

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

Trabajo presentado por:
SALOMON MURILLO PAEZ
GRUPO: 203092_27

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 PROFESIONAL

Trabajo presentado por:
SALOMON MURILLO PAEZ
GRUPO: 203092_27

TUTOR
NILSON ALBEIRO FERREIRA MANZANARES

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

NOTA DE ACEPTACION

FIRMA

FIRMA

FIRMA

Agradezco a Dios por bendecirme con la vida, por guiarme a lo largo de mi existencia, por ser el apoyo y fortaleza en aquellos momentos de dificultad y de debilidad en mi vida.

Agradezco a mis padres Salomón y Elvira (Q.E.P.D.), a Javier Rivero Espitia Niño (Q.E.P.D.), a mi esposa Lina Marcela Erazo Amariles, mis hijos Andrés Felipe (Q.E.P.D), Oscar Daniel, Juan Jafet Felipe y Sara Isabela por su apoyo, comprensión y ser los principales promotores de mis sueños, por confiar y creer en mí.

Agradezco a la Dra. Gloria Isabel Vargas Hurtado y a mis docentes de la ECTBI de la UNAD, por su apoyo y haber compartido sus conocimientos a lo largo de la preparación de ciclo profesional.

Estudiante:

TABLA DE CONTENIDO

Resumen	8
Abstract	9
Introducción	10
Justificación	11
Objetivos	12
DESARROLLO ESCENARIO 1	17
DESARROLLO ESCENARIO 2	49
CONCLUSIONES	93
BIBLIOGRAFIA	94

TABLA DE ILUSTRACIONES.

Ilustración 1: topología en Packet Tracer.	22
Ilustración 2: show ip route.....	27
Ilustración 3: Ping desde Medellín	28
Ilustración 4: Show ip eigrp neighbor Medellín.....	30
Ilustración 5: Show ip eigrp neighbor Bogotá.	31
Ilustración 6: Show ip eigrp neighbor Cali.....	32
Ilustración 7: show ip route Bogota.	33
Ilustración 8: Show ip route Medellín.	34
Ilustración 9: show ip route cali.	36
Ilustración 10: prueba de conectividad desde Cali.....	36
Ilustración 11: prueba de conectividad desde WS	38
Ilustración 12: prueba de conectividad desde Servidor	38
Ilustración 13: prueba de conectividad desde medellín.....	39
Ilustración 14: prueba de conectividad desde Cali.....	40
Ilustración 15: telnet desde Medellín.....	41
Ilustración 16: Ping desde Medellín.	42
Ilustración 17: Ping desde Cali.....	42
Ilustración 18: telnet desde WS-1	43
Ilustración 19: Ping desde la PC10 hacia las subredes.	43
Ilustración 20: Ping desde PC12 hacia las diferentes subredes.....	44
Ilustración 21: Ping desde Server0	45
Ilustración 22: Topología ESCENARIO 2.....	46
Ilustración 23: Configuración interfaces Bucaramanga.....	52
Ilustración 24: Configuración interfaces TUNJA.	54
Ilustración 25: Configuración interfaces CUNDINAMARCA.	55
Ilustración 26: conf. interfaces y tabla Bucaramanga	61
Ilustración 27: conf. interfaces y tabla Tunja	61
Ilustración 28: conf. interfaces y tabla Cundinamarca	62
Ilustración 29: Configuración servidor TFTP	66
Ilustración 30: configuración DHCP.	68
Ilustración 31: verificación PC obtiene IP mediante DHCP	71
Ilustración 32: Traducción de direcciones mediante NAT.....	79
Ilustración 33: ACL Hosts de VLAN 20 en CUNDINAMARCA no acceden a internet, solo a la red TUNJA.....	81
Ilustración 34: ACL Hosts de VLAN 10 en CUNDINAMARCA si acceden a internet y no a TUNJA.	82
Ilustración 35: ACL Hosts de VLAN 30 en TUNJA solo acceden a servidores web y ftp de internet	83
Ilustración 36: ACL Hosts de VLAN 20 en TUNJA solo acceden a la VLAN 20 de CUNDINAMARCA y VLAN 10 de BUCARAMANGA.	85
Ilustración 37: ACL Hosts de VLAN 30 de BUCARAMANGA acceden a internet y a VLAN 10.....	86
Ilustración 38: ACL los hosts de VLAN 10 en BUCARAMANGA acceden a la red de CUNDINAMARCA (VLAN 20) y TUNJA (VLAN 20), no internet.	87
Ilustración 39: ACL Hosts de una VLAN no pueden acceder a los de otra VLAN en una ciudad.	88
Ilustración 40: ACL Los hosts de una VLAN no pueden acceder a los de otra VLAN en una ciudad.....	89

Ilustración 41: ACL Solo los hosts de las VLAN administrativas y de la VLAN de servidores tienen acceso a los routers e internet. 90

RESUMEN

A lo largo del presente trabajo y del Diplomado hemos logrado aprender y aplicar una serie de conocimientos dentro de las redes, hemos llegado al punto de familiarizarnos mucho con simuladores como GNS3 y Packet Tracer los cuales han posibilitado que podemos practicar cada uno de los aspectos tratados durante el transcurso del mismo.

En este curso, se adquirió experiencia usando las herramientas y utilidades de redes, como el Packet Tracer, para explorar protocolos y conceptos de redes. Estas herramientas me ayudo a comprender cómo fluyen los datos en una red, y montar las mismas observando el comportamiento y la configuración de los diferentes dispositivos con el fin de que corriamos posibles errores que hayamos cometido durante la etapa de desarrollo.

Se practicará con una serie de conceptos de redes como lo son el direccionamiento y enrutamiento. Con relación al direccionamiento practicaremos con la utilización de VLSM, además realizaremos la respectiva documentación con el fin de tener un soporte escrito y bien documentado de los pasos realizados. Ya en la parte del enrutamiento abordaremos el estudio de una se comandos y diferentes tipos de protocolos que nos ofrecen diferentes posibilidades dependiendo de las circunstancias en la cual lo queremos emplear.

ABSTRACT

Throughout this work and especially the Diploma we have managed to learn and apply a series of knowledge within the networks, we have reached the point of becoming very familiar with simulators such as GNS3 and Packet Tracer which have enabled us to practice each of the aspects treated during the course of it.

In this course, experience was gained using network tools and utilities, such as the Packet Tracer, to explore protocols and networking concepts. These tools helped me to understand how data flows in a network, and assemble it by observing the behavior and configuration of the different devices in order to correct possible mistakes we made during the development stage.

It will be practiced with a series of network concepts such as addressing and routing. With regard to addressing we will practice with the use of VLSM, in addition we will make the respective documentation in order to have a written and well-documented support of the steps taken. Already in the part of the routing we will address the study of one se commands and different types of protocols that offer us different possibilities depending on the circumstances in which we want to use it.

INTRODUCCION

Mediante el desarrollo del presente TRABAJO buscamos realizar la implementación de la red para los ESCENARIOS 1 y 2. Esperamos ser un punto de apoyo para la misma y una fortaleza para su futuro y su crecimiento a nivel local y nacional.

Es importante poder ayudar, pero al igual en el punto que nos encontramos, el desarrollo de esta propuesta también va a ser excelente para nuestra formación profesional, pues gracias a esta propuesta podremos practicar lo aprendido hasta el momento y que mejor manera que desarrollando directamente sobre un caso real que pueda exigirnos a cada día mejorara más.

La propuesta como vemos el archivo entregado donde los plasman el ejercicio será desarrollada desde cero, no hay nada de esta red sobre lo cual podamos trabajar, debemos analizar la situación actual de la empresa para poder tomar decisiones al respecto. Todo el diseño y el montaje lo realizaremos bajo dispositivos CISCO.

Espero el trabajo sea del agrado de todos ustedes y que les contribuya igualmente a solucionar algunas dudas que en el momento tenga.

El proyecto nos va a favorecer muchísimo puesto que será la forma de que apliquemos todo ese conocimiento que a lo largo del Diplomado hemos adquirido, queremos generar en nosotros esa confianza que necesitamos para poder abordar proyectos de cualquier dificultad.

Las redes han cambiado de forma significativa nuestra forma de vivir, nuestra forma de relacionarnos. Estas nos han permitido realizar muchas cosas que antes pensábamos imposibles pero que ahora las tenemos y las podemos hacer con gran facilidad. Utilizamos la red de distintas formas, entre ellas las aplicaciones Web, la telefonía IP, la videoconferencia, los juegos interactivos, el comercio electrónico, la educación y mucho más.

1. JUSTIFICACION

Dentro de muy poco ya seremos profesionales y es de vital importancia que manejen muy bien cada uno de los temas que hemos tratado a lo largo de nuestros programas, en especial lo relacionado con las telecomunicaciones aspecto que se ha convertido en algo indispensable para nuestras vidas tanto personales como laborales, y que mejor manera que de la mano de una de las organizaciones pioneras dentro del campo "CISCO".

Recordemos que estamos inmersos en un mercado laboral en el cual el que más éxito tendrá será la 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 CASO REAL por medio del cual logremos profundizar todos nuestros conocimientos, diseñando, simulando casos reales de empresas reales.

2. OBJETIVOS

2.1 OBJETIVO GENERAL

Desarrollo e implementación de la red de datos para los ESCENARIOS 1 y 2.

Diseño de la Topología de los ESCENARIOS indicados, la cual tiene una serie de sedes a nivel de diferentes ciudades, siguiendo una serie de pautas y necesidades que se nos establece dentro del documento.

2.2 OBJETIVOS ESPECÍFICOS

- Diseñar la red de datos para la empresa la cual se ajuste a las necesidades reales de la empresa.
- Practicar todo lo aprendido hasta el momento, lo cual nos genere esta confianza que necesitamos para el desarrollo de este tipo de propuesta.
- Aplicaremos VLSM en todo el diseño de la red, la intención es mitigar el desperdicio de direcciones IP.
- Realizar la documentación general de la red.
- Practicarnos en la configuración de protocolos de enrutamiento, reconociendo las posibilidades de cada uno de ellos.
- Comprender mucho mejor la utilización de los diferentes comandos de configuración.

3. ESCENARIO 1.

Descripción de escenarios propuestos para la prueba de habilidades

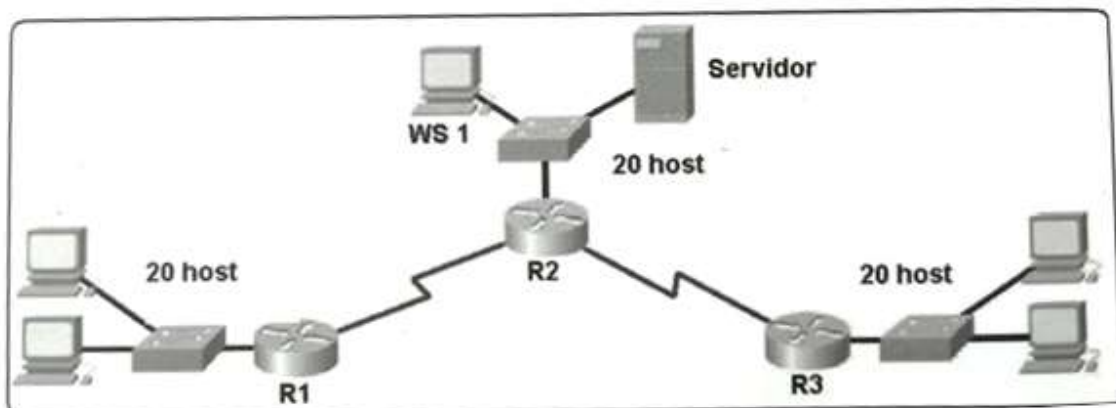
Escenario 1

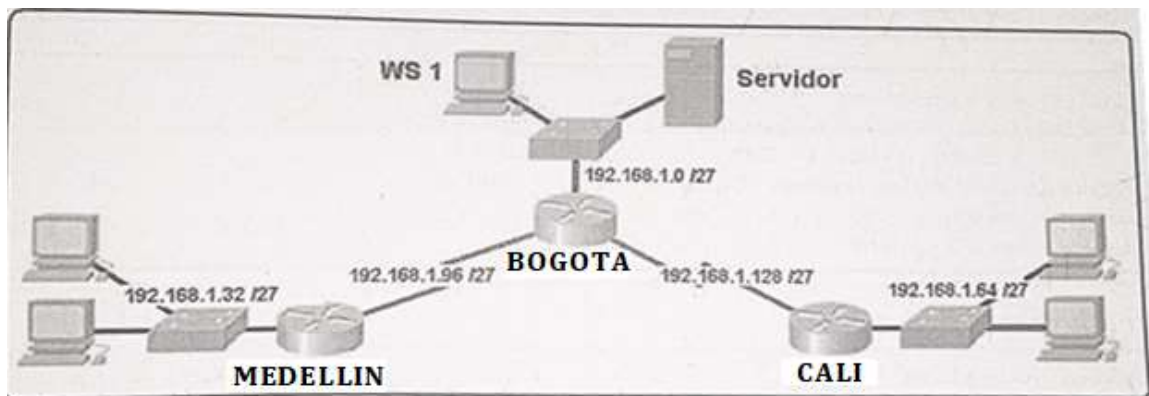
Una empresa posee sucursales distribuidas en las ciudades de Bogotá, Medellín y Cali en donde el estudiante será el administrador de la red, el cual deberá configurar e interconectar entre sí cada uno de los dispositivos que forman parte del escenario, acorde con los lineamientos establecidos para el 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 física 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:

- Se debe dividir (subnetear) la red creando una segmentación en ocho partes, para permitir crecimiento futuro de la red corporativa.
- Asignar una dirección IP a la red.

Parte 2: Configuración Básica.

- 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

- 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 usando 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.

Como trabajo inicial se debe realizar lo siguiente.

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

- Según el cuadro entregado se me está asignando los siguientes rangos para cada una de las subredes, además quedarían disponibles 3 rangos para la posterior utilización de acuerdo al crecimiento de la misma:

LAN BOGOTA	192.168.1.0 / 27
LAN MEDELLIN	192.168.1.32 / 27
LAN CALI	192.168.1.64 / 27
SERIAL - MEDE. - BOG.	192.168.1.96 / 27
SERIAL - CALI - BOGOTA	192.168.1.128 / 27
DISPONIBLES	192.168.1.160 / 27
	192.168.1.192 / 27
	192.168.1.224 / 27

- Tengo que verificar la información de cada una de estas subredes con el fin de poder conocer los rangos de la misma y poder asignar las direcciones IP adecuadas a los diferentes dispositivos e interfaces.

RED	DIR. RED	PRIMER IP	ULTIMA IP	BROADCAST	MASCARA
LAN BOGOTA	192.168.1.0	192.168.1.1	192.168.1.30	192.168.1.31	255.255.255.224
LAN MEDELLIN	192.168.1.32	192.168.1.33	192.168.1.62	192.168.1.63	255.255.255.224
LAN CALI	192.168.1.64	192.168.1.65	192.168.1.94	192.168.1.95	255.255.255.224
SERIAL - MEDE. - BOG.	192.168.1.96	192.168.1.97	192.168.1.126	192.168.1.127	255.255.255.224
SERIAL - CALI - BOGOTA	192.168.1.128	192.168.1.129	192.168.1.158	192.168.1.159	255.255.255.224
DISPONIBLES	192.168.1.160	192.168.1.161	192.168.1.190	192.168.1.191	255.255.255.224
	192.168.1.192	192.168.1.193	192.168.1.222	192.168.1.223	255.255.255.224
	192.168.1.224	192.168.1.225	192.168.1.254	192.168.1.255	255.255.255.224

- Ya con esta información procede a asignar las direcciones IP a las interfaces de los router inicialmente.

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

- Ahora que conozco los rangos de cada una de las subredes proceso a configurar los dispositivos PC y el Servidor.

