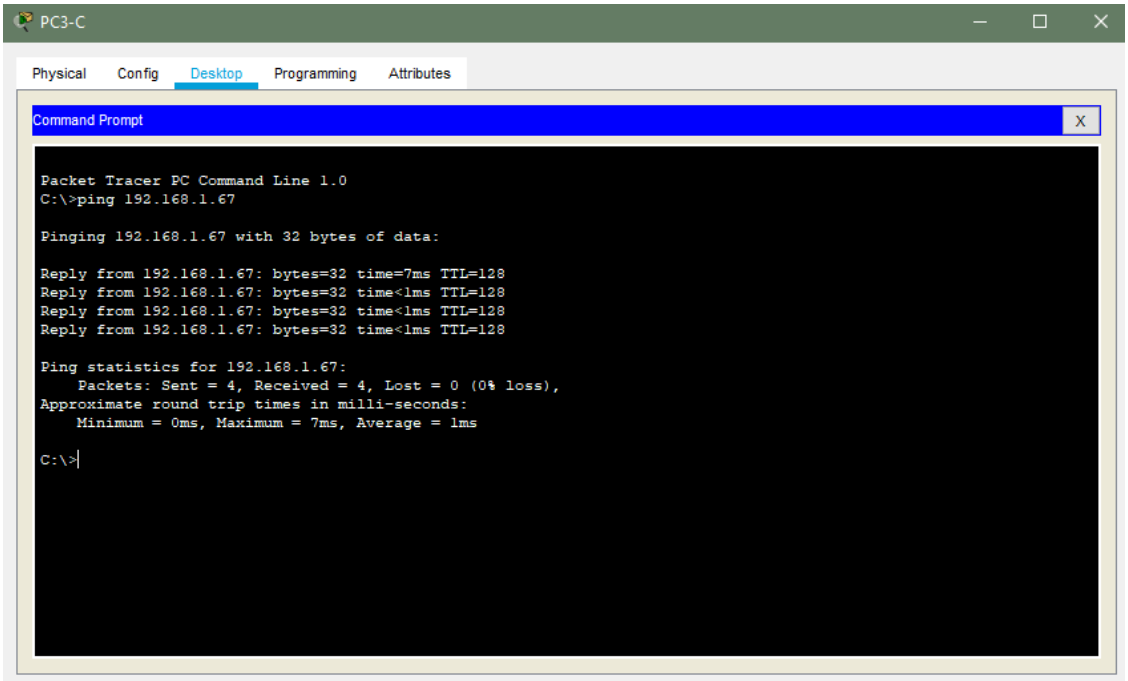


Ilustración 14 ping a PC4-C (2019). Escenario 1

Prueba de conectividad PC3-C ping a R2-BOGOTA.

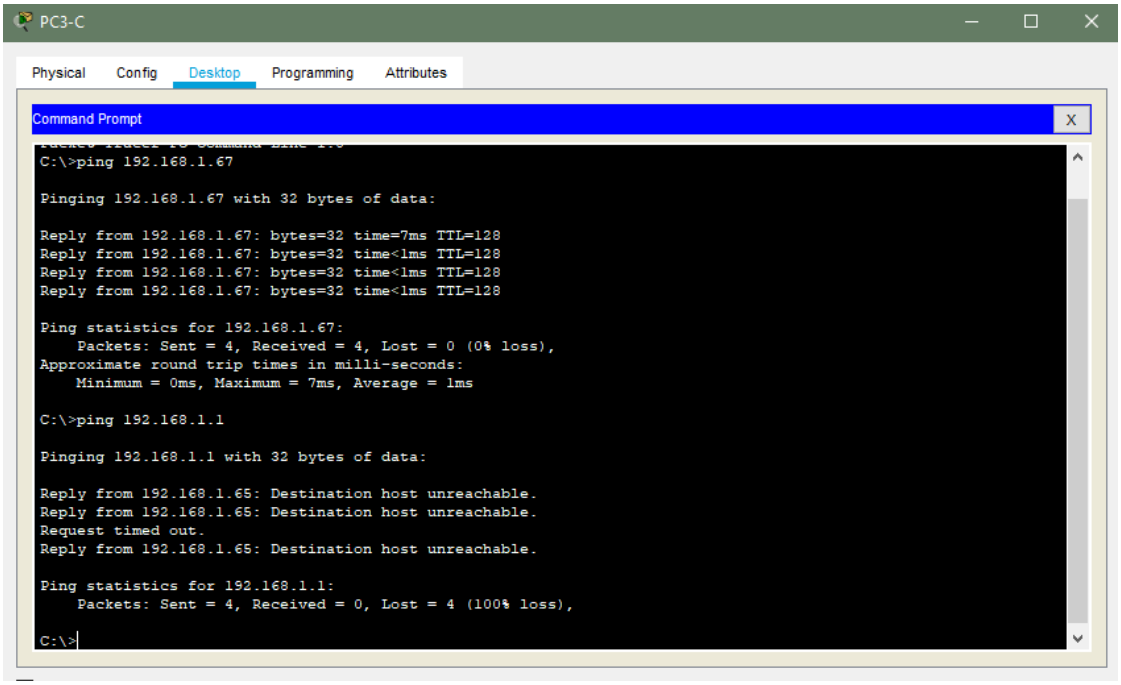


Ilustración 15 ping a R2-BOGOTA (2019). Escenario 1

Prueba de conectividad Server1-B ping R2-BOGOTA.

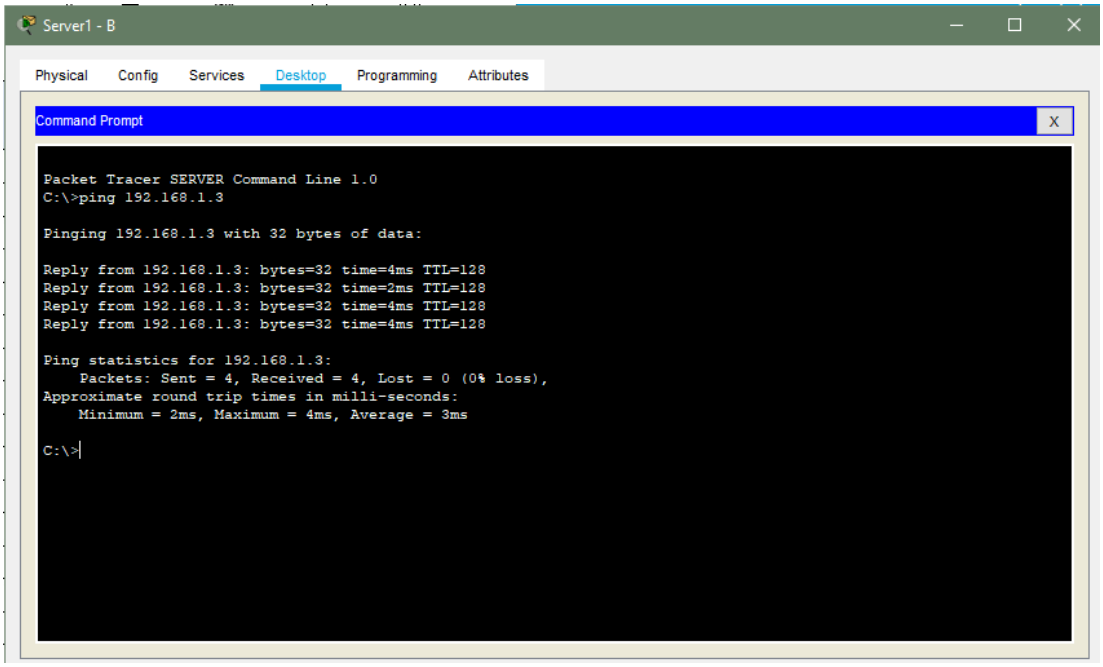


Ilustración 16 ping a R2-BOGOTA (2019). Escenario 1

Prueba de conectividad PC-3 ping PC-1.

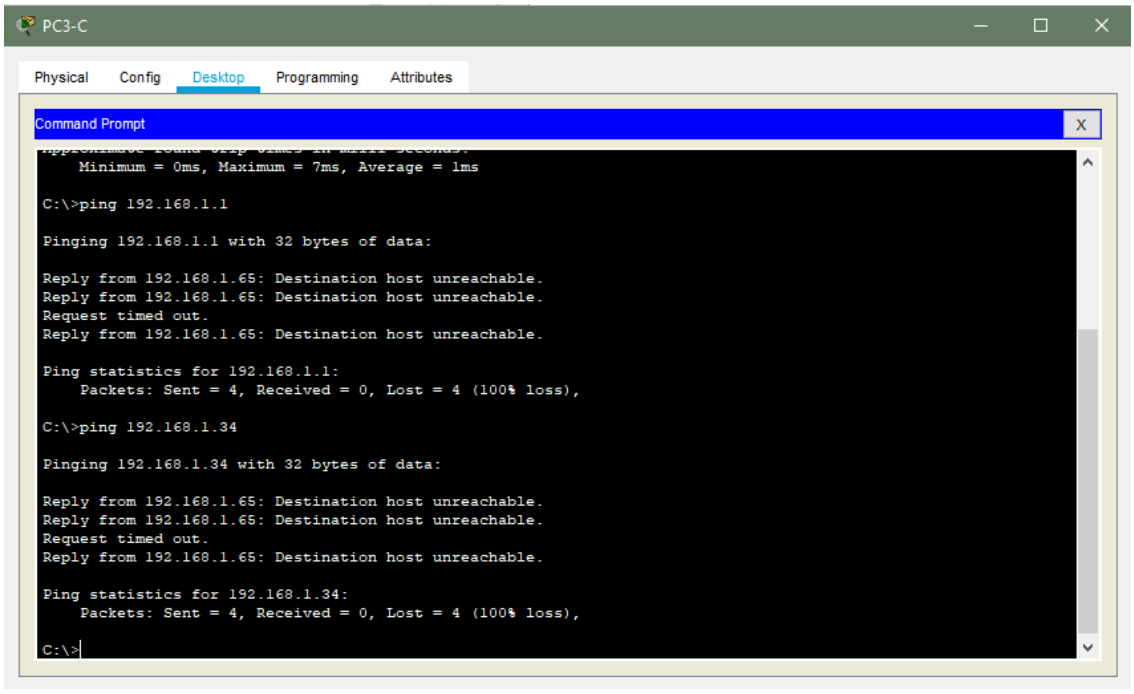


Ilustración 17 ping a PC-1 (2019). Escenario 1

Los pings en las diferentes redes fallan porque no hemos configurado ningún protocolo de enrutamiento.

2.4. Parte 3: Configuración de Enrutamiento.

a) ASIGNAR EL PROTOCOLO DE ENRUTAMIENTO EIGRP A LOS ROUTERS CONSIDERANDO EL DIRECCIONAMIENTO DISEÑADO.

EL EIGRP se han mejorado en el tiempo de convergencia y los aspectos relativos de la capacidad de la ampliación. EIGRP multiplica la métrica de IGRP por un factor de 256. Esto ocurre porque EIGRP usa una métrica que tiene 32 bits de largo. EIGRP ofrece caracterí-sticas que no se encontraban en su antecesor, IGRP como el soporte para VLSM y los resúmenes de ruta arbitrarios. Además, EIGRP ofrece caracterí-sticas que se encuentran en protocolos como OSPF, como las actualizaciones increméntales parciales y un tiempo de convergencia reducido. Para asignar EIGRP en los Router hay que implementar los siguientes comandos.

BOGOTA

#int s0/0/1
#clock rate 64000
#exit
#router eigrp 10
#network 192.168.1.0 0.0.0.31
#network 192.168.1.96 0.0.0.31
#network 192.168.1.128 0.0.0.31
#no auto-summary

MEDELLIN

#int s0/0/0
#clock rate 64000
#exit
#router eigrp 10
#network 192.168.1.32 0.0.0.31
#network 192.168.1.96 0.0.0.31
#no auto-summary

CALI

#router eigrp 10
#network 192.168.1.128 0.0.0.31
#network 192.168.1.64 0.0.0.31
#no auto-summary

b) VERIFICAR SI EXISTE VECINDAD CON LOS ROUTERS CONFIGURADOS CON EIGRP.

