CURSO DE PROFUNDIZACIÓN CISCO (Diseño e implementación de soluciones integradas LAN WAN) FUNDAMENTOS DE NETWORKING Y PRINCIPIOS DE ENRUTAMIENTO

Trabajo presentado por:
JUAN CAMILO CHAMORRO
GRUPO: 203092_5

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD-PASTO
FACULTAD DE CIENCIAS BASICAS TECNOLOGIA E INGENIERIA
INGENIERIA DE SISTEMAS
DICIEMBRE DEL 2019.

CURSO DE PROFUNDIZACIÓN CISCO (Diseño e implementación de soluciones integradas LAN WAN) FUNDAMENTOS DE NETWORKING Y PRINCIPIOS DE ENRUTAMIENTO

MONOGRAFIA DE GRADO PARA OPTAR EL TITULO PREFESIONAL

Trabajo presentado por:
JUAN CAMILO CHAMORRO
GRUPO: 203092_5

TUTOR
EFRAIN ALEJANDRO PEREZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
FACULTAD DE CIENCIAS BASICAS TECNOLOGIA E INGENIERIA
DICIEMBRE DEL 2019.

NOTA DE ACEPTACION

_____

_____

_____

_____

_____

_____
FIRMA

_____
FIRMA

_____
FIRMA

Esta nueva meta dentro de mi vida se la dedico a mi familia los cuales a lo largo de todos estos años de esfuerzo han sido siempre mi puntal y la fuerza para seguir adelante en esos momentos difíciles.

Estudiante:

_____

TABLA DE CONTENIDO

INTRODUCCION

Es importante los avances que se han tenido en los últimos años a nivel tecnológico e informático, la información cumple ahora un papel supremamente importante dentro de cualquier organización, ya que ahora se almacena, se analiza, se comparte y se reutiliza constantemente con el fin de analizar y proyectar. Por estas y muchas otras razones más es vita que como profesionales dentro de esta rama constantemente nos estemos actualizando y empapando de los nuevos avances en la misma. Es por esto que el desarrollo de este trabajo lo que busca es que logremos profundizar en los temas que a lo largo del presente Diplomado hemos abordado, y que mejor manera que a través del desarrollo de un caso ajustado a la vida real e implementando tecnologías de vanguardia que nos permitirán tener más posibilidades profesionalmente.

Realizaremos el diseño de 2 redes según unos parámetros claramente estipulados, de acuerdo a unas exigencias de cada una de estas organizaciones, mediremos claramente el grado de asimilación de conocimiento a lo largo de este semestre, va a ser la forma que nos midamos y sepamos cómo estamos preparados, debemos ser ingeniosos para afrontar la solución de redes de este tipo y lo mejor todo implementado bajo la tecnología de CISCO.

Todo el proceso de direccionamiento realizado en las 2 redes, se la va a desarrollar utilizando VLSM implementando tanto en IPV4 como en IPV6, además se implementaran diferentes protocolos de enrutamiento como EIGRP y OSPF los cuales permitan el intercambio de información entre las diferentes redes, nos brindes seguridad. Se implementan una serie de ACL los cuales nos permitirán tener un control total de cada uno de los espacios de nuestra red lo cual nos brindará una seguridad TOTAL.

1. JUSTIFICACION

Como profesionales dentro del campo de la tecnología y las telecomunicaciones es de vital importancia estar actualizados dentro de los nuevos avances y estar a la vanguardia en el manejo de las mismas.

Recordemos que estamos inmersos en un mercado laboral en el cual el que más éxito tendrá será le persona con mayor experiencia y mayor cantidad de conocimientos en su profesión.

Es trascendental que pongamos en práctica todo lo aprendido en este curso, y que mejor manera que a través del desarrollo de unos CASOS REALES por medio del cual logremos profundizar todos nuestros conocimientos, diseñando, simulando casos reales de empresas reales.

2. OBJETIVOS

2.1 OBJETIVO GENERAL

El objetivo principal de esta actividad es que a través del desarrollo de estos dos escenarios pongamos en práctica la temática que a lo largo del presente semestre hemos abordado para lo cual utilizaremos simuladores con el fin de verificar todo el proceso.

2.2 OBJETIVOS ESPECÍFICOS

- Profundizar en el manejo de la herramienta de simulación de PACKET TRACER sobre el cual tendremos que hacer el montaje de cada una de las 2 simulaciones y gracias al cual podremos verificar que el proceso desarrollado es correcto.
- Realizaremos todo el proceso de direccionamiento siguiendo las indicaciones de la guía aplicando para este tema VLSM.
- Verificar la conectividad de la red utilizando los comandos adecuados para este tema.
- Configurar protocolos de enrutamiento como EIGRP y OSPF.

Descripción de escenarios propuestos para la prueba de habilidades

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.

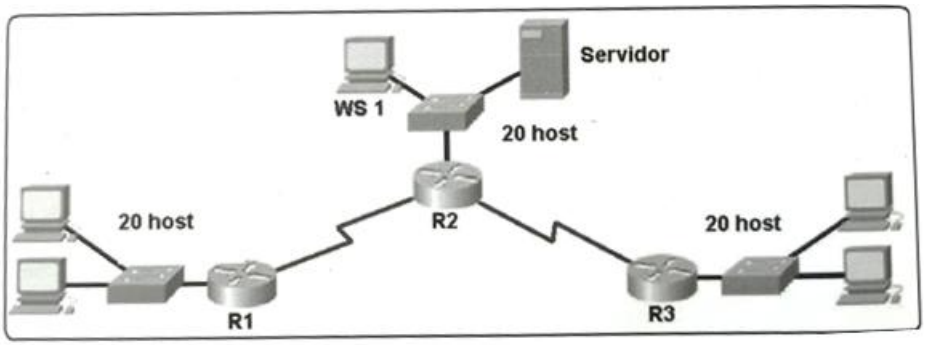
Parte 2: Considerar la asignación de los parámetros básicos y la detección de vecinos directamente conectados.

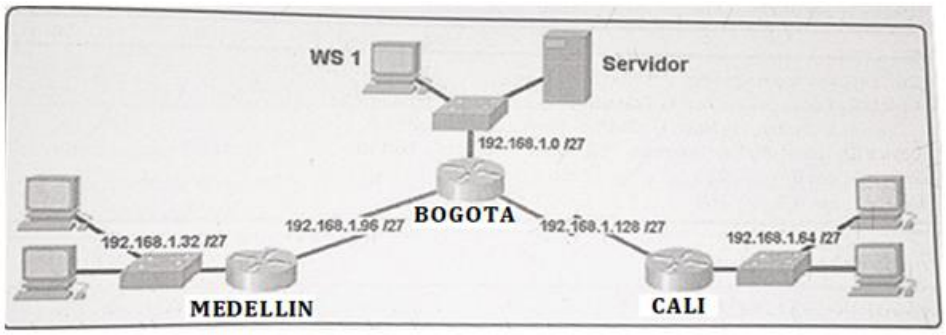
Parte 3: La red y subred establecidas deberán tener una interconexión total, todos los hosts deberán ser visibles y poder comunicarse entre ellos sin restricciones.

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.





Desarrollo

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 fisica de los equipos con base en la topología de red

Configurar la topología de red, de acuerdo con las siguientes especificaciones.

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.
b. Asignar una dirección IP a la red.

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 0/1		192.168.1.130	
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.
c. Verificar el balanceo de carga que presentan los routers.

d. Realizar un diagnóstico de vecinos uando el comando cdp.
e. Realizar una prueba de conectividad en cada tramo de la ruta usando Ping.

Parte 3: Configuración de Enrutamiento.

a. Asignar el protocolo de enrutamiento EIGRP a los routers considerando el direccionamiento diseñado.
b. Verificar si existe vecindad con los routers 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.
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.

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.**
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.
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.

Parte 5: Comprobación de la red instalada.

a. Se debe probar que la configuración de las listas de acceso fue exitosa.
b. Comprobar y Completar la siguiente tabla de condiciones de prueba para confirmar el óptimo funcionamiento de la red e.

	ORIGEN	DESTINO	RESULTADO
TELNET	Router MEDELLIN	Router CALI	
	WS_1	Router BOGOTA	
	Servidor	Router CALI	

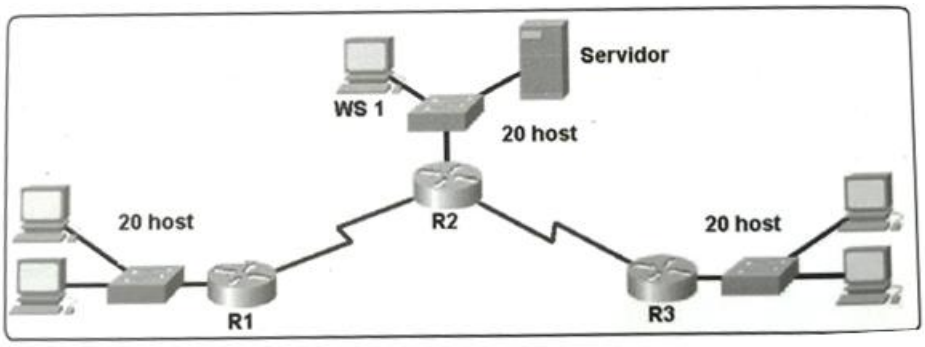
	Servidor	Router MEDELLIN	
TELNET	LAN del Router MEDELLIN	Router CALI	
	LAN del Router CALI	Router CALI	
	LAN del Router MEDELLIN	Router MEDELLIN	
	LAN del Router CALI	Router MEDELLIN	
PING	LAN del Router CALI	WS_1	
	LAN del Router MEDELLIN	WS_1	
	LAN del Router MEDELLIN	LAN del Router CALI	
PING	LAN del Router CALI	Servidor	
	LAN del Router MEDELLIN	Servidor	
	Servidor	LAN del Router MEDELLIN	
	Servidor	LAN del Router CALI	
	Router CALI	LAN del Router MEDELLIN	
	Router MEDELLIN	LAN del Router CALI	

DESARROLLO DEL ESCENARIO 1.

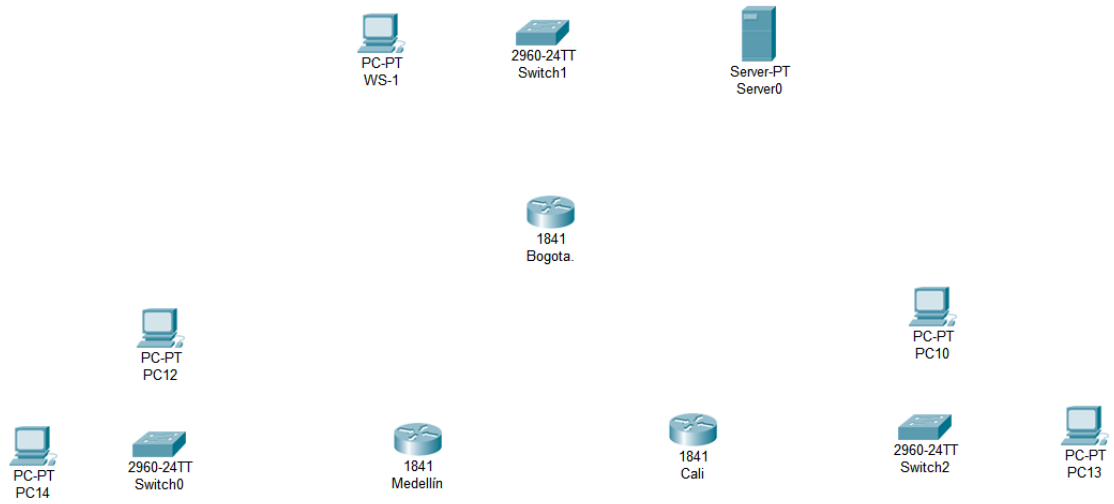
Realizar la conexión fisica de los equipos con base en la topología de red

ESCENARIO 1

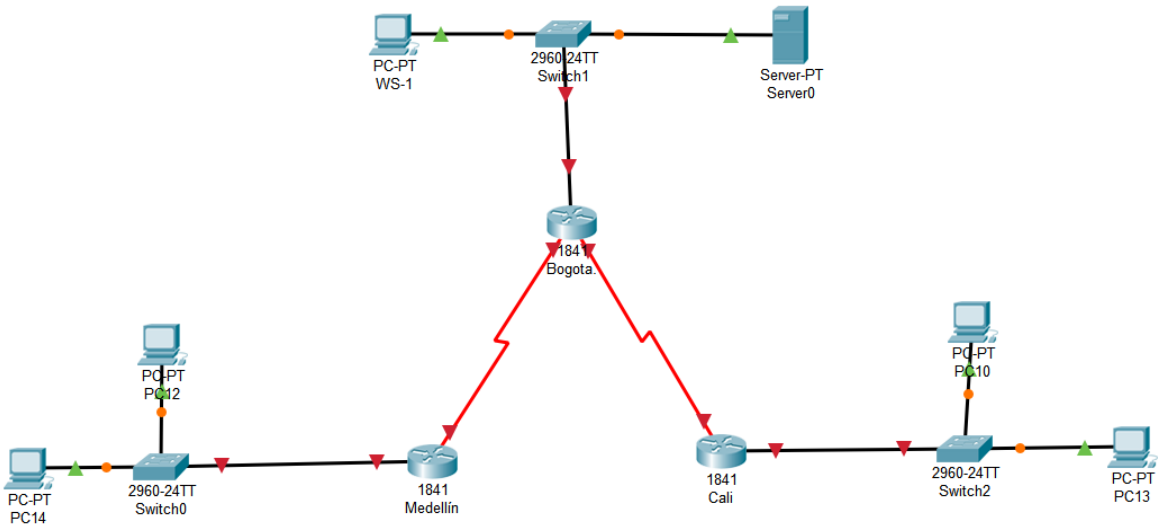
En este caso debemos proceder armar la topología según las indicaciones que se nos está entregando, para nuestro caso la topología 1:



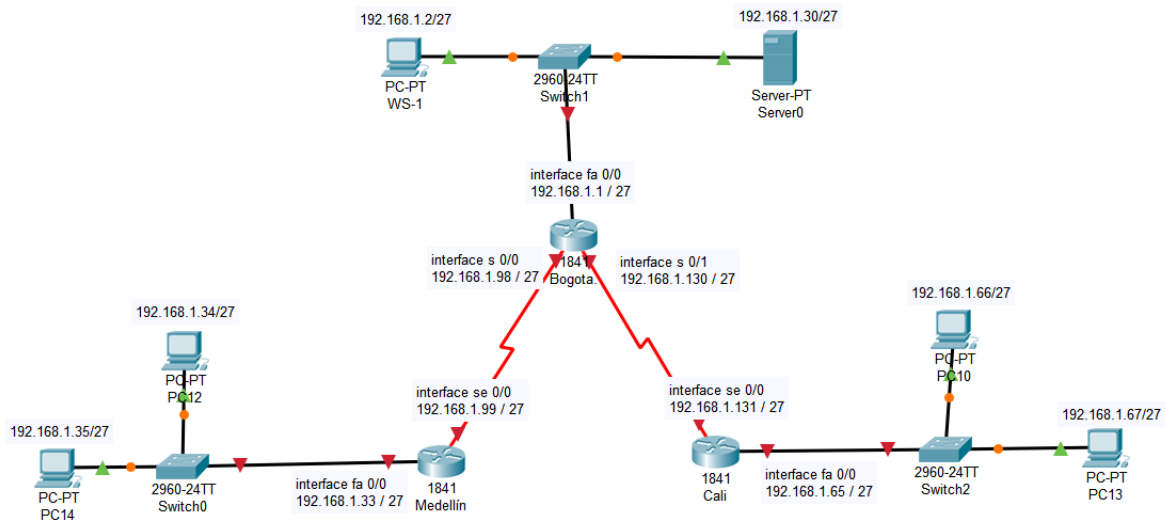
Procedemos entonces a distribuir los dispositivos según muestra la imagen:



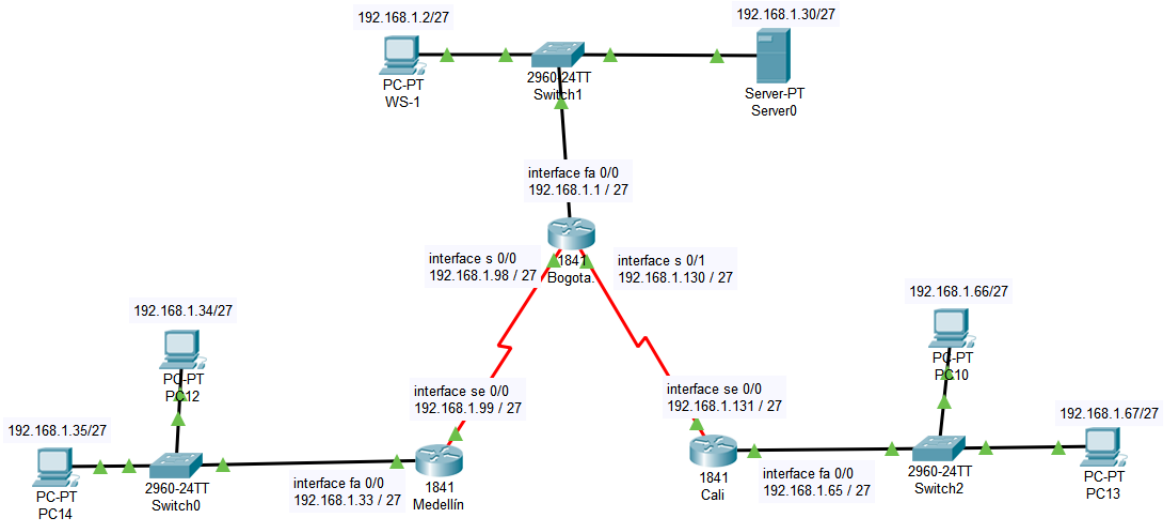
Como segundo paso debemos proceder a conectar los mismos empleando el cable adecuado y las interfaces adecuadas según la información suministrada:



Ya que tenemos conectados los mismos procedemos agrega la información necesaria con el fin de poder configurar los diferentes dispositivos e interfaces, de esta manera nos queda mas sencillo este proceso:



Por ultimo debemos proceder a configurar cada una de las interfaces, miramos que cada uno de los indicadores cambia a color verde.



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).

ROUTER BOGOTA

Router(config)#hostname BOGOTA

BOGOTA(config)#no ip domain-lookup

BOGOTA(config)#service password-encryption

BOGOTA(config)#banner motd $!! **SOLO PERSONAL DE LA EMPRESA - ACCESO DENEGADO**¡¡$

Configuramos las contraseñas:

BOGOTA(config)#enable secret class1

BOGOTA(config)#line console 0

BOGOTA(config-line)#password cisco1

BOGOTA(config-line)#login

BOGOTA(config-line)#line vty 0 15

BOGOTA(config-line)#password cisco1

BOGOTA(config-line)#login

ROUTER MEDELLIN

Router(config)#hostname MEDELLIN

MEDELLIN(config)#no ip domain-lookup

MEDELLIN(config)#service password-encryption

MEDELLIN(config)#banner motd $!! **SOLO PERSONAL DE LA EMPRESA - ACCESO DENEGADO**¡¡$

Configuramos las contraseñas

MEDELLIN(config)#enable secret class1

MEDELLIN(config)#line console 0

MEDELLIN(config-line)#password cisco1

MEDELLIN(config-line)#login

MEDELLIN(config-line)#line vty 0 15

MEDELLIN(config-line)#password cisco1

MEDELLIN(config-line)#login

ROUTER CALI

Router(config)#hostname CALI

CALI(config)#no ip domain-lookup

CALI(config)#service password-encryption

CALI(config)#banner motd $!! **SOLO PERSONAL DE LA EMPRESA - ACCESO DENEGADO**¡¡$

Configuramos las contraseñas

CALI(config)#enable secret class1

CALI(config)#line console 0

CALI(config-line)#password cisco1

CALI(config-line)#login

CALI(config-line)#line vty 0 15

CALI(config-line)#password cisco1

CALI(config-line)#login

Procedemos hacer el proceso con los SWITCH

SWITCH BOGOTA

Switch(config)#hostname switchbogota

switchbogota(config)#no ip domain-lookup

switchbogota(config)#service password-encryption

switchbogota(config)#banner motd $!! **SOLO PERSONAL DE LA EMPRESA - ACCESO DENEGADO**¡¡$

switchbogota(config)#enable secret class1

switchbogota(config)#line console 0

switchbogota(config-line)#password cisco1

switchbogota(config-line)#login

switchbogota(config-line)#line vty 0 15

switchbogota(config-line)#password cisco1

switchbogota(config-line)#login

SWITCH MEDELLIN

Switch#conf term

switchmedellin(config)#hostname switchmedellin

switchmedellin(config)#no ip domain-lookup

switchmedellin(config)#service password-encryption

switchmedellin(config)#banner motd $!! **SOLO PERSONAL DE LA EMPRESA - ACCESO DENEGADO**¡¡$

- Configuramos las ocntraseñas

switchmedellin(config)#enable secret class1

switchmedellin(config)#line console 0

switchmedellin(config-line)#password cisco1

switchmedellin(config-line)#login

switchmedellin(config-line)#line vty 0 15

switchmedellin(config-line)#password cisco1

switchmedellin(config-line)#login

SWITCH CALI

Switch(config)#hostname switchcali

switchcali(config)#no ip domain-lookup

switchcali(config)#service password-encryption

switchcali(config)#banner motd $!! **SOLO PERSONAL DE LA EMPRESA - ACCESO DENEGADO**¡¡$

- Configuramos las contraseñas

```
switchcali(config)#enable secret class1
switchcali(config)#line console 0
switchcali(config-line)#password cisco1
switchcali(config-line)#login
switchcali(config-line)#line vty 0 15
switchcali(config-line)#password cisco1
switchcali(config-line)#login
switchcali(config-line)#
```

Configurar la topología de red, de acuerdo con las siguientes especificaciones.

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.

- BOGOTA-LAN 192.168.1.0/27
- Medellín-LAN 192.168.1.32/27
- CALI-LAN 192.168.1.64/27
- BOGOTA-Medellín 192.168.1.96/27
- BOGOTA-CALI 192.168.1.128/27
- Disponible 192.168.1.160/27
- Disponible 192.168.1.192/27
- Disponible 192.168.1.224/27

b. Asignar una dirección IP a la red.

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	192.168.1.231
Dirección de Ip en interfaz Serial 0/1		192.168.1.130	
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

Según la tabla de enrutamiento procedemos a configurar cada una de las interfaces:

MEDELLIN	interface serial 0/0	192.168.1.99	255.255.255.224
	interface fa 0/0	192.168.1.33	255.255.255.224
BOGOTA	interface serial 0/0	192.168.1.98	255.255.255.224
	interface serial 0/1	192.168.1.130	255.255.255.224
	interface fa 0/0	192.168.1.1	255.255.255.224

CALI	interface serial 0/0	192.168.1.131	255.255.255.224
	interface fa 0/0	192.168.1.65	255.255.255.224

De una vez configuramos las PC:

MEDELLIN	PC12	192.168.1.34	255.255.255.224	192.168.1.33
MEDELLIN	PC14	192.168.1.35	255.255.255.224	192.168.1.33
CALI	PC10	192.168.1.66	255.255.255.224	192.168.1.65
CALI	PC13	192.168.1.67	255.255.255.224	192.168.1.65
BOGOTA	WS-1	192.168.1.2	255.255.255.224	192.168.1.1
BOGOTA	SERVER	192.168.1.30	255.255.255.224	192.168.1.1

Configuración Interfaces Router Bogotá.

BOGOTA(config)#int s0/0/0

BOGOTA(config-if)#ip address 192.168.1.98 255.255.255.224

BOGOTA(config-if)#no shutdown

BOGOTA(config-if)#int s0/0/1

BOGOTA(config-if)#ip address 192.168.1.130 255.255.255.224

BOGOTA(config-if)#no shutdown

BOGOTA(config-if)#int f0/0

BOGOTA(config-if)#ip address 192.168.1.1 255.255.255.224

BOGOTA(config-if)#no shutdown

Configuración Interfaces Router Medellín.

MEDELLIN(config)#int s0/0/0

MEDELLIN(config-if)#ip address 192.168.1.99 255.255.255.224

MEDELLIN(config-if)#no shutdown

MEDELLIN(config-if)#int f0/0

MEDELLIN(config-if)#ip address 192.168.1.33 255.255.255.224

MEDELLIN(config-if)#no shutdown

Configuración Interfaces Router CALI.