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

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

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

- Nombre del dispositivo y mensaje:

```
Router(config)#hostname BOGOTA
BOGOTA(config)#no ip domain-lookup
BOGOTA(config)#service password-encryption
BOGOTA(config)#banner motd $!!ACCESO DENEGADO!!$
```

```
Router(config)#hostname MEDELLIN
MEDELLIN(config)#no ip domain-lookup
MEDELLIN(config)#service password-encryption
MEDELLIN(config)#banner motd $!!ACCESO DENEGADO!!$
```

```
Router(config)#hostname CALI
CALI(config)#no ip domain-lookup
CALI(config)#service password-encryption
CALI(config)#banner motd $!!ACCESO DENEGADO!!$
```

- Contraseñas:

```
BOGOTA(config)#enable secret Class123
BOGOTA(config)#line console 0
BOGOTA(config-line)#password Cisco123
BOGOTA(config-line)#login
BOGOTA(config-line)#line vty 0 15
BOGOTA(config-line)#password Cisco123
```

BOGOTA(config-line)#login

MEDELLIN(config)#enable secret Class123

MEDELLIN(config)#line console 0

MEDELLIN(config-line)#password Cisco123

MEDELLIN(config-line)#login

MEDELLIN(config-line)#line vty 0 15

MEDELLIN(config-line)#password Cisco123

MEDELLIN(config-line)#login

CALI(config)#enable secret Class123

CALI(config)#line console 0

CALI(config-line)#password Cisco123

CALI(config-line)#login

CALI(config-line)#line vty 0 15

CALI(config-line)#password Cisco123

CALI(config-line)#login

- Procedo ahora a configurar los switches, para esta red solo se necesita el nombre, el mensaje y las contraseñas.

Switch(config)#hostname switchbogota

switchbogota(config)#no ip domain-lookup

switchbogota(config)#service password-encryption

switchbogota(config)#banner motd \$!!ACCESO DENEGADOj;\$

switchbogota(config)#enable secret Class123

switchbogota(config)#line console 0

```
switchbogota(config-line)#password Cisco123
```

```
switchbogota(config-line)#login
```

```
switchbogota(config-line)#line vty 0 15
```

```
switchbogota(config-line)#password Cisco123
```

```
switchbogota(config-line)#login
```

```
Switch#conf term
```

```
switchmedellin(config)#hostname switchmedellin
```

```
switchmedellin(config)#no ip domain-lookup
```

```
switchmedellin(config)#service password-encryption
```

```
switchmedellin(config)#banner motd $!!ACCESO DENEGADOj;$
```

```
switchmedellin(config)#enable secret Class123
```

```
switchmedellin(config)#line console 0
```

```
switchmedellin(config-line)#password Cisco123
```

```
switchmedellin(config-line)#login
```

```
switchmedellin(config-line)#line vty 0 15
```

```
switchmedellin(config-line)#password Cisco123
```

```
switchmedellin(config-line)#login
```

```
Switch(config)#hostname switchcali
```

```
switchcali(config)#no ip domain-lookup
```

```
switchcali(config)#service password-encryption
```

```
switchcali(config)#banner motd $!!ACCESO DENEGADOj;$
```

```
switchcali(config)#enable secret Class123
```

```
switchcali(config)#line console 0
```

```
switchcali(config-line)#password Cisco123
```

```
switchcali(config-line)#login
```

```
switchcali(config-line)#line vty 0 15
```

```
switchcali(config-line)#password Cisco123
```

```
switchcali(config-line)#login
```

```
switchcali(config-line)#
```

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

La topología queda montada en packet tracer:

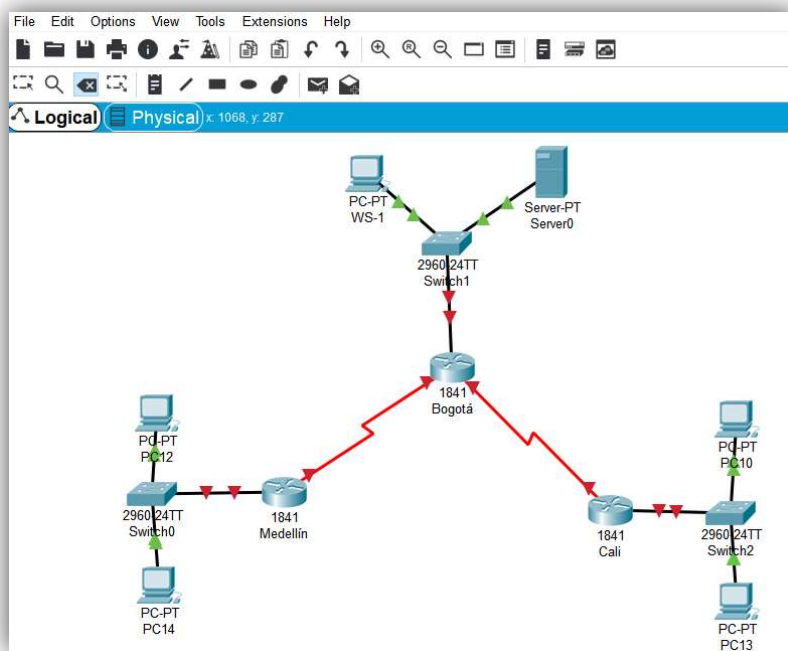


Ilustración 1: topología en Packet Tracer.

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.

LAN BOGOTA	192.168.1.0 / 27
LAN MEDELLIN	192.168.1.32 / 27
LAN CALI	192.168.1.64 / 27
SERIAL - MEDE. - BOG.	192.168.1.96 / 27
SERIAL - CALI - BOGOTA	192.168.1.128 / 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

Y los 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

- Procedemos a realizar la configuración de estos dispositivos y las interfaces.

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#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#

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.

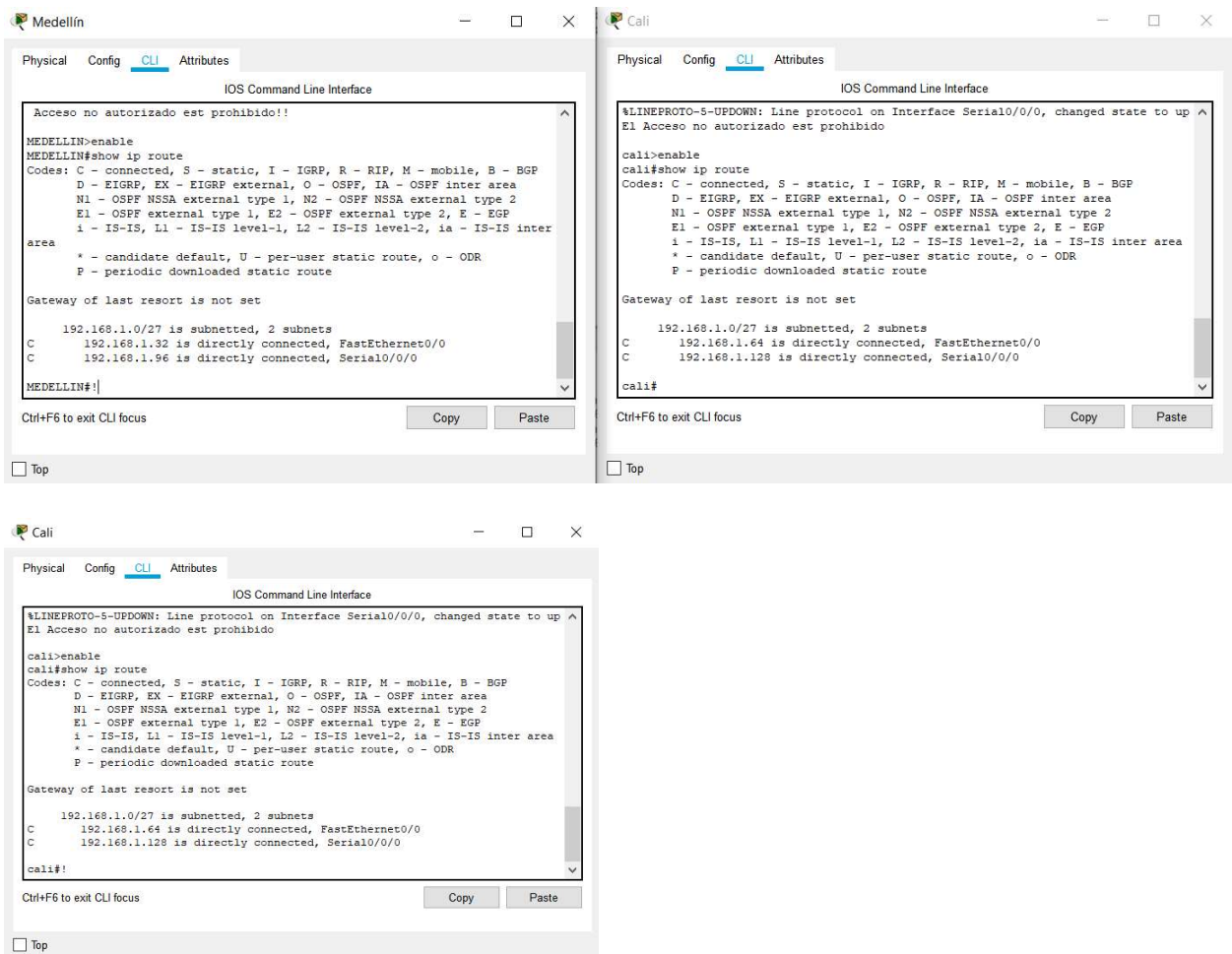


Ilustración 2: show ip route.

Como no contamos con un protocolo de enrutamiento configurado las rutas que se nos muestra solo las redes que estan conectadas directamente.

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

```
MEDELLIN#ping 192.168.1.34

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.34, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 0/1/3 ms

MEDELLIN#ping 192.168.1.35

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.35, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 0/2/4 ms

MEDELLIN#ping 192.168.1.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.2, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)

MEDELLIN#ping 192.168.1.30

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.30, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)

MEDELLIN#ping 192.168.1.66

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.66, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)

MEDELLIN#ping 192.168.1.67

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.67, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)

MEDELLIN#
```

Ilustración 3: Ping desde Medellín

Vemos que solo tenemos acceso a los dispositivos que están conectados directamente.

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)#  
BOGOTA(config-if)#router eigrp 200  
BOGOTA(config-router)#no auto-summary  
BOGOTA(config-router)#network 192.168.1.0  
BOGOTA(config-router)#end
```

Configuración Interfaces Router Medellín.

```
MEDELLIN(config-if)#  
MEDELLIN(config-if)#router eigrp 200  
MEDELLIN(config-router)#no auto-summary  
MEDELLIN(config-router)#network 192.168.1.0  
MEDELLIN(config-router)#end
```

Configuración Interfaces Router CALI.

```
CALI(config-if)#router eigrp 200  
CALI(config-router)#no auto-summary  
CALI(config-router)#network 192.168.1.0  
CALI(config-router)#end
```

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

SHOW IP EIGRP NEIGHBOR

Este comando es el que debemos aplicar a cada uno de los routers con el fin de verificar si existe vecinos EIGRP.

SHOW IP EIGRP TOPOLOGY

Use el comando show ip eigrp topology para determinar los estados del Algoritmo de actualización difusa (DUAL) y para depurar posibles problemas DUAL.



The screenshot shows a terminal window titled 'Medellín' with tabs for 'Physical', 'Config', 'CLI', and 'Attributes'. The 'CLI' tab is active, displaying the 'IOS Command Line Interface'. The user has entered the command 'enable' and then 'show ip eigrp neighbor'. The output shows one neighbor at 192.168.1.98 on interface Serial0/0/0. The user then enters 'show ip eigrp topology', and the output shows the IP-EIGRP topology table for AS 200/ID(192.168.1.99) with codes for Passive, Active, Update, Query, Reply, and Reply status. The topology table lists several routes with their successors and metrics.

```
MEDELLIN>enable
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 12 00:15:22 40 1000 0 6

MEDELLIN#
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

MEDELLIN#
MEDELLIN#!
```

Ilustración 4: Show ip eigrp neighbor Medellín.

The screenshot shows a terminal window titled 'Bogotá' with tabs for 'Physical', 'Config', 'CLI', and 'Attributes'. The 'CLI' tab is active, displaying the 'IOS Command Line Interface'. The user has entered two commands: 'show ip eigrp neighbor' and 'show ip eigrp topology'. The output of the first command is a table of EIGRP neighbors. The output of the second command shows the EIGRP topology table for AS 200/ID(192.168.1.130), listing various routes and their successors.

```
bogota#
bogota#show ip eigrp neighbor
IP-EIGRP neighbors for process 200
H   Address          Interface      Hold Uptime    SRTT   RTO   Q   Seq
   (sec)              (ms)          (ms)          Cnt   Num
0   192.168.1.131     Se0/0/1       13   00:17:04    40    1000  0   7
1   192.168.1.99     Se0/0/0       12   00:17:00    40    1000  0   7

bogota#
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 192.168.1.131 (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
bogota#!
```

Ilustración 5: Show ip eigrp neighbor Bogotá.



The screenshot shows a Cisco CLI window titled 'Cali' with tabs for 'Physical', 'Config', 'CLI', and 'Attributes'. The 'CLI' tab is active, displaying the 'IOS Command Line Interface'. The user has entered the command 'show ip eigrp neighbor', which has been highlighted with a red box. The output shows one EIGRP neighbor at 192.168.1.130 on interface Se0/0/0. The user then enters 'show ip eigrp topology', also highlighted with a red box. The output shows the EIGRP topology table for AS 200/ID(192.168.1.131), listing several routes with their successors and metrics.

```
cali#
cali#show ip eigrp neighbor
IP-EIGRP neighbors for process 200
H   Address          Interface          Hold Uptime      SRTT   RTO   Q   Seq
   (sec)              (ms)              (sec)            (ms)   Cnt   Num
0   192.168.1.130     Se0/0/0           14   00:18:28   40    1000  0   5

cali#
cali#show ip eigrp topology
IP-EIGRP Topology Table for AS 200/ID(192.168.1.131)

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
cali#!
```

Ilustración 6: Show ip eigrp neighbor Cali.

Vemos en los resultados anteriores que luego de aplicar la configuración necesaria todo esta funcionando a la perfección.

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

```
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, 00:04:24, Serial0/0/0
D       192.168.1.64 [90/2172416] via 192.168.1.131, 00:05:07, 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

bogota#
```

Ilustración 7: show ip route Bogota.

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

```
MEDELLIN#
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, 00:04:12, 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, 00:04:12, 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, 00:04:12, Serial0/0/0

MEDELLIN#
```

Ilustración 8: Show ip route Medellín.

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

```

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, 00:05:15, Serial0/0/0
D    192.168.1.32 [90/2684416] via 192.168.1.130, 00:04:32, 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, 00:04:39, Serial0/0/0
C    192.168.1.128 is directly connected, Serial0/0/0

cali#

```

Ilustración 9: show ip route cali.

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.

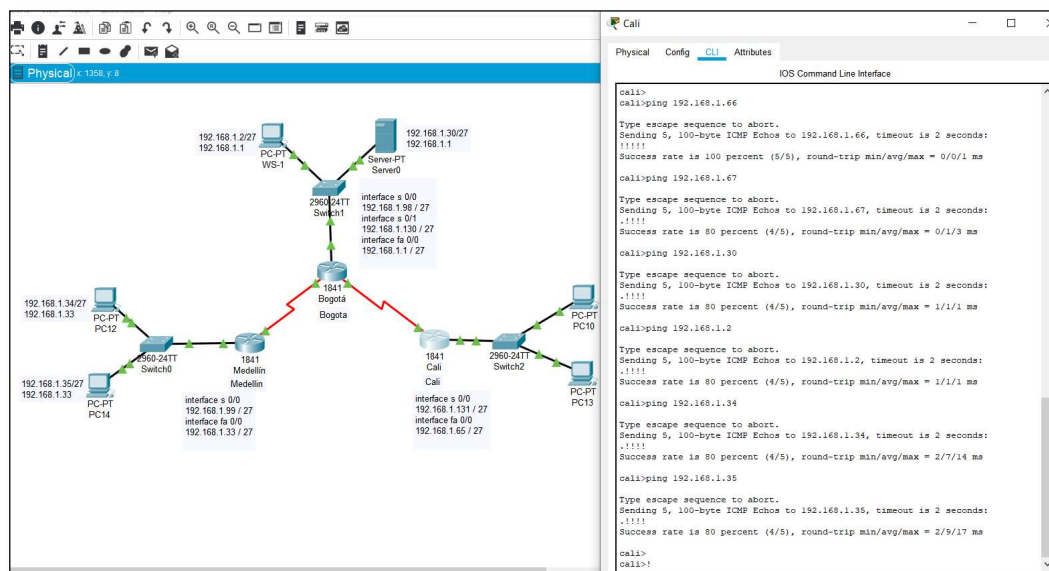


Ilustración 10: prueba de conectividad desde Cali.



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.