Para verificar la vecindad con los routers configurados con EIGRP, podemos utilizar el siguiente comando **show ip eigrp neighbors.**

MEDELLIN

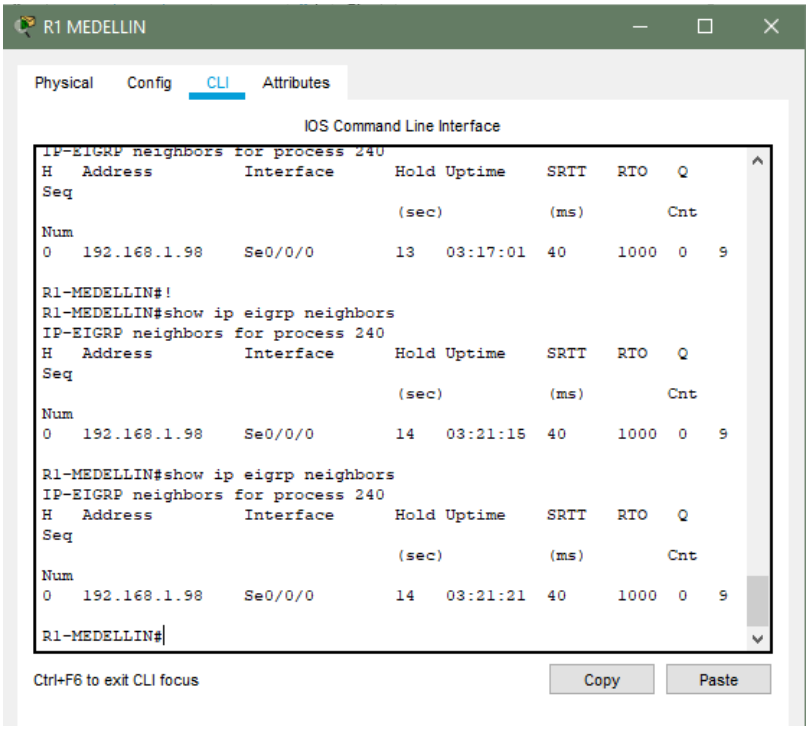


Ilustración 18 Verificación de Vecindad (2019). Escenario 1

BOGOTA

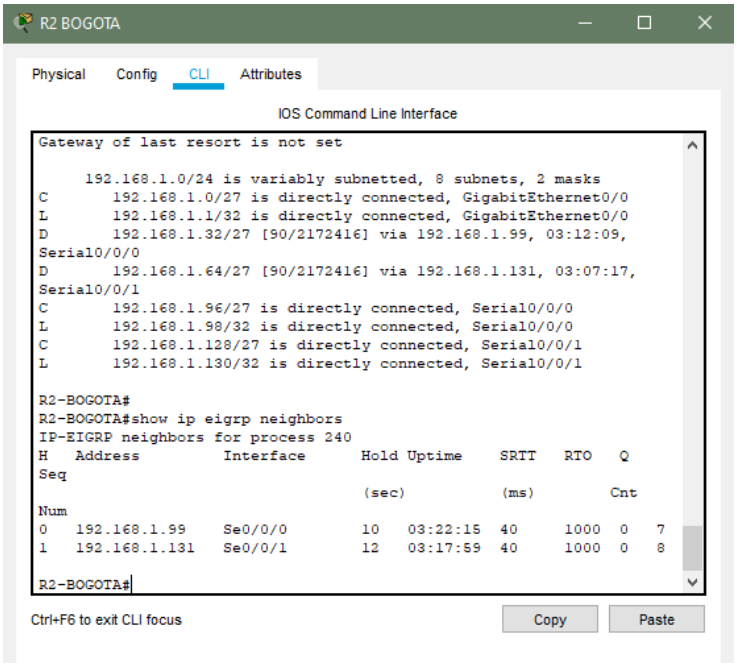


Ilustración 19 Verificación de Vecindad (2019). Escenario 1

CALI

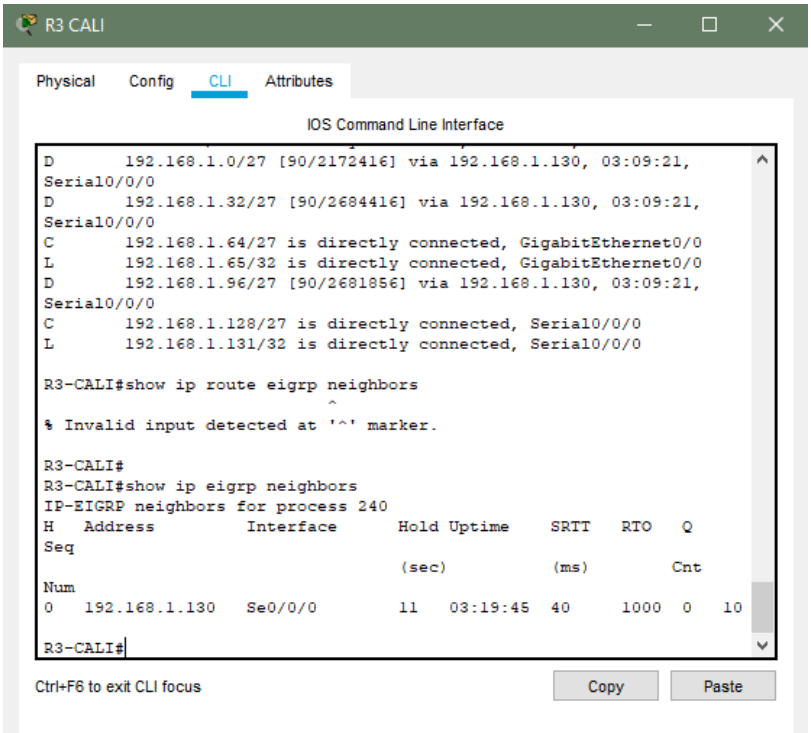


Ilustración 20 Verificación de Vecindad (2019). Escenario 1

c) REALIZAR LA COMPROBACIÓN DE LAS TABLAS DE ENRUTAMIENTO EN CADA UNO DE LOS ROUTERS PARA VERIFICAR CADA UNA DE LAS RUTAS ESTABLECIDAS.

Para realizar la comprobación de las tablas de enrutamiento utilizamos el comando: *show ip route*.

MEDELLIN

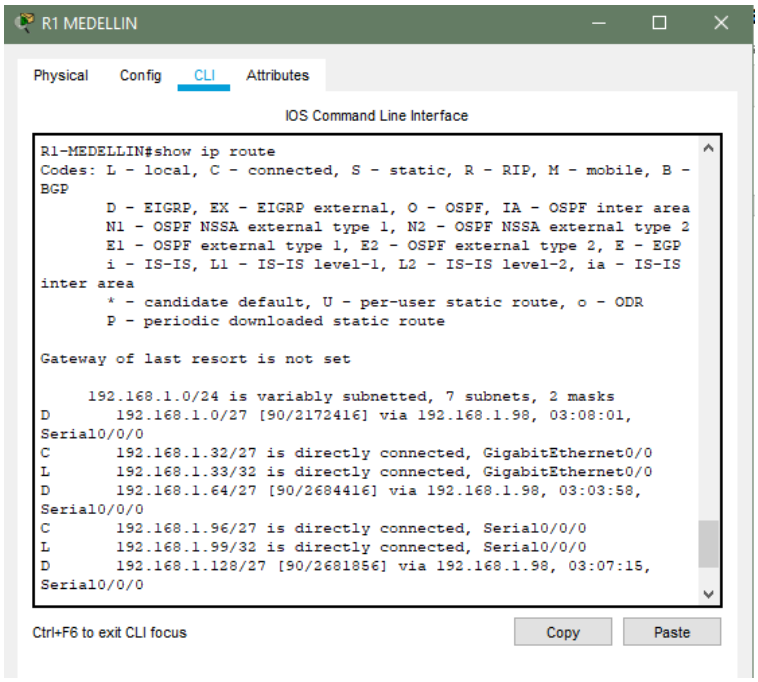


Ilustración 21 Tablas de Enrutamiento (2019). Escenario 1

BOGOTA

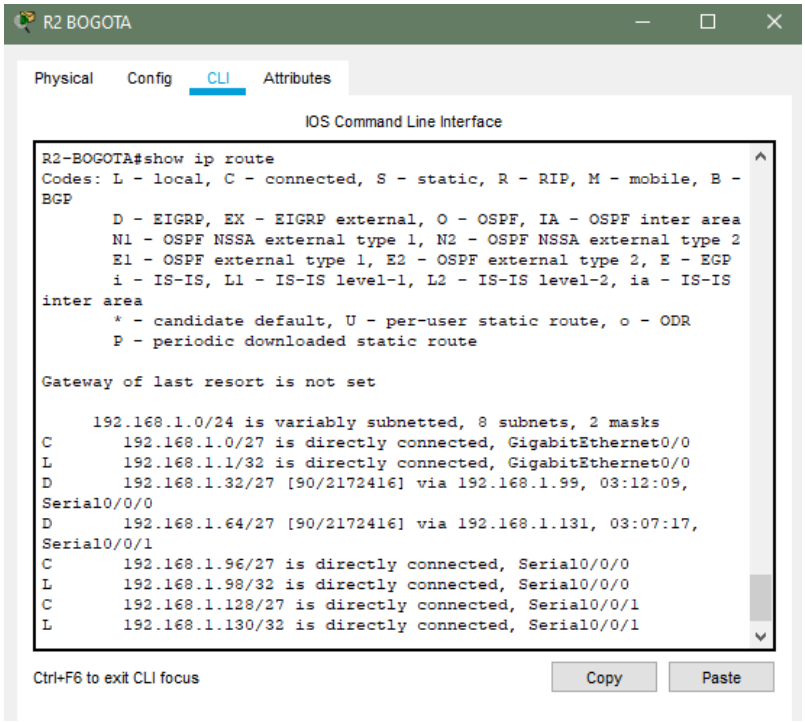


Ilustración 22 Tablas de Enrutamiento (2019). Escenario 1

CALI

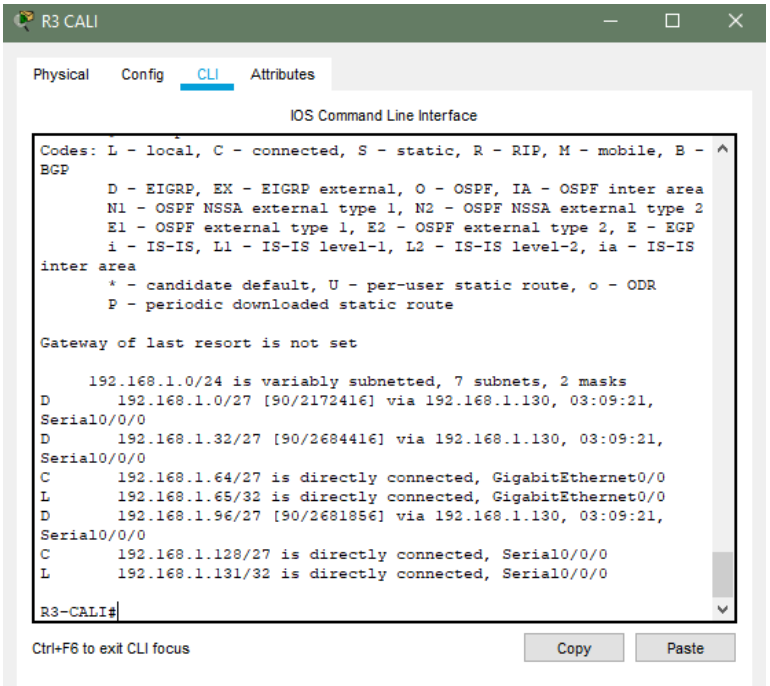


Ilustración 23 Tablas de Enrutamiento (2019). Escenario 1

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.