CALI(config)#int s0/0/0

CALI(config-if)#ip address 192.168.1.231 255.255.255.224

CALI(config-if)#no shutdown

CALI(config-if)#int f0/0

CALI(config-if)#ip address 192.168.1.65 255.255.255.224

CALI(config-if)#no shutdown

Procedemos a verificar la configuración ingresada en cada una de las interfaces del router:

MEDELLIN>

MEDELLIN>enable

MEDELLIN#show ip interface brief

Interface IP-Address OK? Method Status Protocol

FastEthernet0/0 192.168.1.33 YES manual up up

FastEthernet0/1 unassigned YES NVRAM administratively down down

Serial0/0/0 192.168.1.99 YES manual up up

Serial0/0/1 unassigned YES NVRAM administratively down down

Vlan1 unassigned YES unset administratively down down

MEDELLIN#

bogota#

bogota#show ip interface brief

Interface IP-Address OK? Method Status Protocol

FastEthernet0/0 192.168.1.1 YES manual up up

FastEthernet0/1 unassigned YES NVRAM administratively down down

Serial0/0/0 192.168.1.98 YES manual up up

Serial0/0/1 192.168.1.130 YES manual up up

Vlan1 unassigned YES unset administratively down down

bogota#

cali#

cali#show ip interface brief

Interface IP-Address OK? Method Status Protocol

FastEthernet0/0 192.168.1.65 YES manual up up

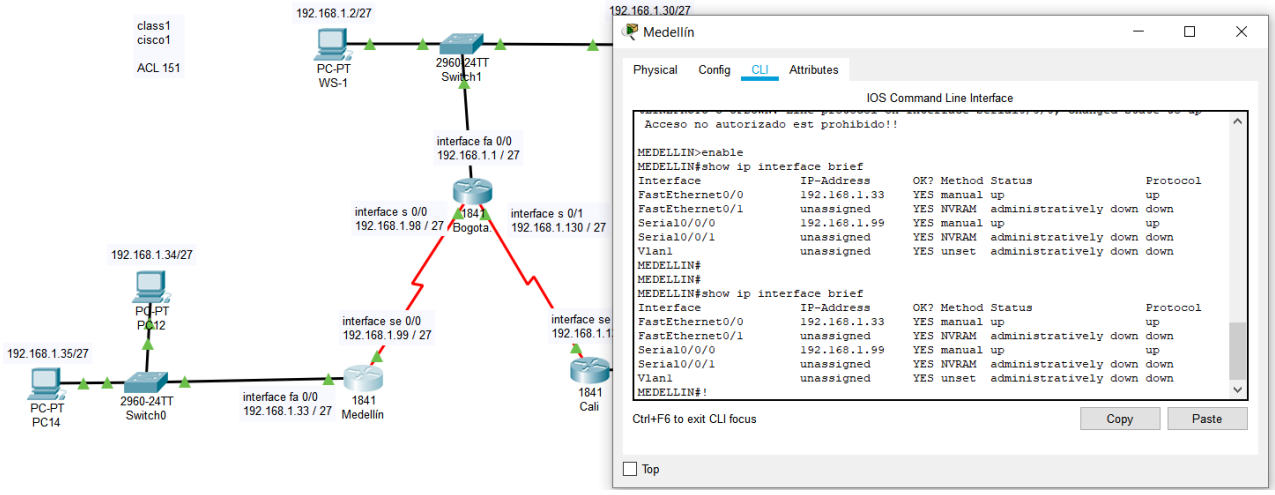
FastEthernet0/1 unassigned YES NVRAM administratively down down

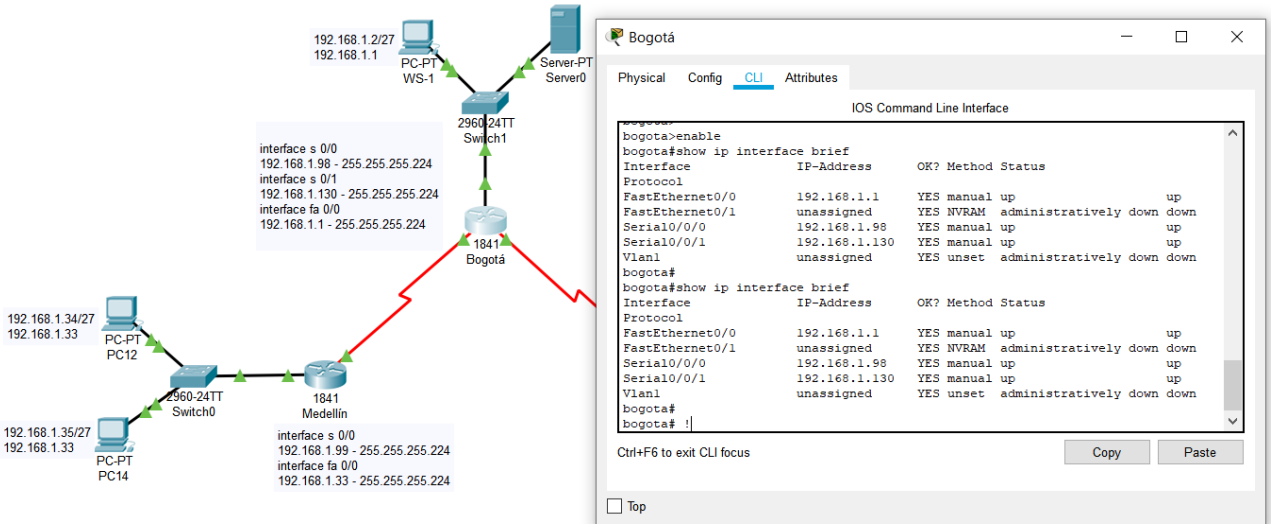
Serial0/0/0 192.168.1.131 YES manual up up

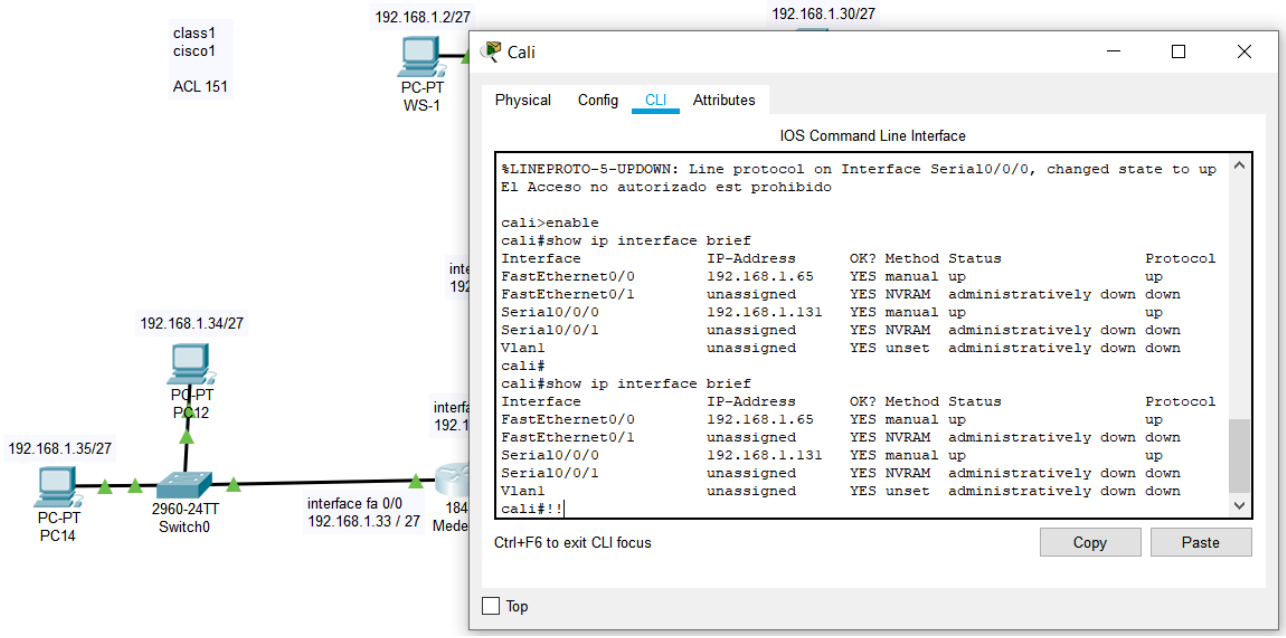
Serial0/0/1 unassigned YES NVRAM administratively down down

Vlan1 unassigned YES unset administratively down down

cali#



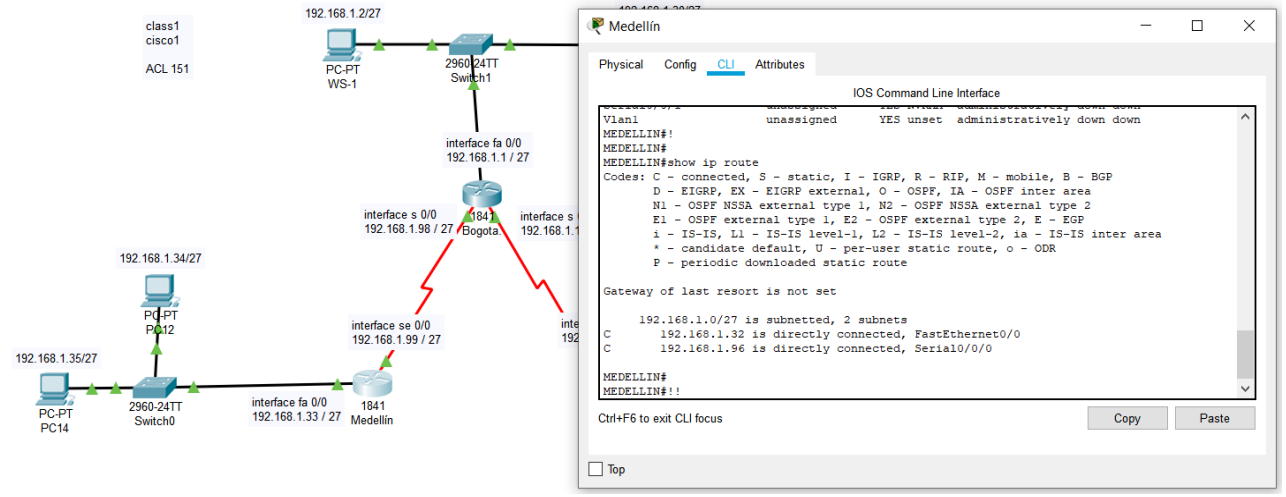


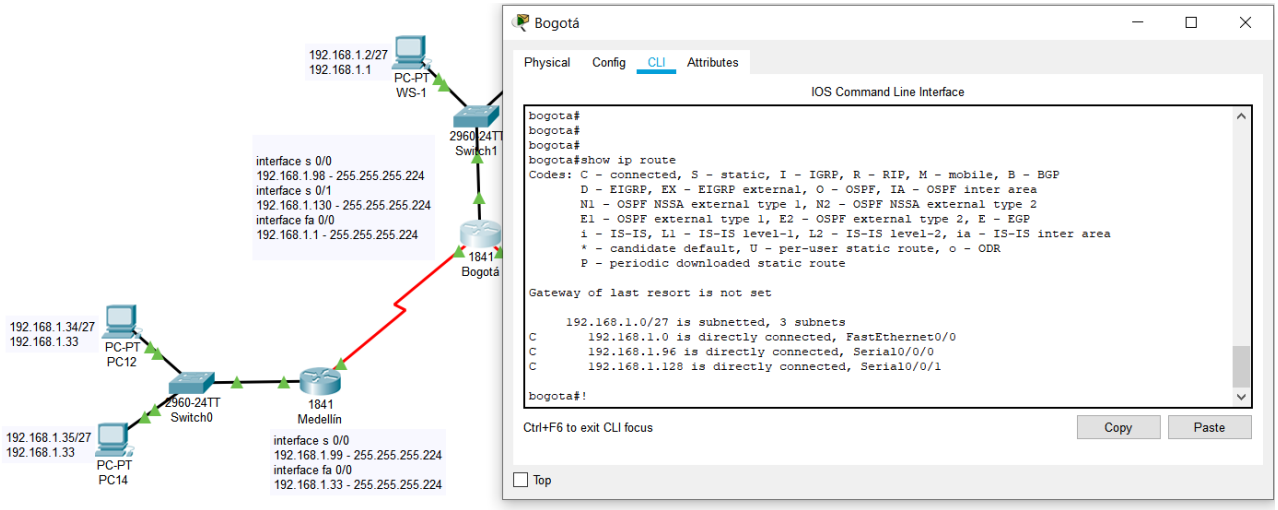


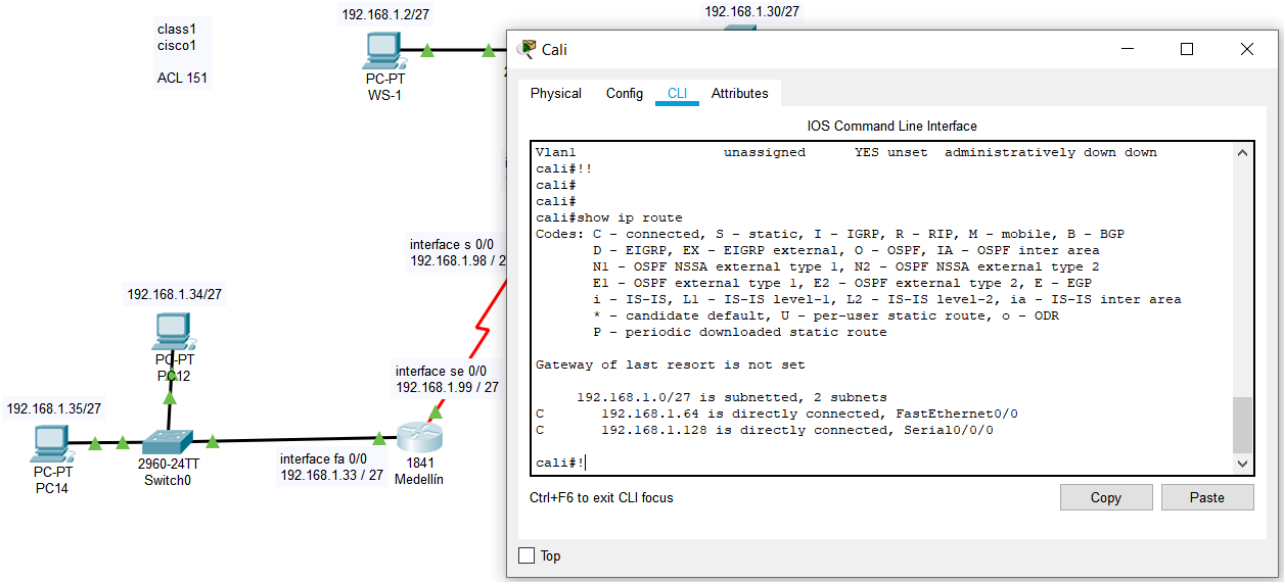
Hemos verificado que las interfaces están bien configurados.

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.

Analizamos las tablas de enrutamiento.

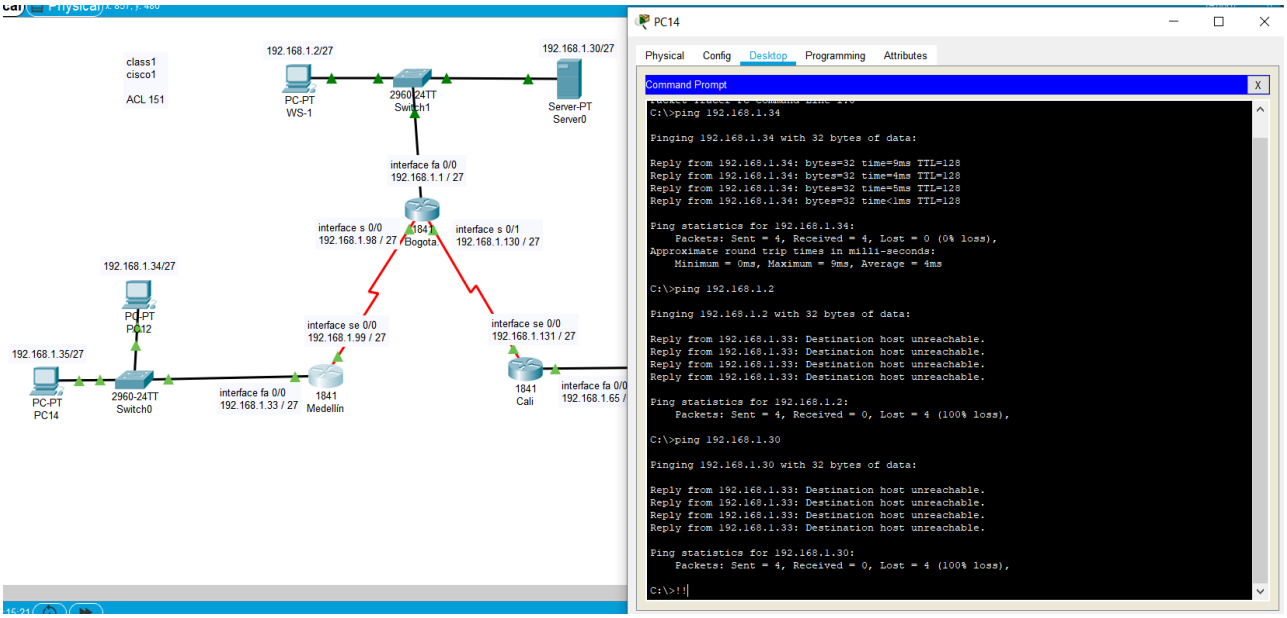






En este caso solo tenemos rutas para las redes conectadas directamente.

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



Según el resultado que tenemos observamos que solo podemos tener concetividad con las redes vecinas.

Parte 3: Configuración de Enrutamiento.

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

Configuración Interfaces Router Bogotá.

BOGOTA(config-if)#router eigrp 200

BOGOTA(config-router)#no auto-summary

BOGOTA(config-router)#network 192.168.1.0

Configuración Interfaces Router Medellín.

MEDELLIN(config-if)#router eigrp 200

MEDELLIN(config-router)#no auto-summary

MEDELLIN(config-router)#network 192.168.1.0

Configuración Interfaces Router CALI.

CALI(config-if)#router eigrp 200

CALI(config-router)#no auto-summary

CALI(config-router)#network 192.168.1.0

A medida que hagamos la configuración del protocolo EIGRP se van generando las adyacencias, hecho el paso anterior debemos proceder a verificar que cada router cuente con una ruta para cada una de las subredes.

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

SHOW IP EIGRP NEIGHBOR

BOGOTA#show ip eigrp neighbor

IP-EIGRP neighbors for process 200

H Address Interface Hold Uptime SRTT RTO Q Seq

(sec) (ms) Cnt Num

0 192.168.1.99 Se0/0/0 13 00:04:34 40 1000 0 7

1 192.168.1.231 Se0/0/1 12 00:03:31 40 1000 0 7

MEDELLIN#show ip eigrp neighbor

IP-EIGRP neighbors for process 200

H Address Interface Hold Uptime SRTT RTO Q Seq

(sec) (ms) Cnt Num

0 192.168.1.98 Se0/0/0 11 00:04:40 40 1000 0 7

CALI#show ip eigrp neighbor

IP-EIGRP neighbors for process 200

H Address Interface Hold Uptime SRTT RTO Q Seq

(sec) (ms) Cnt Num

0 192.168.1.130 Se0/0/0 12 00:03:47 40 1000 0 8

SHOW IP EIGRP TOPOLOGY

BOGOTA#show ip eigrp topology

IP-EIGRP Topology Table for AS 200/ID(192.168.1.130)

Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,

r - Reply status

P 192.168.1.0/27, 1 successors, FD is 28160

via Connected, FastEthernet0/0

P 192.168.1.32/27, 1 successors, FD is 2172416

via 192.168.1.99 (2172416/28160), Serial0/0/0

P 192.168.1.64/27, 1 successors, FD is 2172416

via 192.168.1.231 (2172416/28160), Serial0/0/1

P 192.168.1.96/27, 1 successors, FD is 2169856

via Connected, Serial0/0/0

P 192.168.1.128/27, 1 successors, FD is 2169856

via Connected, Serial0/0/1

MEDELLIN#show ip eigrp topology

IP-EIGRP Topology Table for AS 200/ID(192.168.1.99)

Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,

r - Reply status

P 192.168.1.0/27, 1 successors, FD is 2172416

via 192.168.1.98 (2172416/28160), Serial0/0/0

P 192.168.1.32/27, 1 successors, FD is 28160

via Connected, FastEthernet0/0

P 192.168.1.64/27, 1 successors, FD is 2684416

via 192.168.1.98 (2684416/2172416), Serial0/0/0

P 192.168.1.96/27, 1 successors, FD is 2169856

via Connected, Serial0/0/0

P 192.168.1.128/27, 1 successors, FD is 2681856

via 192.168.1.98 (2681856/2169856), Serial0/0/0

CALI#show ip eigrp topology

IP-EIGRP Topology Table for AS 200/ID(192.168.1.231)

Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,

r - Reply status

P 192.168.1.0/27, 1 successors, FD is 2172416

via 192.168.1.130 (2172416/28160), Serial0/0/0

P 192.168.1.32/27, 1 successors, FD is 2684416

via 192.168.1.130 (2684416/2172416), Serial0/0/0

P 192.168.1.64/27, 1 successors, FD is 28160

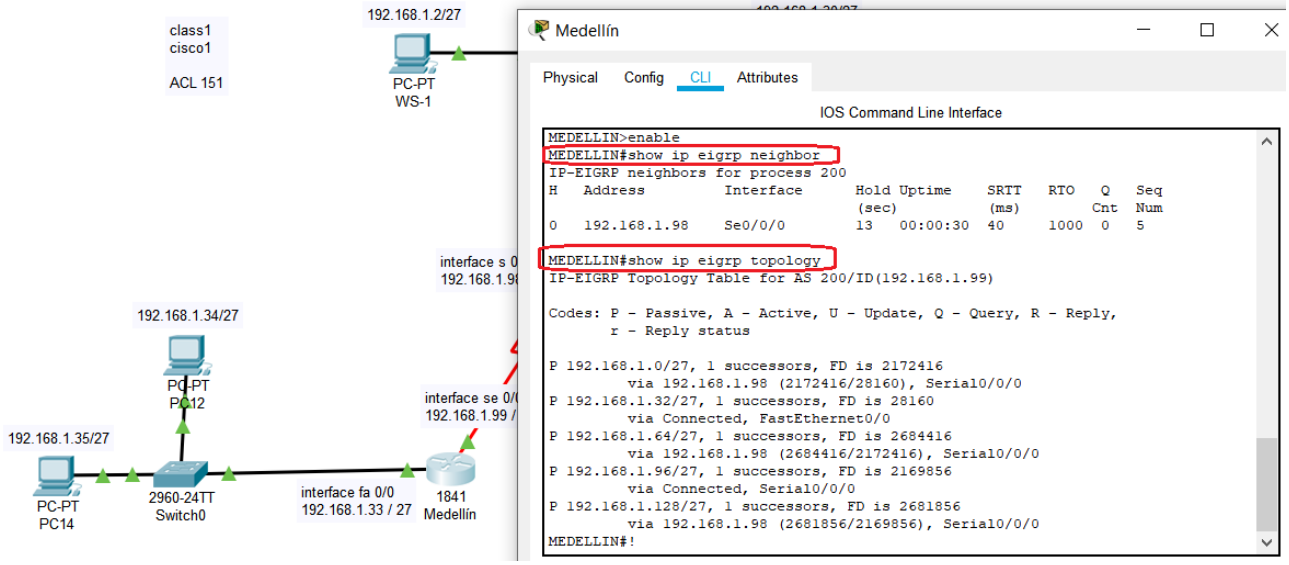
via Connected, FastEthernet0/0

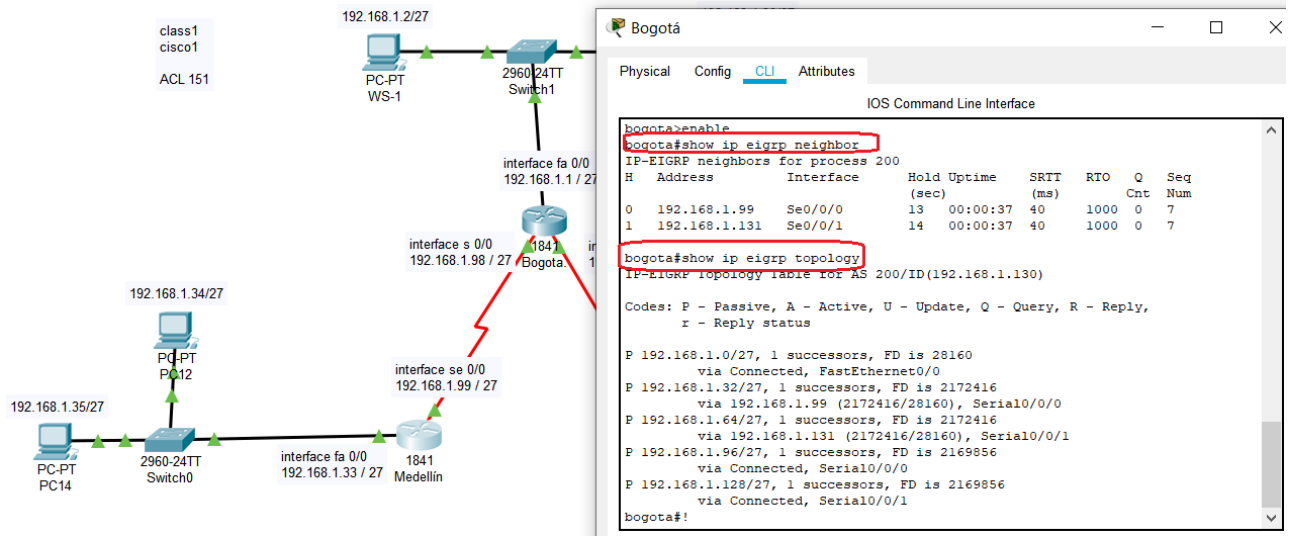
P 192.168.1.96/27, 1 successors, FD is 2681856

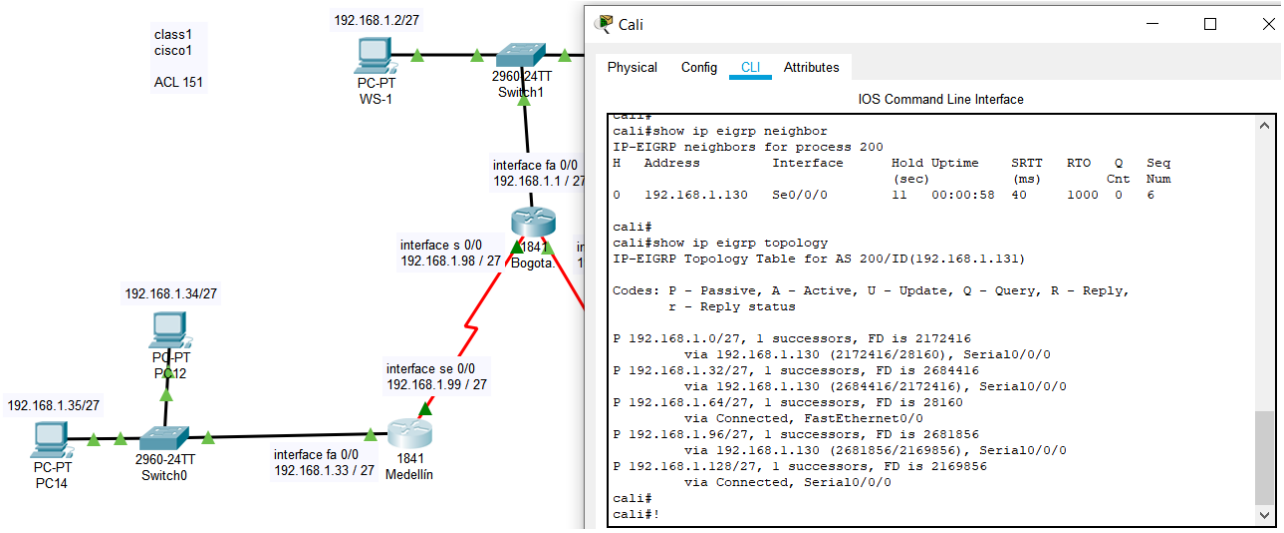
via 192.168.1.130 (2681856/2169856), Serial0/0/0

P 192.168.1.128/27, 1 successors, FD is 2169856

via Connected, Serial0/0/0







Observamos que cada router si esta detectando al VECINO.

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

SHOW IP ROUTE

BOGOTA#show ip route

Codes: C - connected, S - static, I - IGRP, 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

192.168.1.0/27 is subnetted, 5 subnets

C 192.168.1.0 is directly connected, FastEthernet0/0

D 192.168.1.32 [90/2172416] via 192.168.1.99, 00:04:34, Serial0/0/0

D 192.168.1.64 [90/2172416] via 192.168.1.231, 00:03:31, Serial0/0/1

C 192.168.1.96 is directly connected, Serial0/0/0

C 192.168.1.128 is directly connected, Serial0/0/1

MEDELLIN#show ip route

Codes: C - connected, S - static, I - IGRP, 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

192.168.1.0/27 is subnetted, 5 subnets

D 192.168.1.0 [90/2172416] via 192.168.1.98, 00:04:41, Serial0/0/0

C 192.168.1.32 is directly connected, FastEthernet0/0

D 192.168.1.64 [90/2684416] via 192.168.1.98, 00:03:38, Serial0/0/0

C 192.168.1.96 is directly connected, Serial0/0/0

D 192.168.1.128 [90/2681856] via 192.168.1.98, 00:03:44, Serial0/0/0

CALI#show ip route

Codes: C - connected, S - static, I - IGRP, 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

192.168.1.0/27 is subnetted, 5 subnets

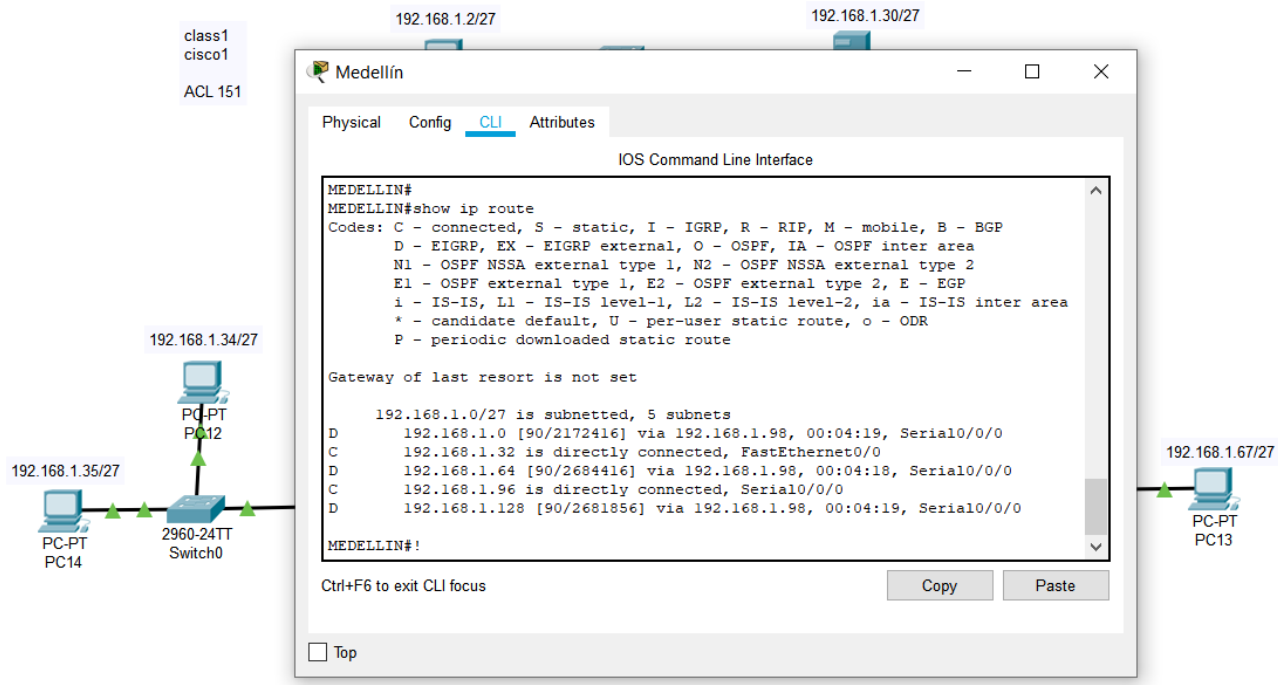
D 192.168.1.0 [90/2172416] via 192.168.1.130, 00:03:47, Serial0/0/0