```
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
```

- Luego de aplicar la ACL si hacemos el ping desde WS1 hacia cualquier punto de la red esta debe ser destino inalcanzable.

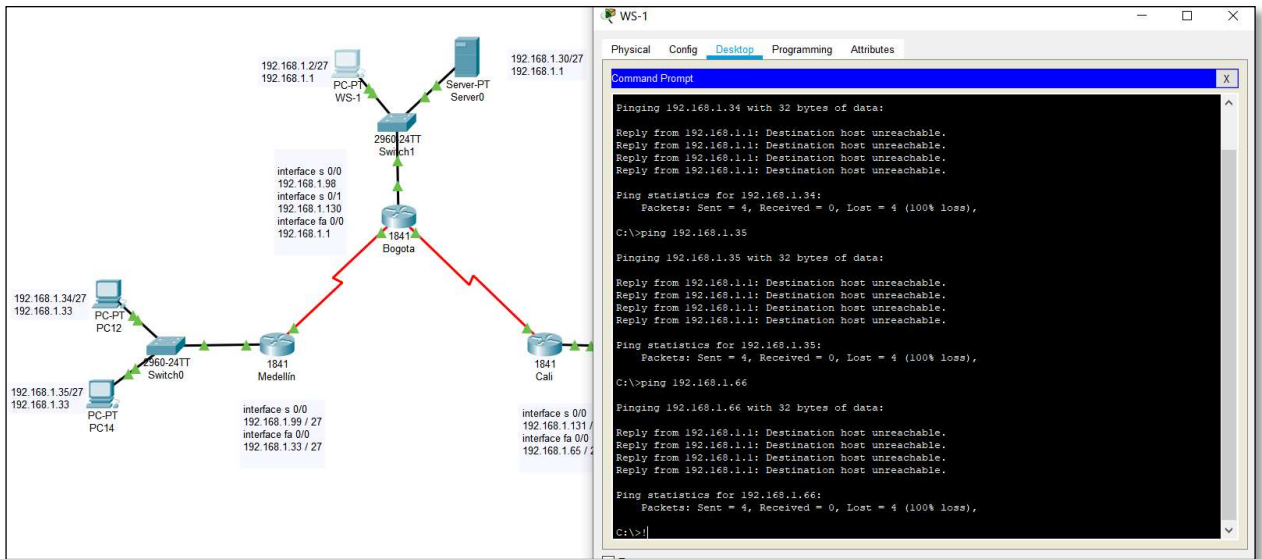


Ilustración 11: prueba de conectividad desde WS

- Si el PING lo hacemos desde el SERVIDOR este debe ser satisfactorios en todos los casos, tal como se muestra a continuación:

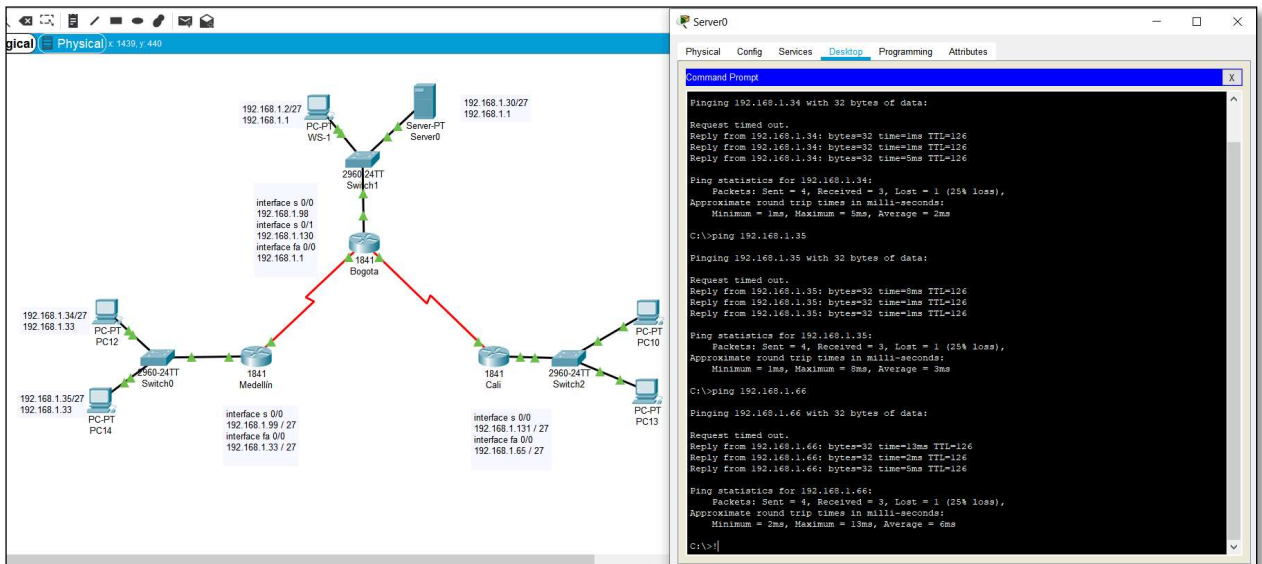


Ilustración 12: prueba de conectividad desde Servidor

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(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)#
```

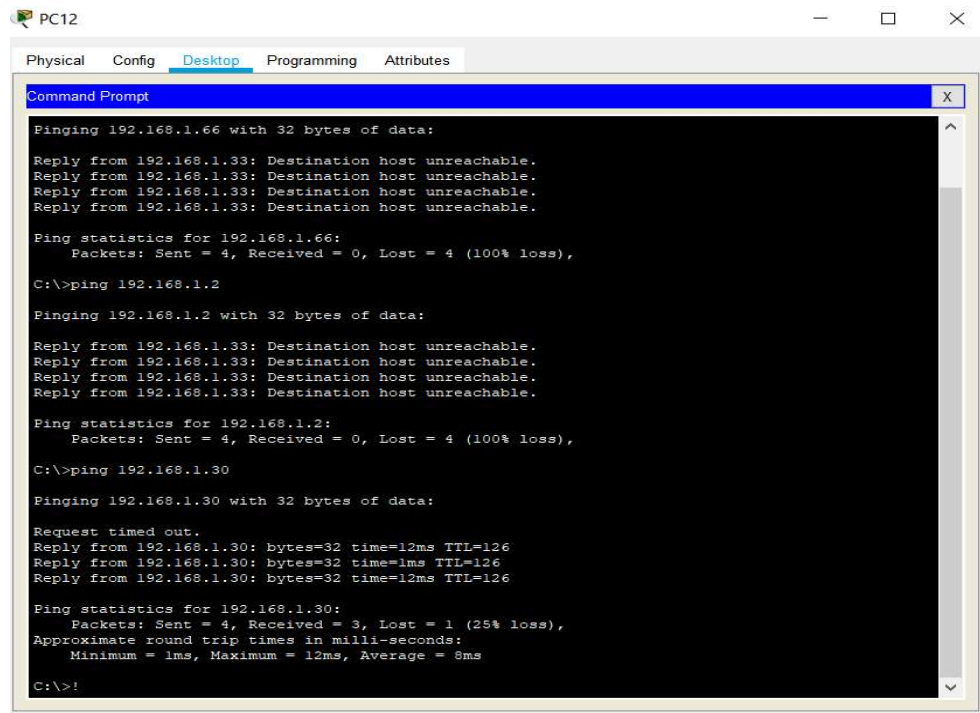
```
CALI(config)#access-list 151 permit ip 192.168.1.64 0.0.0.31 host 192.168.1.30
```

```
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:**



```
PC12
Physical Config Desktop Programming Attributes
Command Prompt
Pinging 192.168.1.66 with 32 bytes of data:
Reply from 192.168.1.33: Destination host unreachable.
Reply from 192.168.1.33: Destination host unreachable.
Reply from 192.168.1.33: Destination host unreachable.
Reply from 192.168.1.33: Destination host unreachable.
Ping statistics for 192.168.1.66:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

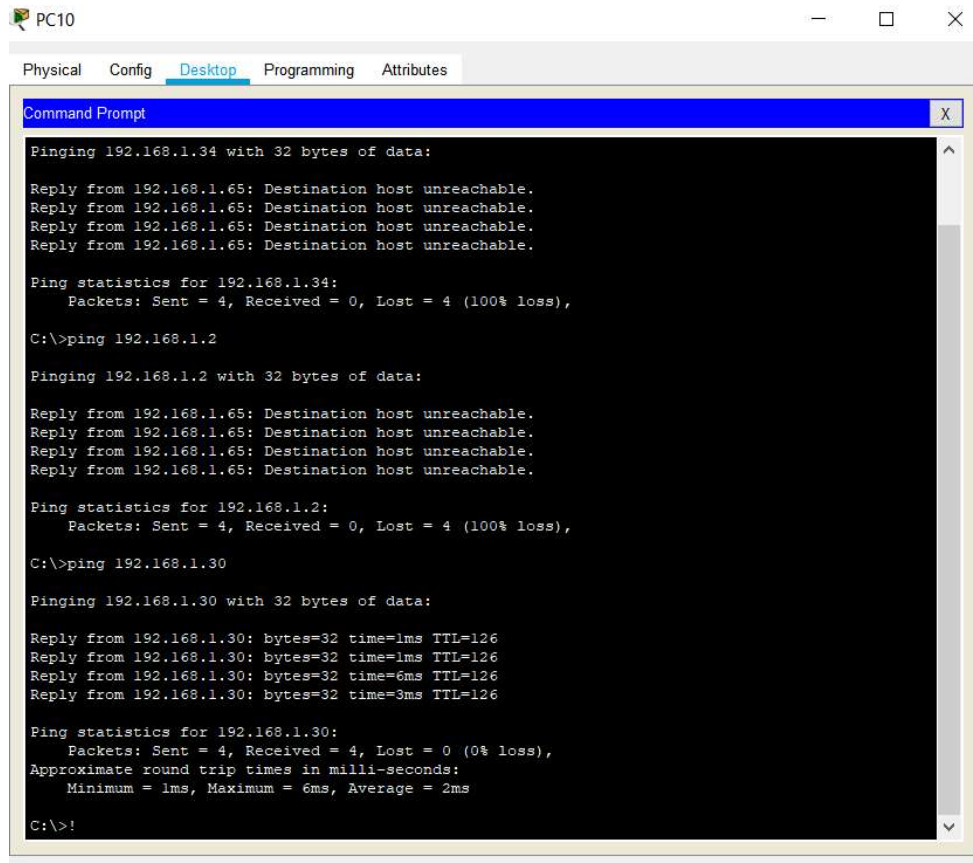
C:\>ping 192.168.1.2
Pinging 192.168.1.2 with 32 bytes of data:
Reply from 192.168.1.33: Destination host unreachable.
Reply from 192.168.1.33: Destination host unreachable.
Reply from 192.168.1.33: Destination host unreachable.
Reply from 192.168.1.33: Destination host unreachable.
Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 192.168.1.30
Pinging 192.168.1.30 with 32 bytes of data:
Request timed out.
Reply from 192.168.1.30: bytes=32 time=12ms TTL=126
Reply from 192.168.1.30: bytes=32 time=1ms TTL=126
Reply from 192.168.1.30: bytes=32 time=12ms TTL=126
Ping statistics for 192.168.1.30:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 12ms, Average = 8ms

C:\>!
```

Ilustración 13: prueba de conectividad desde medellín

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



```
PC10
Physical Config Desktop Programming Attributes
Command Prompt
Pinging 192.168.1.34 with 32 bytes of data:
Reply from 192.168.1.65: Destination host unreachable.
Reply from 192.168.1.65: Destination host unreachable.
Reply from 192.168.1.65: Destination host unreachable.
Reply from 192.168.1.65: Destination host unreachable.

Ping statistics for 192.168.1.34:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:
Reply from 192.168.1.65: Destination host unreachable.
Reply from 192.168.1.65: Destination host unreachable.
Reply from 192.168.1.65: Destination host unreachable.
Reply from 192.168.1.65: Destination host unreachable.

Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 192.168.1.30

Pinging 192.168.1.30 with 32 bytes of data:
Reply from 192.168.1.30: bytes=32 time=1ms TTL=126
Reply from 192.168.1.30: bytes=32 time=1ms TTL=126
Reply from 192.168.1.30: bytes=32 time=6ms TTL=126
Reply from 192.168.1.30: bytes=32 time=3ms TTL=126

Ping statistics for 192.168.1.30:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 6ms, Average = 2ms

C:\>!
```

Ilustración 14: prueba de conectividad desde Cali.

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
	WS_1	Router BOGOTA	Falla
	Servidor	Router CALI	Éxito
	Servidor	Router MEDELLIN	Éxito
TELNET	LAN del Router MEDELLIN	Router CALI	Falla
	LAN del Router CALI	Router CALI	Falla
	LAN del Router MEDELLIN	Router MEDELLIN	Falla
	LAN del Router CALI	Router MEDELLIN	Falla
PING	LAN del Router CALI	WS_1	Falla
	LAN del Router MEDELLIN	WS_1	Falla
	LAN del Router MEDELLIN	LAN del Router CALI	Falla
PING	LAN del Router CALI	Servidor	Éxito
	LAN del Router MEDELLIN	Servidor	Éxito
	Servidor	LAN del Router MEDELLIN	Éxito
	Servidor	LAN del Router CALI	Éxito
	Router CALI	LAN del Router MEDELLIN	Falla
	Router MEDELLIN	LAN del Router CALI	Falla

IOS Command Line Interface

```

Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2007 by Cisco Systems, Inc.
Compiled Wed 18-Jul-07 04:52 by pt_team

Press RETURN to get started!

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up
%DUAL-5-NBRCHANGE: IP-EIGRP 200: Neighbor 192.168.1.98 (Serial0/0/0) is up: new adjacency
  ACCESO DENEGADO!!

User Access Verification

Password:

MEDELLIN>en
Password:
MEDELLIN#telnet 192.168.1.131
Trying 192.168.1.131 ...Open ACCESO DENEGADO!!

User Access Verification

Password:
CALI>en
Password:
CALI#"
```

Ilustración 15: telnet desde Medellín.

IOS Command Line Interface

```
ACCESO DENEGADO!!

User Access Verification

Password:

MEDELLIN>en
Password:
MEDELLIN#telnet 192.168.1.131
Trying 192.168.1.131 ...Open ACCESO DENEGADO!!

User Access Verification

Password:
CALI>en
Password:
CALI#!
Translating "!"
% Unknown command or computer name, or unable to find computer address

CALI#
CALI#exit

[Connection to 192.168.1.131 closed by foreign host]
MEDELLIN#ping 192.168.1.66

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.66, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)

MEDELLIN#!|
```

Ilustración 16: Ping desde Medellín.

IOS Command Line Interface

```
63480K bytes of ATA CompactFlash (read/write)
Cisco IOS Software, 1841 Software (C1841-ADVIPSERVICESK9-M), Version 12.4(15)T1, RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2007 by Cisco Systems, Inc.
Compiled Wed 18-Jul-07 04:52 by pt_team

Press RETURN to get started!

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up
%DUAL-5-NBRCHANGE: IP-EIGRP 200: Neighbor 192.168.1.130 (Serial0/0/0) is up: new adjacency
ACCESO DENEGADO!!