Para realizar un diagnóstico utilizaremos el comando TRACERT determina la ruta a un destino mediante el envío de paquetes de eco de Protocolo de mensajes de control de Internet (ICMP) al destino. En estos paquetes, TRACERT usa valores de período de vida (TTL) IP variables.

Prueba 1: Del PC3-C de la red LAN del Router CALI a la red de MEDELLIN en él PC1-M.

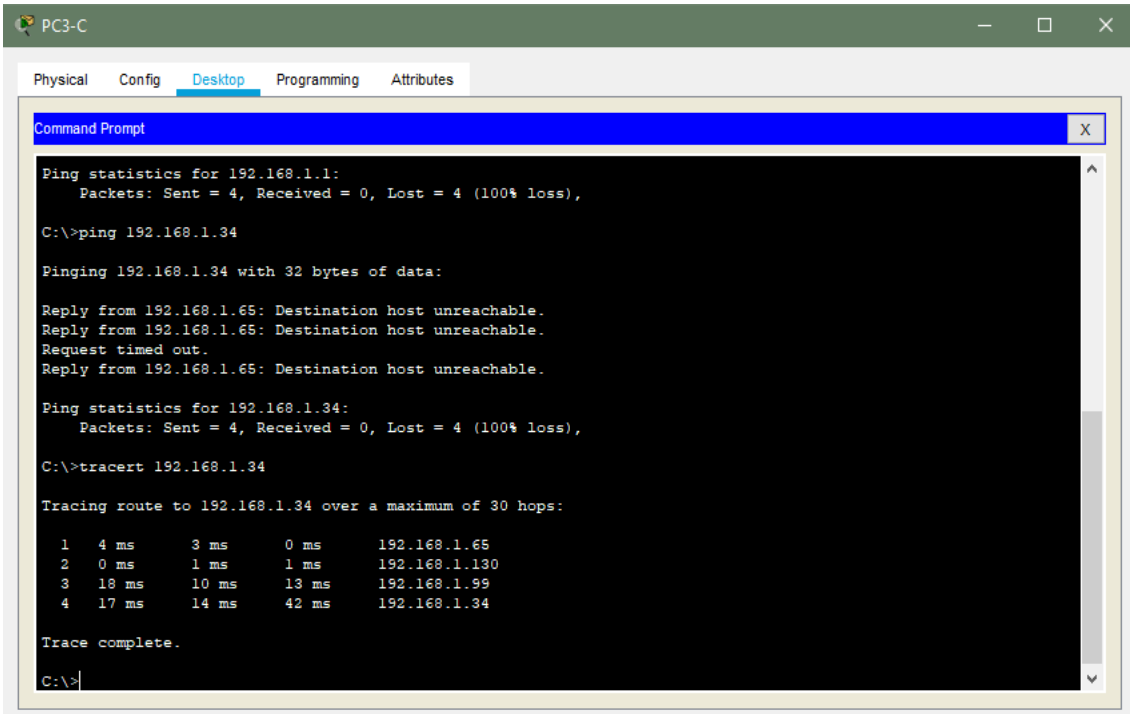


Ilustración 24 Prueba 1 Comando TRACERT (2019). Escenario 1

Prueba 2: Del PC4-C de la red LAN del Router CALI a la red de BOGOTA en él Server1-B.

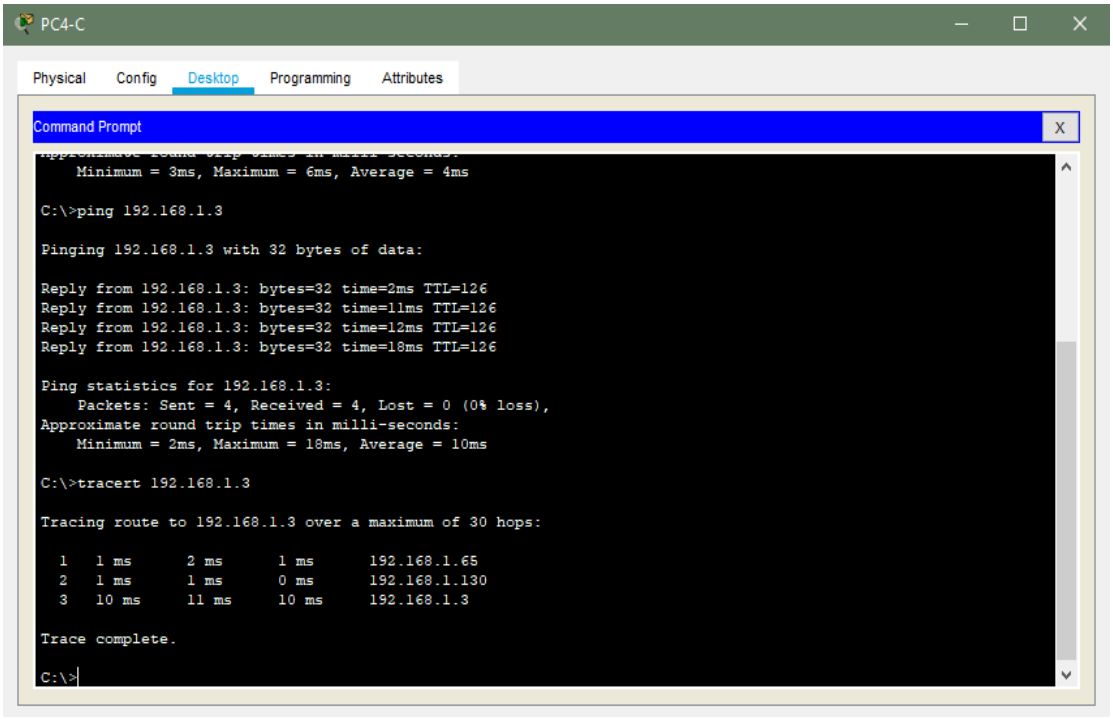


Ilustración 25 Prueba 2 Comando TRACERT (2019). Escenario 1

2.5. 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.

Para realizar la conexión a Telnet utilizamos los siguientes comandos.

MEDELLIN

>enable
#configure terminal
#line vty 0 4
#password cisco
#login
#exit

#enable secret cisco
#exit

BOGOTA

>enable
#configure terminal
#line vty 0 4
#password cisco
#login
#exit
#enable secret cisco
#exit

CALI

>enable
#configure terminal
#line vty 0 4
#password cisco
#login
#exit
#enable secret cisco
#exit

Comprobamos la configuración del Router de Medellín desde el PC1-M.

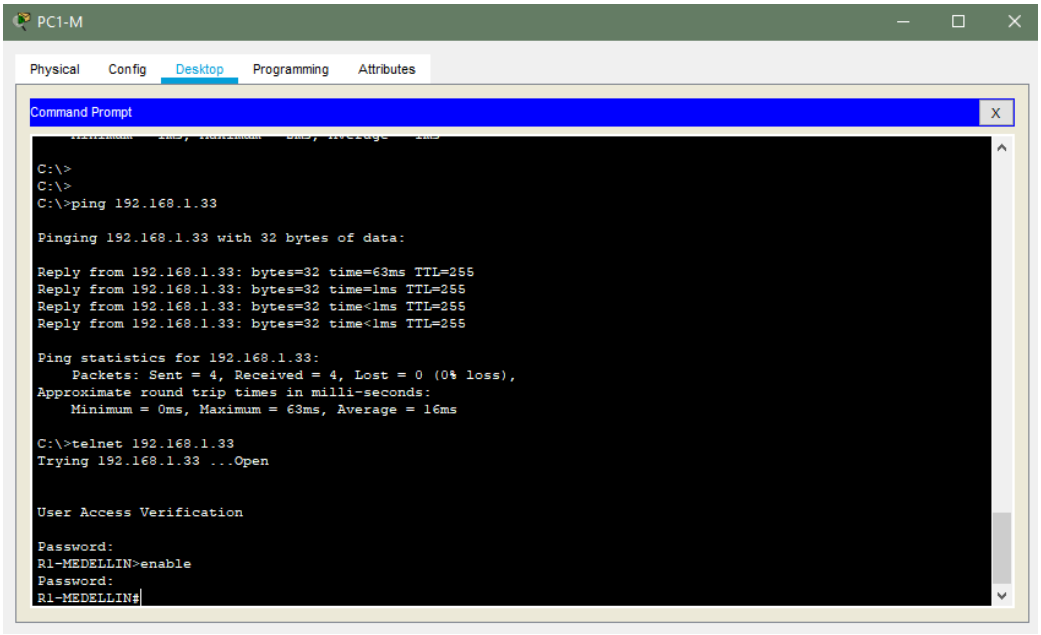


Ilustración 26 Creación de ACL (2019). Escenario 1

Comprobamos la configuración del Router de Bogotá desde el PC3-C.

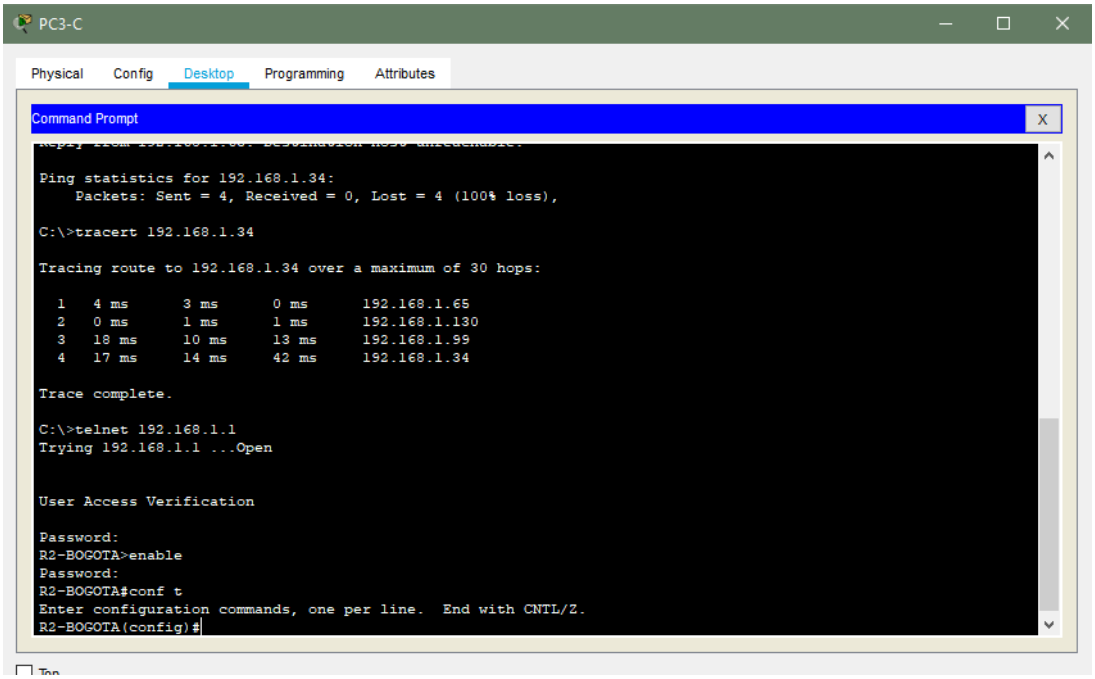


Ilustración 27 Creación de ACL (2019). Escenario 1

Comprobamos la configuración del Router de Cali desde el PC2-M.

