EVALUACIÓN PRUEBA DE HABILIDADES PRÁCTICAS

CRISTIAN EMIRO GASTELBONDO OSPINO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA “UNAD”
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA ECBTI CEAD
“JOSÉ ACEVEDO Y GÓMEZ”
BOGOTÁ
2019

EVALUACIÓN PRUEBA DE HABILIDADES PRÁCTICAS

CRISTIAN EMIRO GASTELBONDO OSPINO

TRABAJO DE GRADO DIPLOMADO DE PROFUNDIZACIÓN CISCO

INGENIERO ALEJANDRO TUTOR DEL DIPLOMADO DE IPLOMADO DE PROFUNDIZACIÓN CISCO (DISEÑO E IMPLEMENTACIÓN DE SOLUCIONES INTEGRADAS LAN / WAN) (OPCI - (203092A_614)

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA “UNAD”
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA ECBTI CEAD
“José Acevedo y Gómez”
Bogotá
2019.

Nota de Aceptación

_____

_____

_____

_____

Presidente del Jurado

_____

Jurado

_____

Jurado

Bogotá 15 de diciembre de 2019

Dedicado a mi amada esposa que siempre ha estado a mi lado en los momentos buenos y malos, y el cual me ha servido de apoyo aun en ese momento que dispuse todo mi ser al cumplimiento satisfactorio de esta prueba de habilidades.

AGRADECIMIENTOS

Gracias a mi esposa por comprender todos y cada una de las situaciones que se me presentaron en el desarrollo de esta esta prueba de habilidades práctica, siendo su apoyo de valiosa importancia al momento de debilidades afrontadas por los diferentes aspectos que se presentaban en el desarrollo de esta actividad.

Agradezco su paciencia, compresión, amor y sobre todo su compañía en todo los momento y aspectos de la vida.

Gracias a mis compañeros de trabajo que durante el desarrollo de la prueba de habilidades me brindaron todo su apoyo y compresión, siendo de vital ayuda en aquellos momentos que por fatiga mental mis pensamientos no eran claro y me orientaban en soluciones lógicas en el desarrollo de las actividades desarrolladas.

Gracias amigos…

TABLA DE CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURAS

GLOSARIO

ACL: Listas de control de acceso configuración utilizada en los router para otorgar privilegios de acceso o no a determinados dispositivos de una red.

COMPUTADORAS: Maquina basada en equipos electrónicos y lógica que en la actualidad es utilizada para procesar y acumular datos.

DHCP: Protocolo de configuración dinámica, protocolo tipo cliente servidor el cual asigna parámetros de red a los dispositivos, con el fin de que estos se puedan comunicar con otros en la red.

ENRUTAMIENTO: Es la accione de establecer un camino entre dos o más dispositivos de una red que tenga una conectividad real.

LAN: Red de área local, es la conexión de varias computadoras en un área determinada que varía entre 200 metros y 1 km.

OSPF: Open shortest path first o su traducción al español es abrir camino más corto primero por la traducción al español, es un protocolo que establece que ruta tomar en relación a su costo, optando en toda ocasión por la que represente el menor costo posible.

ROUTER: Equipos que permite la conexión entre varios dispositivos de una red de datos.

RED DE DATOS: toda aquella arquitectura de comunicación que se desatinado para la transmisión y recepción de datos.

VLAN: Red de área virtual local es la forma de establecer redes lógicas independientes al interior de una red física.

RESUMEN

Hoy por hoy la sociedad en general está atravesando por cambios que está demarcando su forma de actuar, pensar e incluso de interactuar entre las personas, a esta situación no es para nada ajena a las organizaciones privadas y/o públicas que están conformadas por todo este grupo de personas que contribuye al consumo de las tecnologías y medios para agilizar su comunicaciones y procesos. Pero esto en si tiene un nombre y se llama transformación Digital y el cual es definido como *"es la aplicación de capacidades digitales a procesos, productos y activos para mejorar la eficiencia, mejorar el valor para el cliente, gestionar el riesgo y descubrir nuevas oportunidades de generación de ingresos*"[1], y el cual se lleva de la mano con lo conocido actualmente como la industria 4.0, o cuarta revolución industrial que busca en pocas palabras el mismo objetivo.

Todo lo mencionado anteriormente necesita profesionales de distintas áreas de las tecnologías y comunicaciones que contribuyan al desarrollo de estas capacidades a nivel nacional, generando competitividad en los diferentes mercados nacionales e internacionales. En razón a esto y con el ánimo de aportar profesionales que apalanquen esta necesidad de la sociedad actual en el mundo, la Universidad Nacional Abierta y a Distancia UNAD, promueve como opción de grado el Diplomado de profundización CISCO, el cual tiene como uno de sus principales objetivos es formas a los profesionales del mañana para afrontar y general los medios y forma de establecer los canales que estas tecnologías requieran para su utilización de nivel masivo

PALABRAS CLAVE: Cisco, router, VLAN, Enrutamiento, listas, control, acceso, Vecinos, Conectividad.