User Access Verification

Password:

CALI>en
Password:
CALI#192.168.1.34
Trying 192.168.1.34 ...
% Connection timed out; remote host not responding
CALI#
CALI#ping 192.168.1.34

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.34, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)

CALI#|
```

Ilustración 17: Ping desde Cali.

WS-1

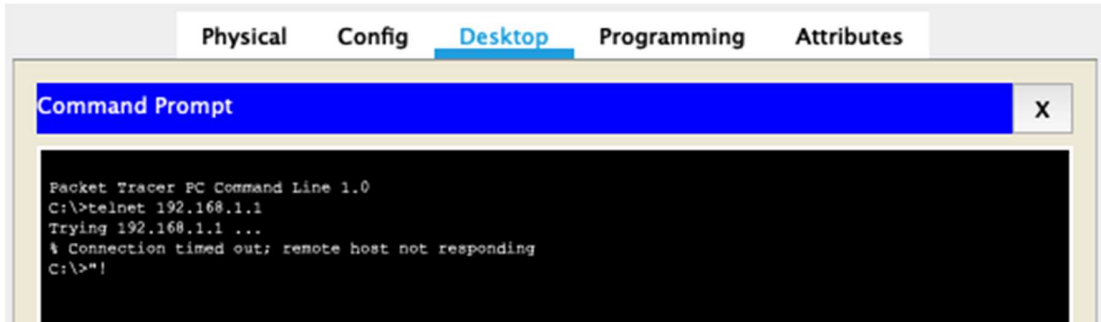


Ilustración 18: telnet desde WS-1

PC10

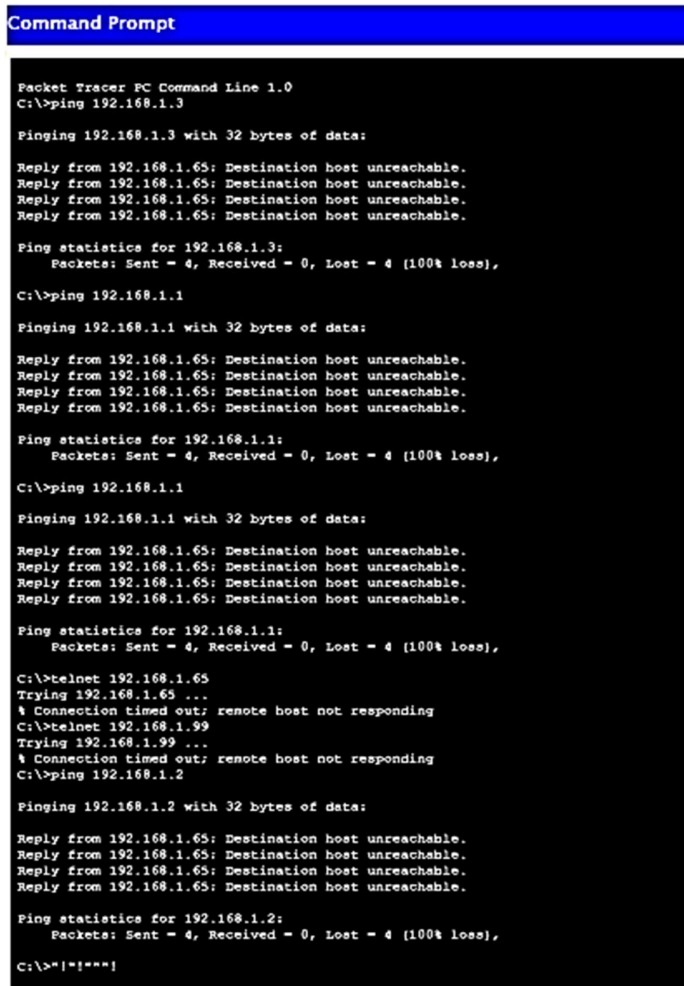


Ilustración 19: Ping desde la PC10 hacia las subredes.

PC12

```
Command Prompt

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:\>telnet 192.168.1.33
Trying 192.168.1.33 ...
% Connection timed out; remote host not responding
C:\>telnet 192.168.1.2
Trying 192.168.1.2 ...
% Connection timed out; remote host not responding
C:\>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:

Reply from 192.168.1.33: Destination host unreachable.
Reply from 192.168.1.33: Destination host unreachable.
Reply from 192.168.1.33: Destination host unreachable.
Reply from 192.168.1.33: Destination host unreachable.

Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 192.168.1.66

Pinging 192.168.1.66 with 32 bytes of data:

Reply from 192.168.1.33: Destination host unreachable.
Reply from 192.168.1.33: Destination host unreachable.
Reply from 192.168.1.33: Destination host unreachable.
Reply from 192.168.1.33: Destination host unreachable.

Ping statistics for 192.168.1.66:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 192.168.1.3

Pinging 192.168.1.3 with 32 bytes of data:

Reply from 192.168.1.33: Destination host unreachable.
Reply from 192.168.1.33: Destination host unreachable.
Reply from 192.168.1.33: Destination host unreachable.
Reply from 192.168.1.33: Destination host unreachable.

Ping statistics for 192.168.1.3:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>*
```

Ilustración 20: Ping desde PC12 hacia las diferentes subredes

Server0

```
Pinging 192.168.1.66 with 32 bytes of data:  
Reply from 192.168.1.66: bytes=32 time=18ms TTL=126  
Reply from 192.168.1.66: bytes=32 time=1ms TTL=126  
Reply from 192.168.1.66: bytes=32 time=1ms TTL=126  
Reply from 192.168.1.66: bytes=32 time=2ms TTL=126  
  
Ping statistics for 192.168.1.66:  
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),  
    Approximate round trip times in milli-seconds:  
        Minimum = 1ms, Maximum = 18ms, Average = 5ms  
  
C:\>!
```

Ilustración 21: Ping desde Server0

4. ESCENARIO 2.

Escenario 2

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

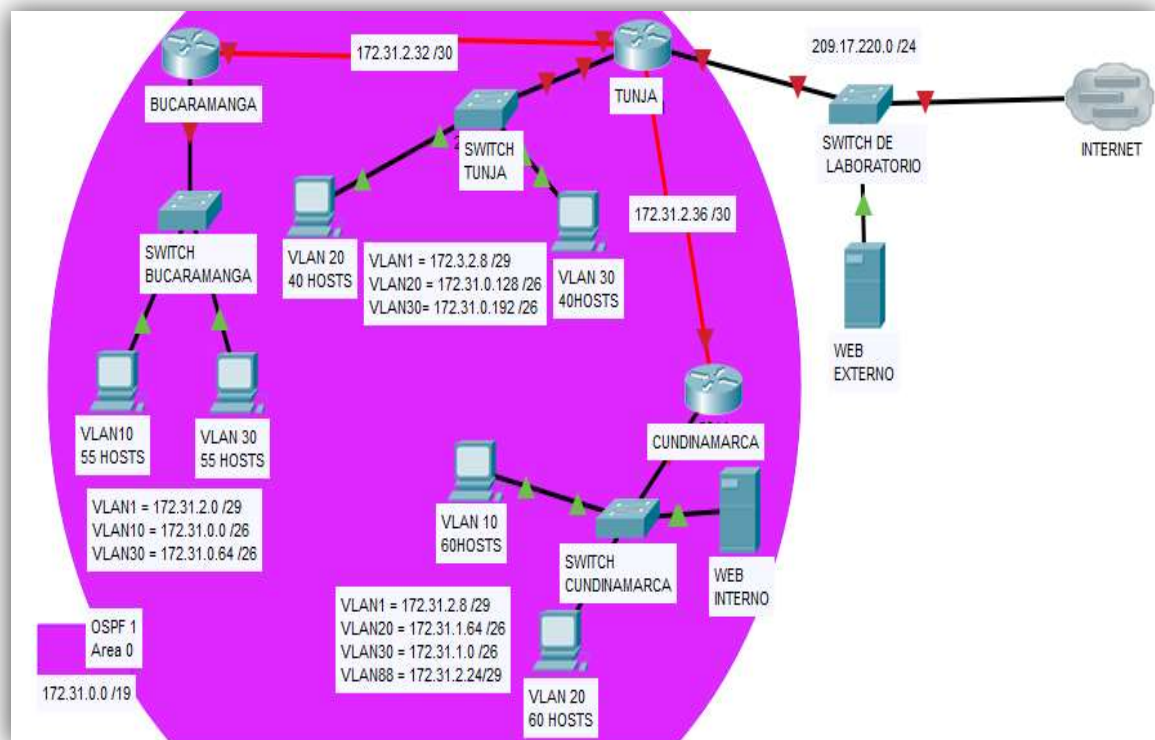


Ilustración 22: Topología ESCENARIO 2.

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 acceso 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 ESCENARIO 2.

Los siguientes son los requerimientos necesarios:

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:

```
Router(config)#hostname BUCARAMANGA
BUCARAMANGA(config)#no ip domain-lookup
BUCARAMANGA(config)#banner motd $!!ACCESO DENEGADO!!$
```

```
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 $!!ACCESO DENEGADO!!$
```

Continuamos configurando las contraseñas:

```
BUCARAMANGA(config)#enable secret Class123
```

```
BUCARAMANGA(config)#line console 0
```

```
BUCARAMANGA(config-line)#password Cisco123
```

```
BUCARAMANGA(config-line)#login
```

```
BUCARAMANGA(config-line)#line vty 0 15
```

```
BUCARAMANGA(config-line)#password Cisco123
```

```
BUCARAMANGA(config-line)#login
```

```
BUCARAMANGA(config)#int f0/0.1
```

```
TUNJA(config)#enable secret Class123
```

```
TUNJA(config)#line console 0
```

```
TUNJA(config-line)#password Cisco123
```

```
TUNJA(config-line)#login
```

```
TUNJA(config-line)#line vty 0 15
```

```
TUNJA(config-line)#password Cisco123
```

```
TUNJA(config-line)#login
```

```
CUNDINAMARCA(config)#enable secret Class123
```

```
CUNDINAMARCA(config)#line console 0
```

```
CUNDINAMARCA(config-line)#password Cisco123
```

```
CUNDINAMARCA(config-line)#login
```

```
CUNDINAMARCA(config-line)#line vty 0 15
CUNDINAMARCA(config-line)#password Cisco123
CUNDINAMARCA(config-line)#login
```

Configuramos las interfaces y el encapsulamiento:

```
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)#
```

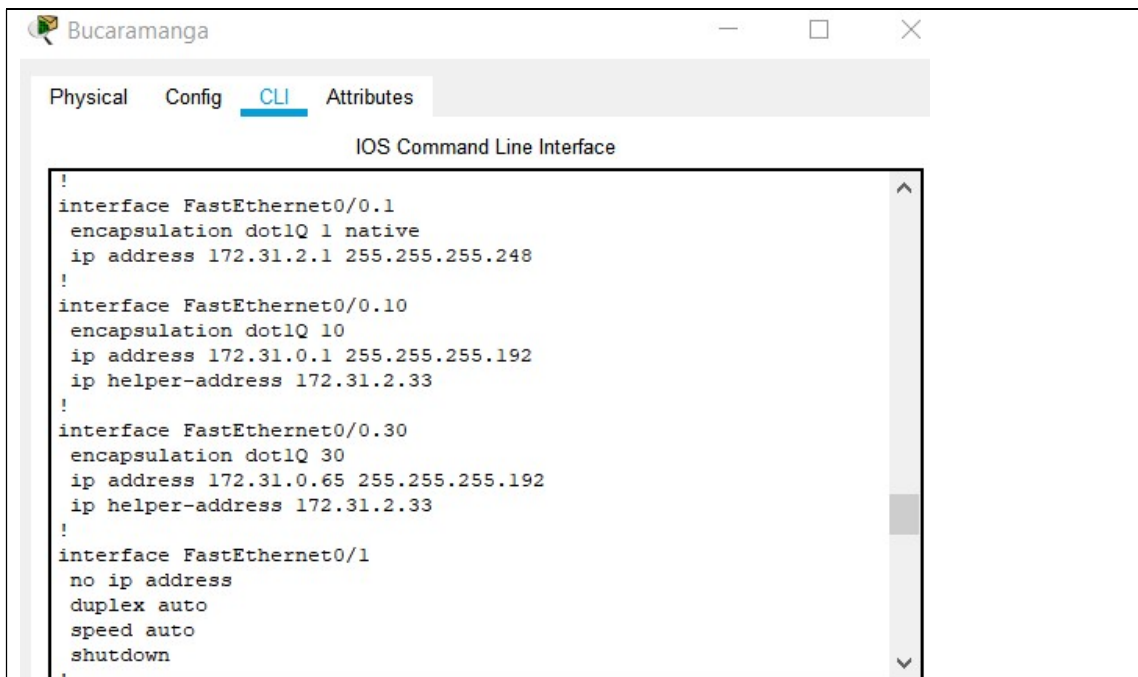


Ilustración 23: Configuración interfaces Bucaramanga.

```
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
```

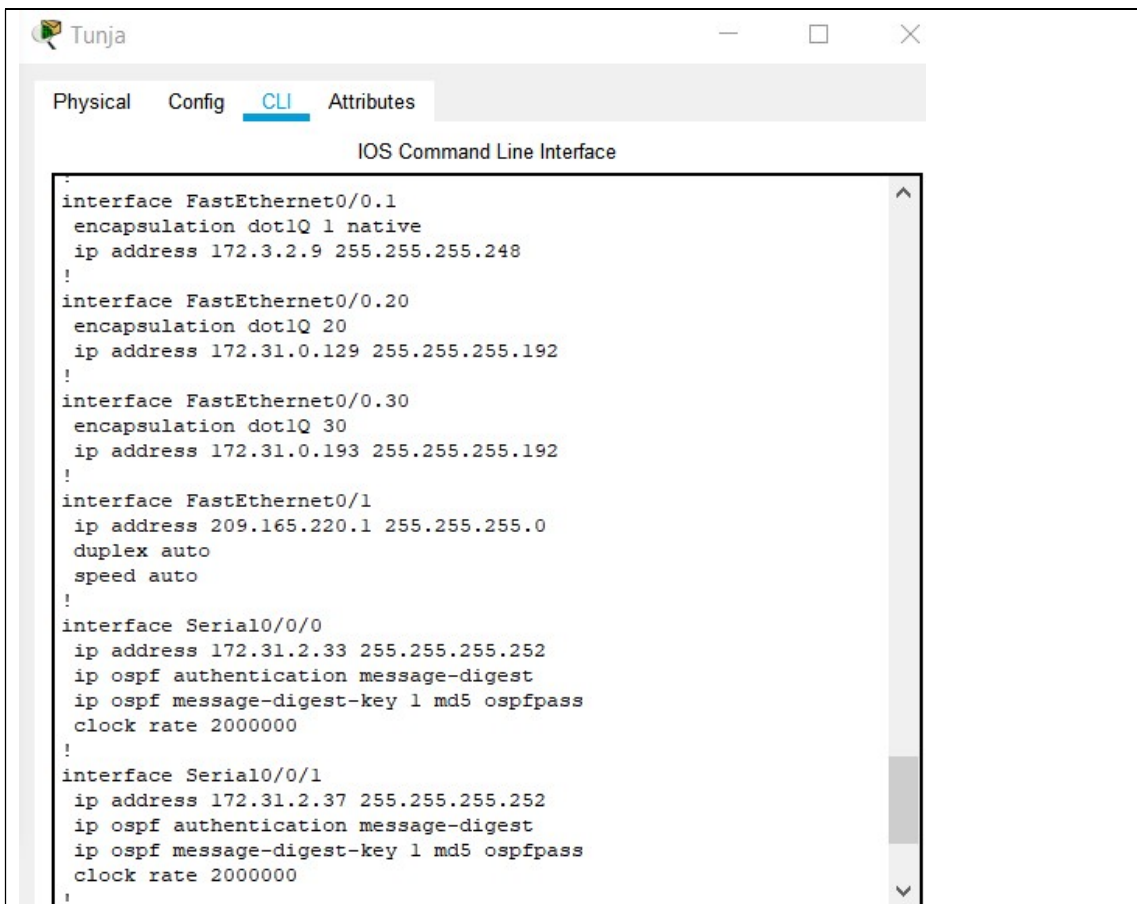
```
TUNJA(config-if)#ip address 172.31.2.37 255.255.255.252
```

```
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
```



The screenshot shows a window titled 'Tunja' with tabs for 'Physical', 'Config', 'CLI', and 'Attributes'. The 'CLI' tab is active, displaying the 'IOS Command Line Interface'. The configuration text is as follows:

```
.
interface FastEthernet0/0.1
 encapsulation dot1Q 1 native
 ip address 172.3.2.9 255.255.255.248
!
interface FastEthernet0/0.20
 encapsulation dot1Q 20
 ip address 172.31.0.129 255.255.255.192
!
interface FastEthernet0/0.30
 encapsulation dot1Q 30
 ip address 172.31.0.193 255.255.255.192
!
interface FastEthernet0/1
 ip address 209.165.220.1 255.255.255.0
 duplex auto
 speed auto
!
interface Serial0/0/0
 ip address 172.31.2.33 255.255.255.252
 ip ospf authentication message-digest
 ip ospf message-digest-key 1 md5 ospfpass
 clock rate 2000000
!
interface Serial0/0/1
 ip address 172.31.2.37 255.255.255.252
 ip ospf authentication message-digest
 ip ospf message-digest-key 1 md5 ospfpass
 clock rate 2000000
!
```

Ilustración 24: Configuración interfaces TUNJA.

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

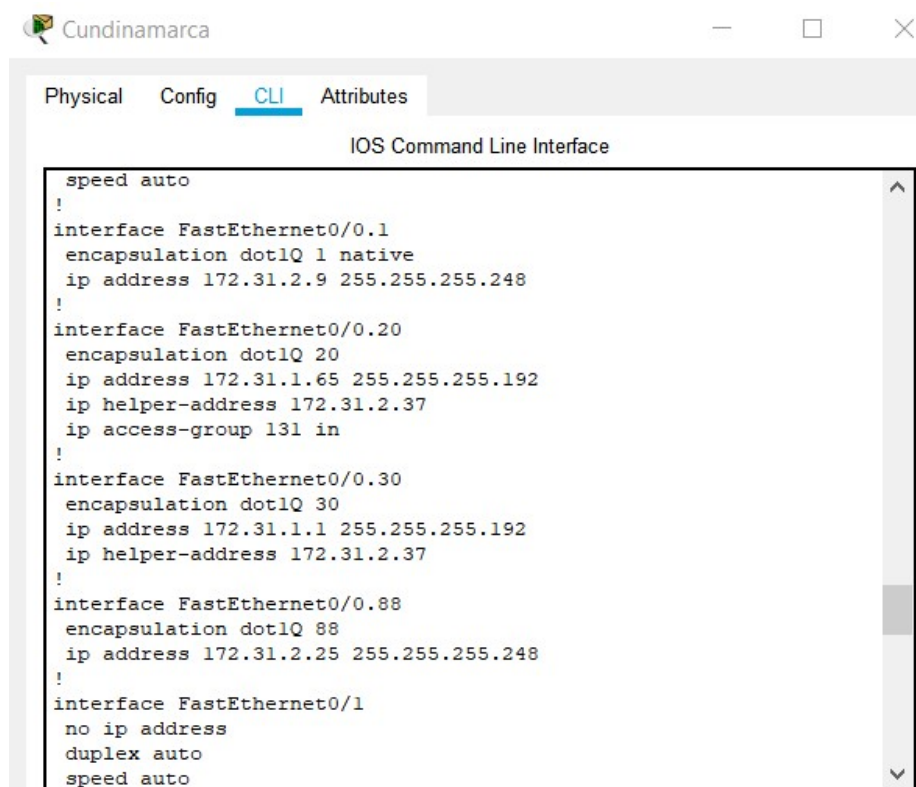
CUNDINAMARCA(config-subif)#int f0/0.20

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
```



The screenshot shows a window titled 'Cundinamarca' with a tabbed interface. The 'CLI' tab is active, displaying the 'IOS Command Line Interface'. The configuration text is as follows:

```
speed auto
!
interface FastEthernet0/0.1
 encapsulation dot1Q 1 native
 ip address 172.31.2.9 255.255.255.248
!
interface FastEthernet0/0.20
 encapsulation dot1Q 20
 ip address 172.31.1.65 255.255.255.192
 ip helper-address 172.31.2.37
 ip access-group 131 in
!
interface FastEthernet0/0.30
 encapsulation dot1Q 30
 ip address 172.31.1.1 255.255.255.192
 ip helper-address 172.31.2.37
!
interface FastEthernet0/0.88
 encapsulation dot1Q 88
 ip address 172.31.2.25 255.255.255.248
!
interface FastEthernet0/1
 no ip address
 duplex auto
 speed auto
```

Ilustración 25: Configuración interfaces CUNDINAMARCA.

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
```

Procedemos ahora a configurar los SWITCHES.

- Creamos las VLAN que vamos a necesitar en cada uno de ellos según la imagen que se nos suministra.

```
Switch(config)#hostname switchbucaramanga
switchbucaramanga(config)#vlan 1
switchbucaramanga(config-vlan)#vlan 10
switchbucaramanga(config-vlan)#vlan 30
```

```
Switch(config)#hostname swtichtunja
swtichtunja(config)#vlan 1
swtichtunja(config-vlan)#vlan 20
swtichtunja(config-vlan)#vlan 30
```

```
Switch(config)#hostname swtichcundinamarca
swtichcundinamarca(config)#vlan 1
swtichcundinamarca(config-vlan)#vlan 20
swtichcundinamarca(config-vlan)#vlan 30
swtichcundinamarca(config-vlan)#vlan 88
swtichcundinamarca(config-vlan)#exit
```

- Configuramos las interfaces y además debemos asignar cada una de ellas a la VLAN correspondiente, tal como lo indicamos a continuación:

```
switchbucaramanga(config-vlan)#int f0/10
switchbucaramanga(config-if)#switchport mode access
switchbucaramanga(config-if)#switchport access vlan 10
switchbucaramanga(config-if)#int f0/14
switchbucaramanga(config-if)#switchport mode access
switchbucaramanga(config-if)#switchport access vlan 30
switchbucaramanga(config-if)#int f0/1
switchbucaramanga(config-if)#switchport mode trunk
switchbucaramanga(config-if)#int vlan 1
switchbucaramanga(config-if)#ip address 172.31.2.3 255.255.255.248
```

```
switchbucaramanga(config-if)#no shutdown
switchbucaramanga(config-if)#ip default-gateway 172.31.2.1
switchbucaramanga(config)#
```

```
swichtunja(config-vlan)#int f0/10
swichtunja(config-if)#switchport mode access
swichtunja(config-if)#switchport access vlan 20
swichtunja(config-if)#int f0/14
swichtunja(config-if)#switchport mode access
swichtunja(config-if)#switchport access vlan 30
swichtunja(config-if)#int f0/1
swichtunja(config-if)#switchport mode trunk
swichtunja(config-if)#int vlan 1
swichtunja(config-if)#ip address 172.3.2.11 255.255.255.248
swichtunja(config-if)#no shutdown
swichtunja(config-if)#ip default-gateway 172.3.2.9
```

```
swichtcundinamarca(config)#int f0/10
swichtcundinamarca(config-if)#switchport mode access
swichtcundinamarca(config-if)#switchport access vlan 20
swichtcundinamarca(config-if)#int f0/14
swichtcundinamarca(config-if)#switchport mode access
```

```
swtichcundinamarca(config-if)#switchport access vlan 30
swtichcundinamarca(config-if)#int f0/20
swtichcundinamarca(config-if)#switchport mode access
swtichcundinamarca(config-if)#switchport access vlan 88
swtichcundinamarca(config-if)#int f0/1
swtichcundinamarca(config-if)#switchport mode trunk
swtichcundinamarca(config-if)#int vlan 1
swtichcundinamarca(config-if)#ip address 172.31.2.11 255.255.255.248
swtichcundinamarca(config-if)#no shutdown
swtichcundinamarca(config-if)#ip default-gateway 172.31.2.9
swtichcundinamarca(config)#
```

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

The screenshot displays the configuration of Router1 in the Bucaramanga network. The network diagram on the left shows Router1 (1941) connected to a 2960-24TT switch (switchbucaramanga), which is connected to PC-PT PC10 (VLAN 10) and PC-PT PC11 (VLAN 30). Router1 is also connected to a 2960-24TT switch (switchlaboratorios), which is connected to a 2960-24TT switch (switchtunja), which is connected to PC-PT PC12 (VLAN 20) and PC-PT PC13 (VLAN 30). Router1 is connected to a 1941 Router0 (Tunja) via a serial link. Router1 is also connected to a Cloud-PT Internet cloud. The CLI window on the right shows the configuration of Router1, including the enable command, the show ip interface brief command, and the show ip route command. The show ip route command output shows the routing table for Router1, including the default route (0.0.0.0/0) and the routes for the connected networks.

```

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

172.3.0.0/29 is subnetted, 1 subnets
O   172.3.2.8 [110/65] via 172.31.2.33, 00:00:34, Serial0/0/0
O   172.31.0.0/16 is variably subnetted, 10 subnets, 3 masks
C   172.31.0.128/26 [110/65] via 172.31.2.33, 00:00:34, Serial0/0/0
O   172.31.0.192/26 [110/65] via 172.31.2.33, 00:00:34, Serial0/0/0
O   172.31.1.0/26 [110/129] via 172.31.2.33, 00:00:34, Serial0/0/0
O   172.31.1.64/26 [110/129] via 172.31.2.33, 00:00:34, Serial0/0/0
O   172.31.2.0/29 is directly connected, FastEthernet0/0.1
C   172.31.2.8/29 [110/129] via 172.31.2.33, 00:00:34, Serial0/0/0
O   172.31.2.24/29 [110/129] via 172.31.2.33, 00:00:34, 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, 00:00:34, Serial0/0/0

bucaramanga#!
  
```

Ilustración 26: conf. interfaces y tabla Bucaramanga

The screenshot displays the configuration of Router0 in the Tunja network. The network diagram on the left shows Router0 (1941) connected to a 2960-24TT switch (switchtunja), which is connected to PC-PT PC12 (VLAN 20) and PC-PT PC13 (VLAN 30). Router0 is connected to a 1941 Router1 (Bucaramanga) via a serial link. Router0 is also connected to a Cloud-PT Internet cloud and a Server-PT Server1. The CLI window on the right shows the configuration of Router0, including the show ip interface brief command and the show ip route command. The show ip route command output shows the routing table for Router0, including the default route (0.0.0.0/0) and the routes for the connected networks.

```

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#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
O   172.31.0.0/16 is variably subnetted, 10 subnets, 3 masks
C   172.31.0.0/26 [110/65] via 172.31.2.34, 00:01:33, 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, 00:01:33, Serial0/0/1
O   172.31.1.64/26 [110/65] via 172.31.2.38, 00:01:33, Serial0/0/1
O   172.31.2.0/29 [110/65] via 172.31.2.34, 00:01:33, Serial0/0/0
O   172.31.2.8/29 [110/65] via 172.31.2.38, 00:01:33, Serial0/0/1
O   172.31.2.24/29 [110/65] via 172.31.2.38, 00:01:33, 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#!
  
```

Ilustración 27: conf. interfaces y tabla Tunja

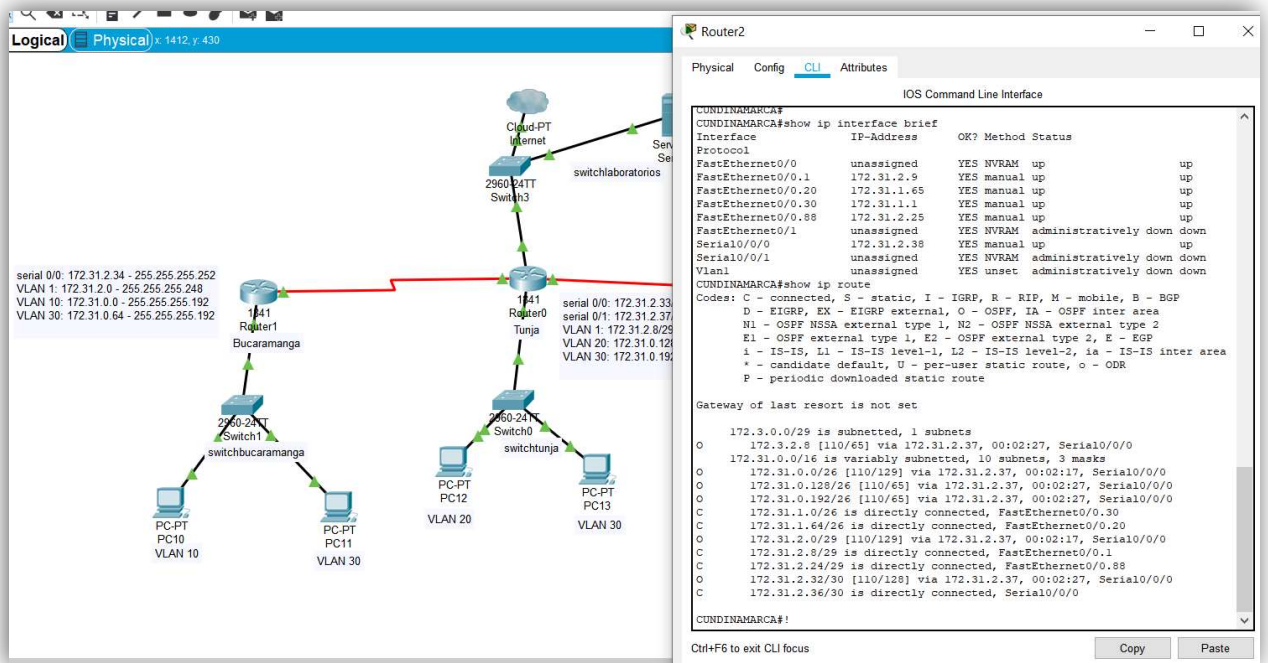


Ilustración 28: conf. interfaces y tabla Cundinamarca

Vemos que las interfaces están configuradas correctamente, que todas se encuentran UP y vemos que los routers ya cuentan con rutas para cada una de las subredes.

- **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 ADMIN123 secret ADMIN123PASS
```

```
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 ADMIN123 secret ADMIN123PASS
```

```
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 ADMIN123 secret ADMIN123PASS
```

```
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
```

- **Cifrado de contraseñas.**

Debemos encriptar las contraseñas por seguridad, esto con el fin de que cuando apliquemos algún tipo de comando este no viaje en formato plano y que sea fácil de descifrar.

```
BUCARAMANGA(config)#service password-encryption
```

```
TUNJA(config)#service password-encryption
```

```
CUNDINAMARCA(config)#service password-encryption
```

- **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
```

- **Máximo tiempo de acceso al detectar ataques.**

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

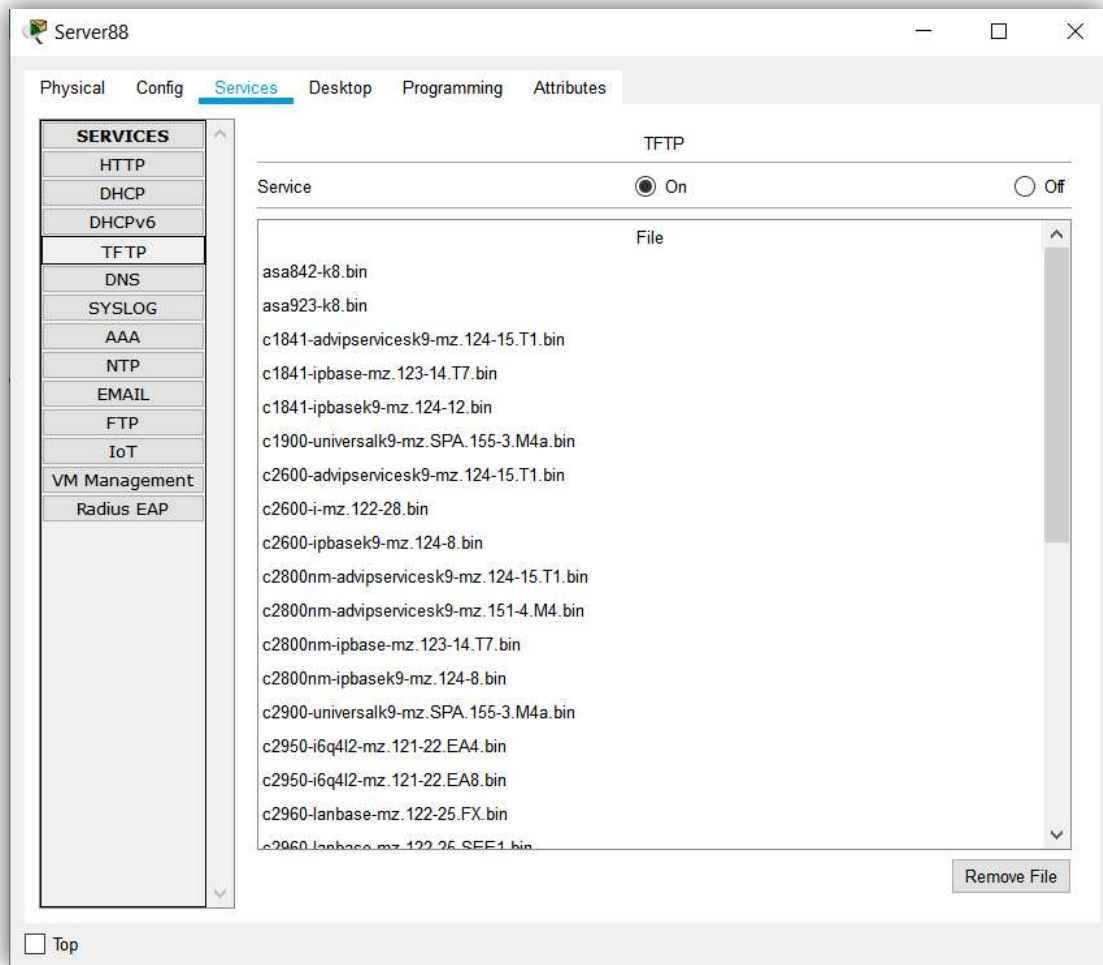


Ilustración 29: Configuración servidor TFTP

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

- Lo primero que se debe hacer en este caso es dejar indicado cuales direcciones IP no vamos a utilizar dentro del POOL de direcciones que vamos a crear para utilizar en DHCP, el proceso que debemos seguir es el siguiente:

```
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
```

- Ya que hemos indicado cuales direcciones no incluir dentro de los POOL procedemos a crear estos rangos IP tal como lo maestro en el siguiente punto, recordemos que este nos va a servir para asignar las direcciones a las subredes de BUCARAMANGA y de CUNDINAMARCA.