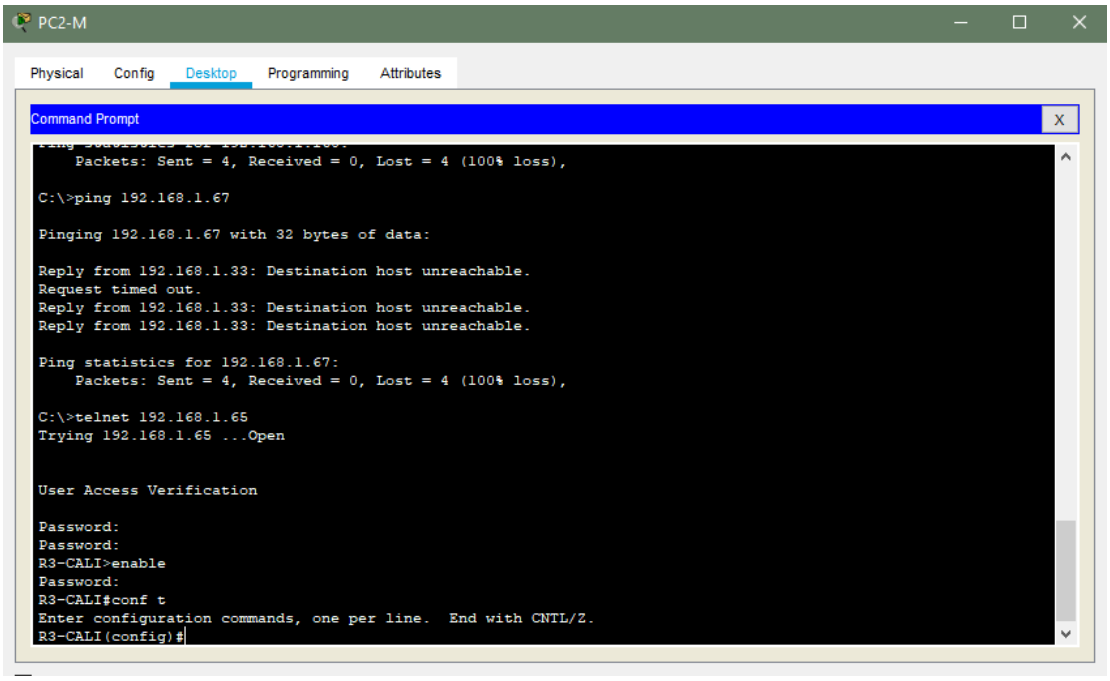


Ilustración 28 Creación de ACL (2019). Escenario 1

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.

Para el desarrollo de esta actividad utilizaremos una Lista de Control de Acceso o ACL (del inglés, Access Control List) es un concepto de seguridad informática usado para fomentar la separación de privilegios. Es una forma de determinar los permisos de acceso apropiados a un determinado objeto, dependiendo de ciertos aspectos del proceso que hace el pedido.

Utilizamos los siguientes comandos para configurar el ACL.

MEDELLIN

#>enable
#configure terminal
#acces-list 1 permit 192.168.1.2
#int fastethernet 0/0
#ip Access-group 1 out

CALI

#>enable
#configure terminal
#acces-list 1 permit 192.168.1.2
#int fastethernet 0/0
#ip Access-group 1 out

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.

MEDELLIN

#>enable
#configure terminal
#access-list 1 deny 192.168.1.66
#access-list 1 deny 192.168.1.67
#access-list 1 deny 192.168.1.3
#int fastethernet 0/0
#ip access-group 1 out

CALI

#>enable
#configure terminal
#access-list 1 deny 192.168.1.34
#access-list 1 deny 192.168.1.35

#access-list 1 deny 192.168.1.3
#int fastethernet 0/0
#ip access-group 1 out

2.6. Parte 5: Comprobación de la red instalada.

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

El PC1-M no tiene acceso a los dispositivos fuera de su red.

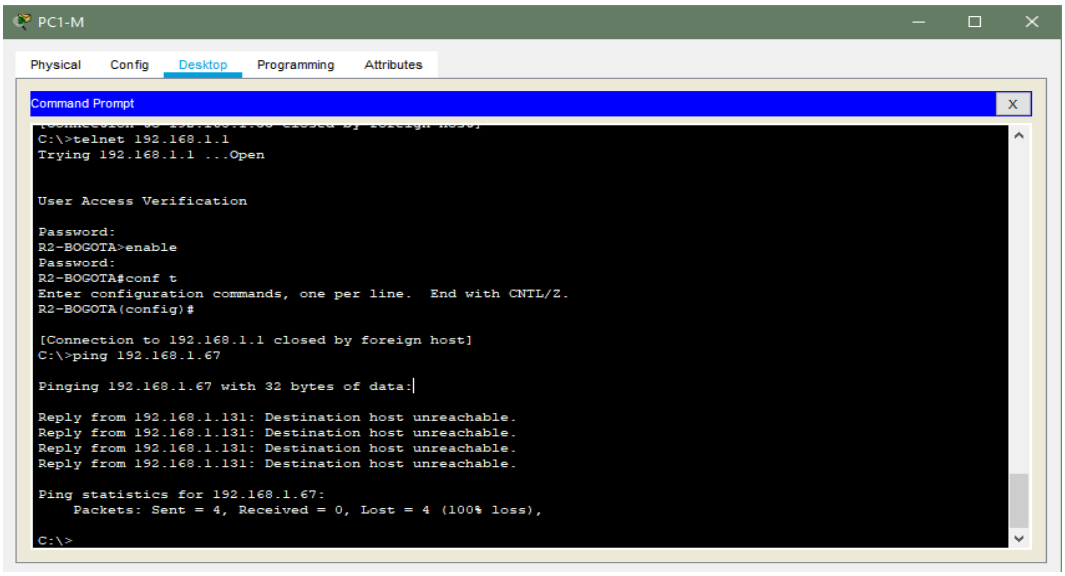
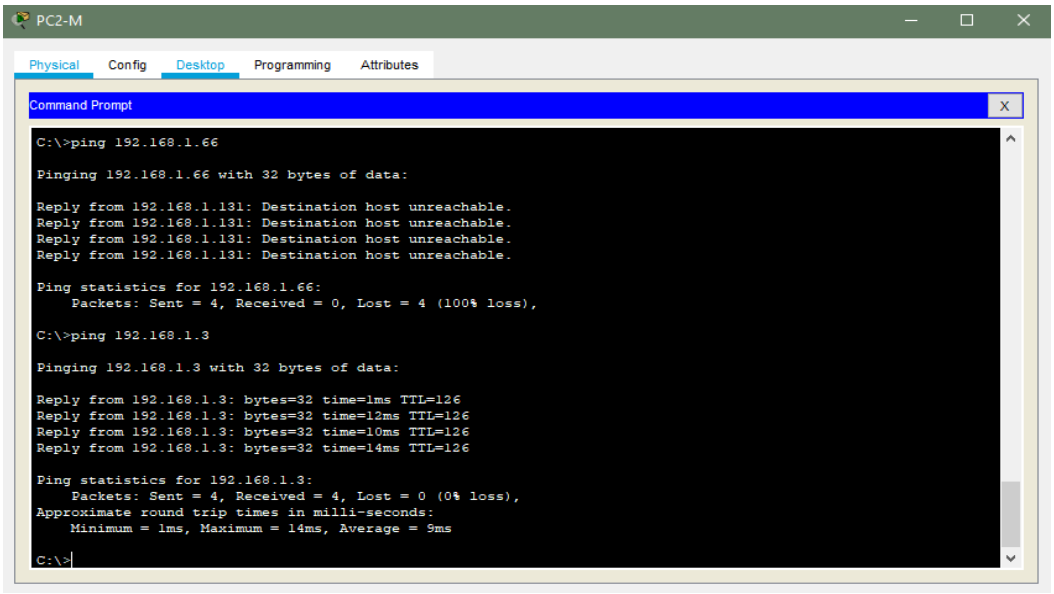


Ilustración 29 Creación de ACL (2019). Escenario 1

El PC2-M tiene acceso a los dispositivos dentro de su red.



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

	ORIGEN	DESTINO	RESULTADO
TELNET	Router MEDELLIN	Router CALI	successful
	WS_1	Router BOGOTA	successful
	Servidor	Router CALI	successful
	Servidor	Router MEDELLIN	successful
TELNET	LAN del Router MEDELLIN	Router CALI	successful
	LAN del Router CALI	Router CALI	successful
	LAN del Router MEDELLIN	Router MEDELLIN	successful
	LAN del Router CALI	Router MEDELLIN	successful
PING	LAN del Router CALI	WS_1	Fail
	LAN del Router MEDELLIN	WS_1	Fail
	LAN del Router MEDELLIN	LAN del Router CALI	Fail
PING	LAN del Router CALI	Servidor	successful
	LAN del Router MEDELLIN	Servidor	successful
	Servidor	LAN del Router MEDELLIN	successful
	Servidor	LAN del Router CALI	successful
	Router CALI	LAN del Router MEDELLIN	successful
	Router MEDELLIN	LAN del Router CALI	successful

3. 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.

3.1. Topología

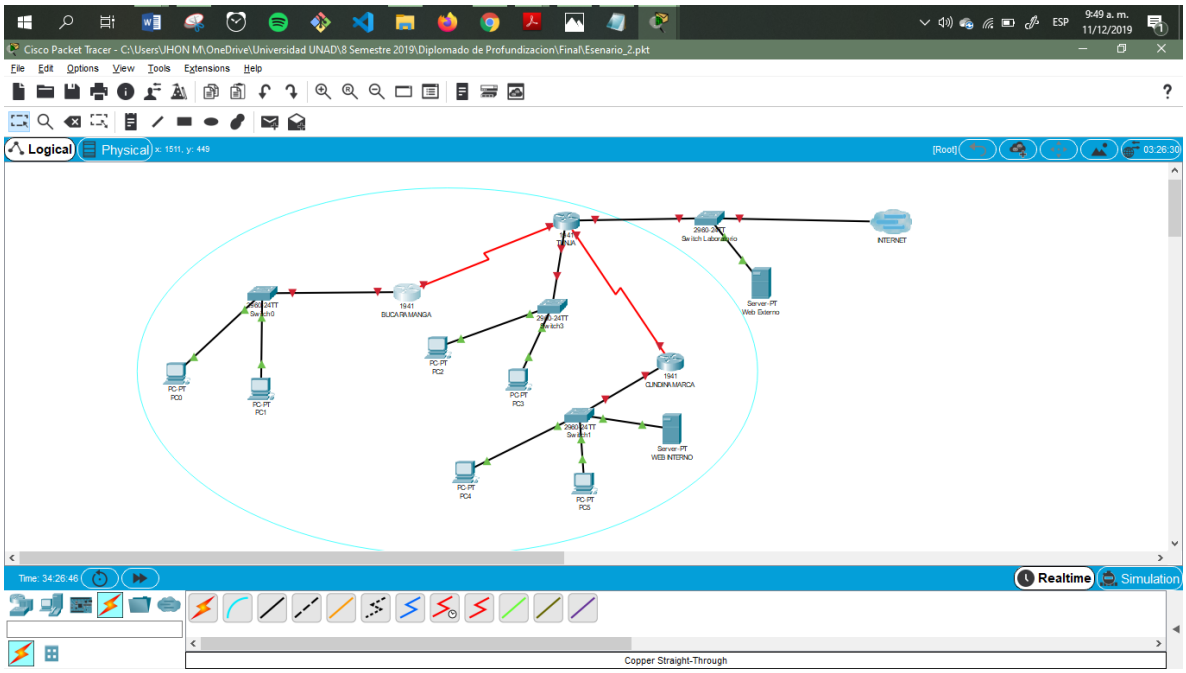


Ilustración 30 Topología Escenario 2 (2019). Escenario 2

3.2. Desarrollo

Los siguientes son los requerimientos necesarios:

3.3. Todos los routers deberán tener los siguiente:

Dispositivo	Interfaz	Dirección IP	Mascara de Sub Red	Gateway
R1-TUNJA	g0/0	172.31.2.1	255.255.255.248	
	g0/1	209.17.220.1	255.255.255.0	
	s0/0/0	172.31.2.33	255.255.255.252	
	s0/0/1	172.31.2.37	255.255.255.252	
R2-CUNDINAMARCA	g0/0	172.31.2.9	255.255.255.248	
	s0/0/0	172.31.2.38	255.255.255.252	
R3-BUCARAMANGA	g0/0	172.31.2.17	255.255.255.248	
	s0/0/0	172.31.2.34	255.255.255.252	

PC0		172.31.2.18	255.255.255.248	172.31.2.17
PC1		172.31.2.19	255.255.255.248	172.31.2.17
PC2		172.31.2.2	255.255.255.248	172.31.2.1
PC3		172.31.2.3	255.255.255.248	172.31.2.1
PC4		172.31.2.10	255.255.255.248	172.31.2.9
PC5		172.31.2.11	255.255.255.248	172.31.2.9
WEB EXTERNO		209.17.220.2	255.255.255.0	209.17.220.1
WEB INTERNO		172.31.2.12	255.255.255.248	172.31.2.9

3.3.1. Configuración básica.

ROUTER TUNJA

>enable
#configure terminal
#hostname R1-TUNJA
#enable secret cisco
#enable password cisco
#service password-encryption
#aaa new-model
#aaa authentication login LOCAL_AUTH local
#Username TUNJA privilege 7 password 123 network
#no ip domain-lookup
#banner motd “Acceso no autorizado”
#line con 0
#loggin synchronous
#line vty 0 15
#password cisco
#exit

#int g0/0
#ip address 172.31.2.1 255.255.255.248
#no shutdown

#int g0/1
#ip address 209.17.220.1 255.255.255.0
#no shutdown

#int s0/0/0
#ip address 172.31.2.33 255.255.255.252
#no shutdown

#int s0/0/1
#ip address 172.31.2.37 255.255.255.252

#no shutdown

ROUTER BUCARAMANGA

>enable
#configure terminal
#hostname R3- BUCARAMANGA
#enable secret cisco
#enable password cisco
#service password-encryption
#aaa new-model
#aaa authentication login LOCAL_AUTH local
#Username BUCARAMANGA privilege 7 password 123 network
#no ip domain-lookup
#banner motd “Acceso no autorizado”
#line con 0
#loggin synchronous
#line vty 0 15
#password cisco
#exit

#int g0/0
#ip address 172.31.2.17 255.255.255.248
#no shutdown

#int s0/0/0
#ip address 172.31.2.34 255.255.255.252
#no shutdown

ROUTER CUNDINAMARCA

>enable
#configure terminal
#hostname R2-CUNDINAMARCA
#enable secret cisco
#enable password cisco
#service password-encryption
#aaa new-model
#aaa authentication login LOCAL_AUTH local
#Username CUNDINAMARCA privilege 7 password 123 network
#no ip domain-lookup
#banner motd “Acceso no autorizado”
#line con 0
#loggin synchronous
#line vty 0 15

#password cisco
#exit

#int g0/0
#ip address 172.31.2.9 255.255.255.248
#no shutdown

#int s0/0/0
#ip address 172.31.2.38 255.255.255.252
#no shutdown

3.3.2. Autenticación local con AAA.

En seguridad informática, el acrónimo AAA corresponde a un tipo de protocolos que realizan tres funciones: autenticación, autorización y contabilización (en inglés, Authentication, Authorization and Accounting). La expresión protocolo AAA no se refiere pues a un protocolo en particular, sino a una familia de protocolos que ofrecen los tres servicios citados.

Antes de comenzar verificamos que el servidor tenga encendido los servicios SYSLOG, NTP y AAA que vamos a configurar.

Configuramos los servicios SYSLOG y NTP.

TUNJA

>enable
#configure terminal
#username administrador secret cisco 123
#aaa new-model
#aaa authentication login AUTH local
#line console 0
#login authentication AUTH
#line vty 0 15
#login authentication AUTH

BUCARAMANGA

>enable
#configure terminal
#username administrador secret cisco 123
#aaa new-model
#aaa authentication login AUTH local
#line console 0
#login authentication AUTH
#line vty 0 15
#login authentication AUTH

CUNDINAMARCA

>enable
#configure terminal
#username administrador secret cisco 123
#aaa new-model
#aaa authentication login AUTH local
#line console 0
#login authentication AUTH
#line vty 0 15
#login authentication AUTH

Nuestro servidor SYSLOG tiene registrado los mensajes de red.

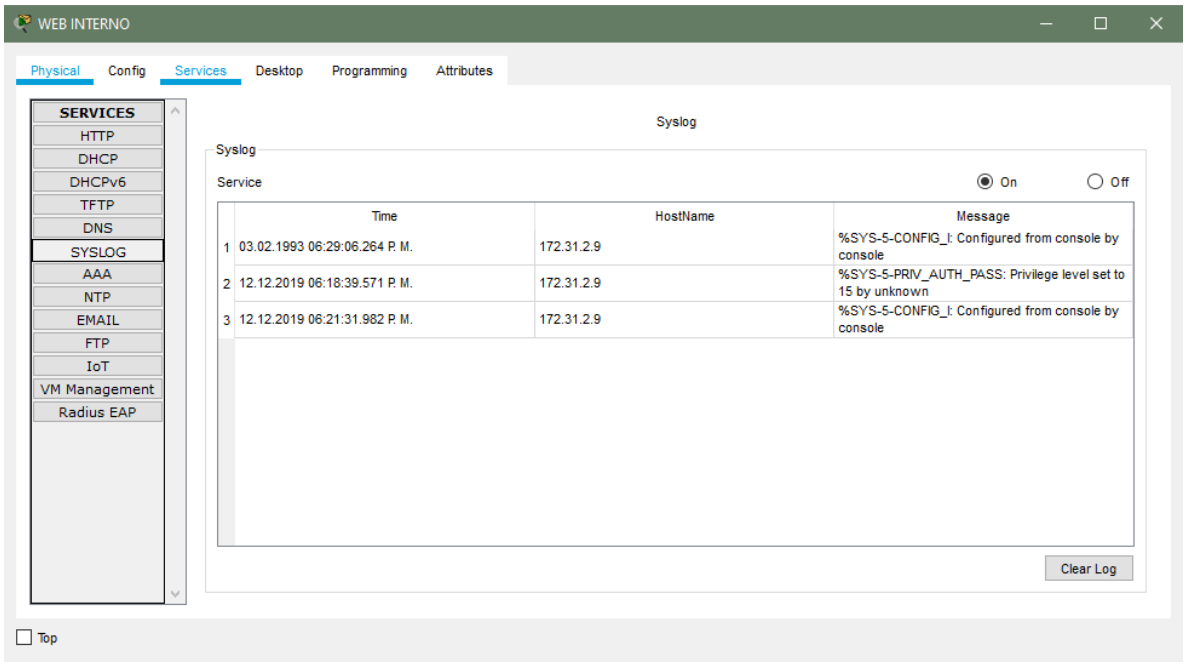


Ilustración 31 Autenticación AAA (2019). Escenario 2

Configuramos nuestro protocolo SSH.

SERVIDOR WEB INTERNO

#ip domain name clase.org
#ip ssh versión 2
#crypto key generate rsa
#tamaña 1024

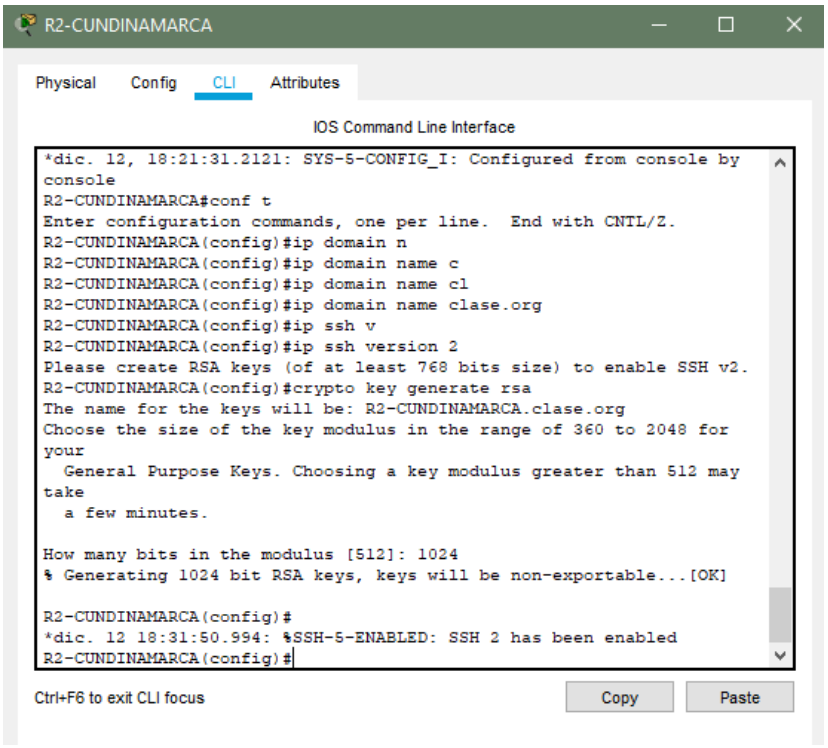


Ilustración 32 Autenticación AAA (2019). Escenario 2

Configuramos nuestro servicio AAA en local como remoto.

ROUTER CUDINAMARCA

#aaa new-model
#aaa authentication login REMOTO group radius local enable
#radius-server host 172.31.2.12 key 123456
#line vty 0 15
#transport input ssh
#login authentication REMOTO
#exit
#username usuario1 secret usuario1
#do wri

Configuramos nuestro servidor AAA, para esto autenticamos nuestro Router con nuestro servidor AAA.

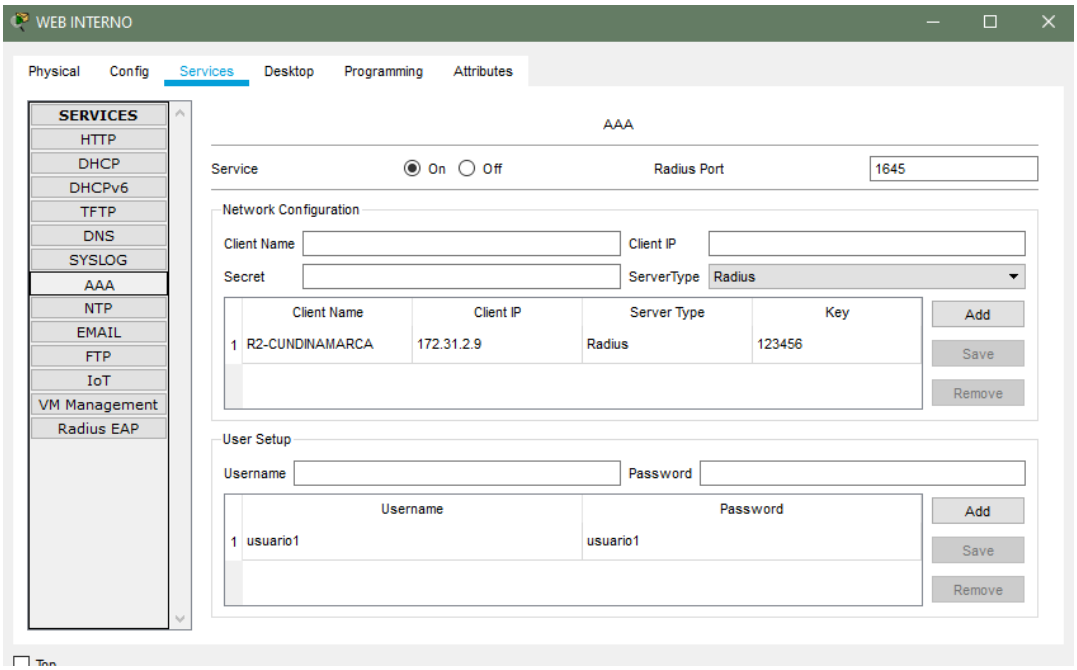


Ilustración 33 Autenticación AAA (2019). Escenario 2

Realizamos las pruebas de acceso desde el PC4 al Router.