[1] Fuente: https://www.powerdata.es/transformacion-digital

ABSTRACT.

Today, society in general is going through changes that are demarcating its way of acting, thinking and even interacting between people, this situation is not at all foreign to private and / or public organizations that are formed by all this group of people who contribute to the consumption of technologies and means to speed up their communications and processes. But this in itself has a name and is called Digital transformation and which is defined as “it is the application of digital capabilities to processes, products and assets to improve efficiency, improve customer value, manage risk and discover new opportunities. of income generation ”, and which is hand in hand with what is currently known as industry 4.0, or fourth industrial revolution that seeks in a few words the same objective.

Everything mentioned above needs professionals from different areas of technology and communications that contribute to the development of these capacities at the national level, generating competitiveness in different national and international markets. Because of this and with the encouragement of providing professionals who leverage this need of today's society in the world, the National Open and Distance University UNAD, promotes as a degree option the CISCO deepening Diploma, which has as one of its main objectives are ways for tomorrow's professionals to face and general means and way to establish the channels that these technologies require for their use of mass level

1. INTRODUCCIÓN

Durante el desarrollo de la presente actividad los estudiantes colocaran a prueba todos los conocimientos adquiridos durante las cuatro unidades abordadas en el diplomado de profundización CISCO con el solo propósito de dar solución a los dos escenarios propuesta en la actividad de prueba de habilidades.

2. OBJETIVOS

2.1 OBJETIVO GENERAL

- Practicar las habilidades adquiridas durante los ejercicios elaborado en las 04 unidades desarrolladas en la resolución de los 02 escenarios planteados en la presente actividad.

2.2 OBJETIVOS ESPECÍFICOS

- Ensamblar los dispositivos acuerdo como lo indica cada escenario a elaborar.
- Establecer el direccionamiento requerido en los dispositivos
- Elaborar las configuraciones lógicas requeridas en cada uno de los escenarios.
- Dejar evidencia del Desarrollo de la actividad.
- Realizar la entrega de trabajo final acuerdo parámetros establecidos.

3 PLANTEAMIENTO DEL PROBLEMA

3.1 DEFINICIÓN DEL PROBLEMA

3.1.1 ESCENARIO 1

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

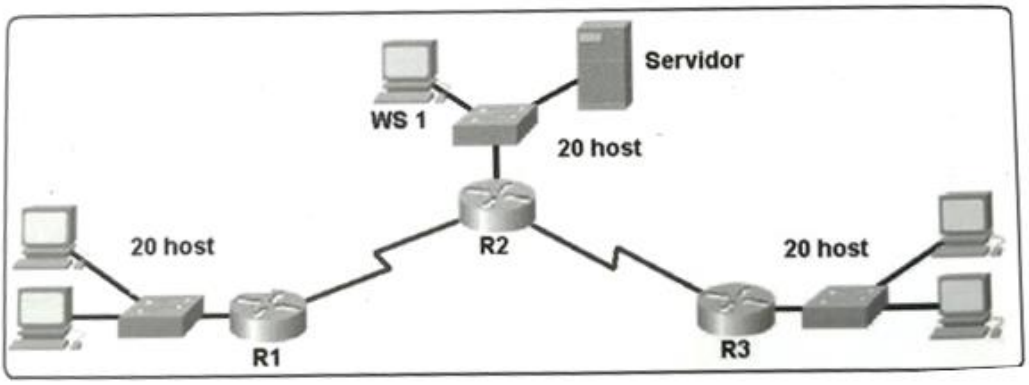


Figura 1 Topología de red host

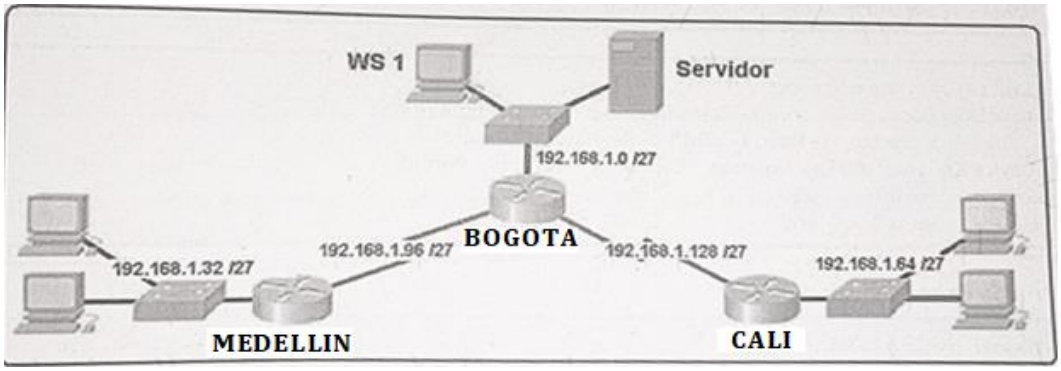


Figura 2 Topología de Red LAN

3.1.1.1 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.