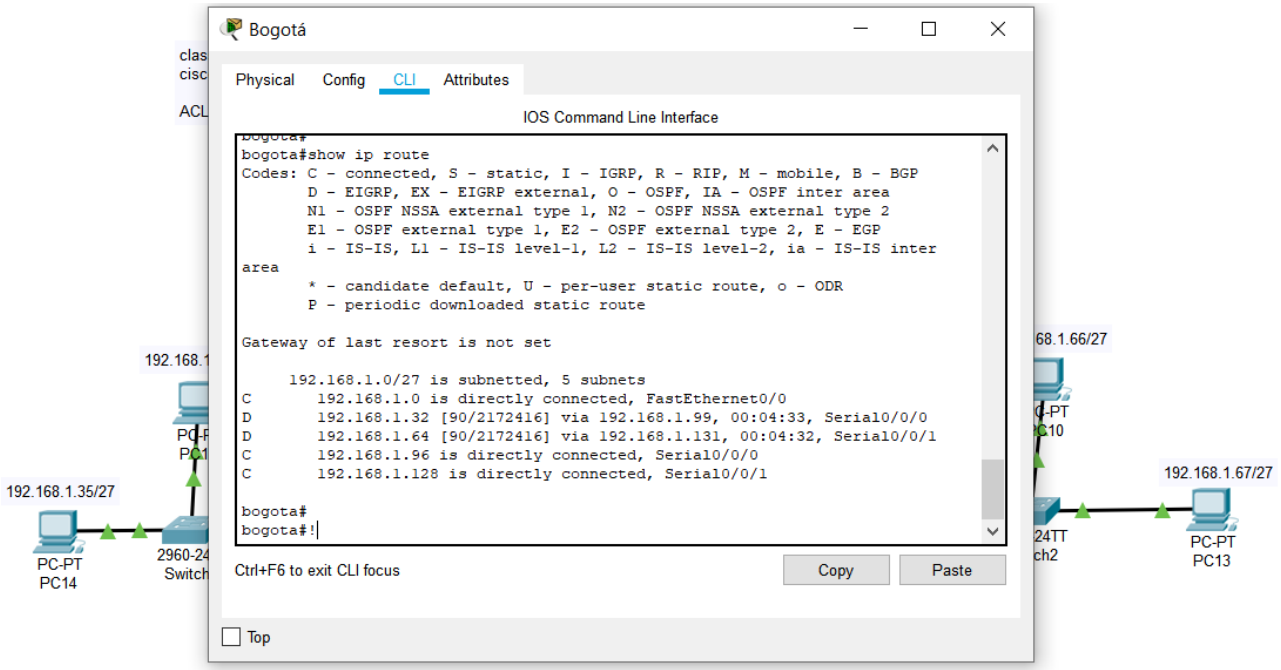
D 192.168.1.32 [90/2684416] via 192.168.1.130, 00:03:47, Serial0/0/0

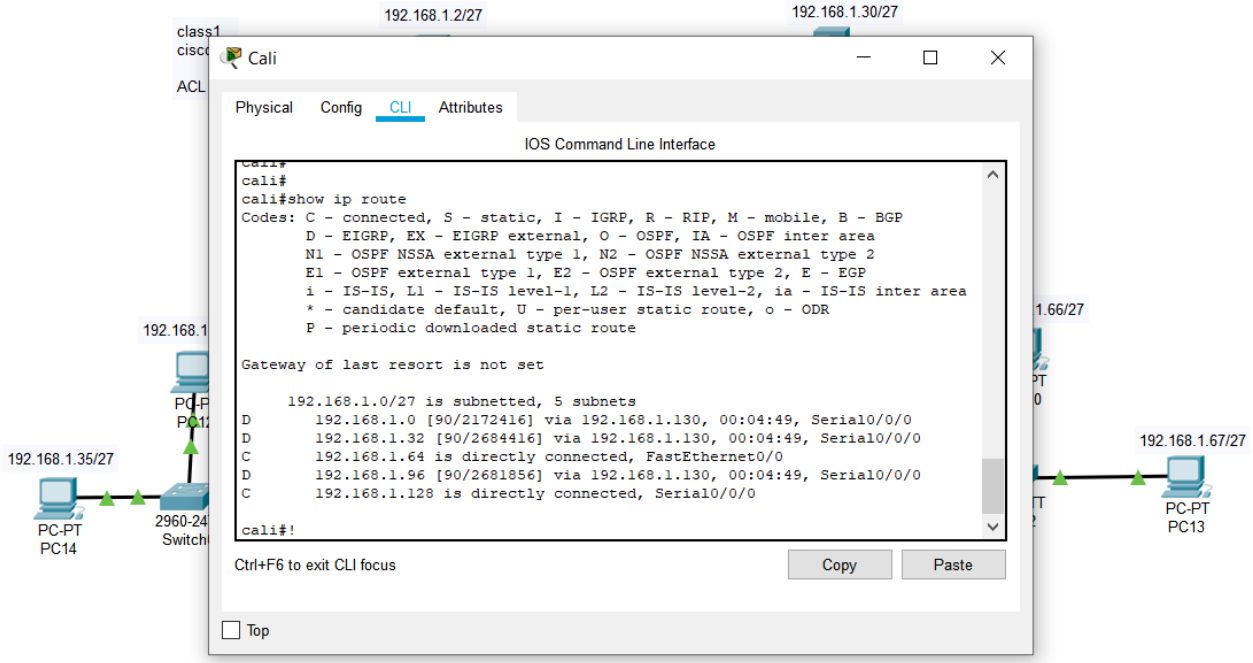
C 192.168.1.64 is directly connected, FastEthernet0/0

D 192.168.1.96 [90/2681856] via 192.168.1.130, 00:03:47, Serial0/0/0

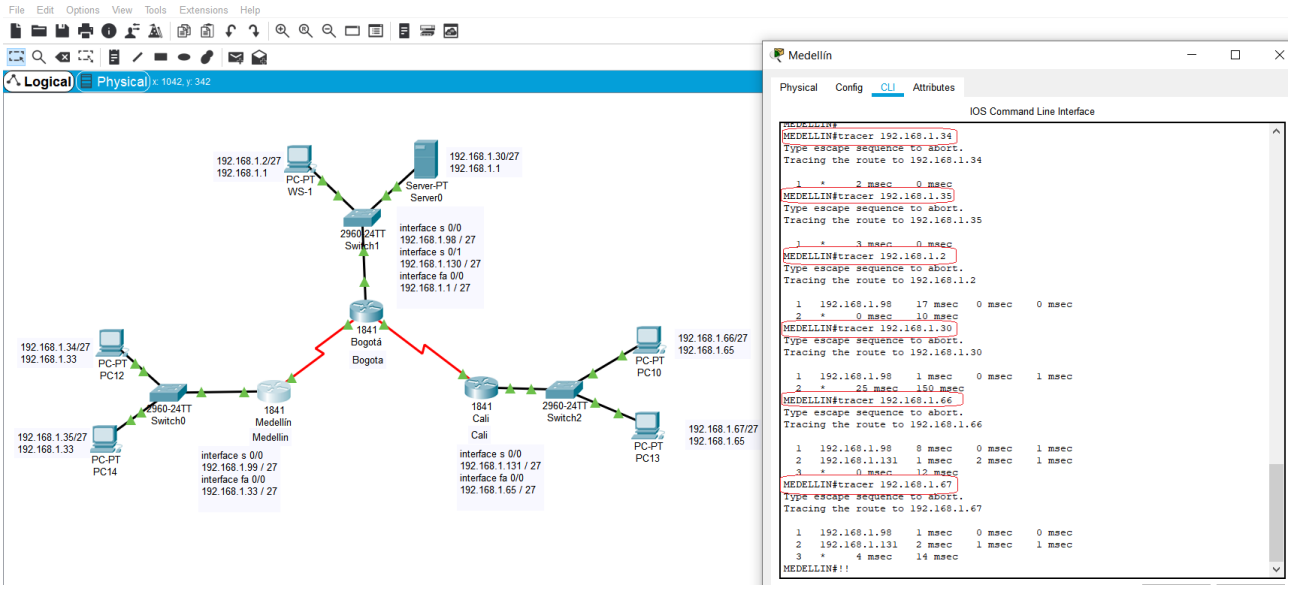
C 192.168.1.128 is directly connected, Serial0/0/0





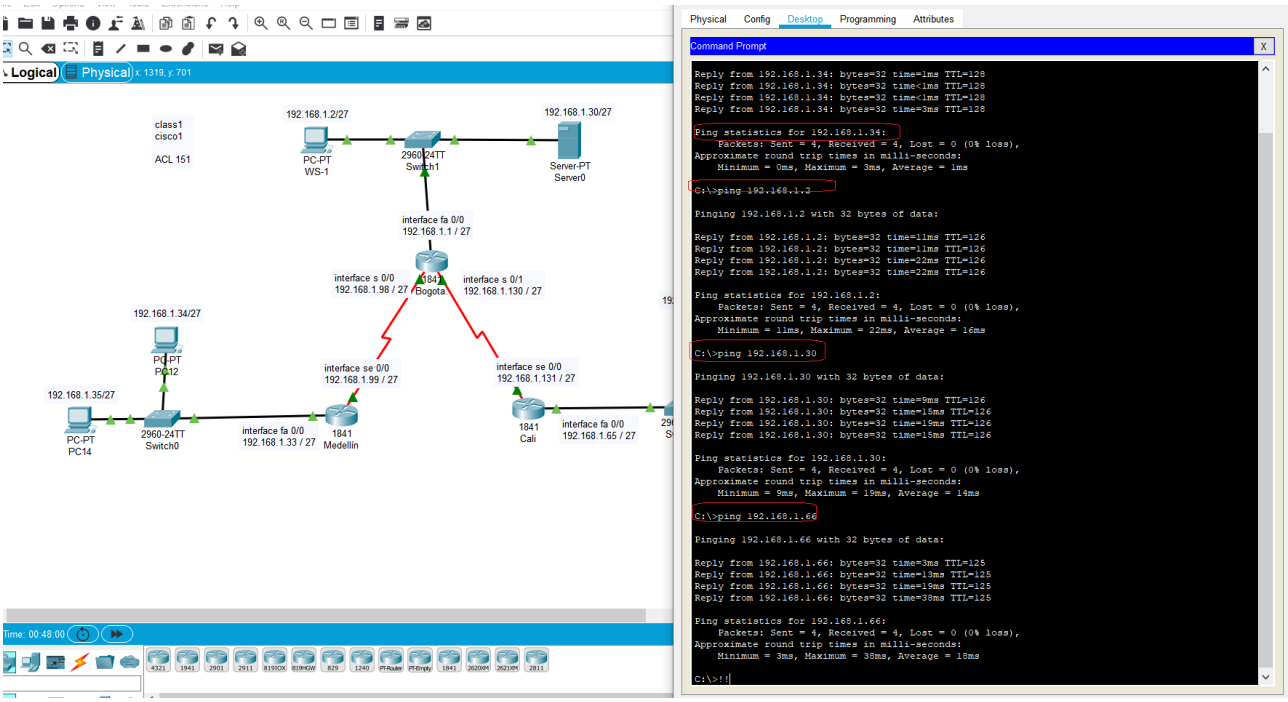


d. Realizar un diagnóstico para comprobar que cada uno de los puntos de la red se puedan ver y tengan conectividad entre sí. Realizar esta prueba desde un host de la red LAN del router CALI, primero a la red de MEDELLIN y luego al servidor.



Este comendo fue aplicado desde MEDELLÍN, vemos que tenemos rutas para cada una de las redes.

PING desde PC 14.



Igualmente empleando el comando PING nos da respuesta desde todos los puntos de la red.

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:

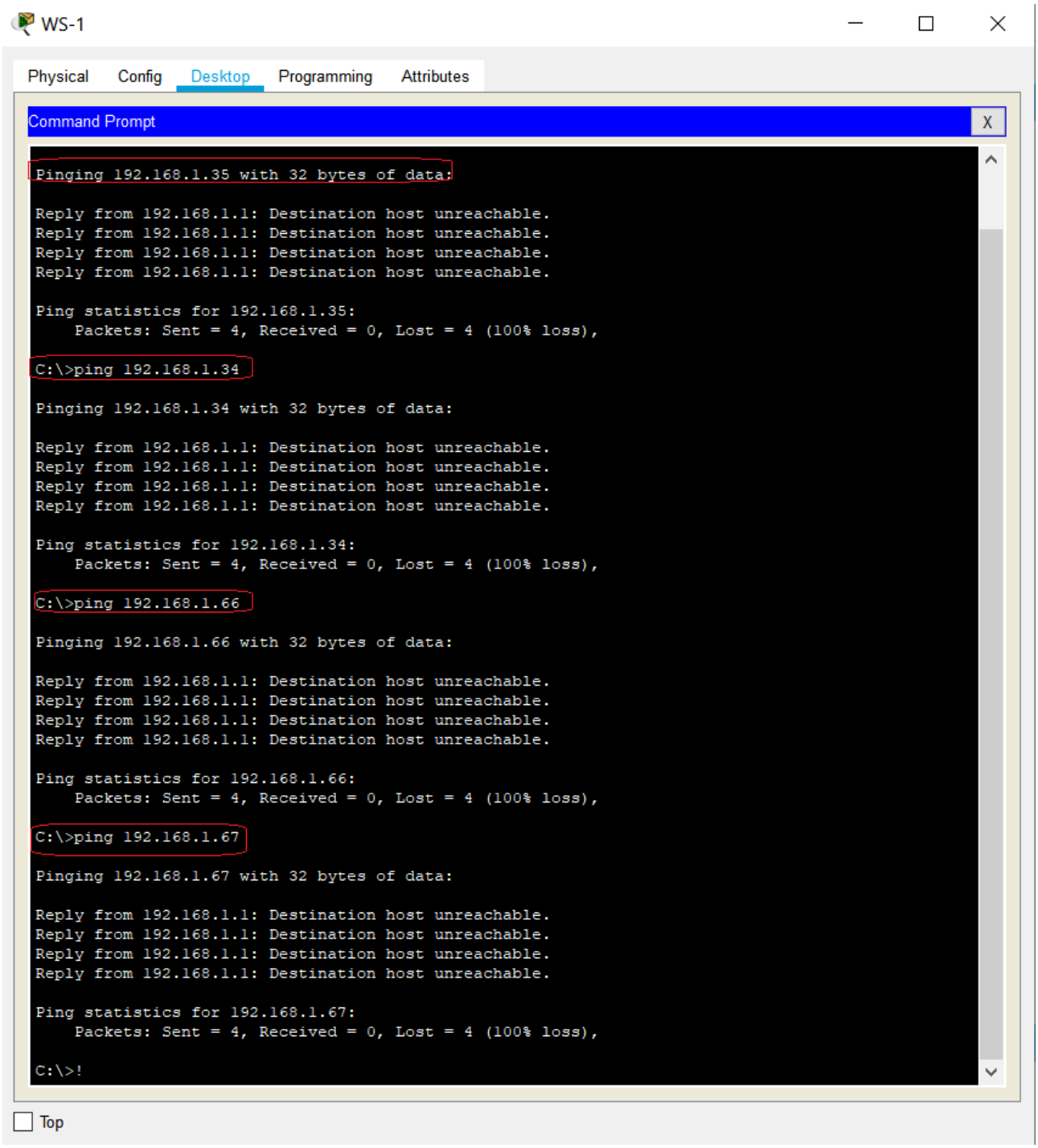
a. El equipo WS1 y el servidor se encuentran en la subred de administración. Solo el servidor de la subred de administración debe tener acceso a cualquier otro dispositivo en cualquier parte de la red.

BOGOTA(config)#access-list **151** permit ip host 192.168.1.30 any

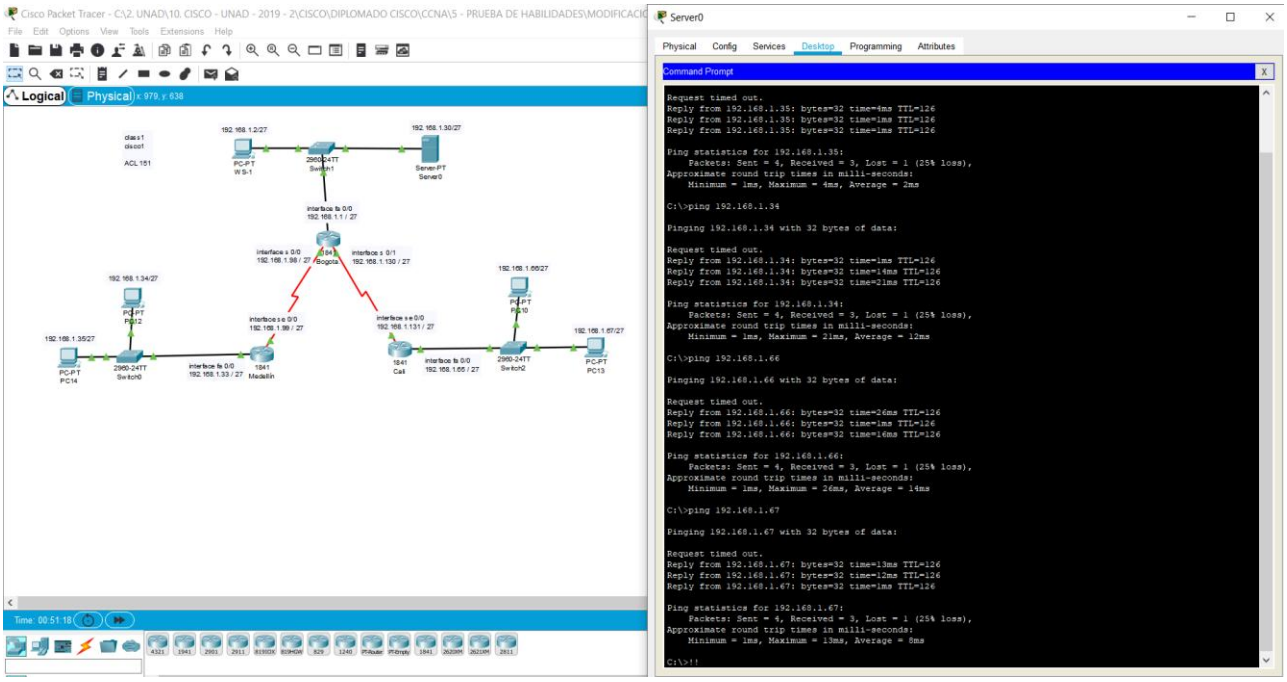
BOGOTA(config)#int f0/0

BOGOTA(config-if)#ip access-group 151 in

- Segun la restricción que hemos aplicado si hacemos un PING desde WS1 la respuesta es Destino Inalcanzable:



- Pero si hacemos el PING desde el SERVIDOR todos deben ser satisfactorios:



b. 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(config)#access-list **151** permit ip 192.168.1.32 0.0.0.31 host 192.168.1.30

MEDELLIN(config)#int f0/0

MEDELLIN(config-if)#ip access-group **151** in

MEDELLIN(config-if)#

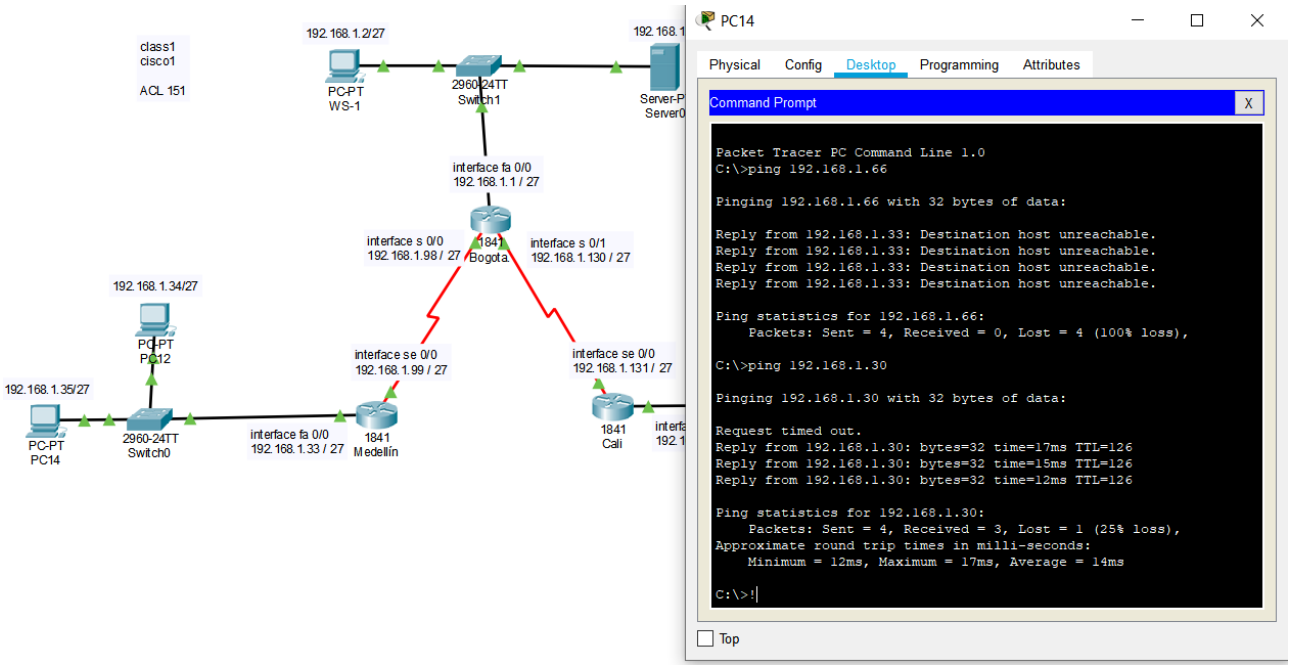
CALI(config)#access-list **151** permit ip 192.168.1.64 0.0.0.31 host 192.168.1.30

CALI(config)#int f0/0

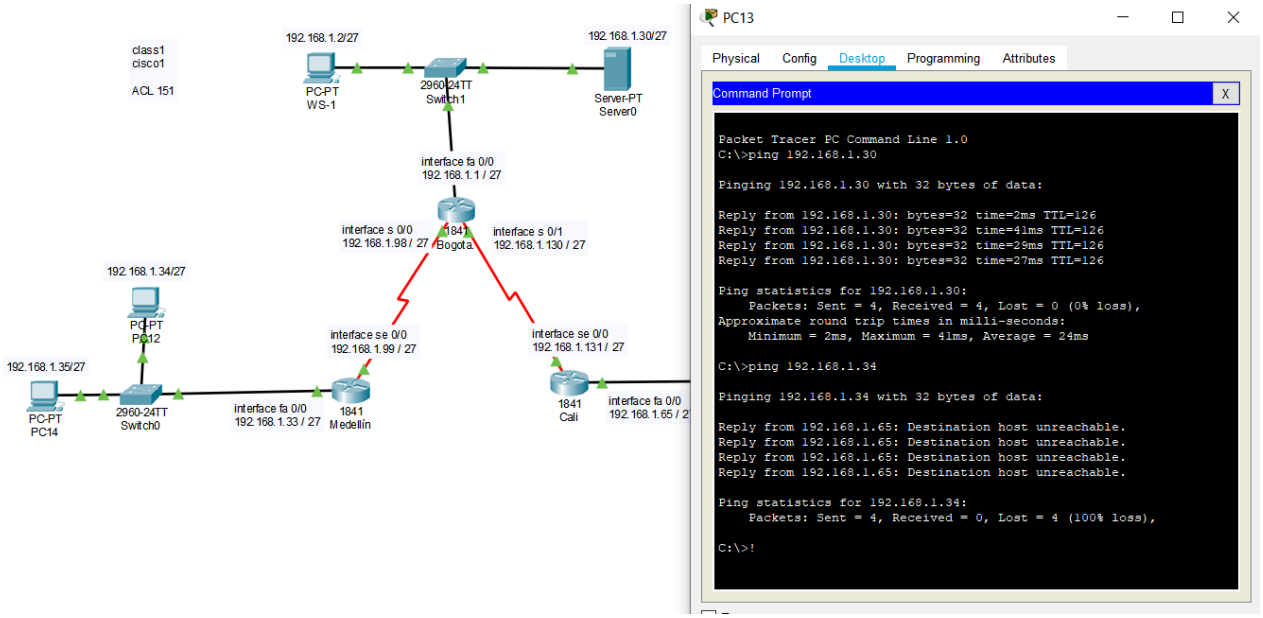
CALI(config-if)#ip access-group 151 in

CALI(config-if)#

- **Ping desde Medellín, hacia los diferentes puntos de la red y hacia el servidor:**



- **Ping desde la LAN de CALI hacia los diferentes puntos de la red y hacia el servidor:**



En los 2 casos verificamos el correcto funcionamiento de la ACL ingresada, en la cual verificamos que podemos hacer PING hacia el servidor pero el ping hacia cualquier punto por fuera de la LAN no debe tener efecto, con esto constatamos que todo está funcionando.

Parte 5: Comprobación de la red instalada.