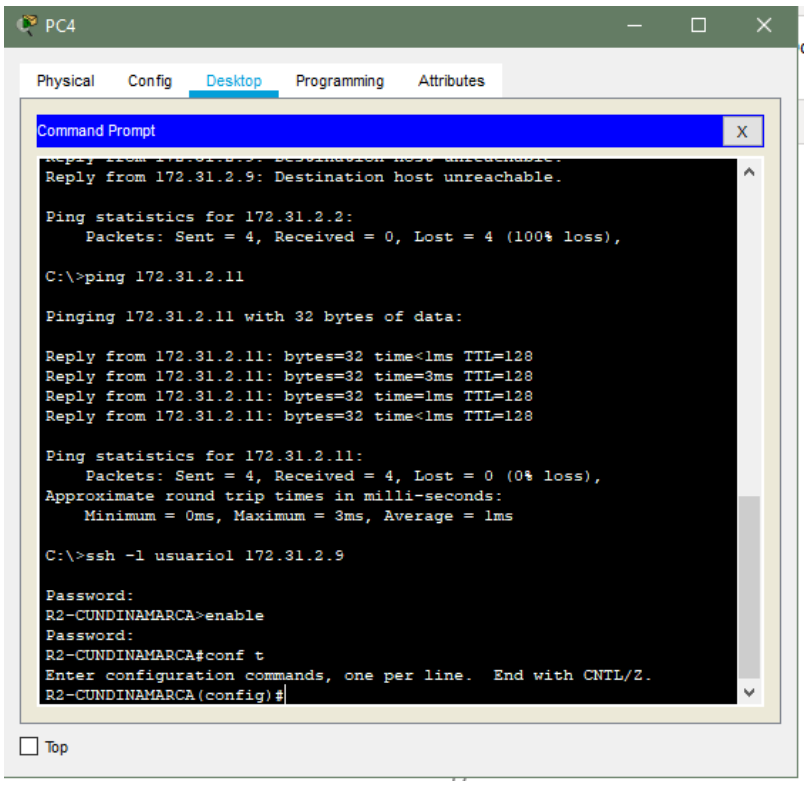


Ilustración 34 Autenticación AAA (2019). Escenario 2

3.3.3. Cifrado de contraseñas.

TUNJA

#service password-encryption

BUCARAMANGA

#service password-encryption

CUNDINAMARCA

#service password-encryption

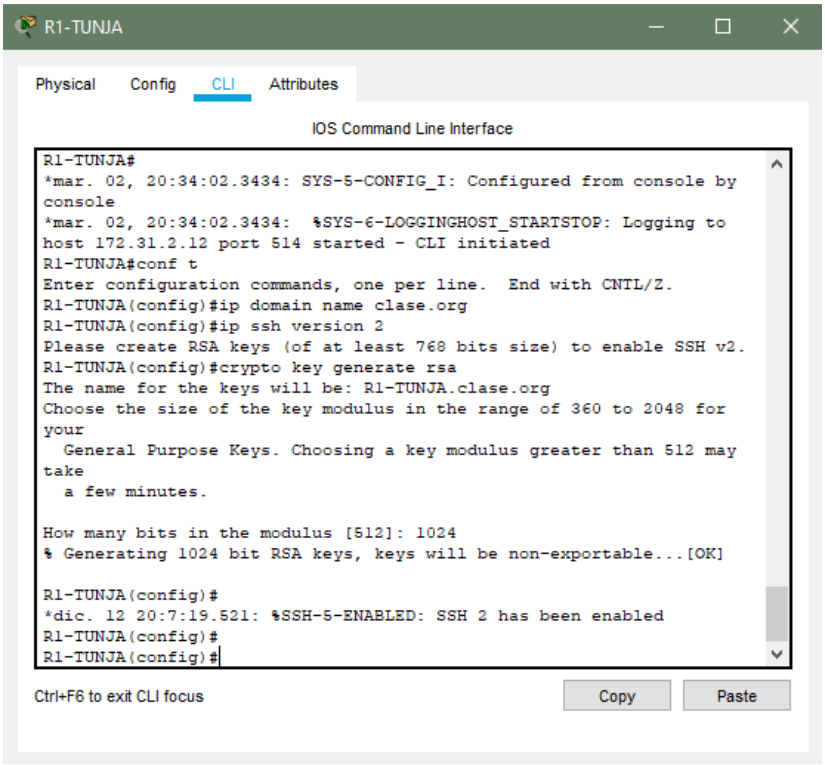


Ilustración 35 Cifrado de Contraseñas (2019). Escenario 2

3.3.4. Un Máximo de Intentos para Acceder al Router

TUNJA

#login block-for 5 attempts 4 within 60

BUCARAMANGA

#login block-for 5 attempts 4 within 60

CUNDINAMARCA

#login block-for 5 attempts 4 within 60

3.3.5. Máximo Tiempo de Acceso al Detectar Ataques

TUNJA

#login block-for 240 attempts 4 within 120

BUCARAMANGA

#login block-for 240 attempts 4 within 120

CUNDINAMARCA

#login block-for 240 attempts 4 within 120

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

TUNJA

#copy running-config startup-config
Destination filename [startup-config]?
Building configuration…
OK

CUNDINAMARCA

#copy running-config startup-config
Destination filename [startup-config]?
Building configuration…
OK

BUCARAMANGA

#copy running-config startup-config
Destination filename [startup-config]?
Building configuration…
OK

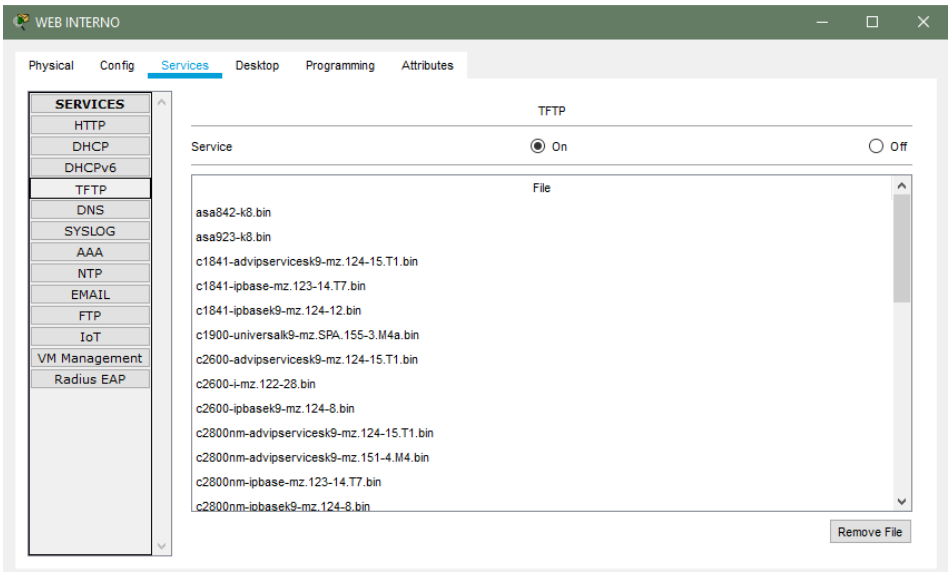


Ilustración 36 Servidor TFTP (2019). Escenario 2

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

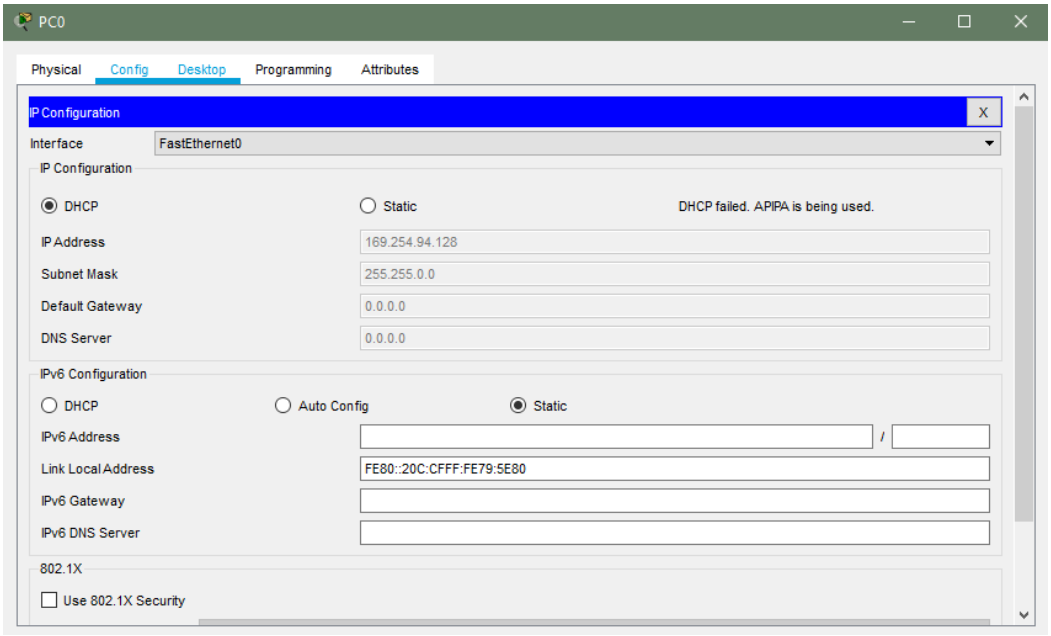


Ilustración 37 DHCP Bucaramanga y Cundinamarca (2019). Escenario 2

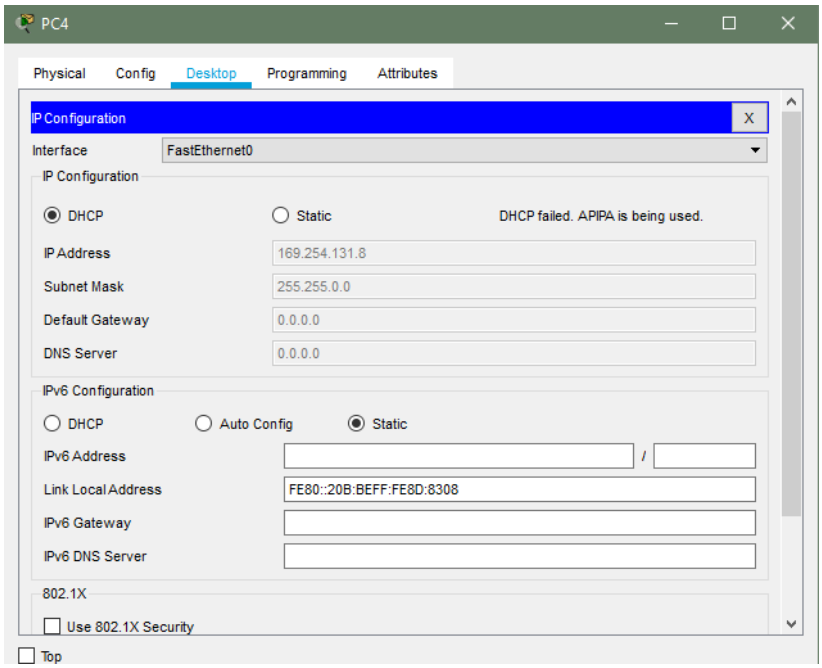


Ilustración 38 DHCP (2019). Escenario 2

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

NAT estático consiste en mapear una dirección IP privada con una dirección IP publica de forma estática. Para esto utilizaremos los siguientes comandos.