```
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
```

```
TUNJA(dhcp-config)#
```

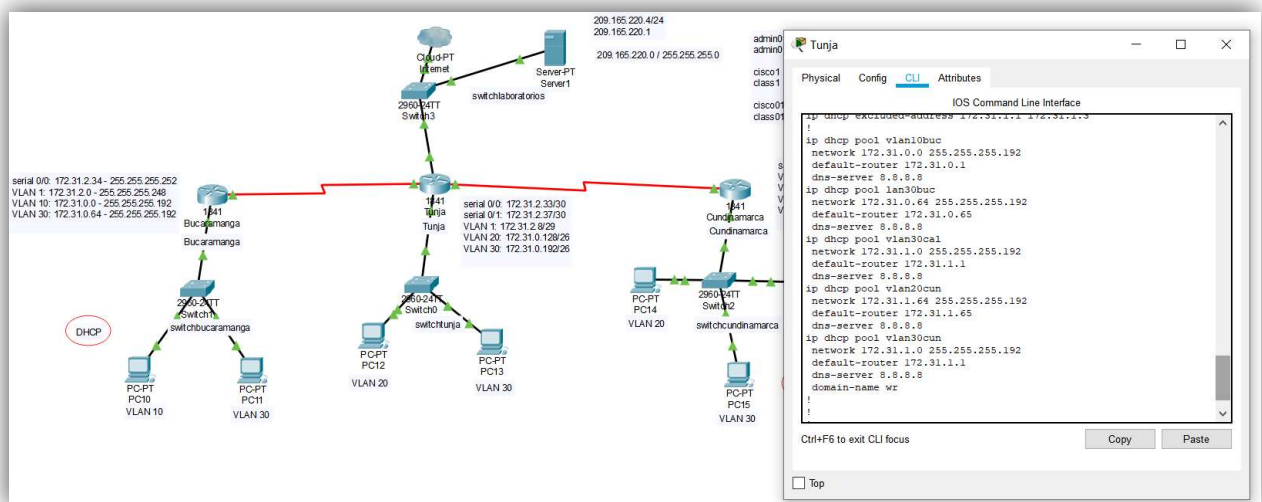


Ilustración 30: configuración DHCP.

- Anteriormente ya configuramos el router que va a ser cargo de asignar las direcciones IP, ahora nos queda configurar los routers de BUCARAMANGA y de CUNDINAMARCA con el fin de que puedan tener acceso a este servicio empleando el comando ip helper-address.

```
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
```

```
CUNDINAMARCA(config)#int f0/0.20
```

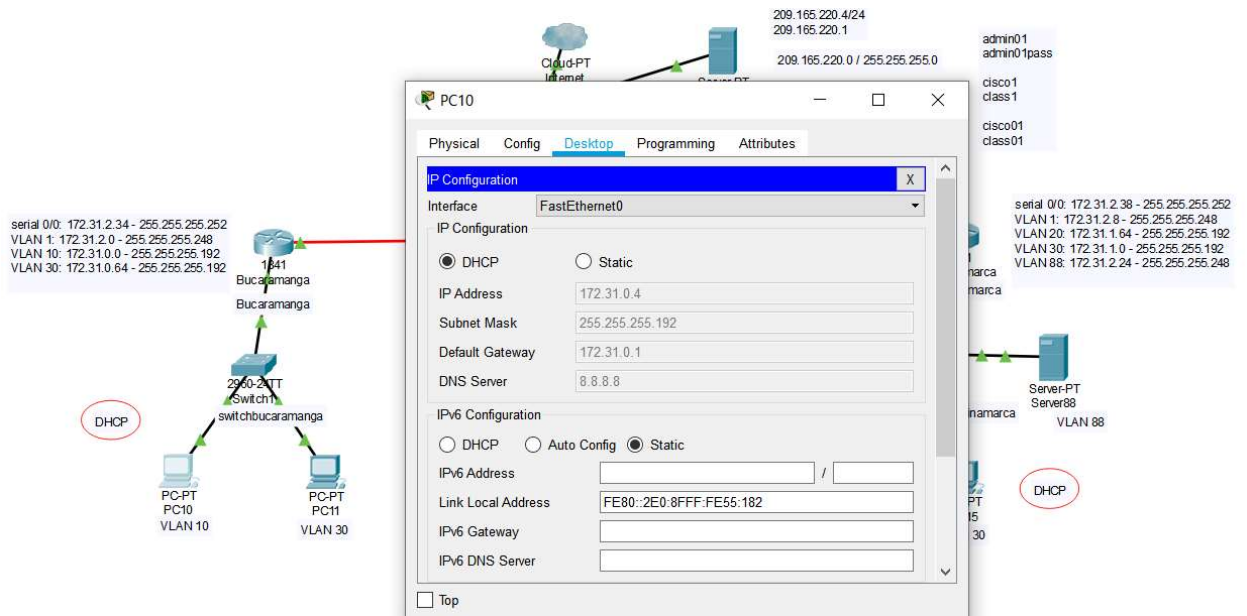
```
CUNDINAMARCA(config-subif)#ip helper-address 172.31.2.37
```

```
CUNDINAMARCA(config-subif)#int f0/0.30
```

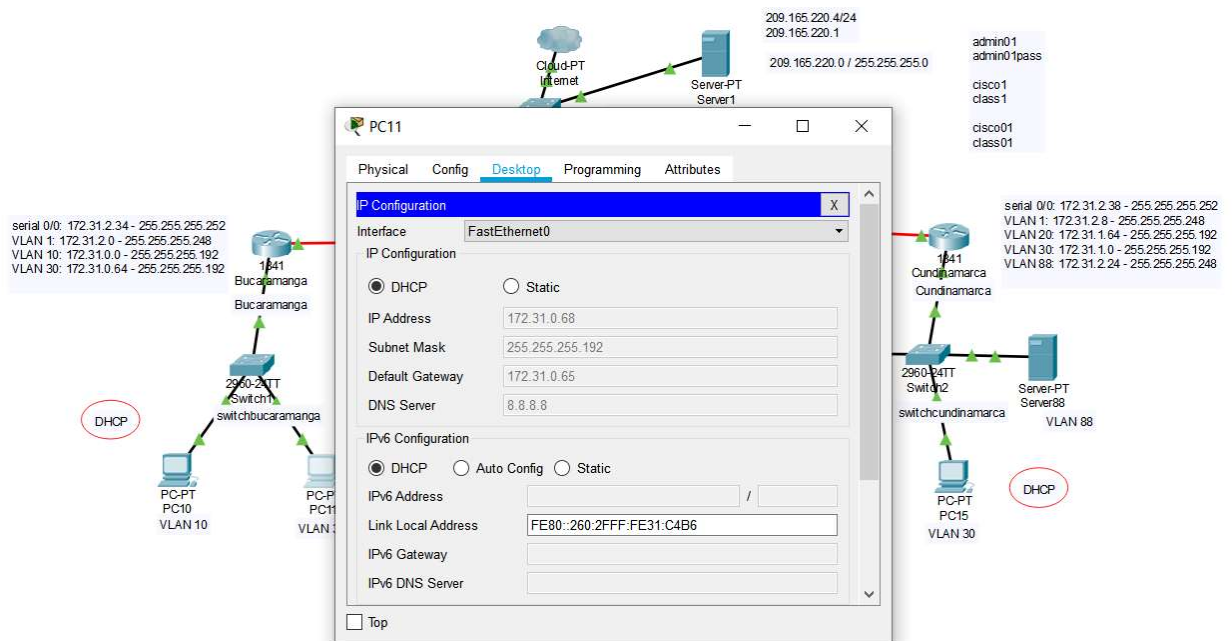
```
CUNDINAMARCA(config-subif)#ip helper-address 172.31.2.37
```

Ya tenemos configurado todo, no olvidemos que debemos configurar cada uno de los PC igualmente con el fin de que puedan acceder al servicio de DHCP.

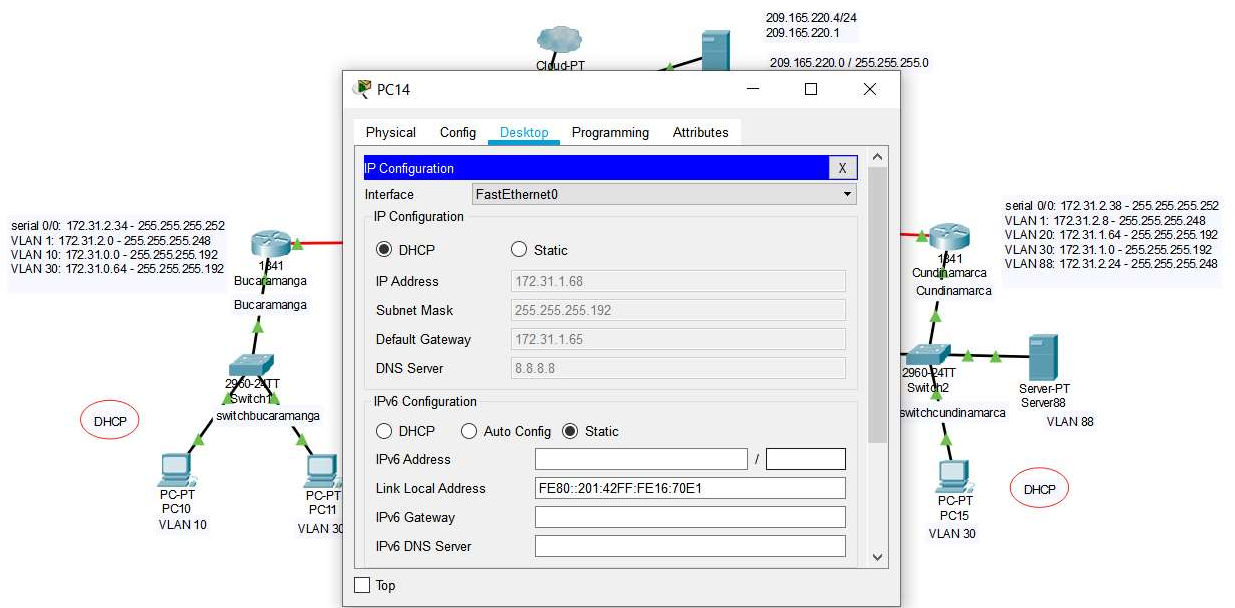
PC10



PC11



PC14



PC15

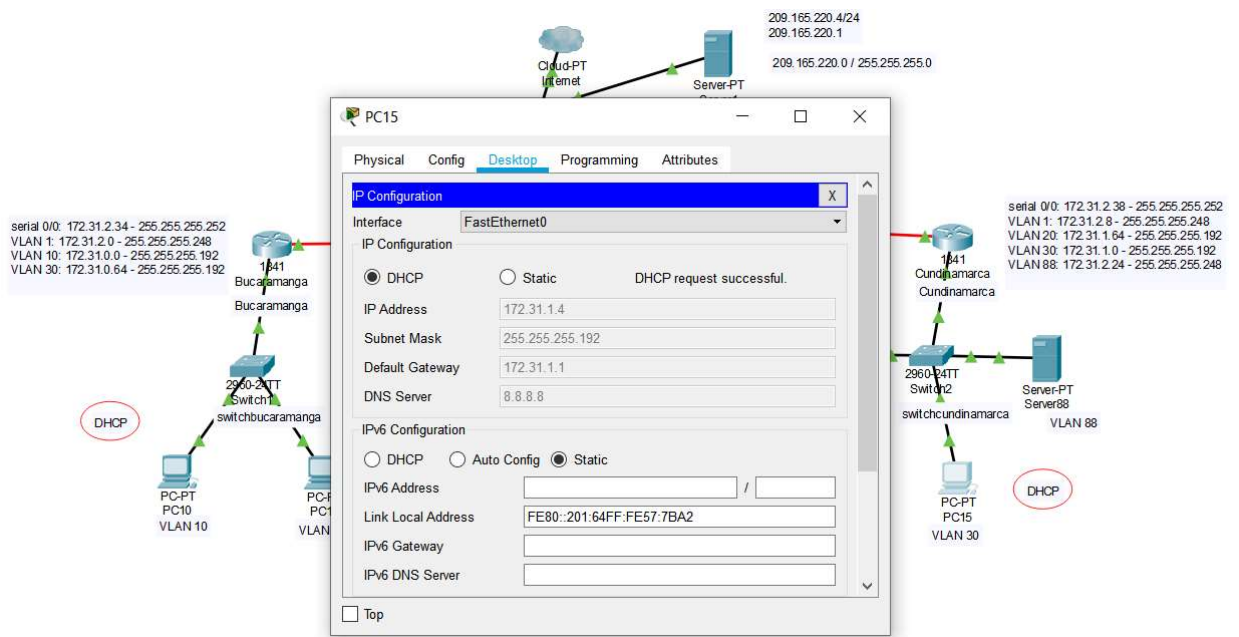


Ilustración 31: verificación PC obtiene IP mediante DHCP

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
```

- Configuramos las diferentes interfaces.

```
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
```

- Creamos una ruta por defecto y la distribuimos empleando 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#

Router1

Physical Config **CLI** Attributes

IOS Command Line Interface

```

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, 00:00:44, 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, 00:00:44, Serial0/0/0
O 172.31.0.192/26 [110/65] via 172.31.2.33, 00:00:44, Serial0/0/0
O 172.31.1.0/26 [110/129] via 172.31.2.33, 00:00:34, Serial0/0/0
O 172.31.1.64/26 [110/129] via 172.31.2.33, 00:00:34, 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, 00:00:34, Serial0/0/0
O 172.31.2.24/29 [110/129] via 172.31.2.33, 00:00:34, 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, 00:00:44, Serial0/0/0
O*E2 0.0.0.0/0 [110/1] via 172.31.2.33, 00:00:44, 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 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, 10 subnets, 3 masks
O 172.31.0.0/26 [110/65] via 172.31.2.34, 00:01:14, 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, 00:01:14, Serial0/0/1
O 172.31.1.64/26 [110/65] via 172.31.2.38, 00:01:14, Serial0/0/1
O 172.31.2.0/29 [110/65] via 172.31.2.34, 00:01:14, Serial0/0/0
O 172.31.2.8/29 [110/65] via 172.31.2.38, 00:01:14, Serial0/0/1
O 172.31.2.24/29 [110/65] via 172.31.2.38, 00:01:14, 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#!