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

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

	ORIGEN	DESTINO	RESULTADO	
TELNET	Router MEDELLIN	Router CALI	Éxito	192.168.1.131
	WS_1	Router BOGOTA	Falla	192.168.1.130
	Servidor	Router CALI	Éxito	192.168.1.131
	Servidor	Router MEDELLIN	Éxito	192.168.1.99
TELNET	LAN del Router	Router CALI	Falla	192.168.1.131
	LAN del Router CALI	Router CALI	Falla	192.168.1.131
	LAN del Router	Router MEDELLIN	Falla	192.168.1.99
	LAN del Router CALI	Router MEDELLIN	Falla	192.168.1.99
PING	LAN del Router CALI	WS_1	Falla	192.168.1.2
	LAN del Router	WS_1	Falla	192.168.1.2
	LAN del Router	LAN del Router CALI	Falla	192.168.1.67
PING	LAN del Router CALI	Servidor	Éxito	192.168.1.30
	LAN del Router	Servidor	Éxito	192.168.1.30
	Servidor	LAN del Router MEDELLIN	Éxito	192.168.1.35
	Servidor	LAN del Router CALI	Éxito	192.168.1.66
	Router CALI	LAN del Router MEDELLIN	Falla	192.168.1.35
	Router MEDELLIN	LAN del Router CALI	Falla	192.168.1.66

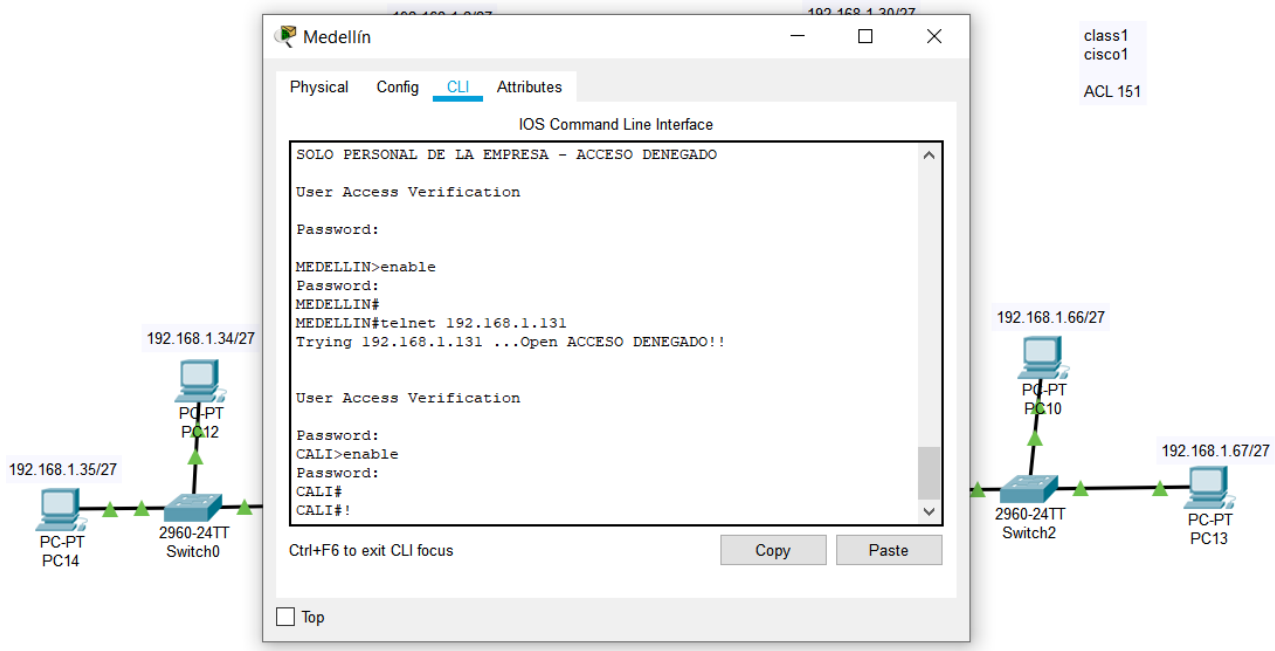
MEDELLIN	interface serial 0/0	192.168.1.99	255.255.255.224
	interface fa 0/0	192.168.1.33	255.255.255.224

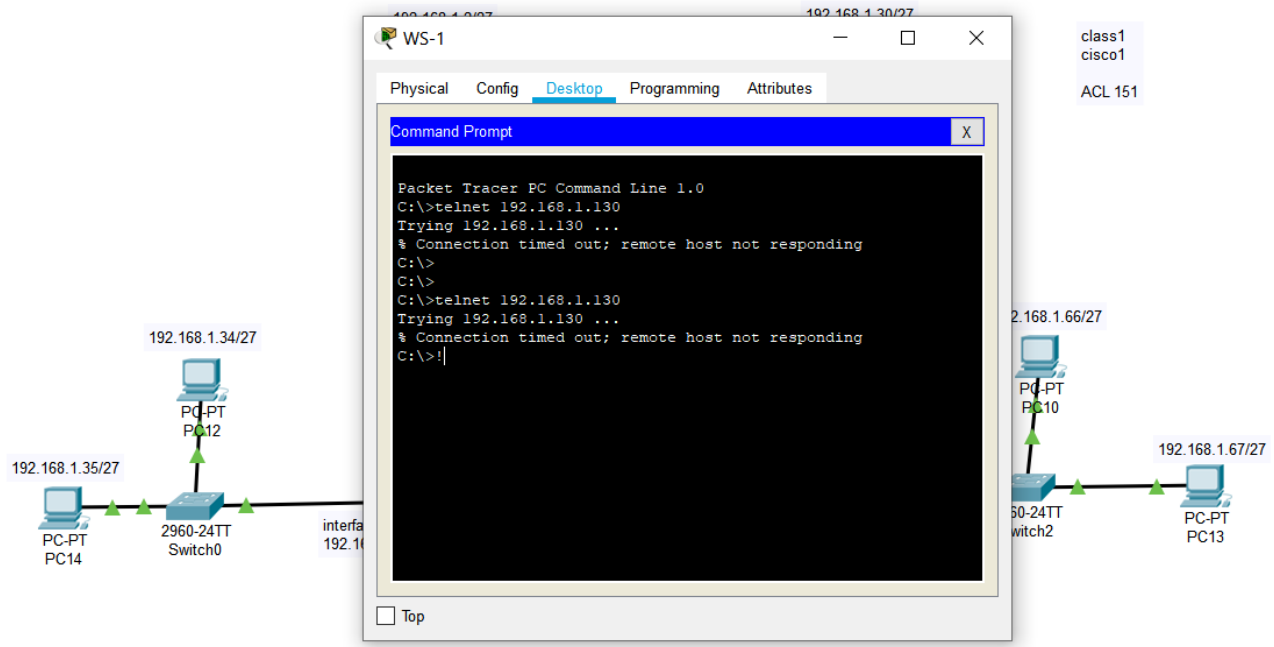
BOGOTA	interface serial 0/0	192.168.1.98	255.255.255.224
	interface serial 0/1	192.168.1.130	255.255.255.224
	interface fa 0/0	192.168.1.1	255.255.255.224
CALI	interface serial 0/0	192.168.1.131	255.255.255.224
	interface fa 0/0	192.168.1.65	255.255.255.224

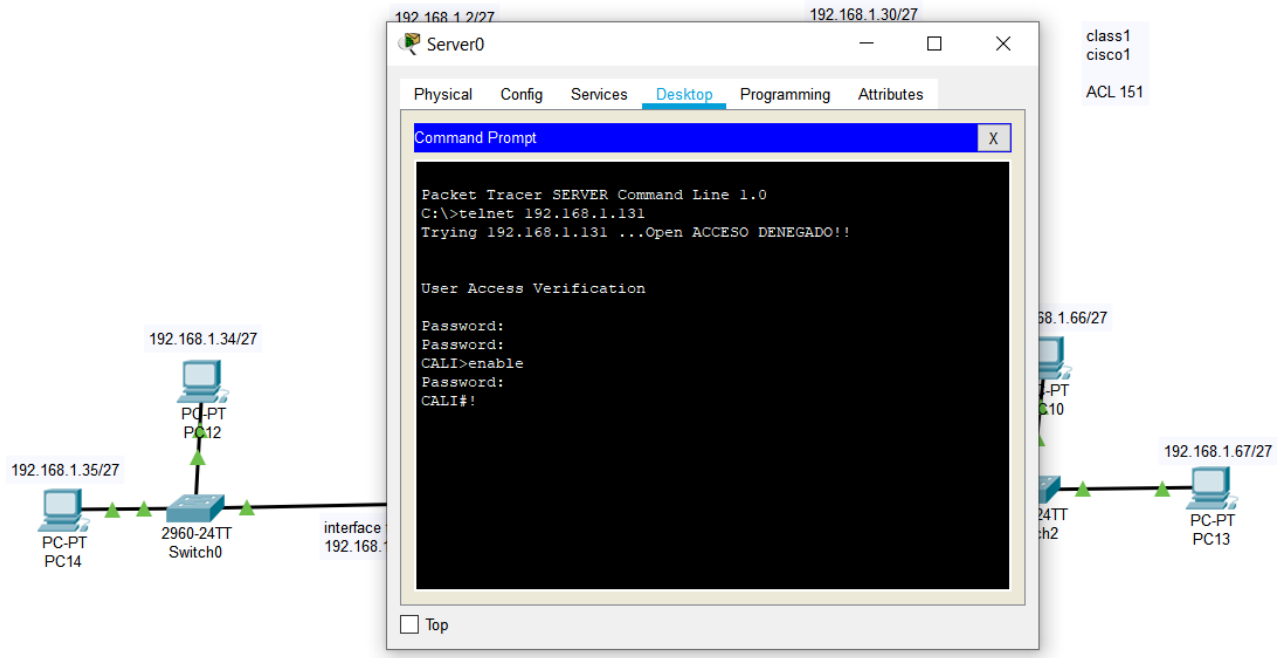
De una vez configuramos las PC:

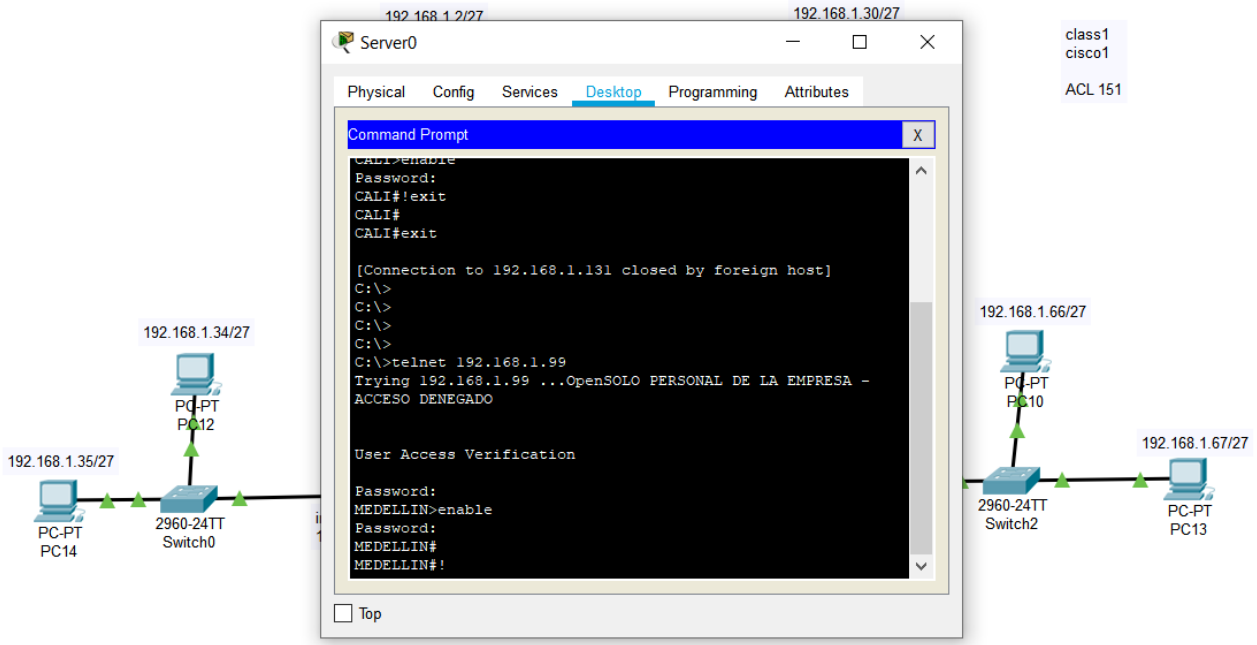
MEDELLIN	PC12	192.168.1.34	255.255.255.224	192.168.1.33
MEDELLIN	PC14	192.168.1.35	255.255.255.224	192.168.1.33
CALI	PC10	192.168.1.66	255.255.255.224	192.168.1.65
CALI	PC13	192.168.1.67	255.255.255.224	192.168.1.65
BOGOTA	WS-1	192.168.1.2	255.255.255.224	192.168.1.1
BOGOTA	SERVER	192.168.1.30	255.255.255.224	192.168.1.1

	ORIGEN	DESTINO	RESULTADO	
TELNET	Router MEDELLIN	Router CALI	Éxito	192.168.1.131
	WS_1	Router BOGOTA	Falla	192.168.1.130
	Servidor	Router CALI	Éxito	192.168.1.131
	Servidor	Router MEDELLIN	Éxito	192.168.1.99

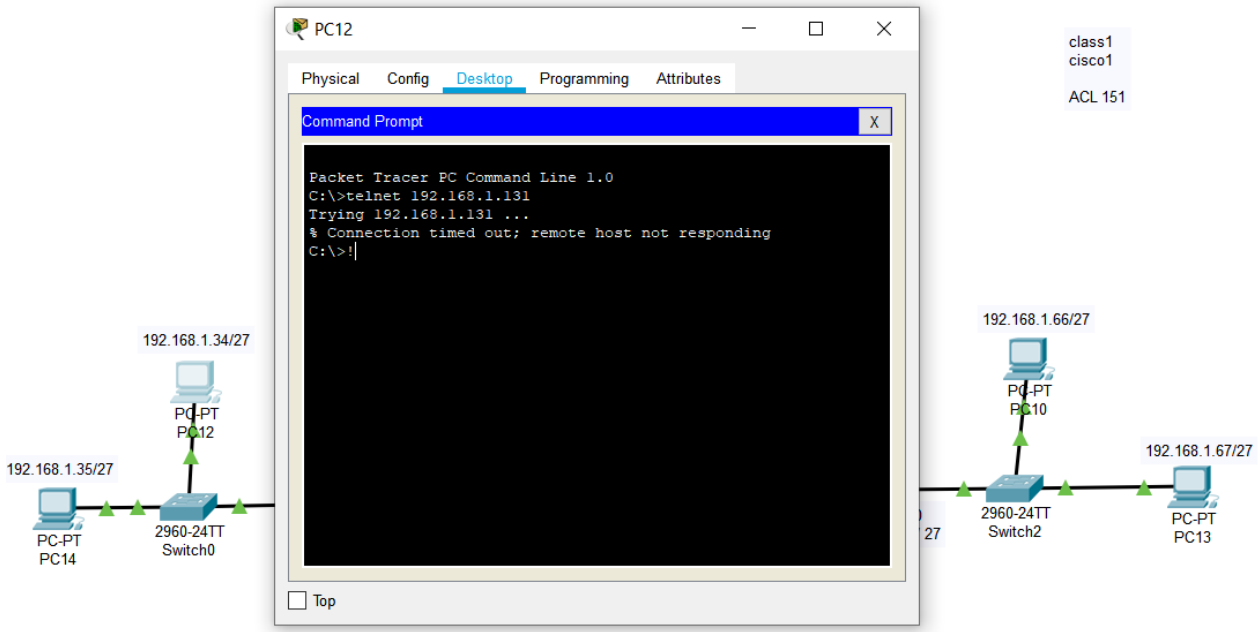


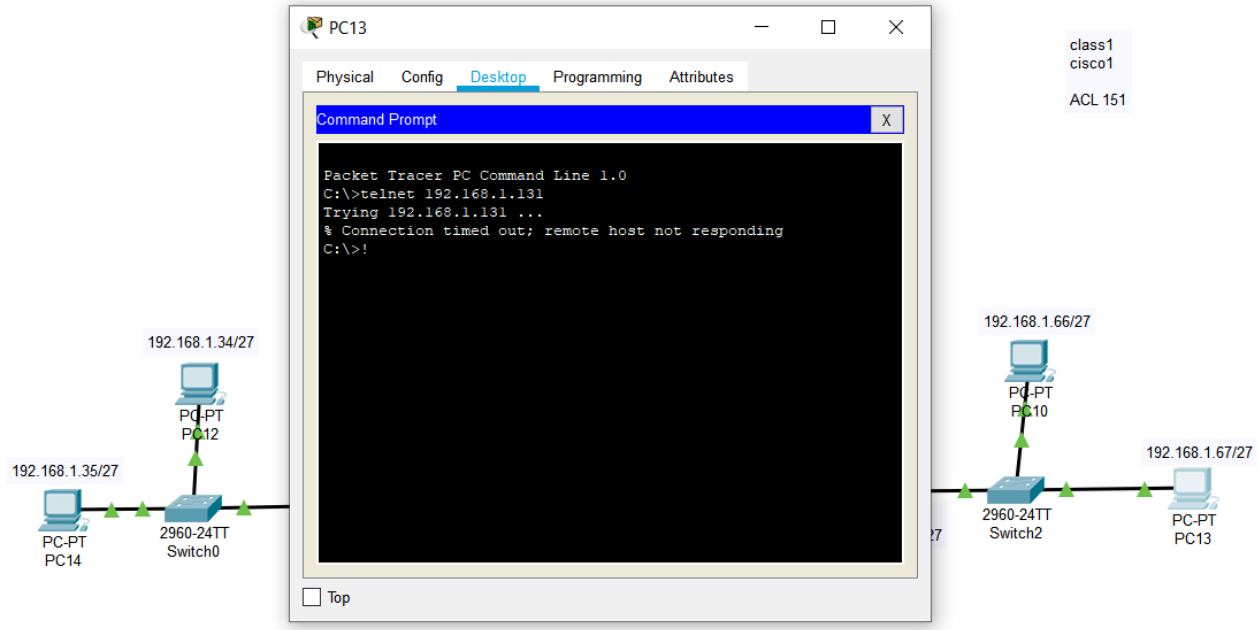

WS-1
Physical
Config
Desktop
Programming
Attributes
Command Prompt
X
Packet Tracer PC Command Line 1.0
C:\>telnet 192.168.1.130
Trying 192.168.1.130 ...
% Connection timed out; remote host not responding
C:\>
C:\>
C:\>telnet 192.168.1.130
Trying 192.168.1.130 ...
% Connection timed out; remote host not responding
C:\>!
Top
192.168.1.30/27
class1
cisco1
ACL 151
192.168.1.34/27
PC-PT
PC12
192.168.1.35/27
PC-PT
PC14
2960-24TT
Switch0
PC-PT
PC10
192.168.1.67/27
PC-PT
PC13

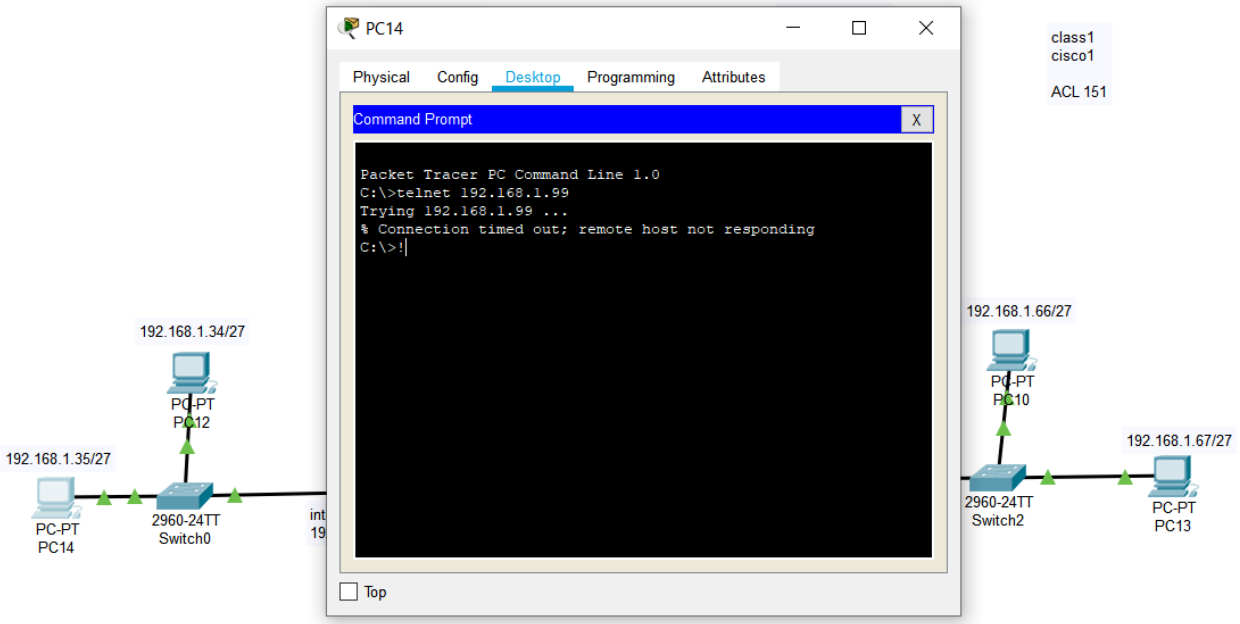

Server0
Physical
Config
Services
Desktop
Programming
Attributes
Command Prompt
X
Packet Tracer SERVER Command Line 1.0
C:\>telnet 192.168.1.131
Trying 192.168.1.131 ...Open ACCESO DENEGADO!!
User Access Verification
Password:
Password:
CALI>enable
Password:
CALI#!
Top
192.168.1.30/27
class1
cisco1
ACL 151
192.168.1.34/27
PC-PT
PC12
192.168.1.35/27
PC-PT
PC14
2960-24TT
Switch0
PC-PT
PC13
192.168.1.67/27

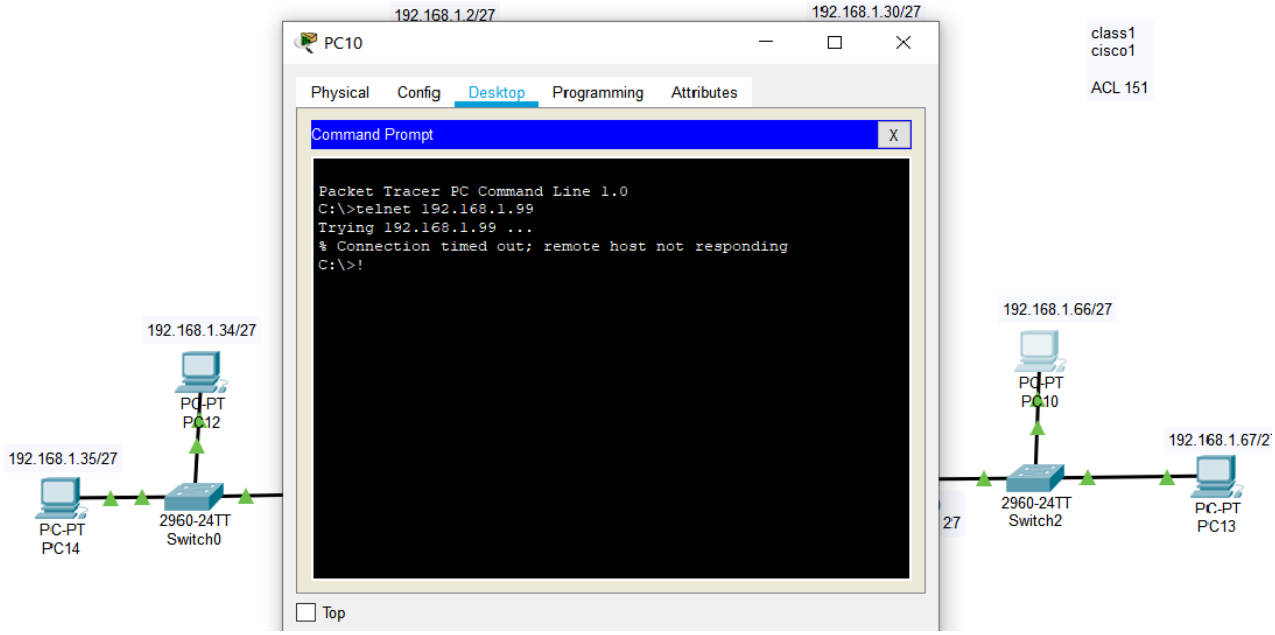


	ORIGEN	DESTINO	RESULTADO	
TELNET	LAN del Router MEDELLIN	Router CALI	Falla	192.168.1.131
	LAN del Router CALI	Router CALI	Falla	192.168.1.131
	LAN del Router MEDELLIN	Router MEDELLIN	Falla	192.168.1.99
	LAN del Router CALI	Router MEDELLIN	Falla	192.168.1.99


PC12
Physical
Config
Desktop
Programming
Attributes
Command Prompt
X
Packet Tracer PC Command Line 1.0
C:\>telnet 192.168.1.131
Trying 192.168.1.131 ...
% Connection timed out; remote host not responding
C:\>!
Top
class1
cisco1
ACL 151
192.168.1.34/27
PC-PT
PC12
192.168.1.35/27
PC-PT
PC14
2960-24TT
Switch0
192.168.1.66/27
PC-PT
PC10
192.168.1.67/27
2960-24TT
Switch2
PC-PT
PC13

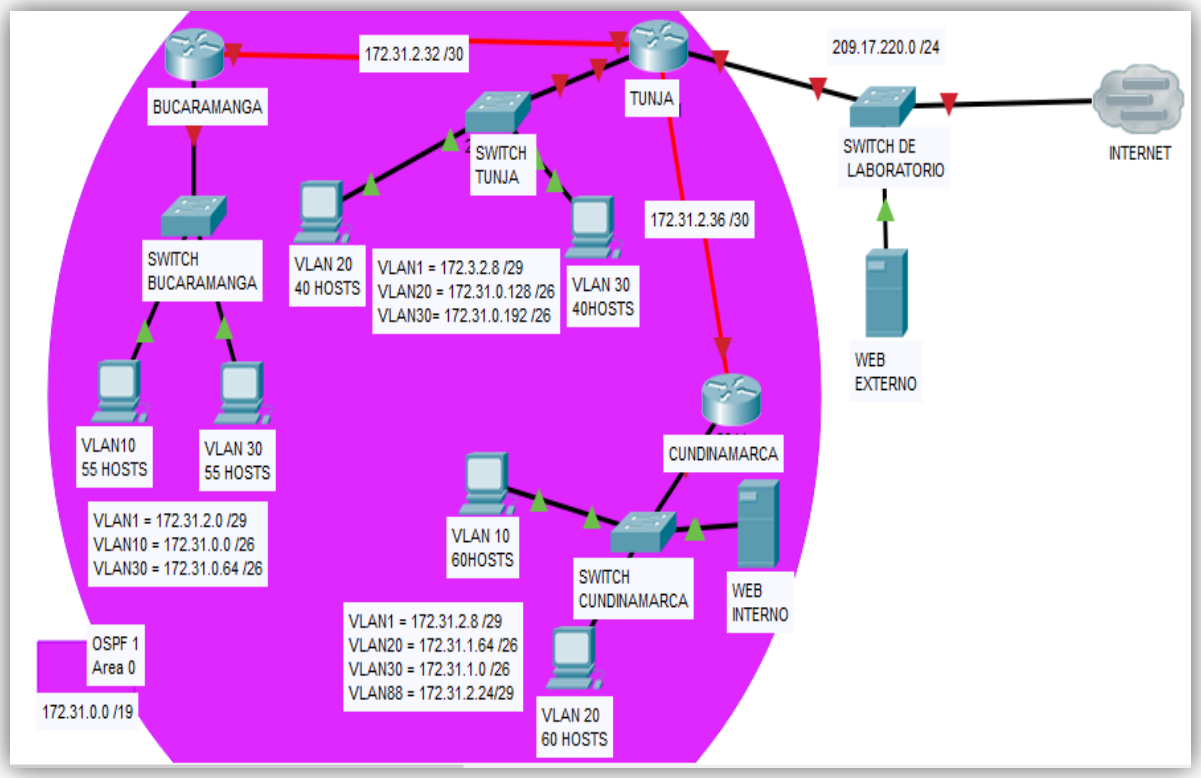

PC13
Physical
Config
Desktop
Programming
Attributes
Command Prompt
X
Packet Tracer PC Command Line 1.0
C:\>telnet 192.168.1.131
Trying 192.168.1.131 ...
% Connection timed out; remote host not responding
C:\>!
Top
class1
cisco1
ACL 151
192.168.1.34/27
PC-PT
PC12
192.168.1.35/27
PC-PT
PC14
2960-24TT
Switch0
192.168.1.66/27
PC-PT
PC10
192.168.1.67/27
2960-24TT
Switch2
PC-PT
PC13


PC14
Physical
Config
Desktop
Programming
Attributes
Command Prompt
X
Packet Tracer PC Command Line 1.0
C:\>telnet 192.168.1.99
Trying 192.168.1.99 ...
% Connection timed out; remote host not responding
C:\>!
Top
class1
cisco1
ACL 151
192.168.1.34/27
PC-PT
PC12
192.168.1.35/27
PC-PT
PC14
2960-24TT
Switch0
192.168.1.66/27
PC-PT
PC10
2960-24TT
Switch2
192.168.1.67/27
PC-PT
PC13


192.168.1.2/27
192.168.1.30/27
PC10
Physical
Config
Desktop
Programming
Attributes
Command Prompt
X
Packet Tracer PC Command Line 1.0
C:\>telnet 192.168.1.99
Trying 192.168.1.99 ...
% Connection timed out; remote host not responding
C:\>!
Top
class1
cisco1
ACL 151
192.168.1.34/27
PC-PT
PC12
192.168.1.35/27
PC-PT
PC14
2960-24TT
Switch0
192.168.1.66/27
PC-PT
PC10
2960-24TT
Switch2
PC-PT
PC13

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.



Desarrollo

Los siguientes son los requerimientos necesarios:

1. Todos los routers deberán tener los siguiente:
    - Configuración básica.
    - Autenticación local con AAA.
    - Cifrado de contraseñas.
    - 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.

2. El DHCP deberá proporcionar solo direcciones a los hosts de Bucaramanga y Cundinamarca
3. El web server deberá tener NAT estático y el resto de los equipos de la topología emplearan NAT de sobrecarga (PAT).

4. El enrutamiento deberá tener autenticación.
5. Listas de control de acceso:

   - Los hosts de VLAN 20 en Cundinamarca no acceden a internet, solo a la red interna de Tunja.
   - Los hosts de VLAN 10 en Cundinamarca si acceden a internet y no a la red interna de 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.
   - Los hosts de VLAN 30 de Bucaramanga acceden a internet y a cualquier equipo de VLAN 10.
   - Los hosts de VLAN 10 en Bucaramanga acceden a la red de Cundinamarca (VLAN 20) y Tunja (VLAN 20), no internet.
   - Los hosts de una VLAN no pueden acceder a los de otra VLAN en una ciudad.
   - Solo los hosts de las VLAN administrativas y de la VLAN de servidores tienen accedo a los routers e internet.

6. VLSM: utilizar la dirección **172.31.0.0 /18** para el direccionamiento.

Aspectos a tener en cuenta

- Habilitar VLAN en cada switch y permitir su enrutamiento.
- Enrutamiento OSPF con autenticación en cada router.
- Servicio **DHCP** en el router Tunja, mediante el **helper address**, para los routers Bucaramanga y Cundinamarca.

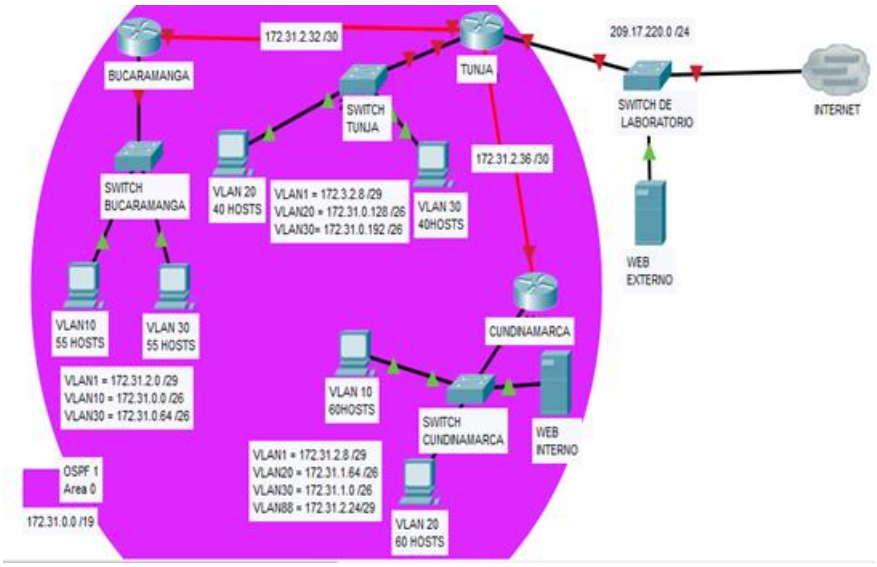
- Configuración de NAT estático y de sobrecarga.
- Establecer una lista de control de acceso de acuerdo con los criterios señalados.
- Habilitar las opciones en puerto consola y terminal virtual

DESARROLLO DE LA GUÍA.