TUNJA

#in nat inside source static 172.31.2.12 255.255.255.248
#access-list 1 permit 172.0.0.0 0.255.255.255
#ip nat inside source list 1 interface g0/0 overload
#int g0/0
#ip nat outside
#int g0/1
#ip nat outside
#int s0/0/0
#ip nat outside
#int s0/0/1
#ip nat outside
#exit
#ip router 0.0.0.0 0.0.0.0 209.165.220.3
#router ospf 1
#default-information originate
#show ip route

Realizamos una prueba ping del Server Interno al Server Externo esta fue exitosa.

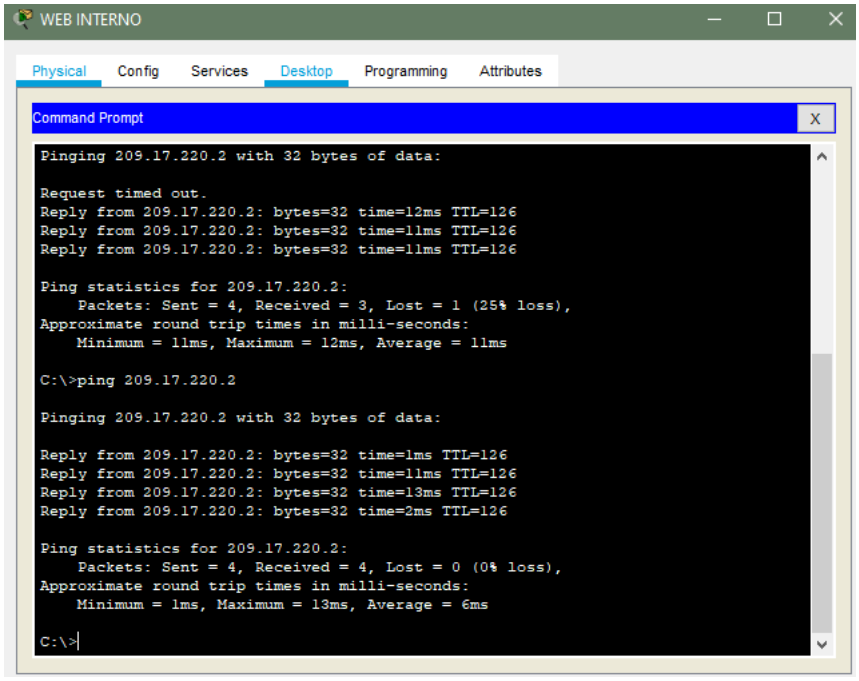


Ilustración 39 NAT Estático (2019). Escenario 2

Verificamos la configuración en el Router, podemos ver que la ip privada fue mapeada y una dirección pública.

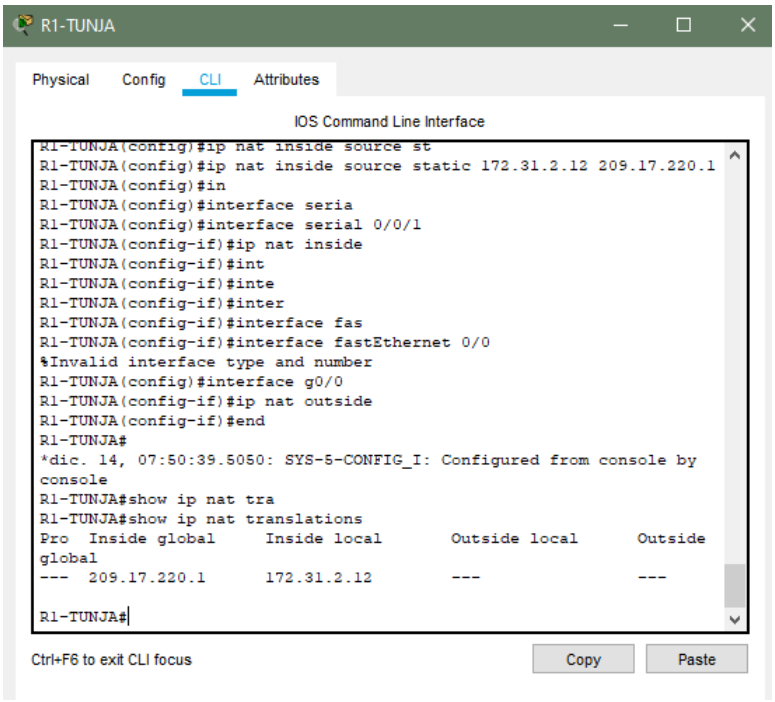


Ilustración 40 NAT Estático (2019). Escenario 2

Implementamos NAT de sobrecarga (PAT) para el resto de la red, utilizaremos los siguientes comandos.

#access-list 1 permit 172.31.2.16 0.0.0.7
#ip nat inside source list 1 interface g0/1 overload
#interface s0/0/0
#ip nat inside
#interface g0/1
#ip nat outside

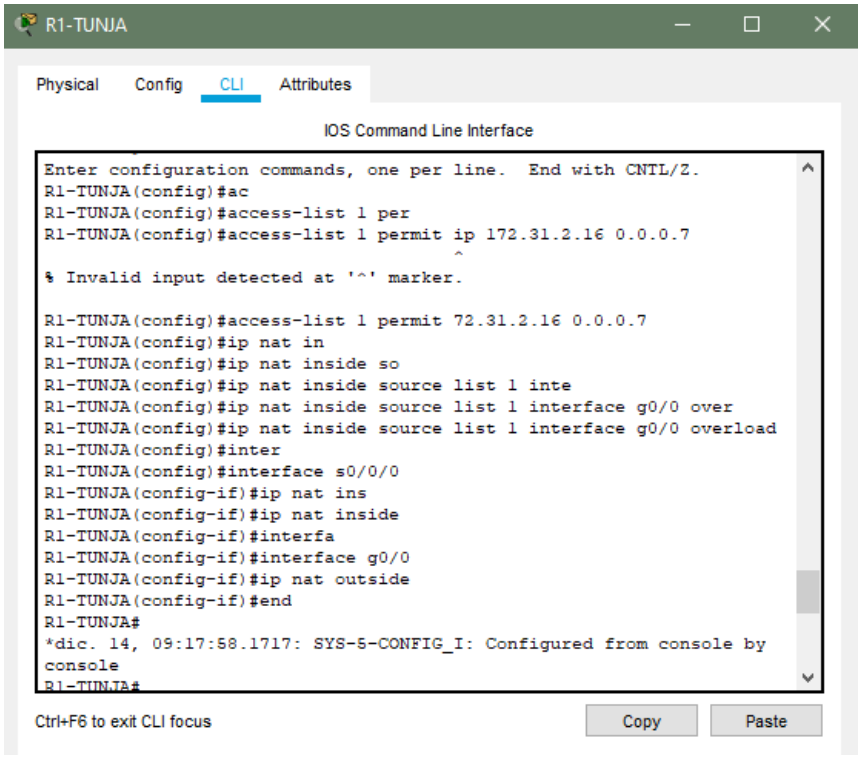


Ilustración 41 NAT Estático (2019). Escenario 2

6. EL Enrutamiento Deberá Tener Autenticación

TUNJA

>enable
#conf t
#int s0/0/0
#ip ospf authentication message-digest
#ip ospf message-digest-key 1 md5 cisco 123
#int s0/0/1
#ip ospf authentication message-digest
#ip ospf message-digest-key 1 md5 cisco 123

BUCARAMANGA

```
>enable
#conf t
#int s0/0/0
#ip ospf authentication message-digest
#ip ospf message-digest-key 1 md5 cisco 123
#int s0/0/1
#ip ospf authentication message-digest
#ip ospf message-digest-key 1 md5 cisco 123
```

CUNDINAMARCA

```
>enable
#conf t
#int s0/0/0
#ip ospf authentication message-digest
#ip ospf message-digest-key 1 md5 cisco 123
#int s0/0/1
#ip ospf authentication message-digest
#ip ospf message-digest-key 1 md5 cisco 123
```

7. Listas de control de acceso:

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

```
#enable
#configure terminal
#access-list 1 deny 172.31.2.16  0.0.0.7  209.165.220.0  0.0.0.255
#access-list 1 permit ip any
#interface s0/0/0
#ip access-group 1 out
```

Realizamos un ping a la red de BUCARAMANGA y el destino no es alcanzable.

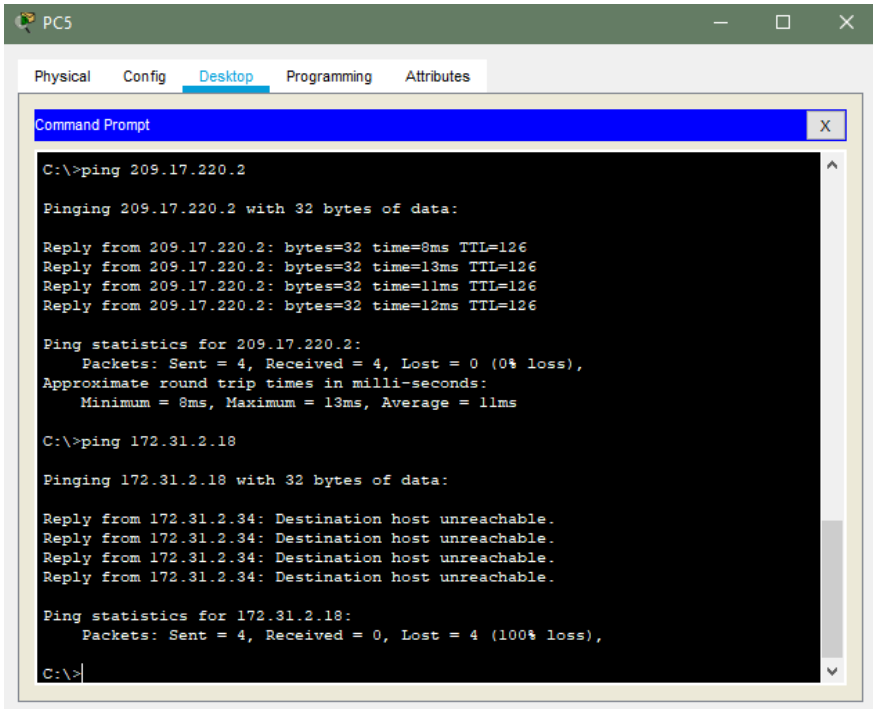


Ilustración 42 CLI ping red de Bucaramanga (2019). Escenario 2

Realizamos un ping a la red de TUNJA y este es exitoso.

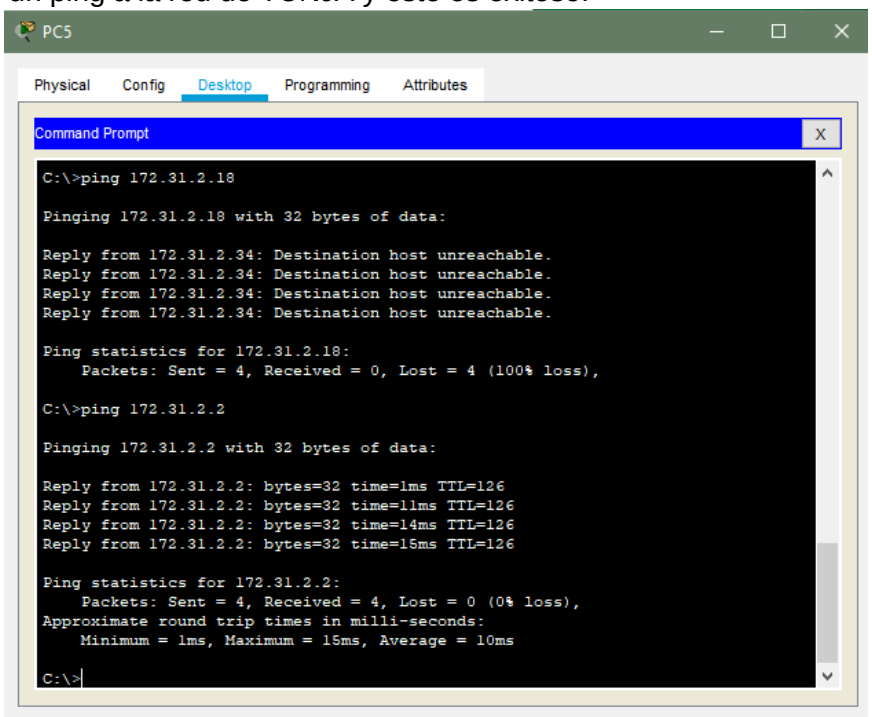


Ilustración 43 CLI ping red Tunja (2019). Escenario 2

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

  #enable
  #configure terminal
  #access-list 1 permit ip 172.31.2.8 0.0.0.7 209.165.220.0 0.0.0.255
  #access-list 1 deny any ip any
  #interface g0/0
  #ip access-group 1 out

Realizamos un ping al Servidor externo y este es satisfactorio.