```

Ctrl+F6 to exit CLI focus

Copy Paste

Top

```
Router2
Physical Config CLI Attributes
IOS Command Line Interface
CUNDINAMARCA#
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, 00:01:38, Serial0/0/0
 172.31.0.0/16 is variably subnetted, 10 subnets, 3 masks
O   172.31.0.0/26 [110/129] via 172.31.2.37, 00:01:38, Serial0/0/0
O   172.31.0.128/26 [110/65] via 172.31.2.37, 00:01:38, Serial0/0/0
O   172.31.0.192/26 [110/65] via 172.31.2.37, 00:01:38, 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, 00:01:38, 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, 00:01:38, 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, 00:01:38, Serial0/0/0
CUNDINAMARCA#|
Ctrl+F6 to exit CLI focus Copy Paste
Top
```

- En este caso observamos que la ruta por defecto si esta siendo propagada por los routers.

```
PC10
Physical Config Desktop Programming Attributes
Command Prompt
Packet Tracer PC Command Line 1.0
C:\>ping 209.165.220.4

Pinging 209.165.220.4 with 32 bytes of data:

Reply from 209.165.220.4: bytes=32 time=1ms TTL=126
Reply from 209.165.220.4: bytes=32 time=24ms TTL=126
Reply from 209.165.220.4: bytes=32 time=14ms TTL=126
Reply from 209.165.220.4: bytes=32 time=13ms TTL=126

Ping statistics for 209.165.220.4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 24ms, Average = 13ms

C:\>

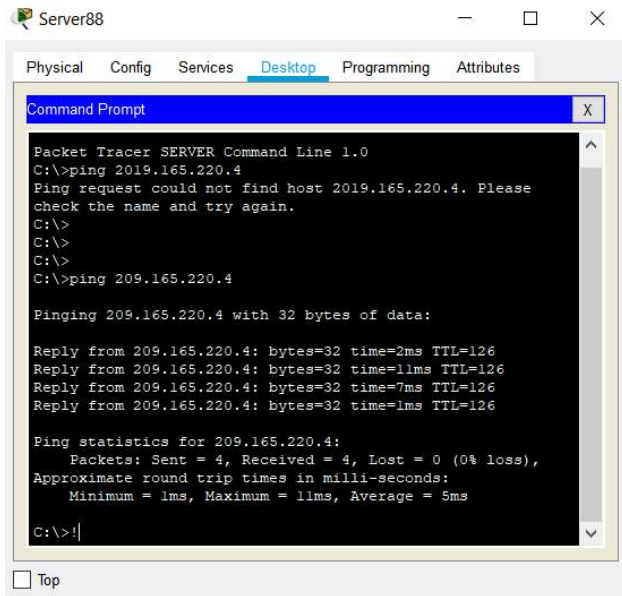
PC13
Physical Config Desktop Programming Attributes
Command Prompt
Packet Tracer PC Command Line 1.0
C:\>ping 209.165.220.4

Pinging 209.165.220.4 with 32 bytes of data:

Reply from 209.165.220.4: bytes=32 time<1ms TTL=127
Reply from 209.165.220.4: bytes=32 time=14ms TTL=127
Reply from 209.165.220.4: bytes=32 time=11ms TTL=127
Reply from 209.165.220.4: bytes=32 time=13ms TTL=127

Ping statistics for 209.165.220.4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 14ms, Average = 9ms

C:\>
```



ROUTERO

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

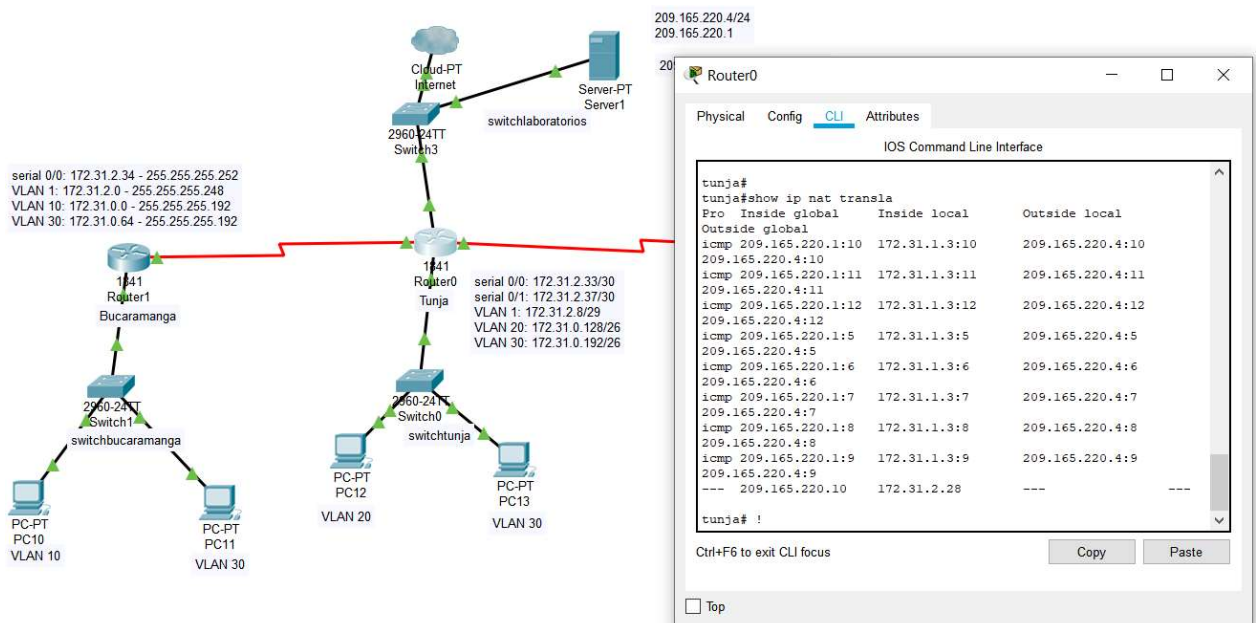


Ilustración 32: Traducción de direcciones mediante NAT.

4. El enrutamiento deberá tener autenticación.

Procedemos ahora a configurar la autenticación, este proceso lo hacemos de la siguiente manera:

Usage Guidelines

Use the `area authentication` command to configure the authentication mode for the entire OSPF area.

The authentication type and authentication password must be the same for all OSPF devices in an area. Use the `ip ospf authentication-key` command in interface configuration mode to specify this password.

If you enable MD5 authentication with the `message-digest` keyword, you must configure a password with the `ip ospf message-digest-key` command in interface configuration mode.

This command requires the LAN Base Services license.

Examples

This example shows how to configure authentication for area 0 of OSPF routing process 201:

```
switch(config)# router ospf 201
switch(config-router)# area 0 authentication message-digest
switch(config-router)# interface ethernet 1/1
switch(config-if)# no switchport
switch(config-if)# ip ospf area 0
switch(config-if)# ip ospf message-digest-key 10 md5 0 adodefgh
switch(config-if)#
```

```
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
```

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)#
```

PC14

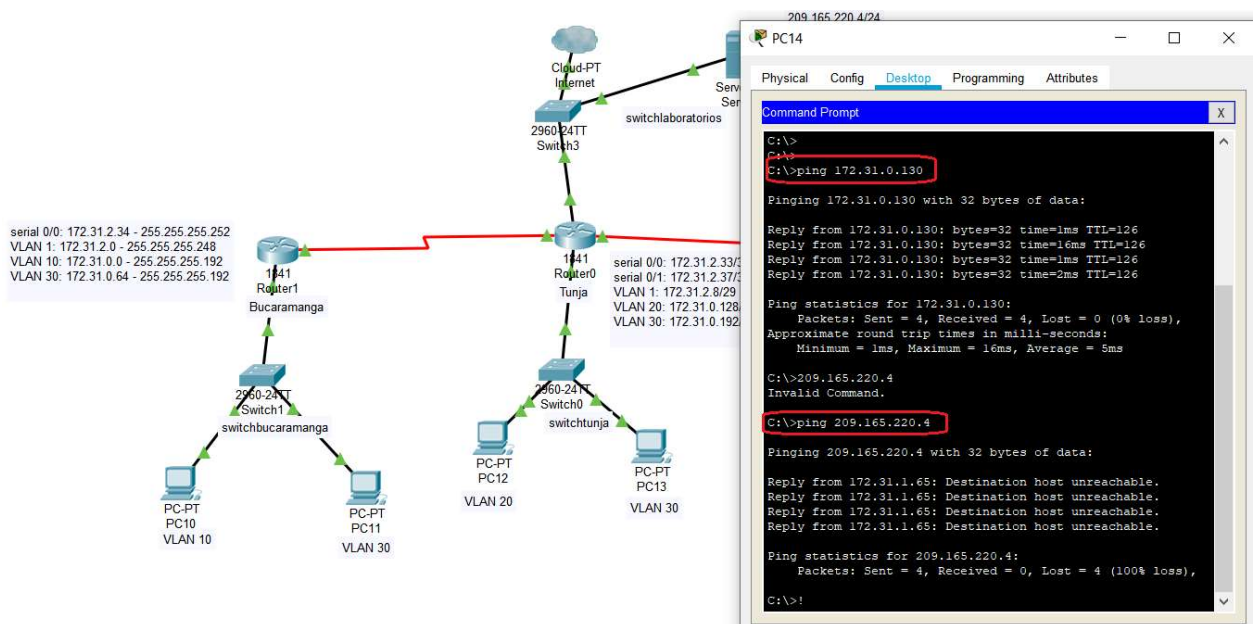


Ilustración 33: ACL - Los hosts de VLAN 20 en CUNDINAMARCA no acceden a internet, solo a la red interna de TUNJA.

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

```
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)#
```

PC15

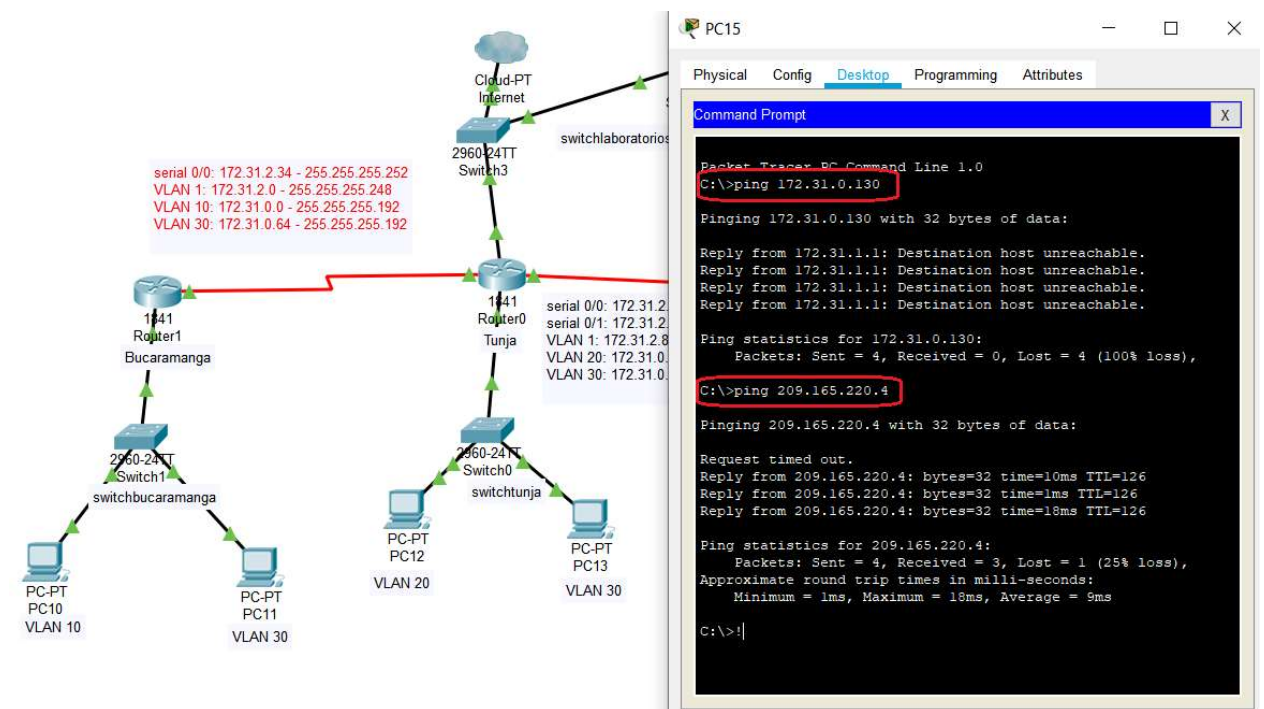


Ilustración 34: ACL Los hosts de VLAN 10 en CUNDINAMARCA si acceden a internet y no a la red interna de TUNJA.

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

```
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
```

```
TUNJA(config-subif)#
```

PC13

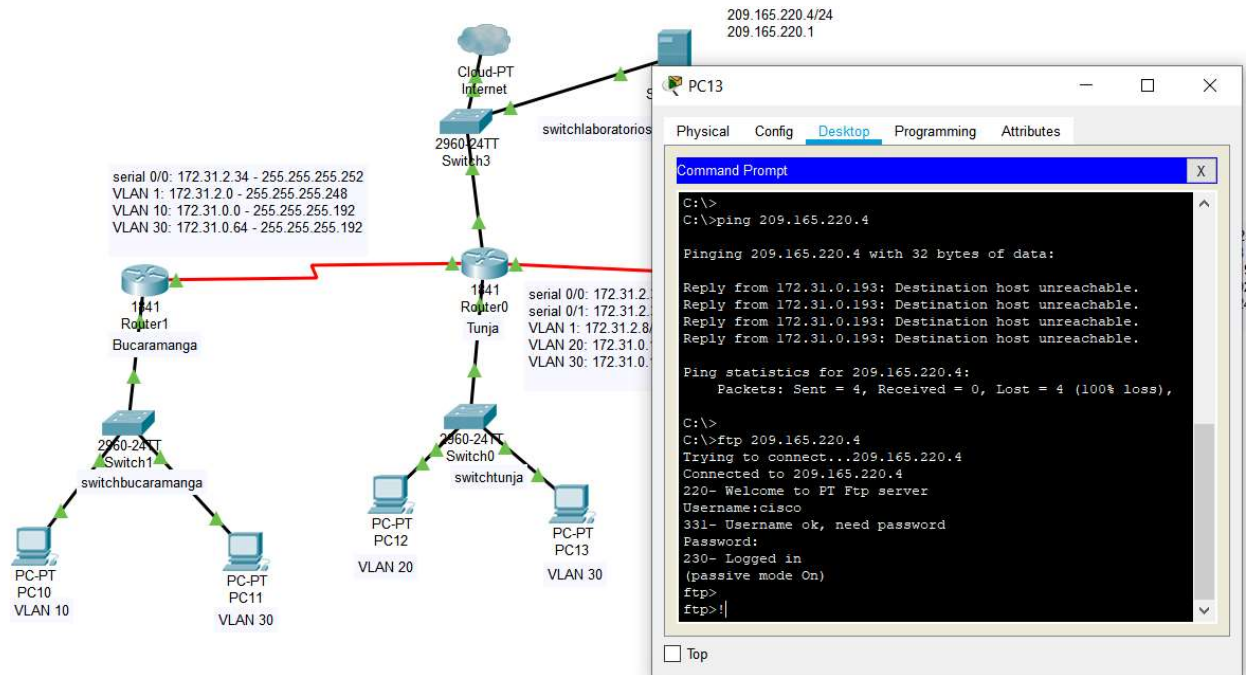
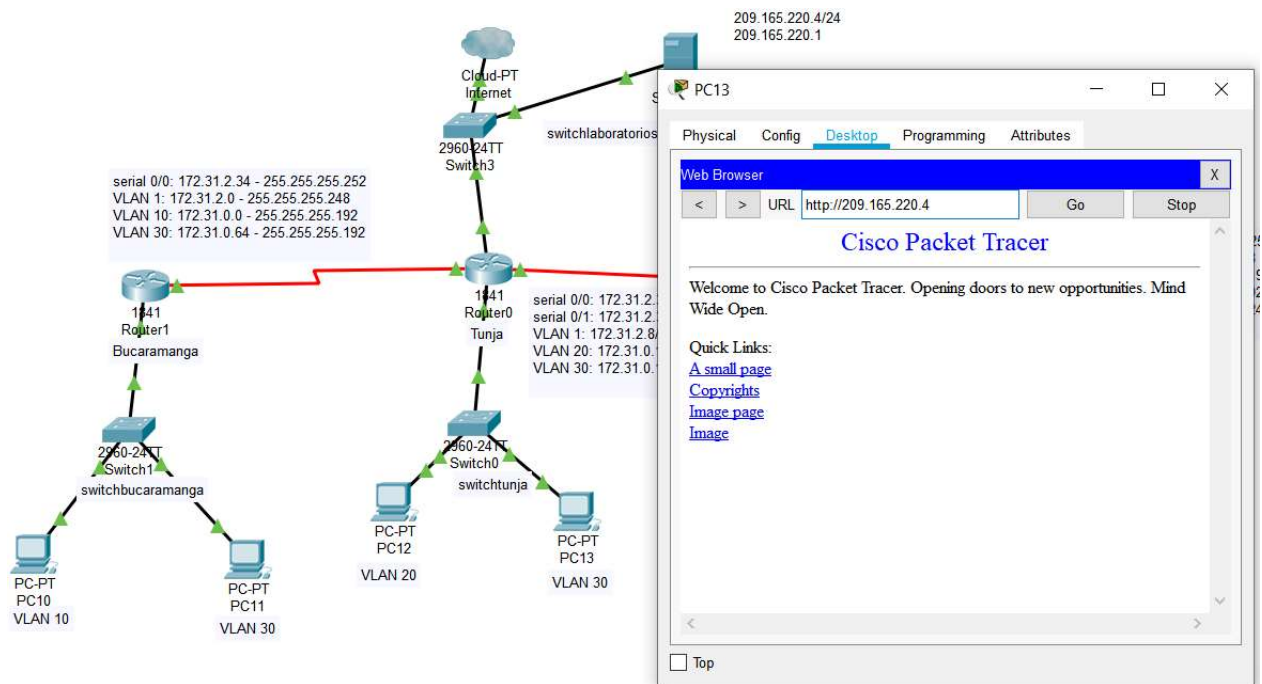


Ilustración 35: ACL los hosts de VLAN 30 en TUNJA solo acceden a servidores web y ftp de internet.



Vemos que en este caso solo accedemos mediante ftp y a través de www.

- 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

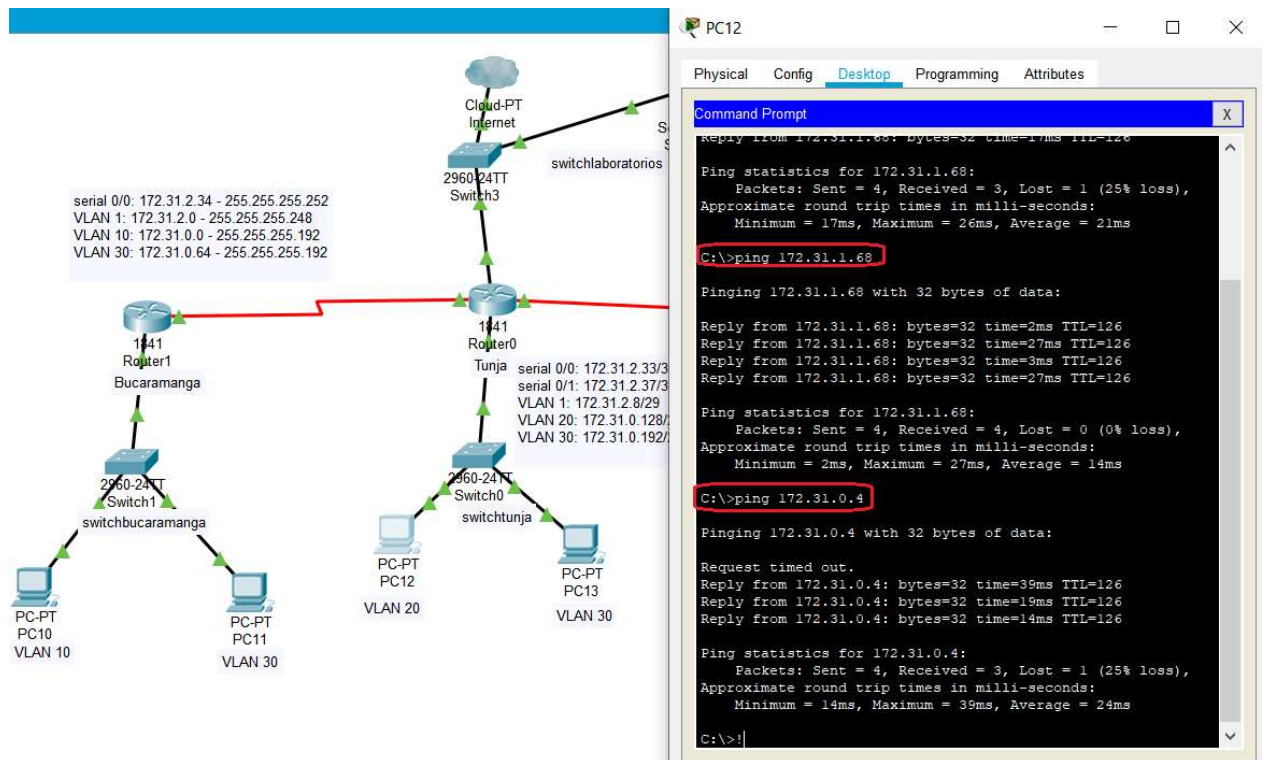


Ilustración 36: ACL los hosts de VLAN 20 en TUNJA solo acceden a la VLAN 20 de CUNDINAMARCA y VLAN 10 de BUCARAMANGA.

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