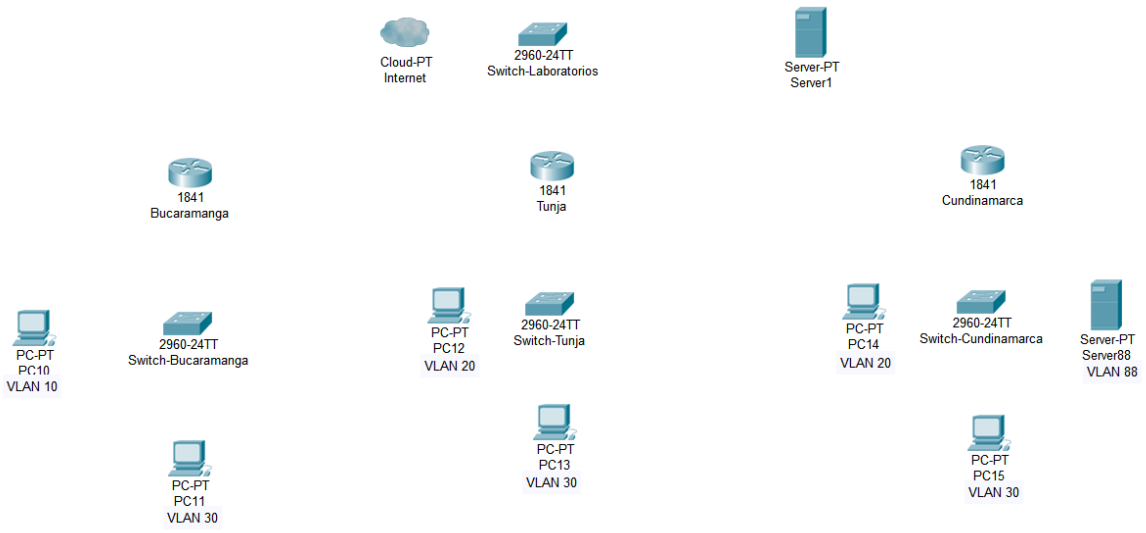
Los siguientes son los requerimientos necesarios:

ESCENARIO 2

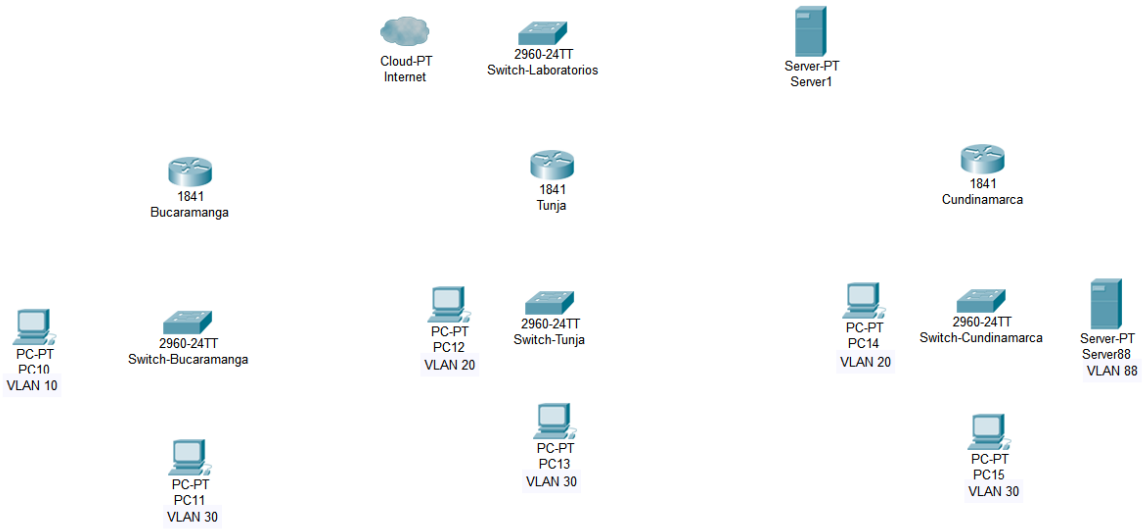
En este caso debemos proceder armar la topología según las indicaciones que se nos está entregando, para nuestro caso la topología 2:



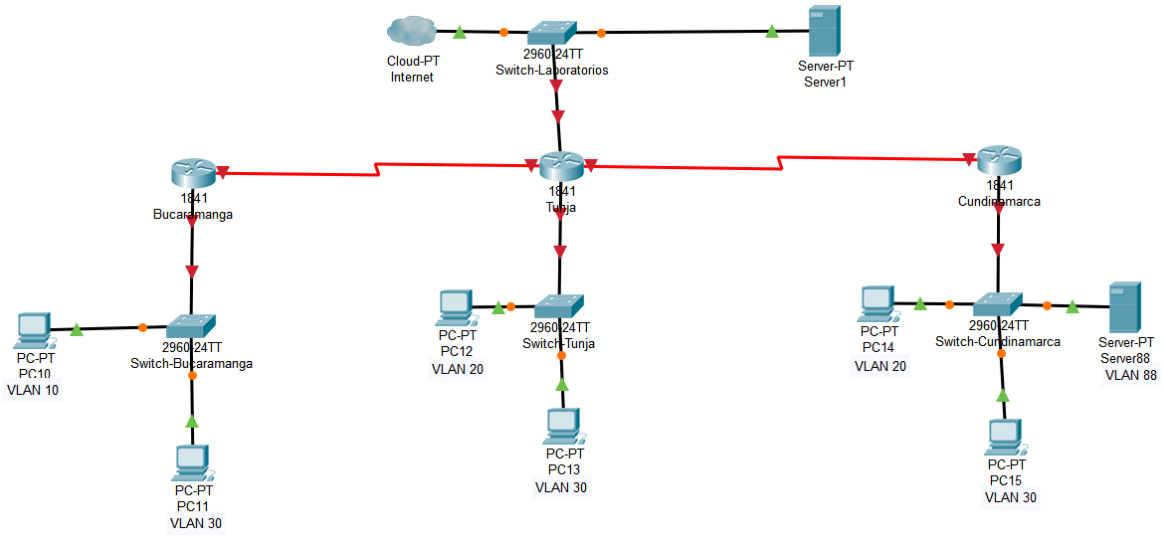
Con el fin de tener observar mejor la distribución de los dispositivos se arma la topología de la siguiente manera:



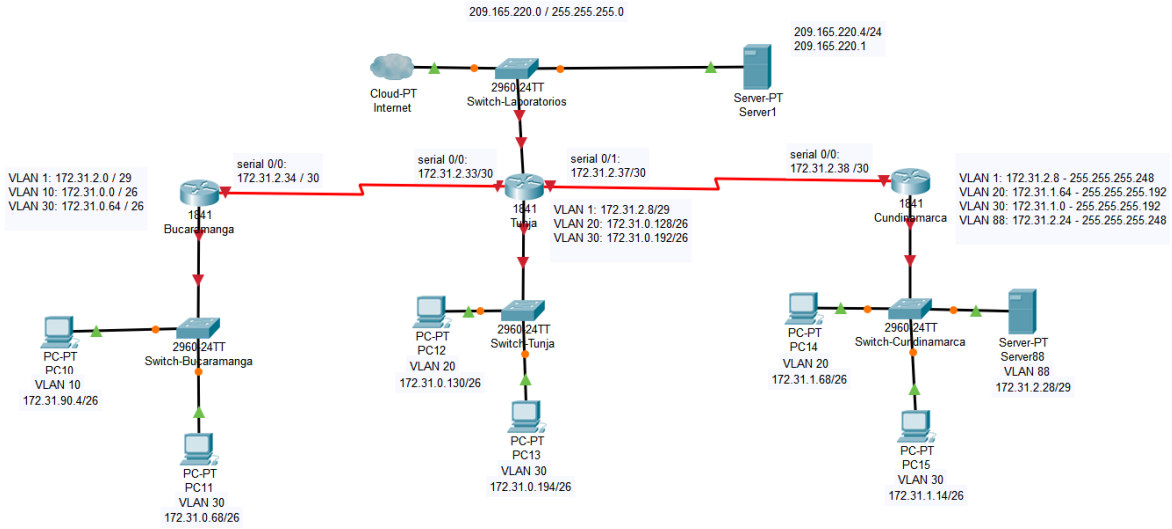
Procedemos entonces a distribuir los dispositivos según muestra la imagen:



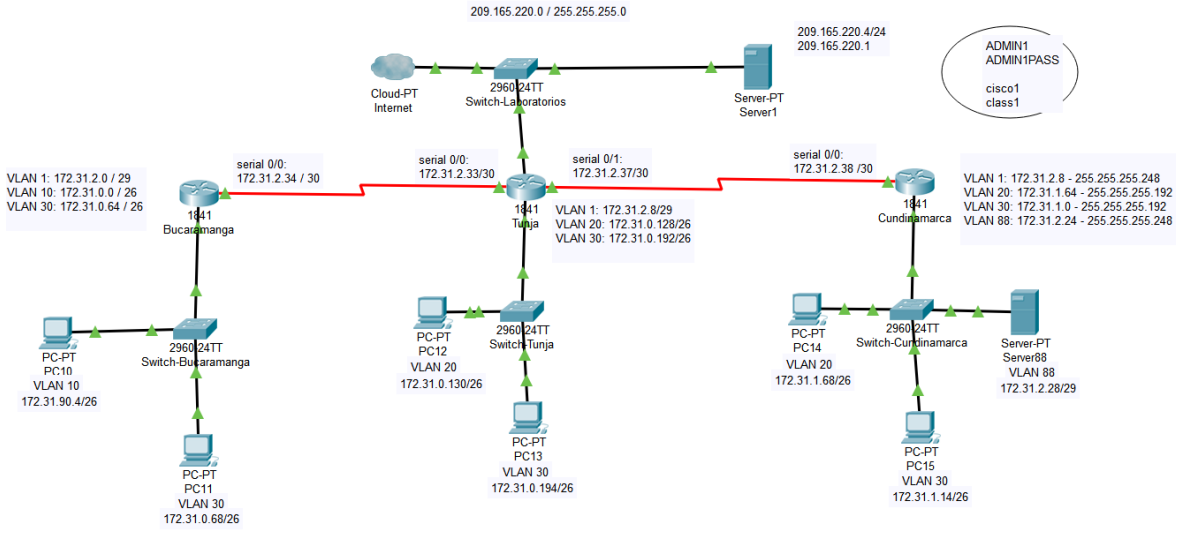
Como segundo paso debemos proceder a conectar los mismos empleando el cable adecuado y las interfaces adecuadas según la información suministrada:



Ya que tenemos conectados los mismos procedemos agrega la información necesaria con el fin de poder configurar los diferentes dispositivos e interfaces, de esta manera nos queda mas sencillo este proceso:



Por ultimo debemos proceder a configurar cada una de las interfaces, miramos que cada uno de los indicadores cambia a color verde.



1. Todos los routers deberán tener los siguiente:
    - Configuración básica.

Lo primero que podemos hacer en este caso es configurar los nombres de los dispositivos y los mensajes, recordemos que este es persuasivo para las personas que ingresan sin autorización debida. Este proceso se hace aplicando los siguientes comandos:

Router(config)#hostname BUCARAMANGA

BUCARAMANGA(config)#no ip domain-lookup

BUCARAMANGA(config)#banner motd $!! **SOLO PERSONAL DE LA EMPRESA - ACCESO DENEGADO**¡¡$

Router(config)#hostname TUNJA

TUNJA(config)#no ip domain-lookup

TUNJA(config)#banner motd $!!ACCESO DENEGADO¡¡$

Router(config)#hostname CUNDINAMARCA

CUNDINAMARCA(config)#no ip domain-lookup

CUNDINAMARCA(config)#banner motd $!! **SOLO PERSONAL DE LA EMPRESA - ACCESO DENEGADO**¡¡$

Continuamos configurando las contraseñas, recordemos que esta parte es muy importante, ya que evitan la vulnerabilidad de nuestros dispositivos y de nuestra red. El proceso seguido en cada uno de los dispositivos se indica a continuación:

BUCARAMANGA(config)#enable secret class1

BUCARAMANGA(config)#line console 0

BUCARAMANGA(config-line)#password cisco1

BUCARAMANGA(config-line)#login

BUCARAMANGA(config-line)#line vty 0 15

BUCARAMANGA(config-line)#password cisco1

BUCARAMANGA(config-line)#login

BUCARAMANGA(config)#int f0/0.1

TUNJA(config)#enable secret class1

TUNJA(config)#line console 0

TUNJA(config-line)#password cisco1

TUNJA(config-line)#login

TUNJA(config-line)#line vty 0 15

TUNJA(config-line)#password cisco1

TUNJA(config-line)#login

CUNDINAMARCA(config)#enable secret class1

CUNDINAMARCA(config)#line console 0

CUNDINAMARCA(config-line)#password cisco1

CUNDINAMARCA(config-line)#login

CUNDINAMARCA(config-line)#line vty 0 15

CUNDINAMARCA(config-line)#password cisco1

CUNDINAMARCA(config-line)#login

Nuestra red está configurada con una serie de VLAN, por consiguiente debemos como siguiente paso configurar las interfaces, sub-interfaces y el correspondiente encapsulación:

BUCARAMANGA(config-subif)#encapsulation dot1q 1

BUCARAMANGA(config-subif)#ip address 172.31.2.1 255.255.255.248

BUCARAMANGA(config-subif)#int f0/0.10

BUCARAMANGA(config-subif)#encapsulation dot1q 10

BUCARAMANGA(config-subif)#ip address 172.31.0.1 255.255.255.192

BUCARAMANGA(config-subif)#int f0/0.30

BUCARAMANGA(config-subif)#encapsulation dot1q 30

BUCARAMANGA(config-subif)#ip address 172.31.0.65 255.255.255.192

BUCARAMANGA(config-subif)#int f0/0

BUCARAMANGA(config-if)#no shutdown

BUCARAMANGA(config-if)#int s0/0/0

BUCARAMANGA(config-if)#ip address 172.31.2.34 255.255.255.252

BUCARAMANGA(config-if)#no shutdown

BUCARAMANGA(config-if)#

No olvidemos que debemos activar cada una de las interfaces. Continuamos el proceso con el router de TUNJA.

TUNJA(config)#int f0/0.1

TUNJA(config-subif)#encapsulation dot1q 1

TUNJA(config-subif)#ip address 172.3.2.9 255.255.255.248

TUNJA(config-subif)#int f0/0.20

TUNJA(config-subif)#encapsulation dot1q 20

TUNJA(config-subif)#ip address 172.31.0.129 255.255.255.192

TUNJA(config-subif)#int f0/0.30

TUNJA(config-subif)#encapsulation dot1q 30

TUNJA(config-subif)#ip address 172.31.0.193 255.255.255.192

TUNJA(config-subif)#int f0/0

TUNJA(config-if)#no shutdown

TUNJA(config-if)#int s0/0/0

TUNJA(config-if)#ip address 172.31.2.33 255.255.255.252

TUNJA(config-if)#no shutdown

TUNJA(config-if)#int s0/0/1

TUNJA(config-if)#ip address 172.31.2.37 255.255.255.252

TUNJA(config-if)#no shutdown

TUNJA(config-if)#int f0/1

TUNJA(config-if)#ip address 209.165.220.1 255.255.255.0

TUNJA(config-if)#no shutdown

Finalizamos nuestro proceso de configuración de las interfaces con el ROUTER CUNDINAMARCA:

CUNDINAMARCA(config)#int f0/0.1

CUNDINAMARCA(config-subif)#encapsulation dot1q 1

CUNDINAMARCA(config-subif)#ip address 172.31.2.9 255.255.255.248

CUNDINAMARCA(config-subif)#int f0/0.20

CUNDINAMARCA(config-subif)#encapsulation dot1q 20

CUNDINAMARCA(config-subif)#ip address 172.31.1.65 255.255.255.192

CUNDINAMARCA(config-subif)#int f0/0.30

CUNDINAMARCA(config-subif)#encapsulation dot1q 30

CUNDINAMARCA(config-subif)#ip address 172.31.1.1 255.255.255.192

CUNDINAMARCA(config-subif)#int f0/0.88

CUNDINAMARCA(config-subif)#encapsulation dot1q 88

CUNDINAMARCA(config-subif)#ip address 172.31.2.25 255.255.255.248

CUNDINAMARCA(config-subif)#int f0/0

CUNDINAMARCA(config-if)#no shutdown

CUNDINAMARCA(config-if)#int s0/0/0

CUNDINAMARCA(config-if)#ip address 172.31.2.38 255.255.255.252

CUNDINAMARCA(config-if)#no shutdown

Procedemos ahora a configurar los SWITCHES.

Creamos las VLAN que vamos a necesitar en cada uno de ellos según la imagen que se nos suminstra y debemos asignar las interfaces de cada uno de los switches a estas vlan.

Switch-Bucaramanga(config)#vlan 1

Switch-Bucaramanga (config-vlan)#vlan 10

Switch-Bucaramanga (config-vlan)#vlan 30

Swtich-Tunja(config)#vlan 1

Swtich-Tunja(config-vlan)#vlan 20

Swtich-Tunja(config-vlan)#vlan 30

Swtich-Cundinamarca(config)#vlan 1

Swtich-Cundinamarca(config-vlan)#vlan 20

Swtich-Cundinamarca(config-vlan)#vlan 30

Swtich-Cundinamarca(config-vlan)#vlan 88

- Tenemos ya creadas las VLAN, pero entonces se debe proceder a asignar las interfaces de los switch a cada una de estas VLAN, con el fin de crear las subredes, tal como lo indicamos a continuación:

Switch-Bucaramanga(config-vlan)#int f0/10

Switch-Bucaramanga(config-if)#switchport mode access

Switch-Bucaramanga(config-if)#switchport access vlan 10

Switch-Bucaramanga(config-if)#int f0/14

Switch-Bucaramanga(config-if)#switchport mode access

Switch-Bucaramanga(config-if)#switchport access vlan 30

Switch-Bucaramanga(config-if)#int f0/1

Switch-Bucaramanga(config-if)#switchport mode trunk

Switch-Bucaramanga(config-if)#int vlan 1

Switch-Bucaramanga(config-if)#ip address 172.31.2.3 255.255.255.248

Switch-Bucaramanga(config-if)#no shutdown

Switch-Bucaramanga(config-if)#ip default-gateway 172.31.2.1

Switch-Bucaramanga(config)#

Switch-Tunja(config-vlan)#int f0/10

Switch-Tunja(config-if)#switchport mode access

Switch-Tunja(config-if)#switchport access vlan 20

Switch-Tunja(config-if)#int f0/14

Switch-Tunja(config-if)#switchport mode access

Switch-Tunja(config-if)#switchport access vlan 30

Switch-Tunja(config-if)#int f0/1

Switch-Tunja(config-if)#switchport mode trunk

Switch-Tunja(config-if)#int vlan 1

Switch-Tunja(config-if)#ip address 172.3.2.11 255.255.255.248

Switch-Tunja(config-if)#no shutdown

Switch-Tunja(config-if)#ip default-gateway 172.3.2.9

Switch-Cundinamarca(config)#int f0/10

Switch-Cundinamarca(config-if)#switchport mode access

Switch-Cundinamarca(config-if)#switchport access vlan 20

Switch-Cundinamarca(config-if)#int f0/14

Switch-Cundinamarca(config-if)#switchport mode access

Switch-Cundinamarca(config-if)#switchport access vlan 30

Switch-Cundinamarca(config-if)#int f0/20

Switch-Cundinamarca(config-if)#switchport mode access

Switch-Cundinamarca(config-if)#switchport access vlan 88

Switch-Cundinamarca(config-if)#int f0/1

Switch-Cundinamarca(config-if)#switchport mode trunk

Switch-Cundinamarca(config-if)#int vlan 1

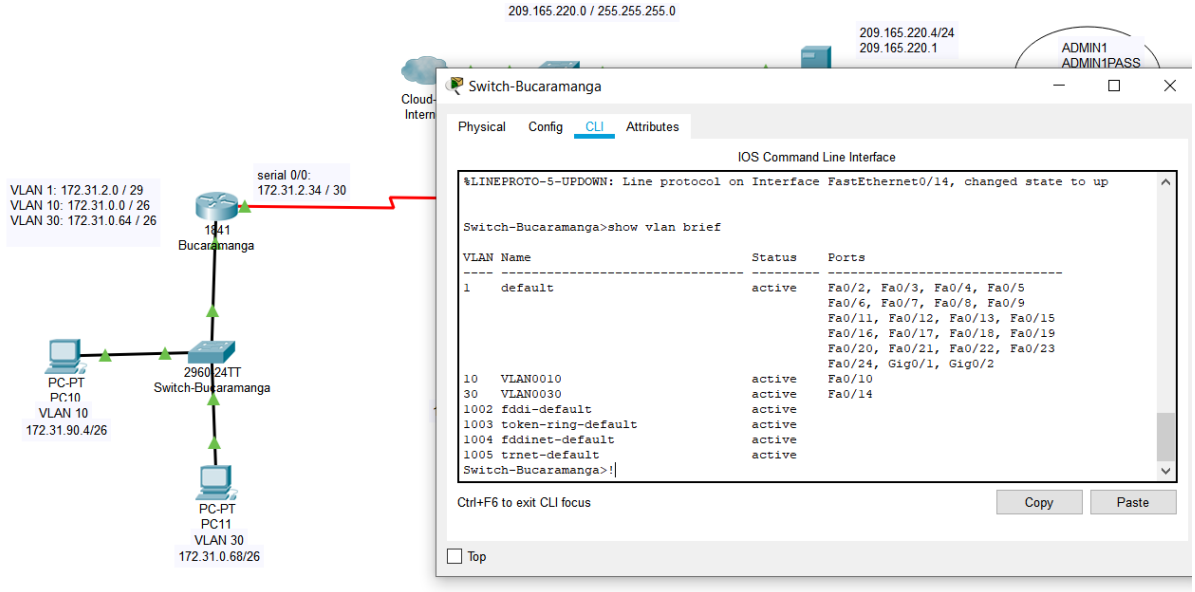
Switch-Cundinamarca(config-if)#ip address 172.31.2.11 255.255.255.248

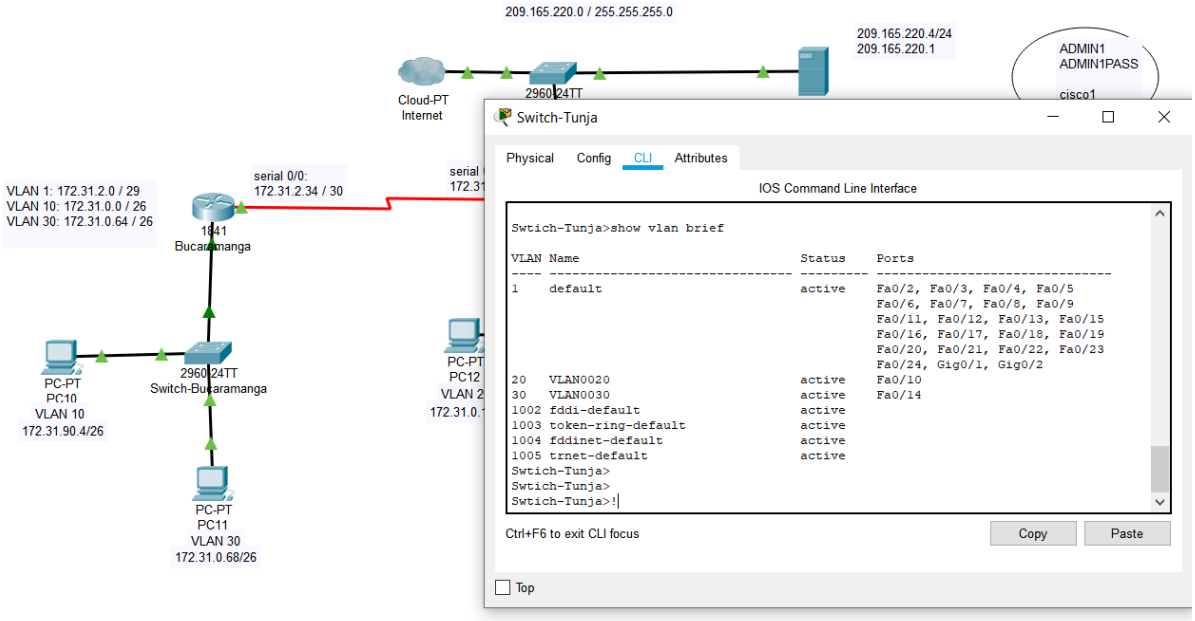
Switch-Cundinamarca(config-if)#no shutdown

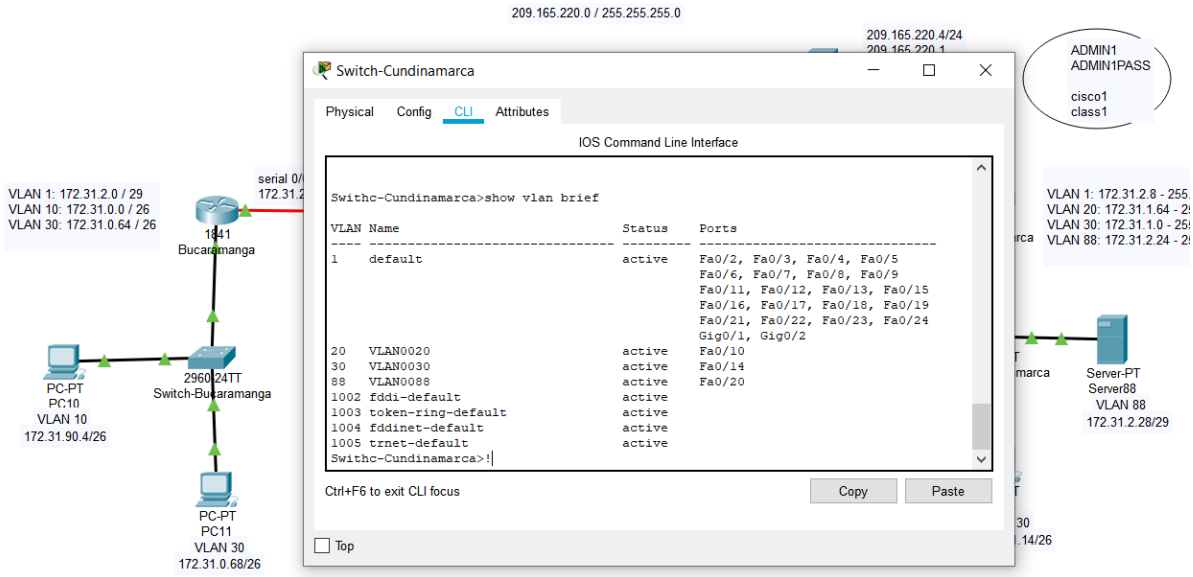
Switch-Cundinamarca(config-if)#ip default-gateway 172.31.2.9

Switch-Cundinamarca(config)#

En este punto es importante tambien verificar que nuestra configuración ingresada sea la corresta, este lo hacemos con la utilización de los siguientes commandos:

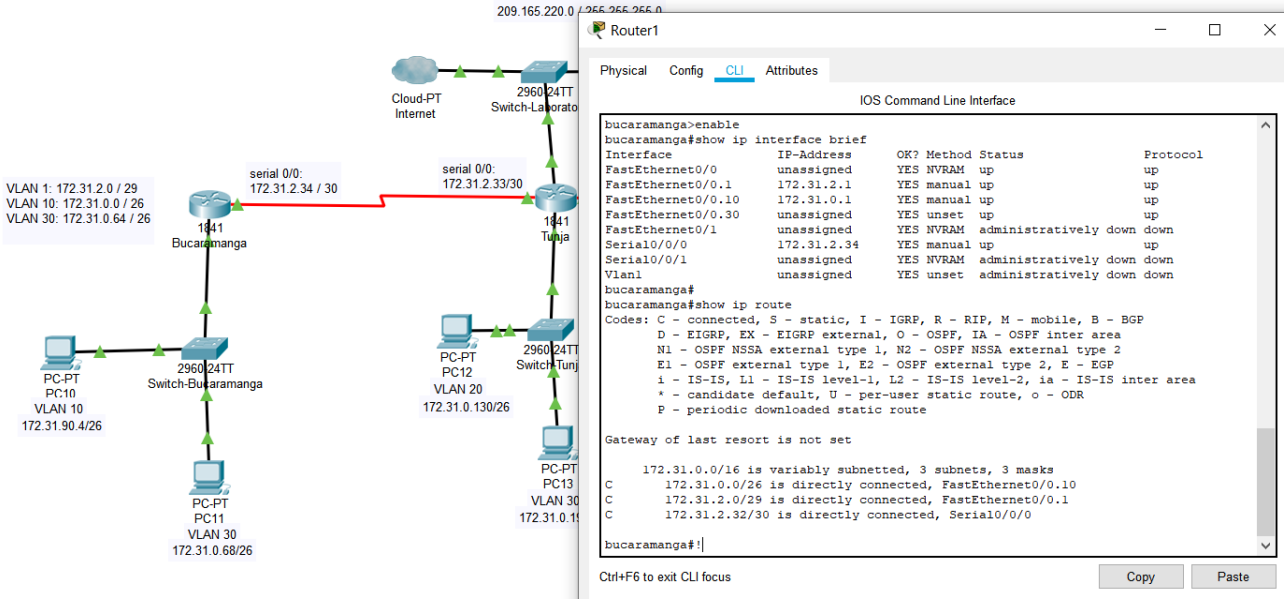

209.165.220.0 / 255.255.255.0
209.165.220.4/24
209.165.220.1
ADMIN1
ADMIN1PASS
Switch-Bucaramanga
Physical
Config
CLI
Attributes
IOS Command Line Interface
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/14, changed state to up
Switch-Bucaramanga>show vlan brief
VLAN Name Status Ports
1 default active Fa0/2, Fa0/3, Fa0/4, Fa0/5
Fa0/6, Fa0/7, Fa0/8, Fa0/9
Fa0/11, Fa0/12, Fa0/13, Fa0/15
Fa0/16, Fa0/17, Fa0/18, Fa0/19
Fa0/20, Fa0/21, Fa0/22, Fa0/23
Fa0/24, Gig0/1, Gig0/2
10 VLAN0010 active Fa0/10
30 VLAN0030 active Fa0/14
1002 fddi-default active
1003 token-ring-default active
1004 fddinet-default active
1005 trnet-default active
Switch-Bucaramanga>!
Ctrl+F6 to exit CLI focus
Copy
Paste
Top
VLAN 1: 172.31.2.0 / 29
VLAN 10: 172.31.0.0 / 26
VLAN 30: 172.31.0.64 / 26
serial 0/0:
172.31.2.34 / 30
1841
Bucaramanga
2960-24TT
Switch-Bucaramanga
PC-PT
PC10
VLAN 10
172.31.90.4/26
PC-PT
PC11
VLAN 30
172.31.0.68/26

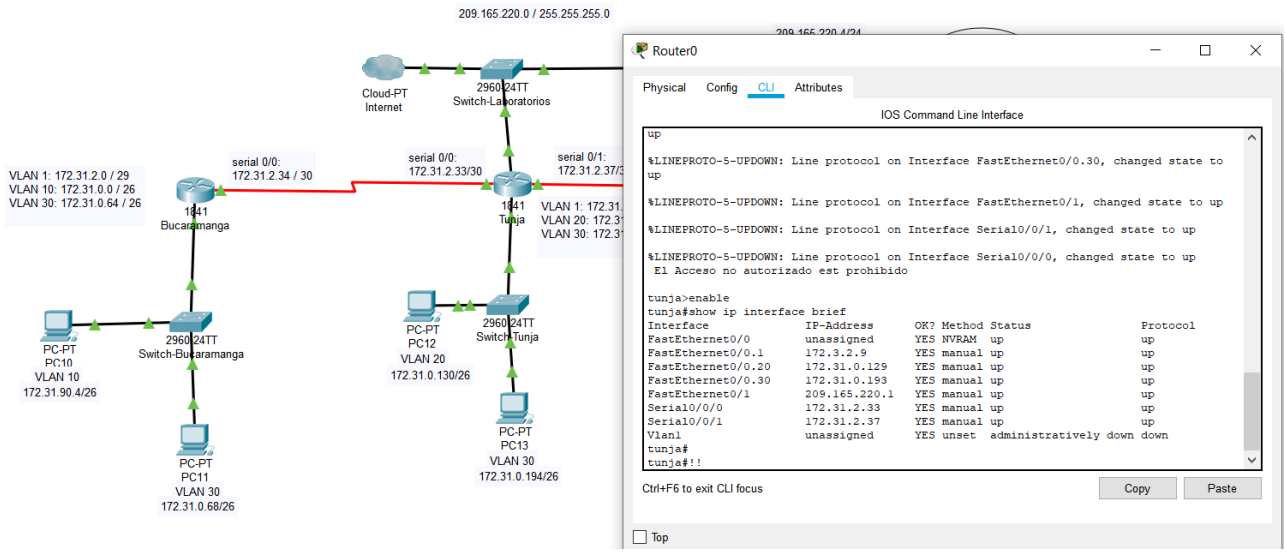

209.165.220.0 / 255.255.255.0
209.165.220.4/24
209.165.220.1
ADMIN1
ADMIN1PASS
cisco1
Cloud-PT
Internet
2960-24TT
Switch-Tunja
Physical
Config
CLI
Attributes
IOS Command Line Interface
Swtich-Tunja>show vlan brief
VLAN Name Status Ports
1 default active Fa0/2, Fa0/3, Fa0/4, Fa0/5
Fa0/6, Fa0/7, Fa0/8, Fa0/9
Fa0/11, Fa0/12, Fa0/13, Fa0/15
Fa0/16, Fa0/17, Fa0/18, Fa0/19
Fa0/20, Fa0/21, Fa0/22, Fa0/23
Fa0/24, Gig0/1, Gig0/2
20 VLAN0020 active Fa0/10
30 VLAN0030 active Fa0/14
1002 fddi-default active
1003 token-ring-default active
1004 fddinet-default active
1005 trnet-default active
Swtich-Tunja>
Swtich-Tunja>
Swtich-Tunja>!
Ctrl+F6 to exit CLI focus
Copy
Paste
Top
VLAN 1: 172.31.2.0 / 29
VLAN 10: 172.31.0.0 / 26
VLAN 30: 172.31.0.64 / 26
serial 0/0:
172.31.2.34 / 30
1841
2960-24TT
Switch-Bucaramanga
PC-PT
PC10
VLAN 10
172.31.90.4/26
PC-PT
PC11
VLAN 30
172.31.0.68/26
PC-PT
PC12

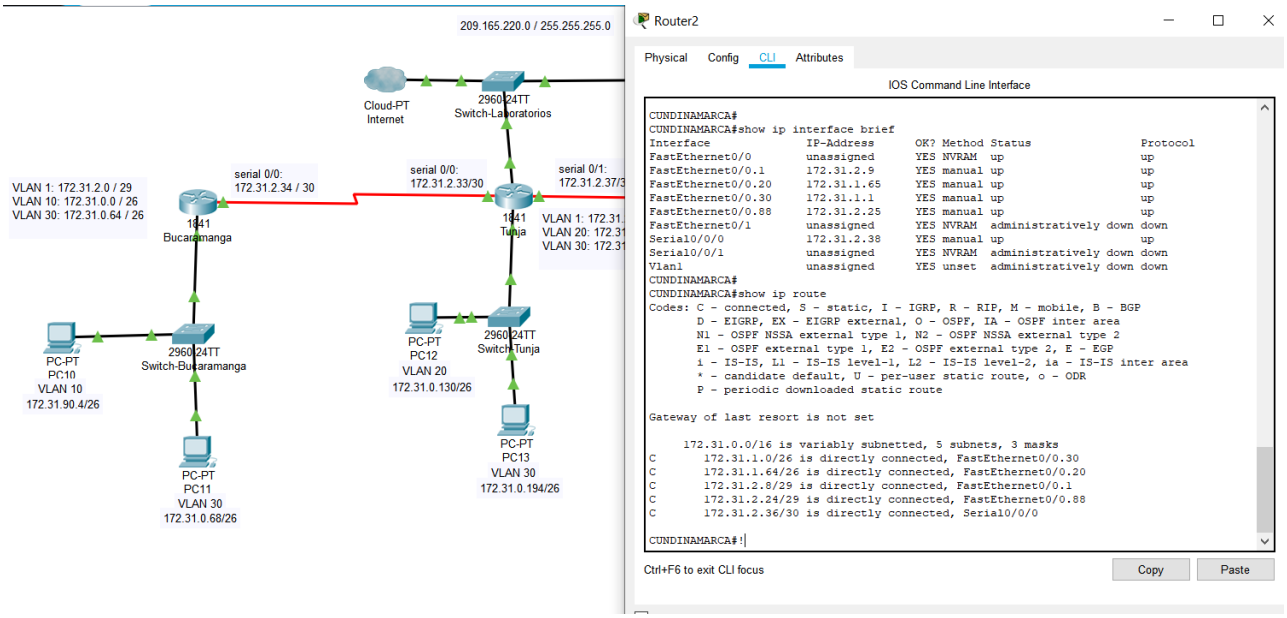


Podemos verificar en este punto la configuración de las interfaces ya realizada y además las respectivas tablas de enrutamiento:

Ya en este punto tenemos configurados todas las interfaces de los router y de los switch, debemos verificar lo hecho hasta el momento, vamos a ver la configuración de las interfaces de cada dispositivo ingresado y vamos a ver las rutas que conoce cada router:


209.165.220.0 / 255.255.255.0
Cloud-PT
Internet
2960-24TT
Switch-Laboratorios
VLAN 1: 172.31.2.0 / 29
VLAN 10: 172.31.0.0 / 26
VLAN 30: 172.31.0.64 / 26
serial 0/0:
172.31.2.34 / 30
serial 0/0:
172.31.2.33/30
1841
Bucaramanga
1841
Tunja
2960-24TT
Switch-Bucaramanga
2960-24TT
Switch-Tunja
PC-PT
PC10
VLAN 10
172.31.90.4/26
PC-PT
PC12
VLAN 20
172.31.0.130/26
PC-PT
PC11
VLAN 30
172.31.0.68/26
PC-PT
PC13
VLAN 30
Router1
Physical
Config
CLI
Attributes
IOS Command Line Interface
bucaramanga>enable
bucaramanga#show ip interface brief
Interface Ip-Address OK? Method Status Protocol
FastEthernet0/0 unassigned YES NVRAM up up
FastEthernet0/0.1 172.31.2.1 YES manual up up
FastEthernet0/0.10 172.31.0.1 YES manual up up
FastEthernet0/0.30 unassigned YES unset up up
FastEthernet0/1 unassigned YES NVRAM administratively down down
Serial0/0/0 172.31.2.34 YES manual up up
Serial0/0/1 unassigned YES NVRAM administratively down down
Vlan1 unassigned YES unset administratively down down
bucaramanga#
bucaramanga#show ip route
Codes: C - connected, S - static, I - IGRP, 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
172.31.0.0/16 is variably subnetted, 3 subnets, 3 masks
C 172.31.0.0/26 is directly connected, FastEthernet0/0.10
C 172.31.2.0/29 is directly connected, FastEthernet0/0.1
C 172.31.2.32/30 is directly connected, Serial0/0/0
bucaramanga#!
Ctrl+F6 to exit CLI focus
Copy
Paste


209.165.220.0 / 255.255.255.0
Cloud-PT
Internet
2960-24TT
Switch-Laboratorios
VLAN 1: 172.31.2.0 / 29
VLAN 10: 172.31.0.0 / 26
VLAN 30: 172.31.0.64 / 26
serial 0/0:
172.31.2.34 / 30
serial 0/0:
172.31.2.33/30
serial 0/1:
1841
Bucaramanga
1841
Tunja
2960-24TT
Switch-Bucaramanga
2960-24TT
Switch-Tunja
PC-PT
PC10
VLAN 10
172.31.90.4/26
PC-PT
PC12
VLAN 20
172.31.0.130/26
PC-PT
PC11
VLAN 30
172.31.0.68/26
PC-PT
PC13
VLAN 30
172.31.0.194/26
Router0
Physical
Config
CLI
Attributes
IOS Command Line Interface
up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0.30, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, 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
El Acceso no autorizado est prohibido
tunja>enable
tunja#show ip interface brief
Interface IP-Address OK? Method Status Protocol
FastEthernet0/0 unassigned YES NVRAM up up
FastEthernet0/0.1 172.3.2.9 YES manual up up
FastEthernet0/0.20 172.31.0.129 YES manual up up
FastEthernet0/0.30 172.31.0.193 YES manual up up
FastEthernet0/1 209.165.220.1 YES manual up up
Serial0/0/0 172.31.2.33 YES manual up up
Serial0/0/1 172.31.2.37 YES manual up up
Vlan1 unassigned YES unset administratively down down
tunja#
tunja#!!
Ctrl+F6 to exit CLI focus
Copy
Paste
Top



Podemos ver en los resultados obtenidos 2 cosas, primero la configuración de las interfaces de los dispositivos es correcto, y segundo vemos que tienen rutas para las diferentes redes, pero solo las conectadas directamente, esto porque no tenemos configurado aún un protocolo de enrutamiento.

Configuramos el protocolo de enrutamiento en cada uno de los routers

BUCARAMANGA(config-if)#router ospf 1

BUCARAMANGA(config-router)#network 172.31.0.0 0.0.0.63 area 0

BUCARAMANGA(config-router)#network 172.31.0.64 0.0.0.63 area 0

BUCARAMANGA(config-router)#network 172.31.2.0 0.0.0.7 area 0

BUCARAMANGA(config-router)#network 172.31.2.32 0.0.0.3 area 0

BUCARAMANGA(config-router)#end

TUNJA(config-if)#router ospf 1

TUNJA(config-router)#network 172.3.2.8 0.0.0.7 area 0

TUNJA(config-router)#network 172.31.0.128 0.0.0.63 area 0

TUNJA(config-router)#network 172.31.0.192 0.0.0.63 area 0

TUNJA(config-router)#network 172.31.2.32 0.0.0.3 area 0

TUNJA(config-router)#network 172.31.2.36 0.0.0.3 area 0

TUNJA(config-router)#end

CUNDINAMARCA(config-if)#router ospf 1

CUNDINAMARCA(config-router)#network 172.31.1.0 0.0.0.63 area 0

CUNDINAMARCA(config-router)#network 172.31.1.64 0.0.0.63 area 0

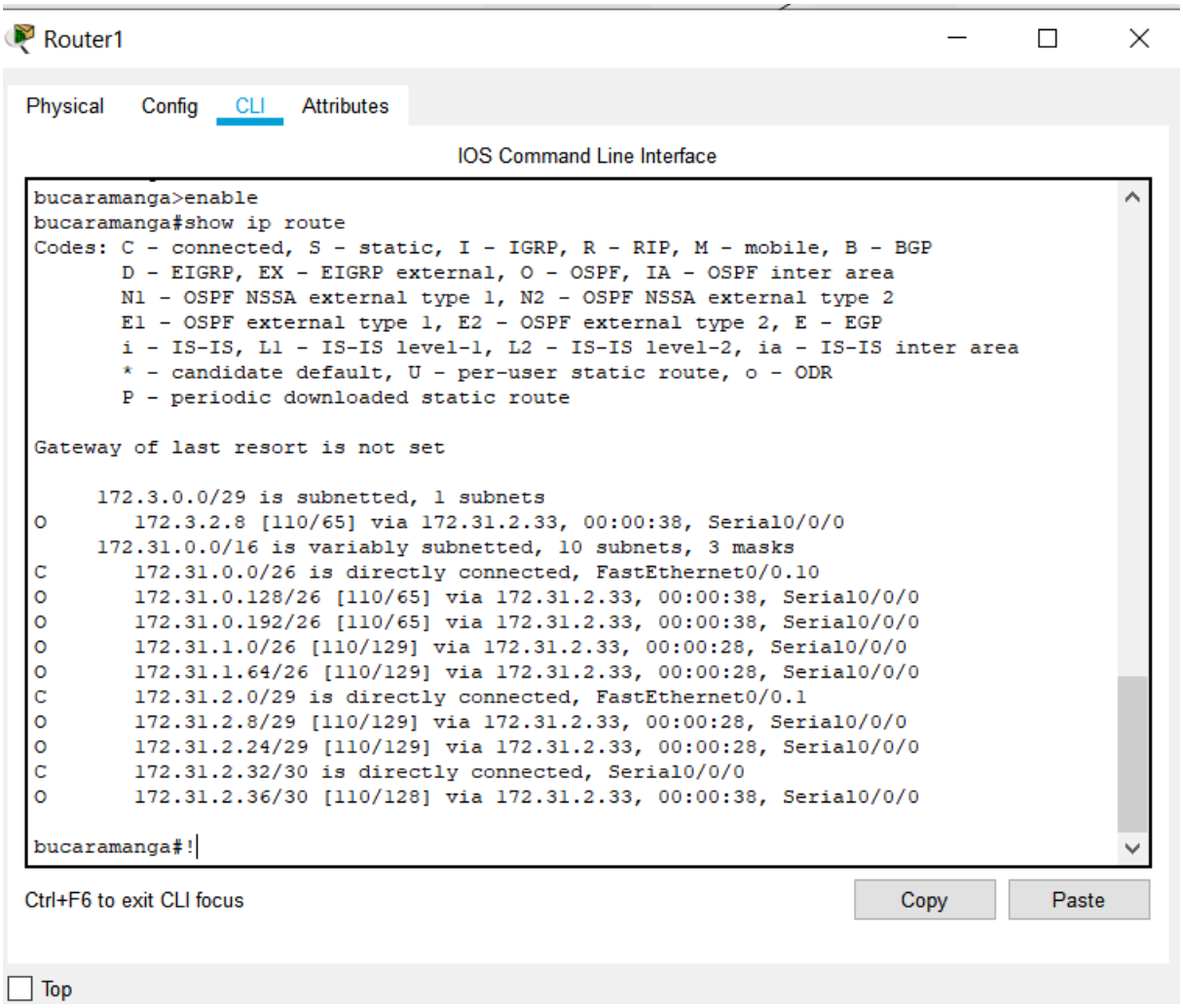
CUNDINAMARCA(config-router)#network 172.31.2.8 0.0.0.7 area 0

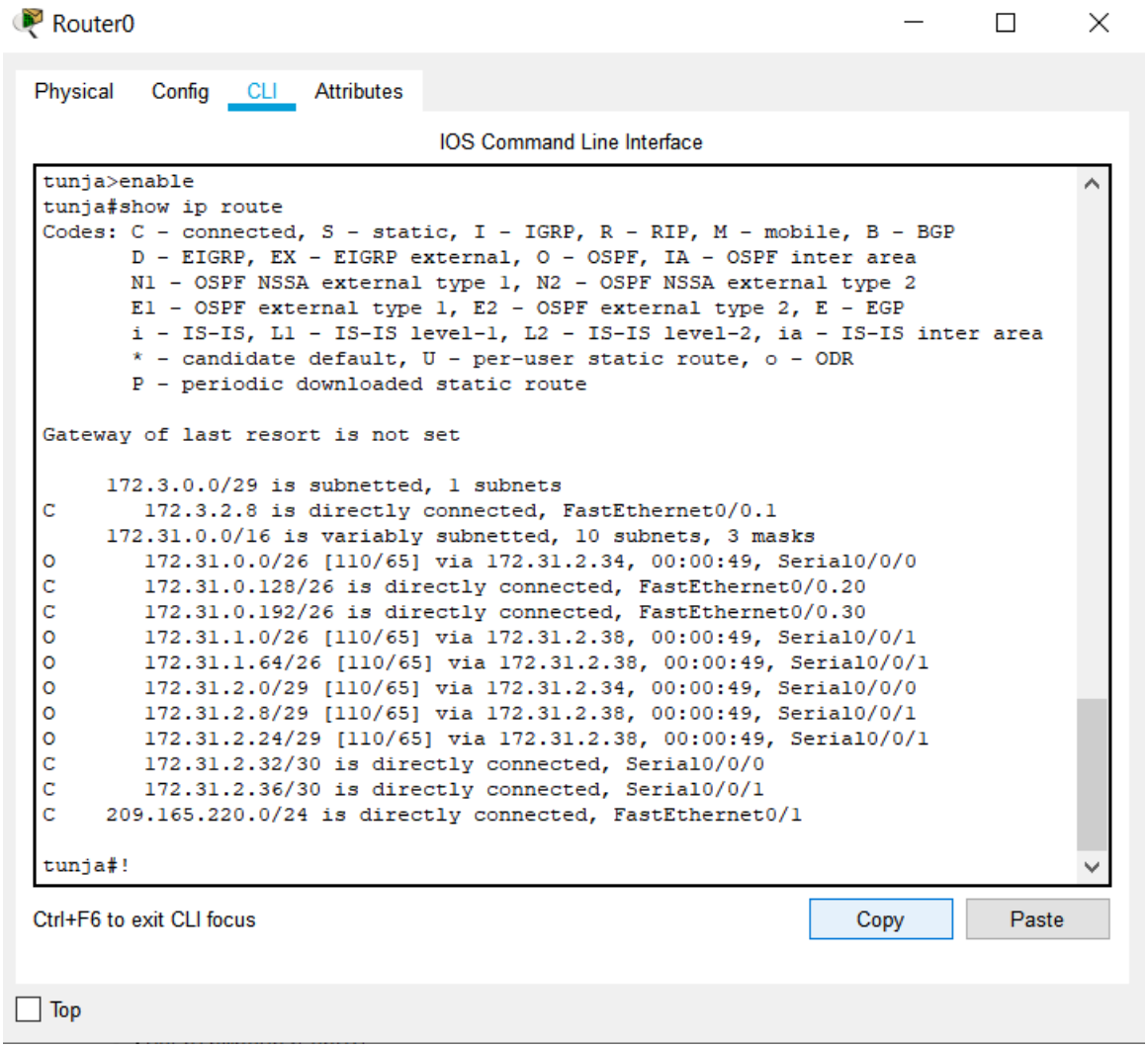
CUNDINAMARCA(config-router)#network 172.31.2.24 0.0.0.7 area 0

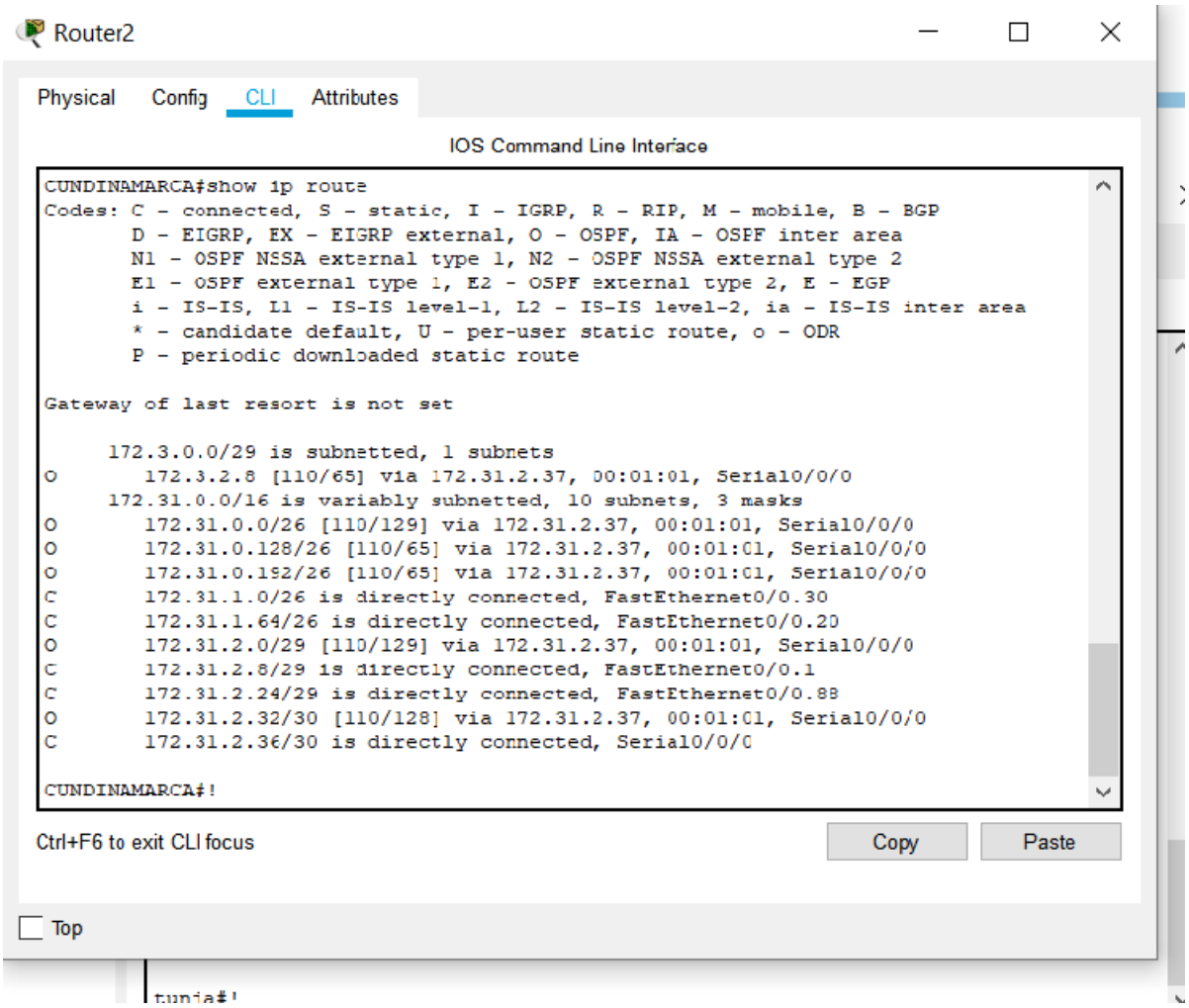
CUNDINAMARCA(config-router)#network 172.31.2.36 0.0.0.3 area 0

CUNDINAMARCA(config-router)#end

Podemos ahora verificar que cada uno de los router aprenda las rutas de los demás routers que hacen parte de la red:


Router1
Physical
Config
CLI
Attributes
IOS Command Line Interface
bucaramanga>enable
bucaramanga#show ip route
Codes: C - connected, S - static, I - IGRP, 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
172.3.0.0/29 is subnetted, 1 subnets
O 172.3.2.8 [110/65] via 172.31.2.33, 00:00:38, Serial0/0/0
172.31.0.0/16 is variably subnetted, 10 subnets, 3 masks
C 172.31.0.0/26 is directly connected, FastEthernet0/0.10
O 172.31.0.128/26 [110/65] via 172.31.2.33, 00:00:38, Serial0/0/0
O 172.31.0.192/26 [110/65] via 172.31.2.33, 00:00:38, Serial0/0/0
O 172.31.1.0/26 [110/129] via 172.31.2.33, 00:00:28, Serial0/0/0
O 172.31.1.64/26 [110/129] via 172.31.2.33, 00:00:28, Serial0/0/0
C 172.31.2.0/29 is directly connected, FastEthernet0/0.1
O 172.31.2.8/29 [110/129] via 172.31.2.33, 00:00:28, Serial0/0/0
O 172.31.2.24/29 [110/129] via 172.31.2.33, 00:00:28, Serial0/0/0
C 172.31.2.32/30 is directly connected, Serial0/0/0
O 172.31.2.36/30 [110/128] via 172.31.2.33, 00:00:38, Serial0/0/0
bucaramanga#!
Ctrl+F6 to exit CLI focus
Copy
Paste
Top


Router0
Physical
Config
CLI
Attributes
IOS Command Line Interface
tunja>enable
tunja#show ip route
Codes: C - connected, S - static, I - IGRP, 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
172.3.0.0/29 is subnetted, 1 subnets
C 172.3.2.8 is directly connected, FastEthernet0/0.1
172.31.0.0/16 is variably subnetted, 10 subnets, 3 masks
O 172.31.0.0/26 [110/65] via 172.31.2.34, 00:00:49, Serial0/0/0
C 172.31.0.128/26 is directly connected, FastEthernet0/0.20
C 172.31.0.192/26 is directly connected, FastEthernet0/0.30
O 172.31.1.0/26 [110/65] via 172.31.2.38, 00:00:49, Serial0/0/1
O 172.31.1.64/26 [110/65] via 172.31.2.38, 00:00:49, Serial0/0/1
O 172.31.2.0/29 [110/65] via 172.31.2.34, 00:00:49, Serial0/0/0
O 172.31.2.8/29 [110/65] via 172.31.2.38, 00:00:49, Serial0/0/1
O 172.31.2.24/29 [110/65] via 172.31.2.38, 00:00:49, Serial0/0/1
C 172.31.2.32/30 is directly connected, Serial0/0/0
C 172.31.2.36/30 is directly connected, Serial0/0/1
C 209.165.220.0/24 is directly connected, FastEthernet0/1
tunja#!
Ctrl+F6 to exit CLI focus
Copy
Paste
Top



- **Autenticación local con AAA.**

Configuramos la autenticación AAA en cada uno de los routers y la aplicamos a las líneas de consola y vty.