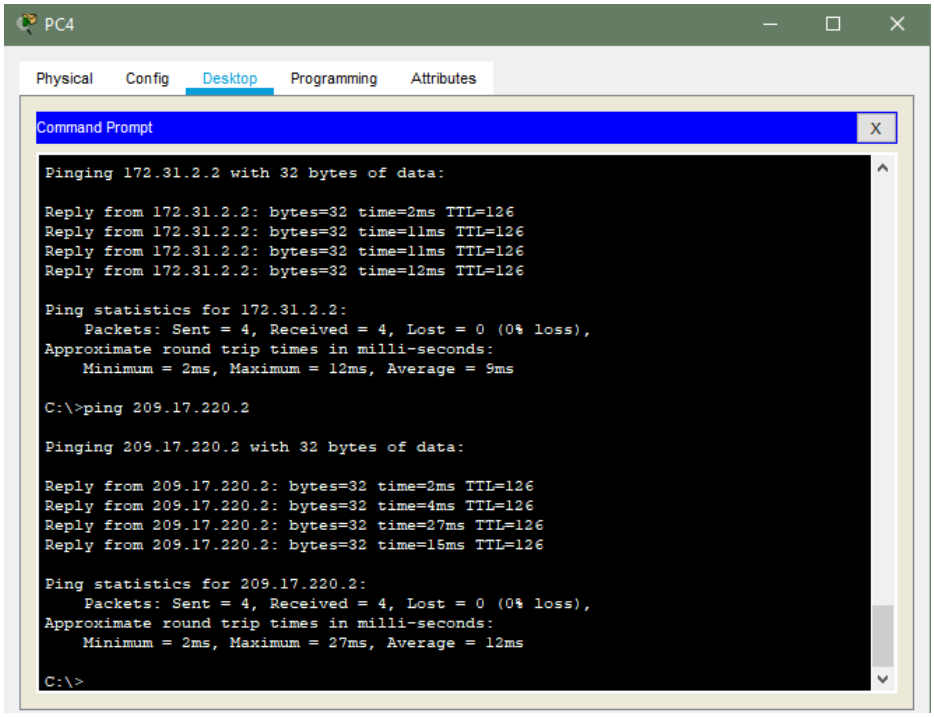


Ilustración 44 CLI Servidor Externo (2019). Escenario 2

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

  #enable
  #configure terminal
  #access-list 1 permit tcp 172.31.2.0 0.0.0.7 209.165.220 0.0.0.255 eq 80
  #access-list 1 permit tcp 172.31.2.0 0.0.0.7 209.165.220 0.0.0.255 eq 21
  #access-list 1 permit any
  #interface g0/0
  #ip access-group 1 out

Realizamos un ping al servidor interno y externo este es exitoso.

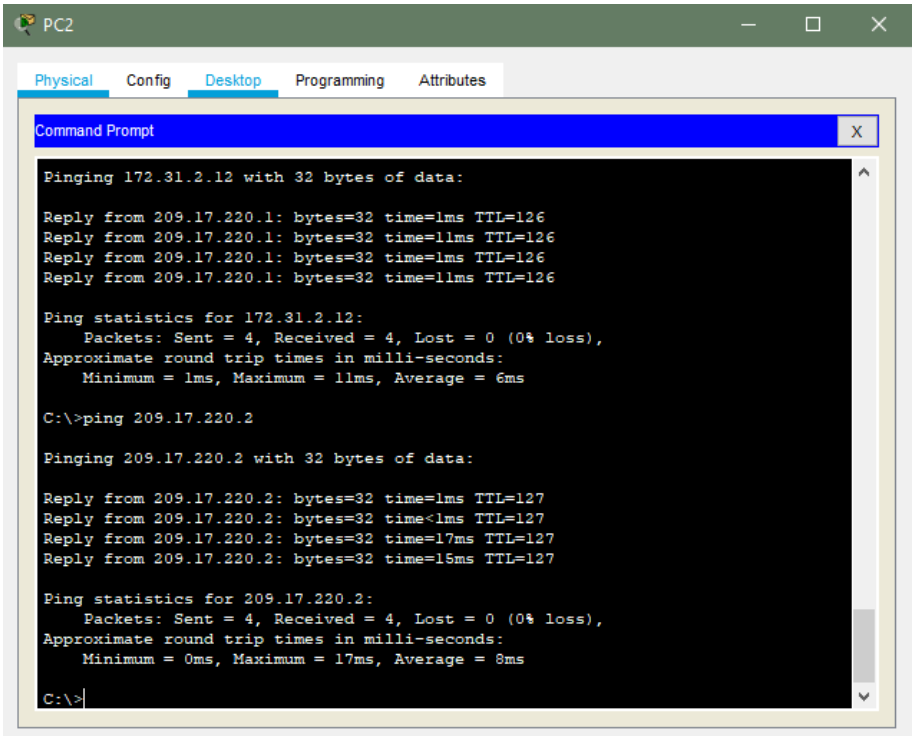


Ilustración 45 CLI ping al Servidor Interno (2019). Escenario 2

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

  #enable
  #configure terminal
  #access-list 1 permit ip 172.31.2.0 0.0.0.7 172.31.1.64 0.0.0.63
  #access-list 1 permit any
  #interface g0/1
  #ip access-group 1 out

Realizamos un ping a la red de Cundinamarca y Bucaramanga y este es exitoso.

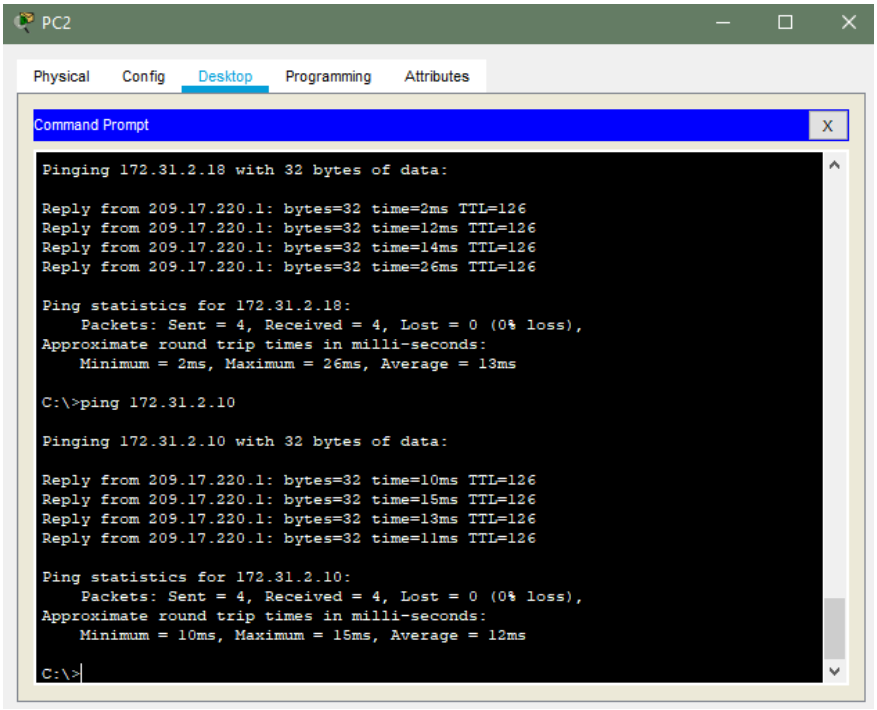


Ilustración 46 CLI ping red de Cundinamarca (2019). Escenario 2

- Los hosts de VLAN 30 de Bucaramanga acceden a internet y a cualquier equipo de VLAN 10.

  #enable
  #configure terminal
  #access-list 1 permit 172.31.2.0 0.0.0.7 209.165.220.0 0.0.0.255
  #access-list 1 permit any
  #interface g0/1
  #ip access-group 1 out

Realizamos un ping a internet y a la red y este es exitoso.

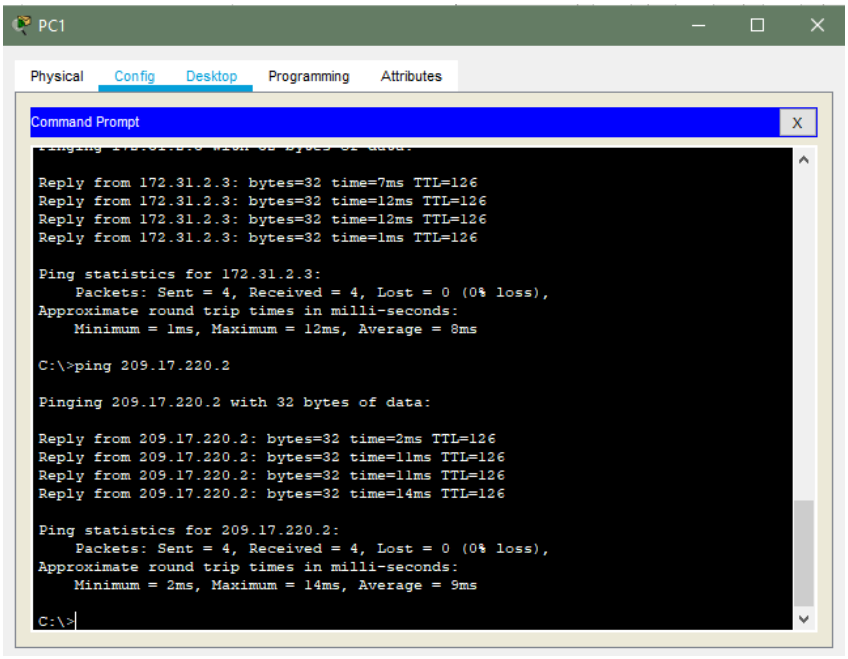


Ilustración 47 CLI ping a la red (2019). Escenario 2

CONCLUSIONES

- Gracias al desarrollo de este trabajo se logró reforzar habilidades y conocimientos en el mundo del Networking, con esto adquirimos la competencia suficiente para implementar redes empresariales básicas o con un cierto grado de dificultad que necesiten una buena administración configuración.

- Así mismo logramos evidenciar que estamos en la capacidad de comprender y dar solución a problemas que se van a presentar en nuestros futuros trabajos como administradores de redes.

- Podemos considerar que este diplomado es de gran importancia ya que nos profundiza sobre temas complejos en la implementación de redes empresariales, logrando así que tengamos una mayor comprensión y conocimiento en la resolución de problemas.

BIBLIOGRAFÍA

- *CISCO. (2014). Exploración de la red. Fundamentos de Networking. Recuperado de https://static-course-assets.s3.amazonaws.com/ITN50ES/module1/index.html#1.0.1.1*

- *CISCO. (2014). Configuración de un sistema operativo de red. Fundamentos de Networking. Recuperado de https://static-course-assets.s3.amazonaws.com/ITN50ES/module2/index.html#2.0.1.1*