```
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)#
```

PC11

```
Command Prompt

Packet Tracer PC Command Line 1.0
C:\>PING 209.165.220.4

Pinging 209.165.220.4 with 32 bytes of data:

Request timed out.
Reply from 209.165.220.4: bytes=32 time=1ms TTL=126
Reply from 209.165.220.4: bytes=32 time=1ms TTL=126
Reply from 209.165.220.4: bytes=32 time=1ms TTL=126

Ping statistics for 209.165.220.4:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 1ms, Average = 1ms

C:\>"|
```

Ilustración 37: ACL 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.**

```
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

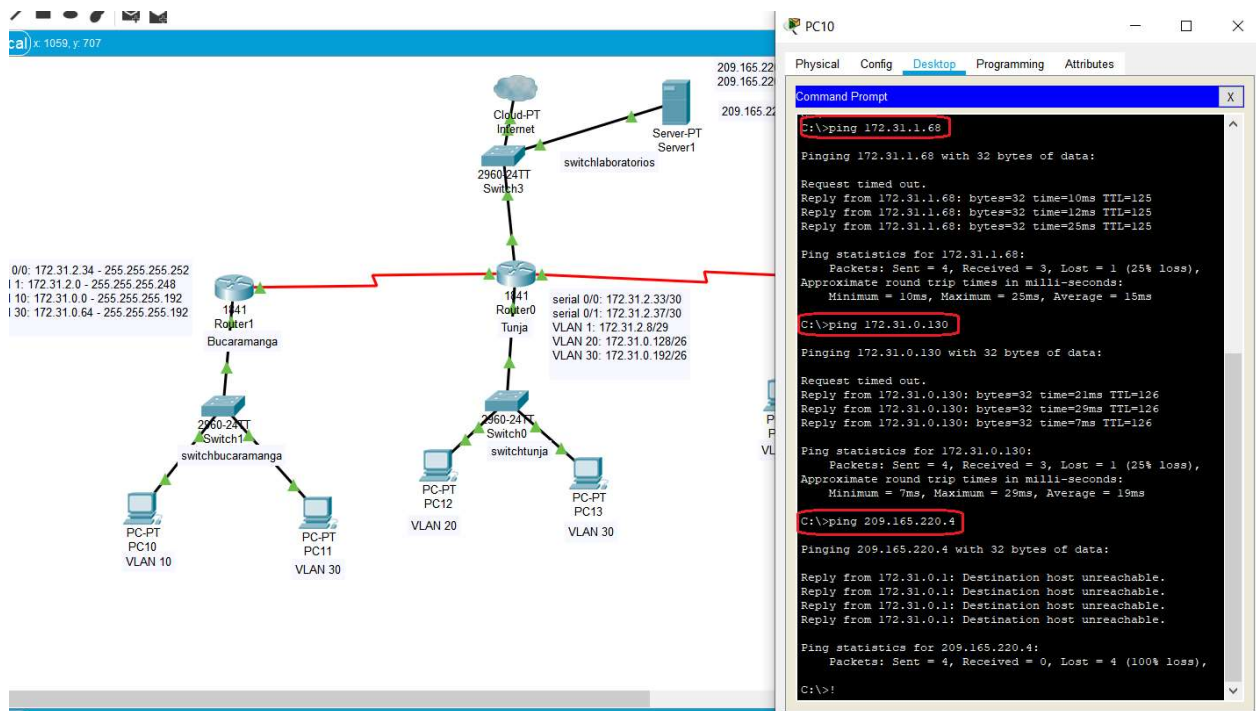


Ilustración 38: ACL los hosts de VLAN 10 en BUCARAMANGA acceden a la red de CUNDINAMARCA (VLAN 20) y TUNJA (VLAN 20), no internet.

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

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

The image shows a network diagram on the left and a command prompt window on the right. The network diagram illustrates a multi-site setup with two routers, Router1 (Bucaramanga) and Router0 (Tunja), connected via a serial link. Each router is connected to a switch (Switch1 and Switch0) which in turn connects to multiple PCs (PC10-PC11 and PC12-PC13) in different VLANs (VLAN 10, 30, 20, 30). The command prompt window shows the execution of ping commands from PC10 to various destinations, all resulting in 100% packet loss, indicating that the ACL is blocking traffic between VLANs.

```

Command Prompt
C:\>ping 172.3.0.68
Pinging 172.3.0.68 with 32 bytes of data:
Reply from 172.31.0.1: Destination host unreachable.
Reply from 172.31.0.1: Destination host unreachable.
Reply from 172.31.0.1: Destination host unreachable.
Reply from 172.31.0.1: Destination host unreachable.

Ping statistics for 172.3.0.68:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 172.3.0.130
Pinging 172.3.0.130 with 32 bytes of data:
Reply from 172.31.0.1: Destination host unreachable.
Reply from 172.31.0.1: Destination host unreachable.
Reply from 172.31.0.1: Destination host unreachable.
Reply from 172.31.0.1: Destination host unreachable.

Ping statistics for 172.3.0.130:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 172.3.0.194
Pinging 172.3.0.194 with 32 bytes of data:
Reply from 172.31.0.1: Destination host unreachable.
Reply from 172.31.0.1: Destination host unreachable.
Reply from 172.31.0.1: Destination host unreachable.
Reply from 172.31.0.1: Destination host unreachable.

Ping statistics for 172.3.0.194:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>!

```

Ilustración 39: ACL Los hosts de una VLAN no pueden acceder a los de otra VLAN en una ciudad.

PC10

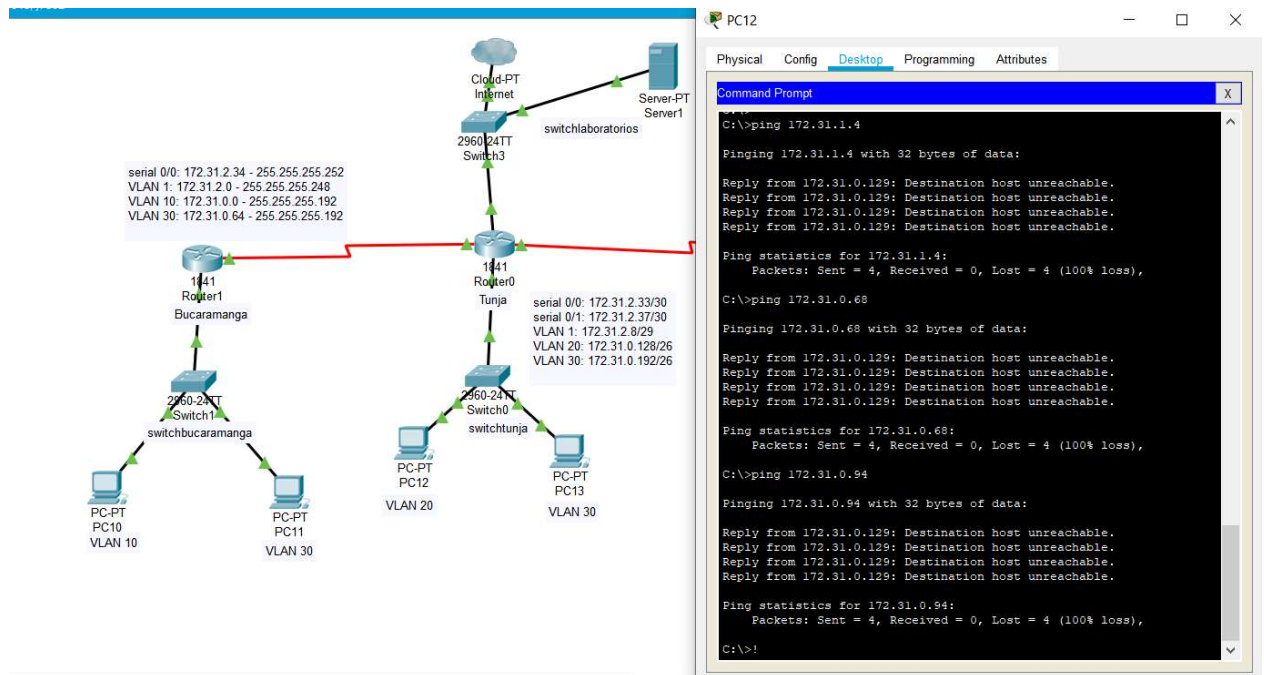


Ilustración 40: ACL Los hosts de una VLAN no pueden acceder a los de otra VLAN en una ciudad.

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

Debemos crear estas lista de acceso y deben ser aplicadas a las líneas VTY.

```
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
```

```
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
```

```
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
```

SWITCH1

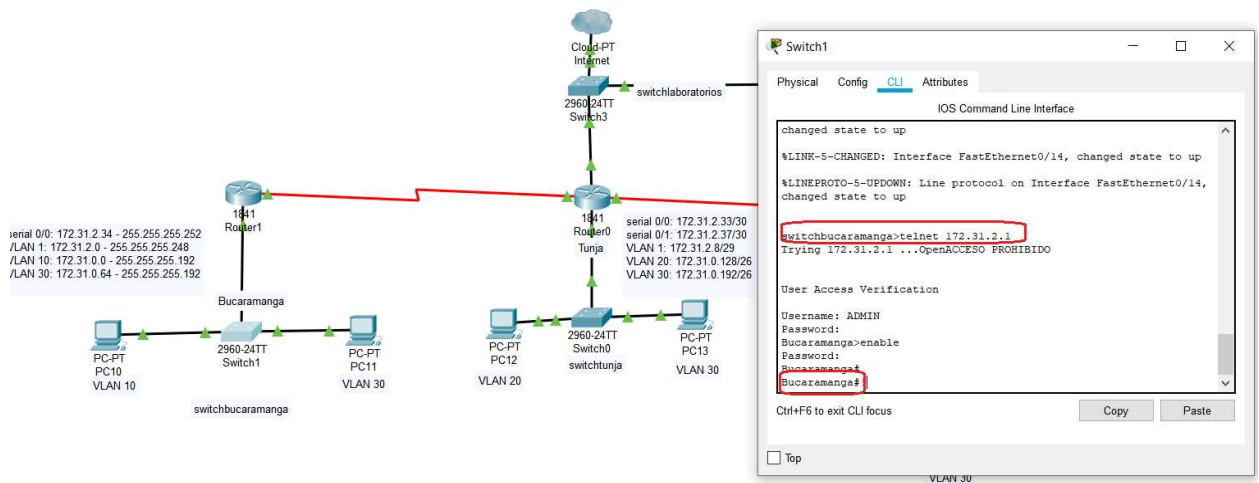


Ilustración 41: Solo los hosts de las VLAN administrativas y de la VLAN de servidores tienen acceso a los routers e internet.

Switch2

Physical Config CLI Attributes

IOS Command Line Interface

changed state to up

switchcundinamarca>telnet 172.31.2.9

Trying 172.31.2.9 ...Open ACCESO PROHIBIDO

User Access Verification

Username: ADMIN

Password:

% Login invalid

Username:

Username: ADMIN

Password:

Cundinamarca>enable

Password:

Cundinamarca#

Cundinamarca#!

Ctrl+F6 to exit CLI focus

Copy

Paste

Top

5. CONCLUSIONES

- Lo importante para desarrollar confianza en nosotros para en la implementación de este tipo de propuestas es practicar mucho.
- Cada vez más debemos fortalecer nuestros conocimientos profundizando constantemente en los cambios que cada uno de ellos ha tenido.
- En todo el diseño de la red aplicamos VLSM gracias al cual el desperdicio de direcciones IP es mínimo y ajustado realmente a las necesidades Ip de cada una de las subredes.
- Bueno, definitivamente todo lo trabajado y el material didáctico utilizado en el transcurso del diplomado han sido de vital importancia para llegar donde estamos, todo lo hemos utilizado en este punto del curso, los cuadros, los comandos, etc.
- El diseño que realice para la empresa funciona a la perfección, se realizaron todas las pruebas de caso y todas arrojan resultado favorable.
- La vida que tenemos está muy relacionada con la tecnología, esta ocupa parte fundamental dentro de nuestras vidas tanto familiares como laborales.
- Ya no tenemos barreras ni de tiempo ni mucho menos de espacio, podemos acceder a los que queramos en el lugar donde se encuentre.
- Veo con mucha seguridad que el Diplomado me ha aportado mucho para mi vida laboral.
- Veo que la temática desarrollada ha ayudado a mi formación integral.
- He desarrollado este proyecto desde cero y me agrada el grado de conocimiento que tengo relacionado a los dispositivos y su configuración.

BIBLIOGRAFIA Y WEBGRAFIA

- <http://www.cisco.com/>
- MODULO CISCO.

BIBLIOGRAFIA

- CISCO SYSTEM. Modulo Curso de entrenamiento CCNA 1 EXPLORATION (Network Fundamentals y Routing Protocols and Concepts).