BUCARAMANGA(config-line)#username ADMIN1 secret ADMIN1PASS

BUCARAMANGA(config)#aaa new-model

BUCARAMANGA(config)#aaa authentication login aaalocal local

BUCARAMANGA(config)#line console 0

BUCARAMANGA(config-line)#login authentication aaalocal

BUCARAMANGA(config-line)#line vty 0 15

BUCARAMANGA(config-line)#login authentication aaalocal

TUNJA(config-line)#username ADMIN1 secret ADMIN1PASS

TUNJA(config)#aaa new-model

TUNJA(config)#aaa authentication login aaalocal local

TUNJA(config)#line console 0

TUNJA(config-line)#login authentication aaalocal

TUNJA(config-line)#line vty 0 15

TUNJA(config-line)#login authentication aaalocal

CUNDINAMARCA(config-line)#username ADMIN1 secret ADMIN1PASS

CUNDINAMARCA(config)#aaa new-model

CUNDINAMARCA(config)#aaa authentication login aaalocal local

CUNDINAMARCA(config)#line console 0

CUNDINAMARCA(config-line)#login authentication aaalocal

CUNDINAMARCA(config-line)#line vty 0 15

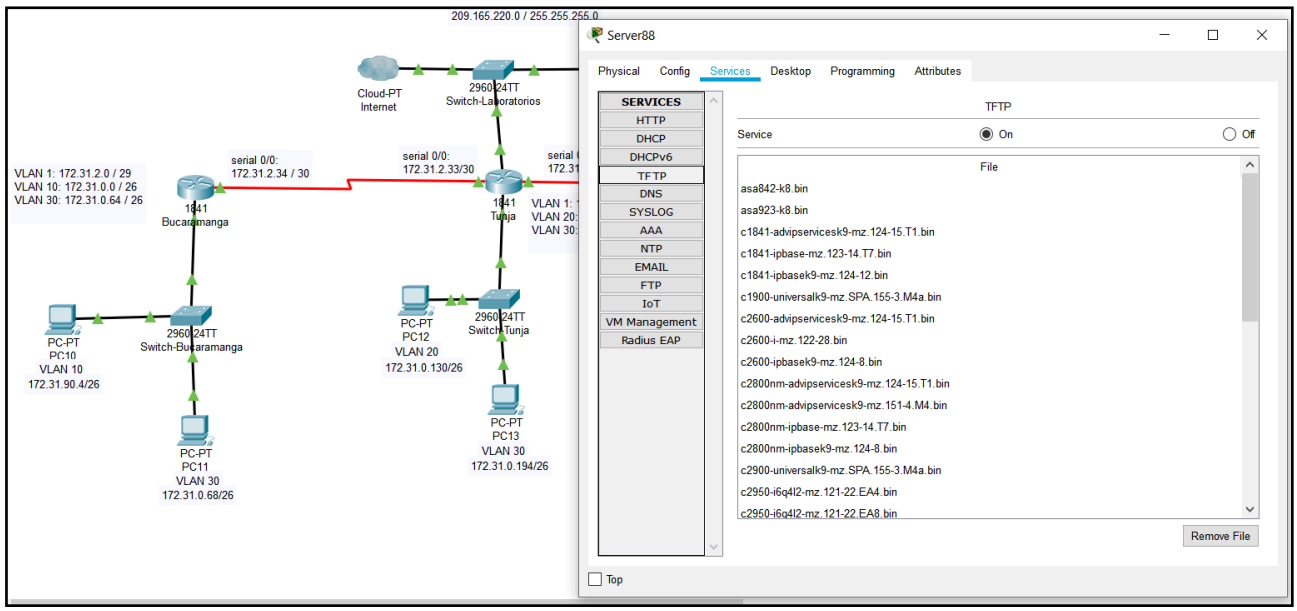
CUNDINAMARCA(config-line)#login authentication aaalocal

- **Un máximo de internos para acceder al router.**

1. **enable**
2. **configure terminal**
3. **login block-for** *seconds* **attempts** *tries* **within** *seconds*
4. **login quiet-mode access-class** {*acl-name* | *acl-number*}
5. **login delay** *seconds*

- BUCARAMANGA(config-line)#login block-for 20 attempts 10 within 60
- TUNJA(config-line)#login block-for 20 attempts 10 within 60
- CUNDINAMARCA(config-line)#login block-for 20 attempts 10 within 60
- **Establezca un servidor TFTP y almacene todos los archivos necesarios de los routers**

SERVER88



Vemos que nuestro servidos TFTP está configurado y funcionando.

2. **El DHCP deberá proporcionar solo direcciones a los hosts de BUCARAMANGA y CUNDINAMARCA**

Vamos a excluir las primeras direcciones IP de cada uno de los rangos antes de asignarlas a los POOL de direcciones que serán asignadas por medio de DHCP.

- TUNJA(config)#ip dhcp excluded-address 172.31.0.1 172.31.0.3
- TUNJA(config)#ip dhcp excluded-address 172.31.0.65 172.31.0.67
- TUNJA(config)#ip dhcp excluded-address 172.31.1.65 172.31.1.67
- TUNJA(config)#ip dhcp excluded-address 172.31.1.1 172.31.1.3

- Ahora ya podemos proceder a configurar y crear los POOL que vamos a emplear, decordemos que padre nuestro caso le vamos a suministrar las IP a las VLAN de BUCARAMANDA y de CUNDINAMARCA, por lo tanto debemos crear 4 POOL diferentes, tal como lo mostramos a continuación, el router encargado de realizer esta asignación va a ser el router de TUNJA:

TUNJA(config)#ip dhcp pool **vlan10buc**

TUNJA(dhcp-config)#network 172.31.0.0 255.255.255.192

TUNJA(dhcp-config)#default-router 172.31.0.1

TUNJA(dhcp-config)#dns-server 8.8.8.8

TUNJA(dhcp-config)#ip dhcp pool **lan30buc**

TUNJA(dhcp-config)#network 172.31.0.64 255.255.255.192

TUNJA(dhcp-config)#default-router 172.31.0.65

TUNJA(dhcp-config)#dns-server 8.8.8.8

TUNJA(dhcp-config)#ip dhcp pool **vlan20cun**

TUNJA(dhcp-config)#network 172.31.1.64 255.255.255.192

TUNJA(dhcp-config)#default-router 172.31.1.65

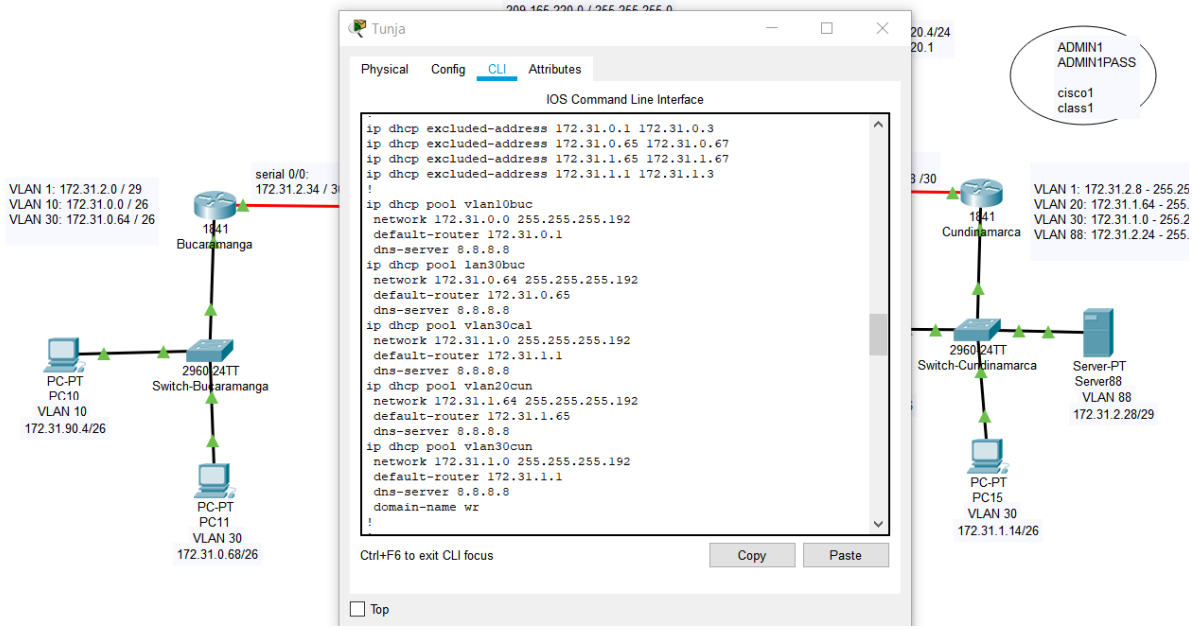
TUNJA(dhcp-config)#dns-server 8.8.8.8

TUNJA(dhcp-config)#ip dhcp pool **vlan30cun**

TUNJA(dhcp-config)#network 172.31.1.0 255.255.255.192

TUNJA(dhcp-config)#default-router 172.31.1.1

TUNJA(dhcp-config)#dns-server 8.8.8.8



Verificamos la configuración del router de TUNJA.

Ahora debemos configurar los router de CUNDINAMARCA y de TUNJA con el fin de que estos puedan acceder al servicio proporcionado por TUNJA de DHCP.

BUCARAMANGA(config)#int f0/0.10

BUCARAMANGA(config-subif)#ip helper-address 172.31.2.33

BUCARAMANGA(config-subif)#int f0/0.30

BUCARAMANGA(config-subif)#ip helper-address 172.31.2.33

BUCARAMANGA(config-subif)#end

BUCARAMANGA#

CUNDINAMARCA(config)#int f0/0.20

CUNDINAMARCA(config-subif)#ip helper-address 172.31.2.37

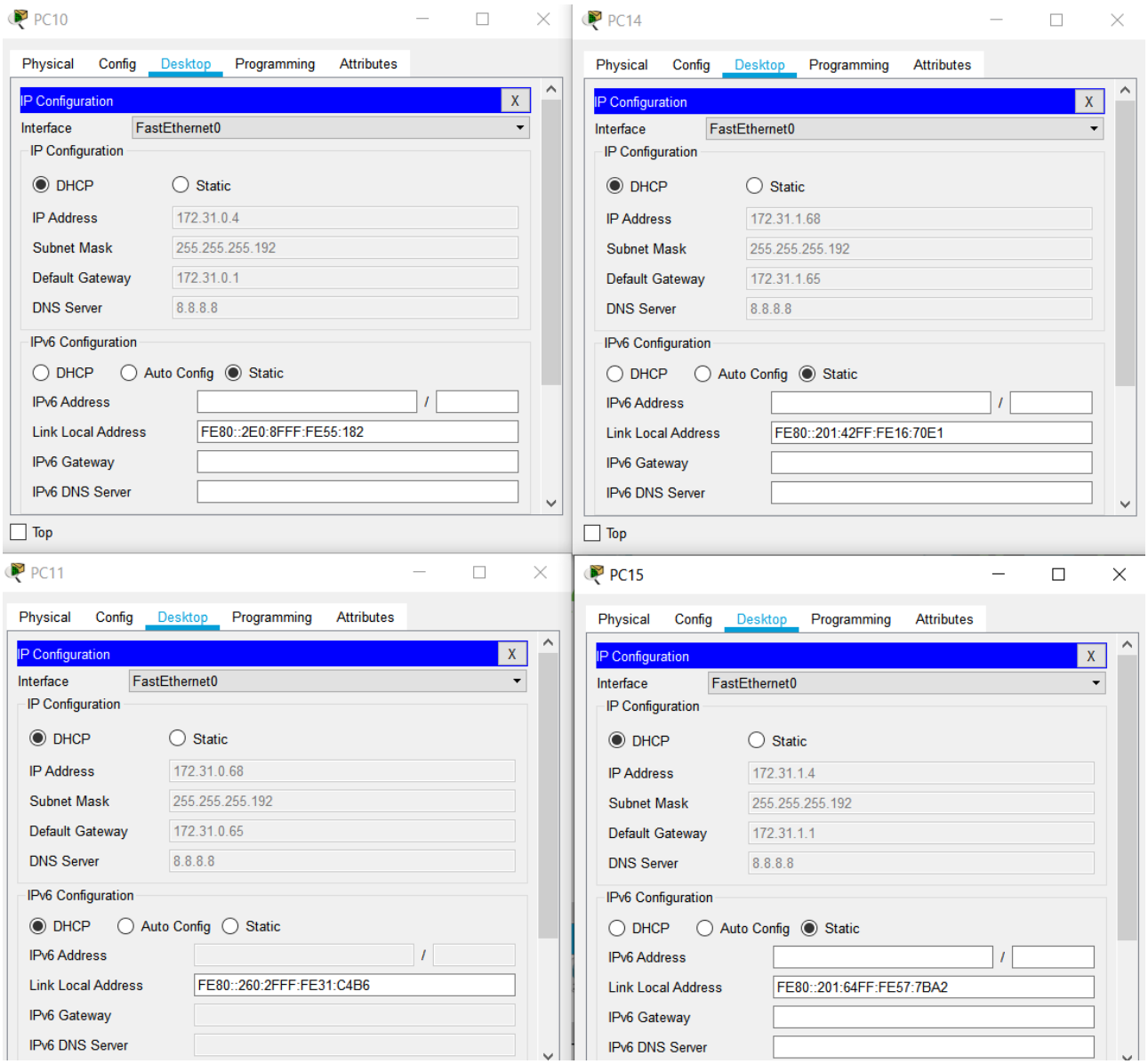
CUNDINAMARCA(config-subif)#int f0/0.30

CUNDINAMARCA(config-subif)#ip helper-address 172.31.2.37

CUNDINAMARCA(config-subif)#end

CUNDINAMARCA#

Debemos verificar que los PC obtengan la IP mediante DHCP:



Se observa que las 4 vlan de BUCARAMANDA y CUNDINAMARCA obtienen sus direcciones automáticamente empleando DHCP.

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

- Asignamos IP NAT STATIC para el servidor:

TUNJA(config)#ip nat inside source static 172.31.2.28 209.165.220.10

TUNJA(config)#access-list 11 permit 172.0.0.0 0.255.255.255

TUNJA(config)#ip nat inside source list 11 interface f0/1 overload

TUNJA(config)#int f0/1

TUNJA(config-if)#ip nat outside

TUNJA(config-if)#int f0/0.1

TUNJA(config-subif)#ip nat inside

TUNJA(config-subif)#int f0/0.20

TUNJA(config-subif)#ip nat inside

TUNJA(config-subif)#int f0/0.30

TUNJA(config-subif)#ip nat inside

TUNJA(config-subif)#int s0/0/0

TUNJA(config-if)#ip nat inside

TUNJA(config-if)#int s0/0/1

TUNJA(config-if)#ip nat inside

TUNJA(config-if)#exit

- Cremos una ruta por defecto y la distribuimos enpleando OSPF.

TUNJA(config)#ip route 0.0.0.0 0.0.0.0 209.165.220.4

TUNJA(config)#router ospf 1

TUNJA(config-router)#default-information originate

TUNJA(config-router)#end

- Aplicamos SHOW IP ROUTE en los routers con el fin de verificar las nuevas configuraciones y que la ruta por defecto se este propagando.

TUNJA#show ip route

Codes: C - connected, S - static, I - IGRP, 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 209.165.220.4 to network 0.0.0.0

172.3.0.0/29 is subnetted, 1 subnets

C 172.3.2.8 is directly connected, FastEthernet0/0.1

172.31.0.0/16 is variably subnetted, 11 subnets, 3 masks

O 172.31.0.0/26 [110/65] via 172.31.2.34, 00:10:47, Serial0/0/0

O 172.31.0.64/26 [110/65] via 172.31.2.34, 00:10:47, Serial0/0/0

C 172.31.0.128/26 is directly connected, FastEthernet0/0.20

C 172.31.0.192/26 is directly connected, FastEthernet0/0.30

O 172.31.1.0/26 [110/65] via 172.31.2.38, 00:10:47, Serial0/0/1

O 172.31.1.64/26 [110/65] via 172.31.2.38, 00:10:47, Serial0/0/1

O 172.31.2.0/29 [110/65] via 172.31.2.34, 00:10:47, Serial0/0/0

O 172.31.2.8/29 [110/65] via 172.31.2.38, 00:10:47, Serial0/0/1

O 172.31.2.24/29 [110/65] via 172.31.2.38, 00:10:47, Serial0/0/1

C 172.31.2.32/30 is directly connected, Serial0/0/0

C 172.31.2.36/30 is directly connected, Serial0/0/1

C 209.165.220.0/24 is directly connected, FastEthernet0/1

S* 0.0.0.0/0 [1/0] via 209.165.220.4

TUNJA#

BUCARAMANGA#show ip route

Codes: C - connected, S - static, I - IGRP, 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 172.31.2.33 to network 0.0.0.0

172.3.0.0/29 is subnetted, 1 subnets

O 172.3.2.8 [110/65] via 172.31.2.33, 00:11:18, Serial0/0/0

172.31.0.0/16 is variably subnetted, 11 subnets, 3 masks

C 172.31.0.0/26 is directly connected, FastEthernet0/0.10

C 172.31.0.64/26 is directly connected, FastEthernet0/0.30

O 172.31.0.128/26 [110/65] via 172.31.2.33, 00:11:18, Serial0/0/0

O 172.31.0.192/26 [110/65] via 172.31.2.33, 00:11:18, Serial0/0/0

O 172.31.1.0/26 [110/129] via 172.31.2.33, 00:11:18, Serial0/0/0

O 172.31.1.64/26 [110/129] via 172.31.2.33, 00:11:18, Serial0/0/0

C 172.31.2.0/29 is directly connected, FastEthernet0/0.1

O 172.31.2.8/29 [110/129] via 172.31.2.33, 00:11:18, Serial0/0/0

O 172.31.2.24/29 [110/129] via 172.31.2.33, 00:11:18, Serial0/0/0

C 172.31.2.32/30 is directly connected, Serial0/0/0

O 172.31.2.36/30 [110/128] via 172.31.2.33, 00:11:18, Serial0/0/0

O*E2 0.0.0.0/0 [110/1] via 172.31.2.33, 00:00:51, Serial0/0/0

BUCARAMANGA#

CUNDINAMARCA#show ip route

Codes: C - connected, S - static, I - IGRP, 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 172.31.2.37 to network 0.0.0.0

172.3.0.0/29 is subnetted, 1 subnets

O 172.3.2.8 [110/65] via 172.31.2.37, 00:12:02, Serial0/0/0

172.31.0.0/16 is variably subnetted, 11 subnets, 3 masks

O 172.31.0.0/26 [110/129] via 172.31.2.37, 00:11:52, Serial0/0/0

O 172.31.0.64/26 [110/129] via 172.31.2.37, 00:11:52, Serial0/0/0

O 172.31.0.128/26 [110/65] via 172.31.2.37, 00:12:02, Serial0/0/0

O 172.31.0.192/26 [110/65] via 172.31.2.37, 00:12:02, Serial0/0/0

C 172.31.1.0/26 is directly connected, FastEthernet0/0.30

C 172.31.1.64/26 is directly connected, FastEthernet0/0.20

O 172.31.2.0/29 [110/129] via 172.31.2.37, 00:11:52, Serial0/0/0

C 172.31.2.8/29 is directly connected, FastEthernet0/0.1

C 172.31.2.24/29 is directly connected, FastEthernet0/0.88

O 172.31.2.32/30 [110/128] via 172.31.2.37, 00:12:02, Serial0/0/0

C 172.31.2.36/30 is directly connected, Serial0/0/0

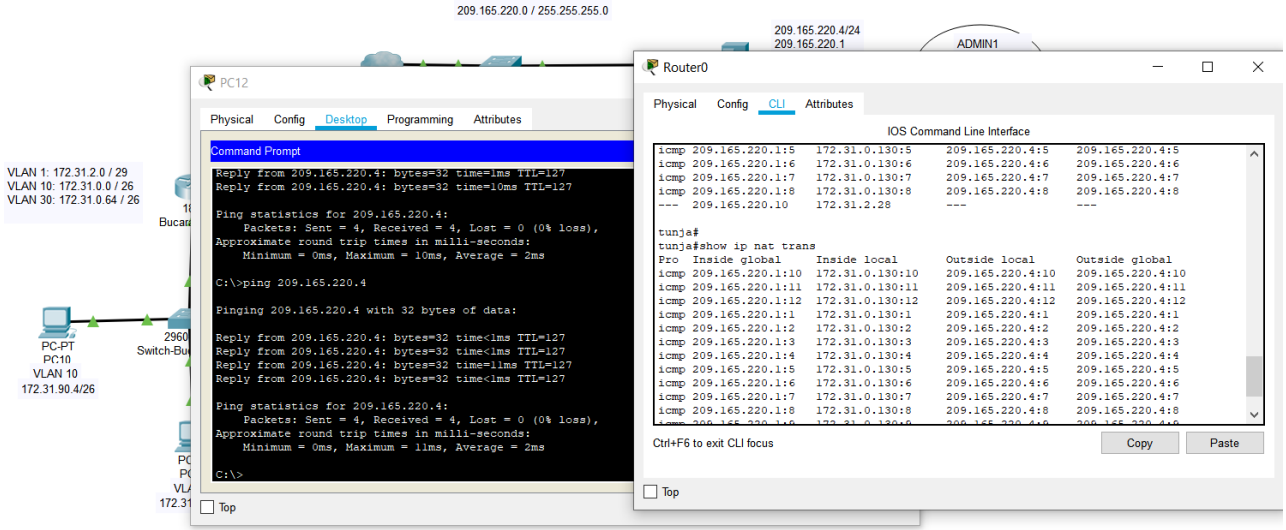
O*E2 0.0.0.0/0 [110/1] via 172.31.2.37, 00:01:34, Serial0/0/0

CUNDINAMARCA#

Vemos que todos los routers cuentan con la ruta por defecto.

ROUTER0

Procedemos a verificar que la traducción de direcciones IP se este llevando a cabo.



4. El enrutamiento deberá tener autenticación.

BUCARAMANGA(config)#int s0/0/0

BUCARAMANGA(config-if)#ip ospf authentication message-digest

BUCARAMANGA(config-if)#ip ospf message-digest-key 1 md5 ospfpass

TUNJA(config)#int s0/0/0

TUNJA(config-if)#ip ospf authentication message-digest

TUNJA(config-if)#ip ospf message-digest-key 1 md5 ospfpass

TUNJA(config-if)#int s0/0/1

TUNJA(config-if)#ip ospf authentication message-digest

TUNJA(config-if)#ip ospf message-digest-key 1 md5 ospfpass

CUNDINAMARCA(config)#int s0/0/0

CUNDINAMARCA(config-if)#ip ospf authentication message-digest

CUNDINAMARCA(config-if)#ip ospf message-digest-key 1 md5 ospfpass

CUNDINAMARCA(config-if)#

5. Listas de control de acceso:

- **Los hosts de VLAN 20 en CUNDINAMARCA no acceden a internet, solo a la red interna de TUNJA.**

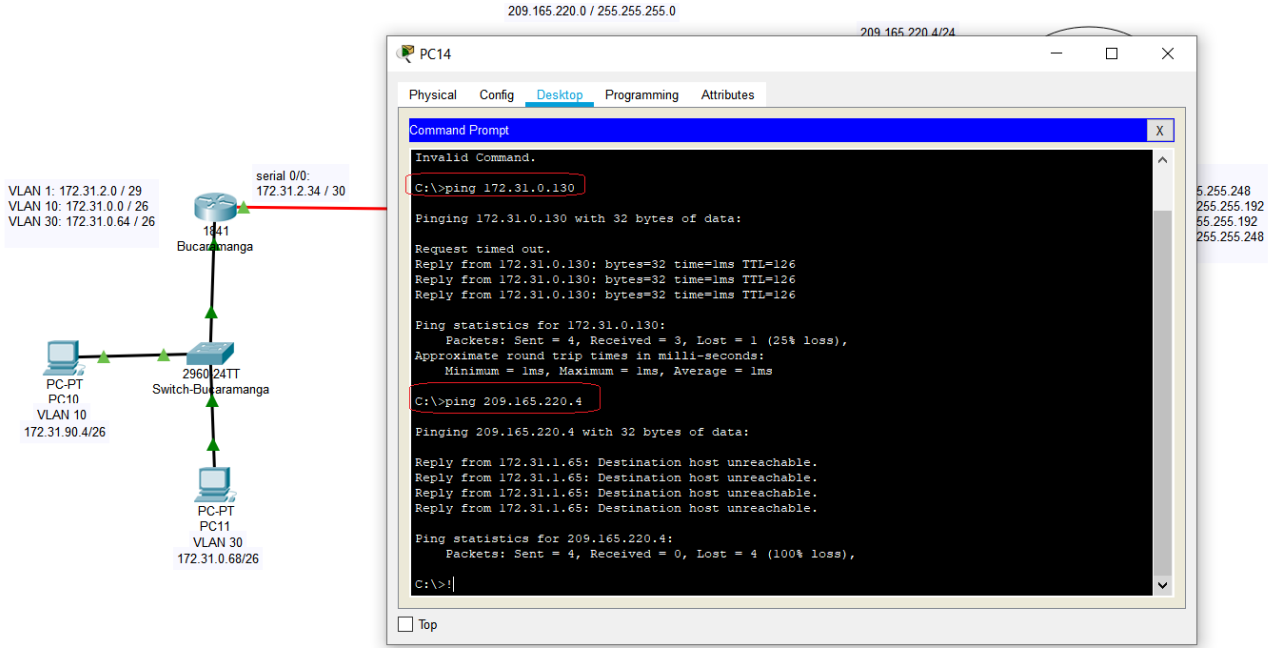
CUNDINAMARCA(config-if)#access-list **151** deny ip 172.31.1.64 0.0.0.63 209.165.220.0 0.0.0.255

CUNDINAMARCA(config)#access-list 151 permit ip any any

CUNDINAMARCA(config)#int f0/0.20

CUNDINAMARCA(config-subif)#ip access-group **151** in

CUNDINAMARCA(config-subif)#



La ACL creada esta cumpliendo con su cometido

- **Los hosts de VLAN 10 en CUNDINAMARCA si acceden a internet y no a la red interna de TUNJA.**

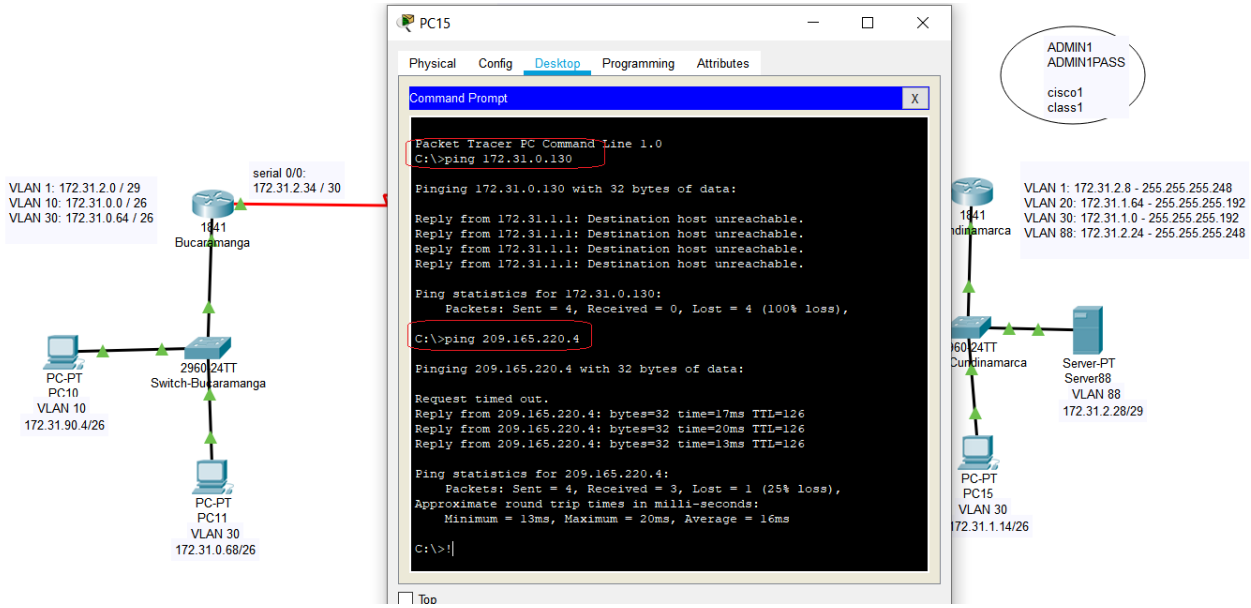
CUNDINAMARCA(config-subif)#access-list **152** permit ip 172.31.1.0 0.0.0.63 209.165.220.0 0.0.0.255

CUNDINAMARCA(config)#access-list **152** deny ip any any

CUNDINAMARCA(config)#int f0/0.30

CUNDINAMARCA(config-subif)#ip access-group **152** in

CUNDINAMARCA(config-subif)#



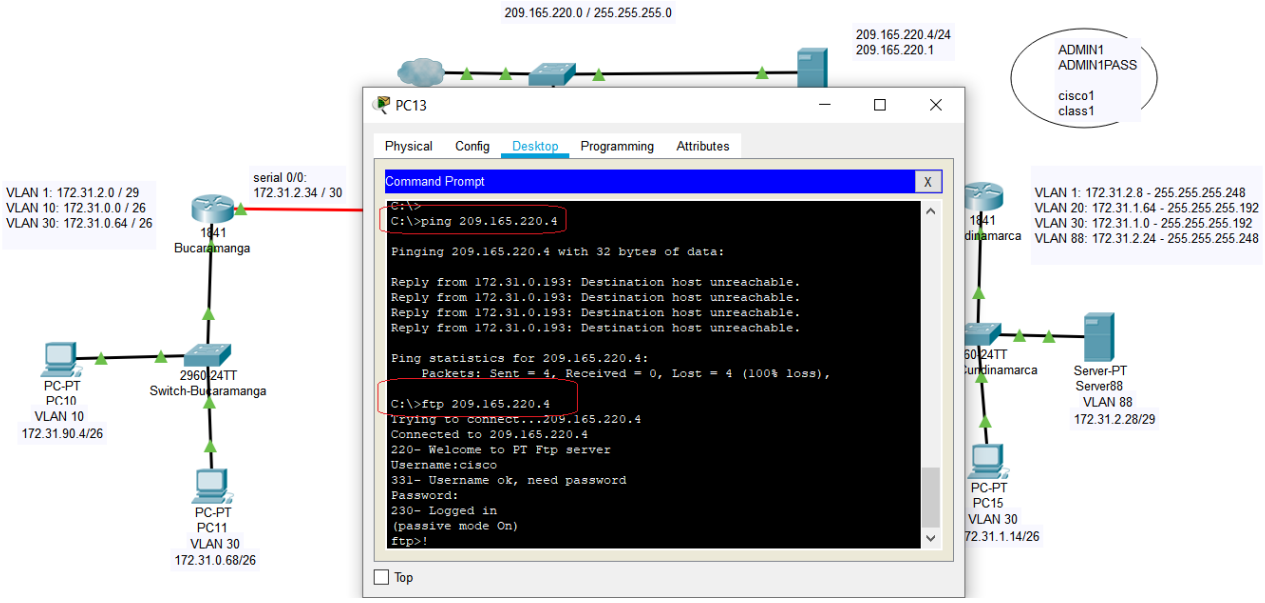
- **Los hosts de VLAN 30 en TUNJA solo acceden a servidores web y ftp de internet.**

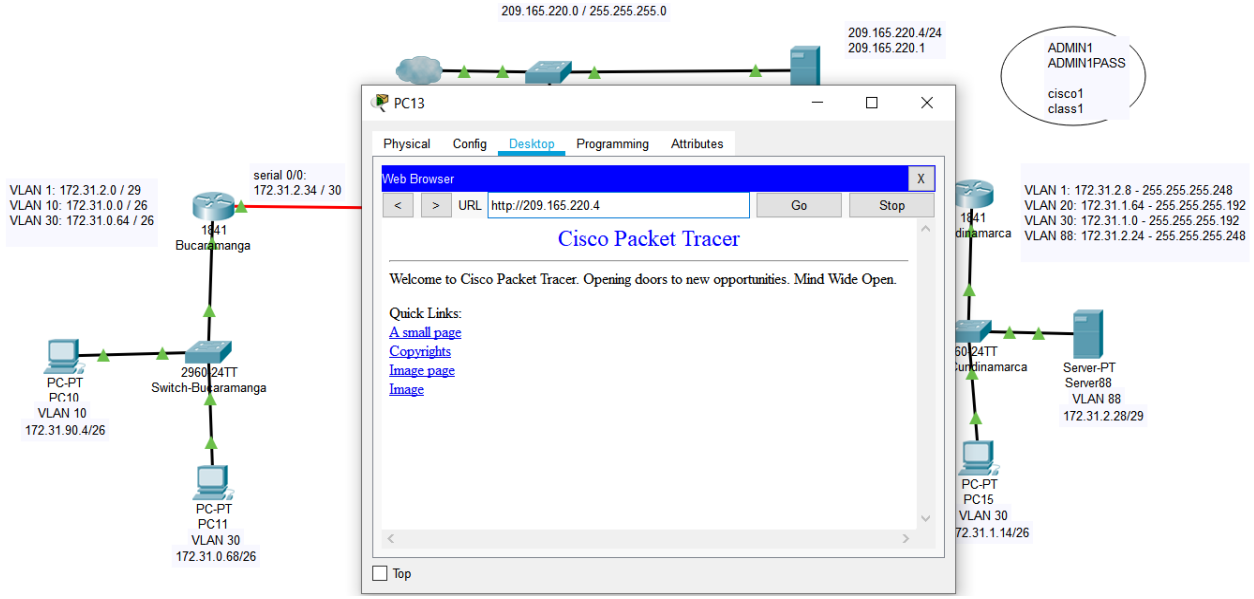
TUNJA(config)#access-list **151** permit tcp 172.31.0.192 0.0.0.63 209.165.220.0 0.0.0.255 eq www

TUNJA(config)#access-list **151** permit tcp 172.31.0.192 0.0.0.63 209.165.220.0 0.0.0.255 eq ftp

TUNJA(config)#int f0/0.30

TUNJA(config-subif)#ip access-group **151** in





- **Los hosts de VLAN 20 en TUNJA solo acceden a la VLAN 20 de CUNDINAMARCA y VLAN 10 de BUCARAMANGA.**

TUNJA(config-subif)#access-list 152 permit ip 172.31.0.128 0.0.0.63 172.31.1.64 0.0.0.63

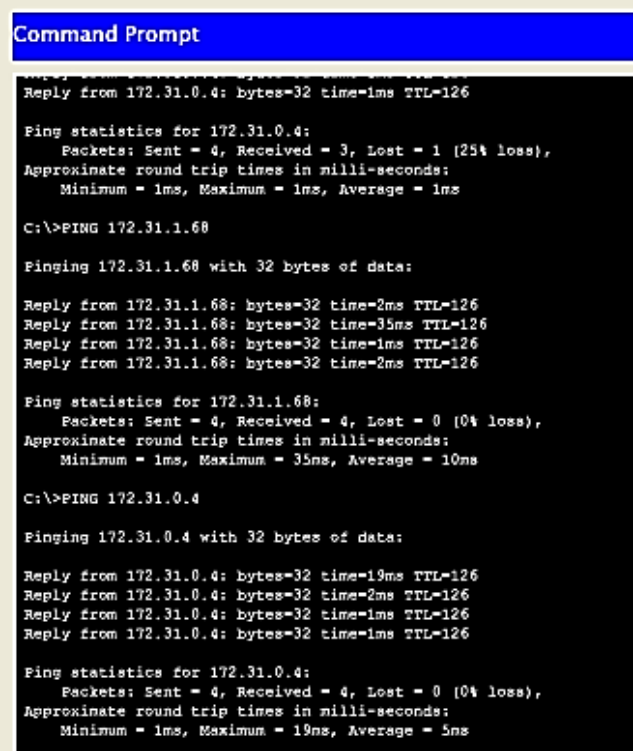
TUNJA(config)#access-list 152 permit ip 172.31.0.128 0.0.0.63 172.31.0.0 0.0.0.63

TUNJA(config)#int f0/0.20

TUNJA(config-subif)#ip access-group **152** in

TUNJA(config-subif)#

PC12



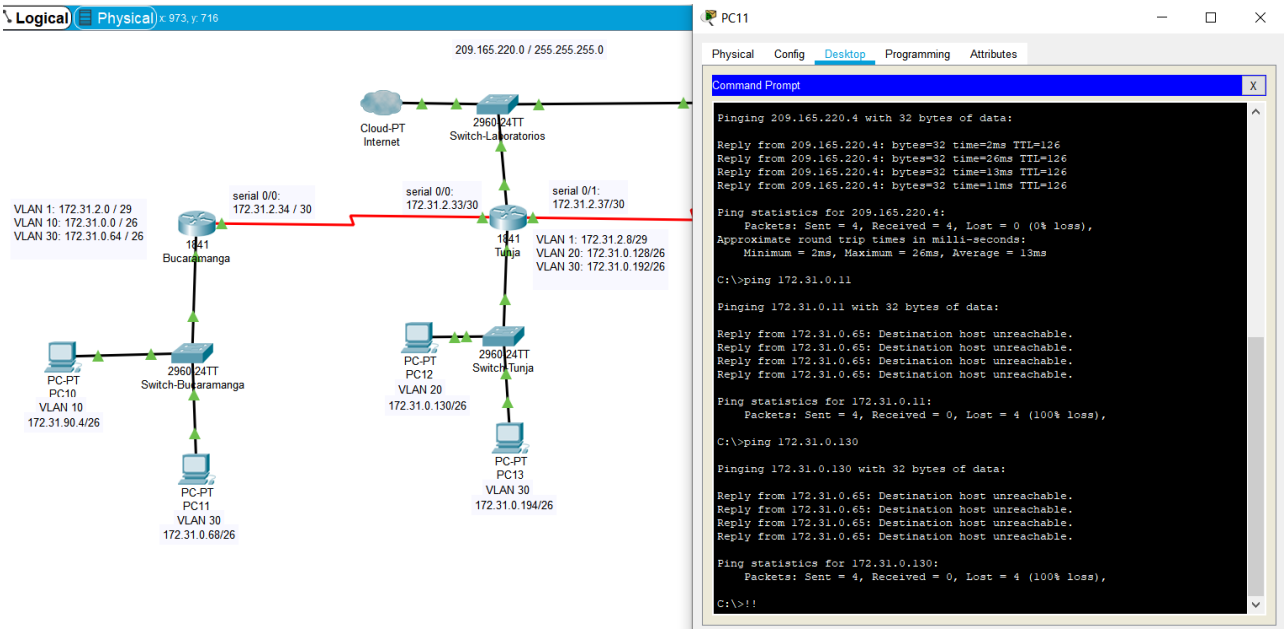
- **Los hosts de VLAN 30 de BUCARAMANGA acceden a internet y a cualquier equipo de VLAN 10.**

BUCARAMANGA(config)#access-list **151** permit ip 172.31.0.64 0.0.0.63 209.165.220.0 0.0.0.255

BUCARAMANGA(config)#int f0/0.30

BUCARAMANGA(config-subif)#ip access-group **151** in

BUCARAMANGA(config-subif)#



Los hosts de VLAN 10 en BUCARAMANGA acceden a la red de CUNDINAMARCA (VLAN 20) y TUNJA (VLAN 20), no internet.

BUCARAMANGA(config-subif)#access-list 152 permit ip 172.31.0.0 0.0.0.63 172.31.1.64 0.0.0.63

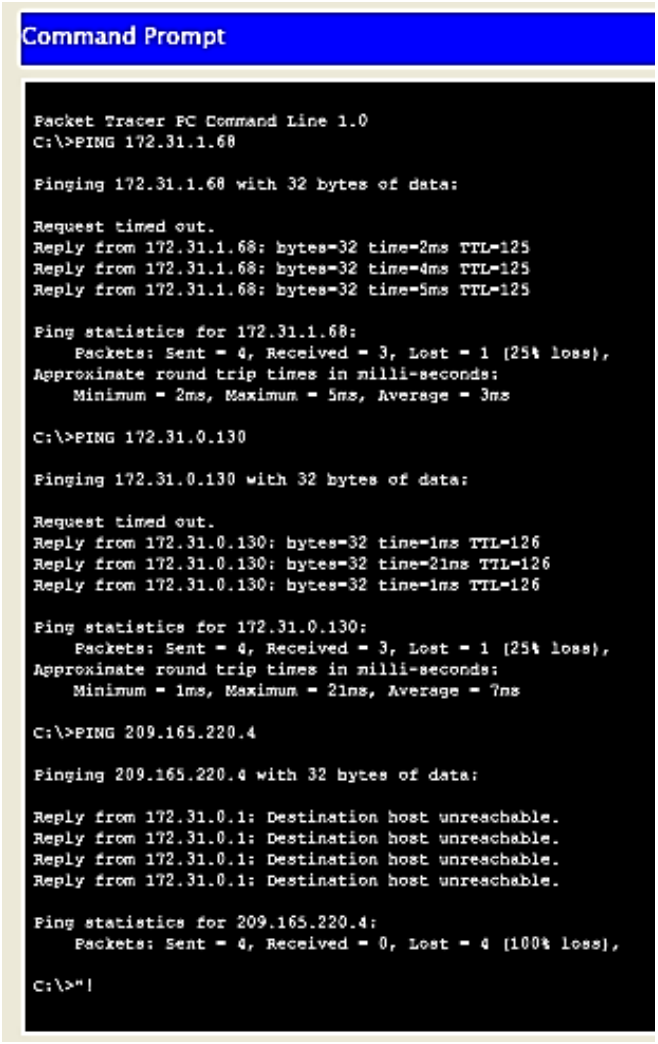
BUCARAMANGA(config)#access-list 152 permit ip 172.31.0.0 0.0.0.63 172.31.0.128 0.0.0.63

BUCARAMANGA(config)#int f0/0.10

BUCARAMANGA(config-subif)#ip access-group 152 in

BUCARAMANGA(config-subif)#

PC10



- **Los hosts de una VLAN no pueden acceder a los de otra VLAN en una ciudad.**

BUCARAMANGA(config-subif)#access-list 153 deny ip 172.31.2.0 0.0.0.7 172.31.0.0 0.0.0.63

BUCARAMANGA(config)#access-list 153 deny ip 172.31.0.64 0.0.0.63 172.31.0.0 0.0.0.63

BUCARAMANGA(config)#access-list 153 permit ip any any

BUCARAMANGA(config)#int f0/0.10

BUCARAMANGA(config-subif)#ip access-group 153 out

TUNJA(config)#access-list 153 deny ip 172.3.2.8 0.0.0.7 172.31.0.128 0.0.0.63

TUNJA(config)#access-list 153 deny ip 172.3.0.192 0.0.0.63 172.31.0.128 0.0.0.63

TUNJA(config)#access-list 153 permit ip any any

TUNJA(config)#int f0/0.20

TUNJA(config-subif)#ip access-group 153 out

CUNDINAMARCA(config)#access-list 153 deny ip 172.31.2.8 0.0.0.7 172.31.1.64 0.0.0.63

CUNDINAMARCA(config)#access-list 153 deny ip 172.31.1.0 0.0.0.63 172.31.1.64 0.0.0.63

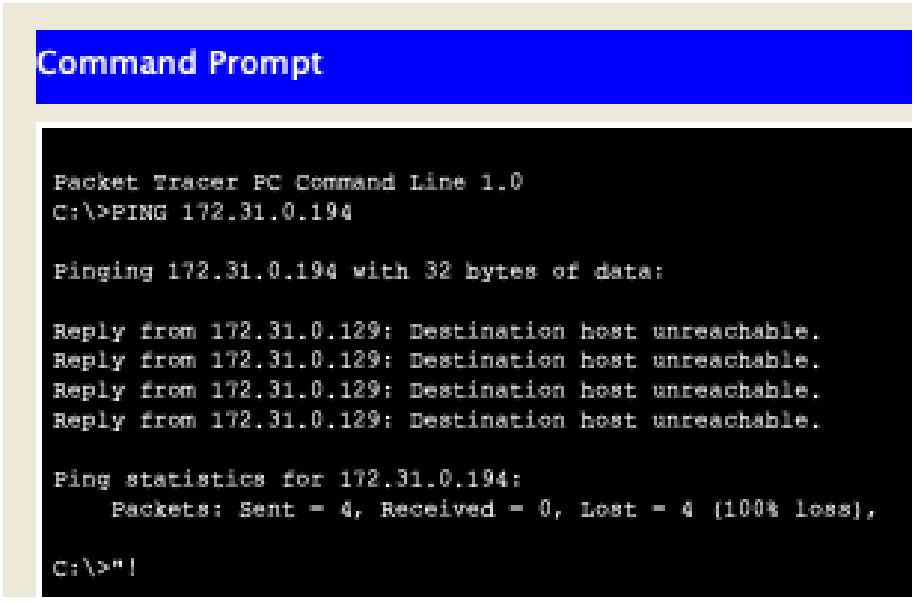
CUNDINAMARCA(config)#access-list 153 deny ip 172.31.2.24 0.0.0.7 172.31.1.64 0.0.0.63

CUNDINAMARCA(config)#access-list 153 permit ip any any

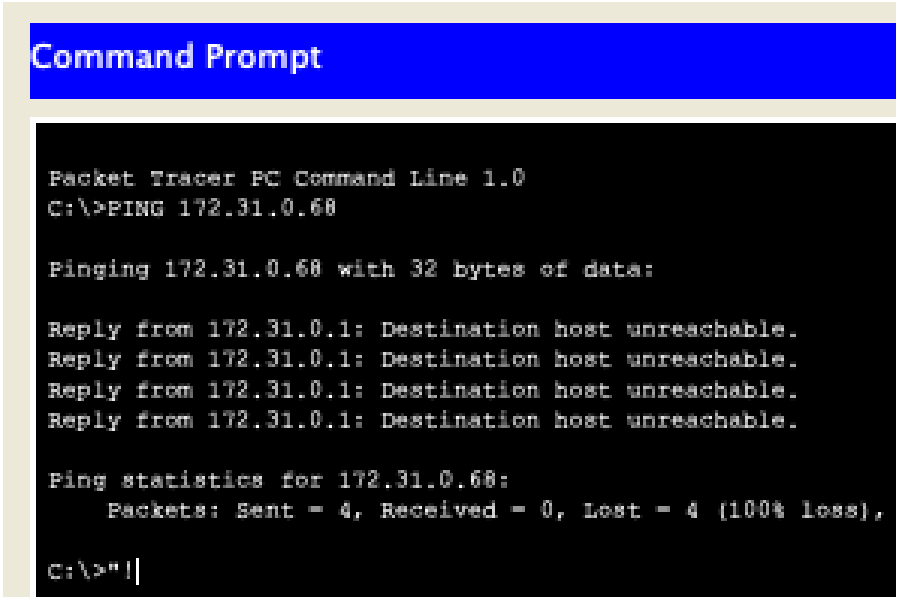
CUNDINAMARCA(config)#int f0/0.20

CUNDINAMARCA(config-subif)#ip access-group **153** out

PC12



PC10



- **Solo los hosts de las VLAN administrativas y de la VLAN de servidores tienen accedo a los routers e internet.**

BUCARAMANGA(config-subif)#access-list 10 permit 172.31.2.0 0.0.0.7

BUCARAMANGA(config)#access-list 10 permit 172.3.2.8 0.0.0.7

BUCARAMANGA(config)#access-list 10 permit 172.31.2.8 0.0.0.7

BUCARAMANGA(config)#line vty 0 15

BUCARAMANGA(config-line)#access-class 10 in

BUCARAMANGA(config-line)#

TUNJA(config-subif)#access-list 10 permit 172.31.2.0 0.0.0.7

TUNJA(config)#access-list 10 permit 172.3.2.8 0.0.0.7

TUNJA(config)#access-list 10 permit 172.31.2.8 0.0.0.7

TUNJA(config)#line vty 0 15

TUNJA(config-line)#access-class 10 in

TUNJA(config-line)#

CUNDINAMARCA(config-subif)#access-list 10 permit 172.31.2.0 0.0.0.7

CUNDINAMARCA(config)#access-list 10 permit 172.3.2.8 0.0.0.7

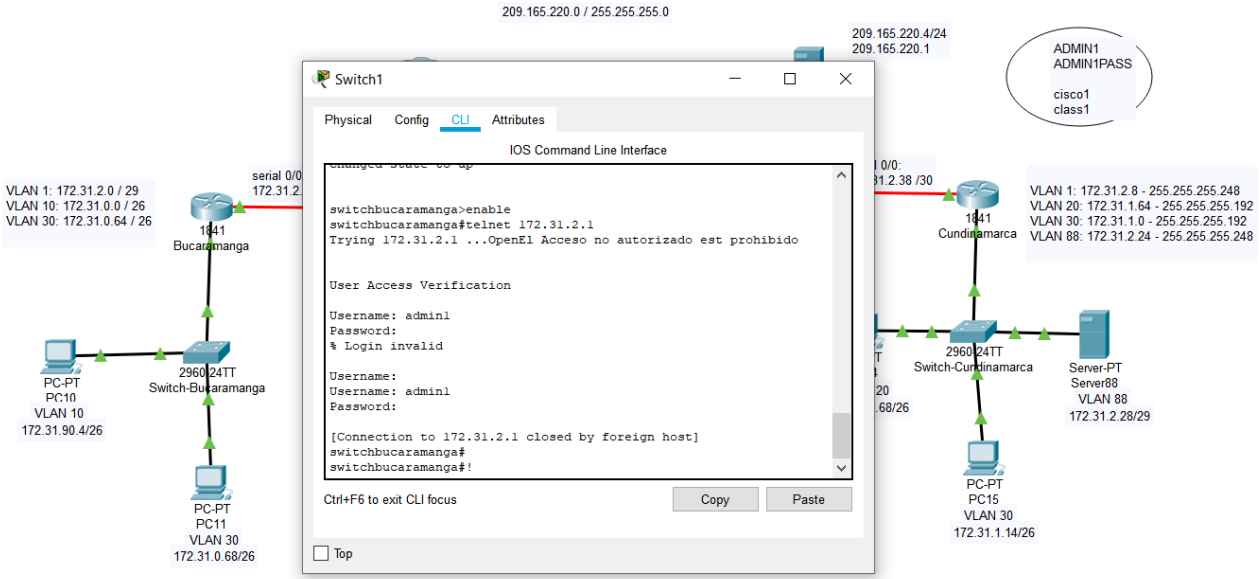
CUNDINAMARCA(config)#access-list 10 permit 172.31.2.8 0.0.0.7

CUNDINAMARCA(config)#line vty 0 15

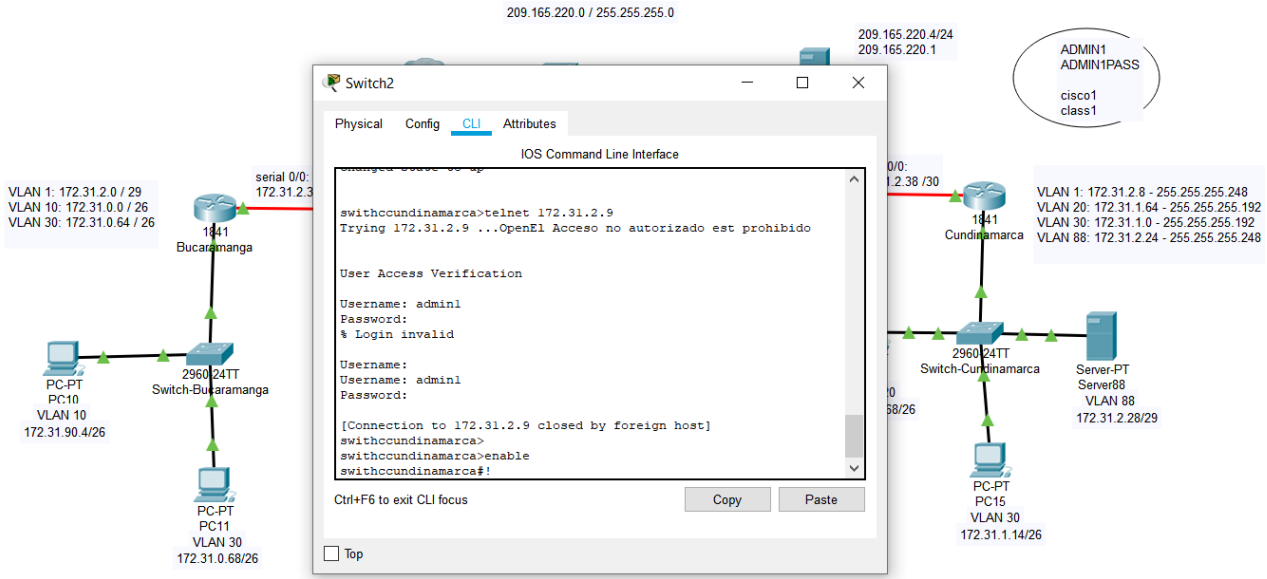
CUNDINAMARCA(config-line)#access-class 10 in

CUNDINAMARCA(config-line)#

SWITCH1



SWITCH2


209.165.220.0 / 255.255.255.0
209.165.220.4/24
209.165.220.1
ADMIN1
ADMIN1PASS
cisco1
class1
VLAN 1: 172.31.2.0 / 29
VLAN 10: 172.31.0.0 / 26
VLAN 30: 172.31.0.64 / 26
1841
Bucaramanga
2960-24TT
Switch-Bucaramanga
PC-PT
PC10
VLAN 10
172.31.90.4/26
PC-PT
PC11
VLAN 30
172.31.0.68/26
1841
Cundinamarca
2960-24TT
Switch-Cundinamarca
Server-PT
Server88
VLAN 88
172.31.2.28/29
PC-PT
PC15
VLAN 30
172.31.1.14/26
VLAN 1: 172.31.2.8 - 255.255.255.248
VLAN 20: 172.31.1.64 - 255.255.255.192
VLAN 30: 172.31.1.0 - 255.255.255.192
VLAN 88: 172.31.2.24 - 255.255.255.248
Switch2
Physical
Config
CLI
Attributes
IOS Command Line Interface
switchcundinamarca>telnet 172.31.2.9
Trying 172.31.2.9 ...OpenEl Acceso no autorizado est prohibido
User Access Verification
Username: admin1
Password:
% Login invalid
Username:
Username: admin1
Password:
[Connection to 172.31.2.9 closed by foreign host]
switchcundinamarca>
switchcundinamarca>enable
switchcundinamarca#!
Ctrl+F6 to exit CLI focus
Copy
Paste
Top

CONCLUSIONES

- Tenemos comunicación de extremo a extremo en nuestra red según la configuración realizada.
- Tuve muchos inconvenientes en la configuración de cada una de las parte de la red, pero gracias al material de apoyo con el que cuenta el Diplomado me fue posible aclarar cada una de ellas y poder llegar a feliz término ¿ el mismo.
- PACKET TRACER se convirtió en nuestra mano derecha, todo lo podemos probar es este simulador una y otra vez hasta que todo funcione.
- Veo con agrado luego de desarrollar el presente trabajo que me ha servido de mucho, la temática aprendida es muy productiva.
- La documentación de la red es completa, desde la etapa de montaje pasando por la etapa de configuración y verificación, aspectos que son muy importantes ya que nos posibilitan la posibilidad de encontrar posibles inconvenientes dentro de la misma.
- Veo que es posible unificar la temática que hemos desarrollado en la solución e implementación de una propuesta real.
- A todo el direccionamiento IP de la red aplicamos VLSM lo cual nos permitió optimizar el número de direcciones por cada subsistema de acuerdo a los requerimientos específicos.
- Se Comprendo muy bien el funcionamiento de cada uno de los protocolos de enrutamiento que intervienen en la red, gracias a ellos puedo optimizar su funcionamiento.
- Se documentó cada uno de los pasos realizados en la red y en cada uno de los dispositivos, lo cual permitió y posibilitó en gran medida el encontrar errores de configuración.
- Para una red grande es prácticamente imposible el manejo manual de las rutas para entrega de paquetes, en estos casos debemos utilizar el direccionamiento dinámico

- Nuestra red es totalmente funcional.

BIBLIOGRAFIA

- CISCO SYSTEM. Modulo Curso de entrenamiento CCNA 1 EXPLORATION (Network Fundamentals y Routing Protocols and Concepts).
- https://www.cisco.com/c/m/en_us/techdoc/dc/reference/cli/n5k/commands/show-ip-eigrp-neighbors.html
-