3.1.1.2 Parte 1: Asignación de direcciones IP:

- Se debe dividir (subnetear) la red creando una segmentación en ocho partes, para permitir creciemiento futuro de la red corporativa.

- Asignar una dirección IP a la red.

3.1.1.3 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

Tabla 1 Direccionamiento de red

- 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.

- Verificar el balanceo de carga que presentan los routers.

- Realizar un diagnóstico de vecinos uando el comando cdp.

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

3.1.1.4 Parte 3: Configuración de Enrutamiento.

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

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

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

- 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.

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

En este momento cualquier usuario de la red tiene acceso a todos sus dispositivos y estaciones de trabajo. El jefe de redes le solicita implementar seguridad en la red. Para esta labor se decide configurar listas de control de acceso (ACL) a los routers.

Las condiciones para crear las ACL son las siguientes:

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

3.1.1.6 Parte 5: Comprobación de la red instalada.

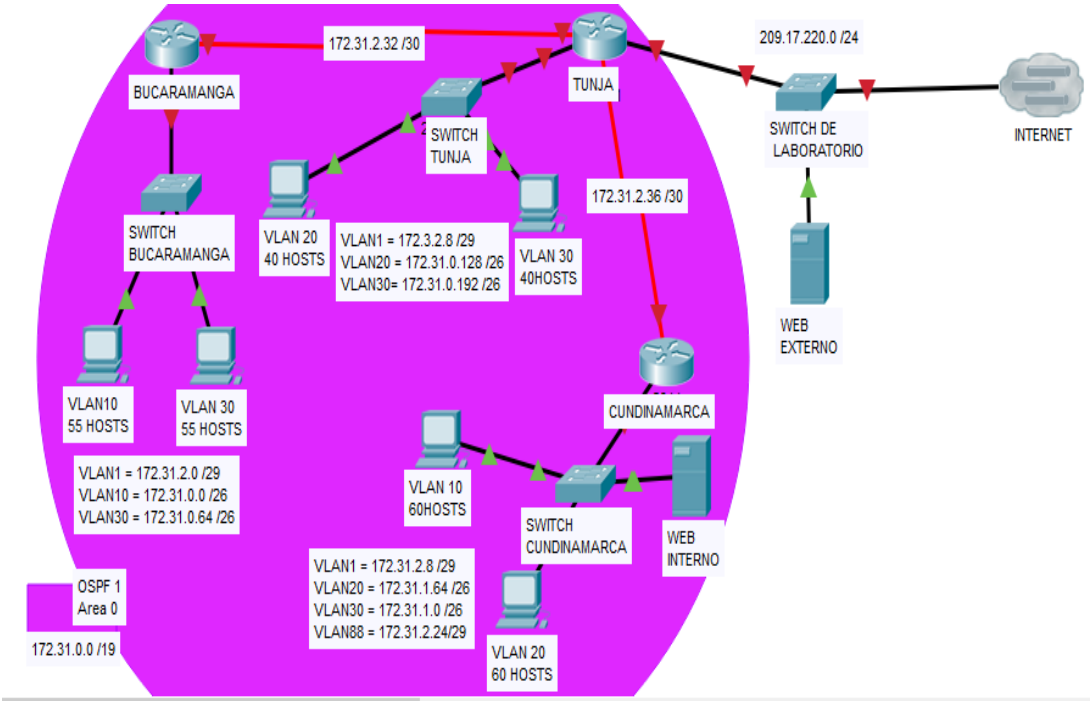
a. Se debe probar que la configuración de las listas de acceso fue exitosa.
b. Comprobar y Completar la siguiente tabla de condiciones de prueba para confirmar el óptimo funcionamiento de la red e.

	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	

Tabla 2 Verificación Listas control de acceso.

3.1.2 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.



Los siguientes son los requerimientos necesarios:

3.1.2.1 Todos los routers deberán tener los siguiente:

- 3.1.2.1.1 Configuración básica.
- 3.1.2.1.2 Autenticación local con AAA.
- 3.1.2.1.3 Cifrado de contraseñas.

- 3.1.2.1.4 Un máximo de internos para acceder al router.

- 3.1.2.1.5 Máximo tiempo de acceso al detectar ataques.

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

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

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

3.1.2.4 El enrutamiento deberá tener autenticación.

3.1.2.5 Listas de control de acceso:

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

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

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

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

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

- Los hosts de VLAN 10 en Bucaramanga acceden a la red de Cundinamarca (VLAN 20) y Tunja (VLAN 20), no internet.

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

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

3.1.2.6 VLSM: utilizar la dirección 172.31.0.0 /18 para el direccionamiento

3.2 JUSTIFICACIÓN

Dos empresas tienen serias dificultades al momento de administrar y gestionar su red de datos, siendo de vital importancia establecer de forma eficiente la conectividad entre los diferentes dispositivos que componen estas redes, así como el establecimiento de protocolos de enrutamiento y políticas de acceso a los diferentes recursos dispuestos en las diferentes topologías.

La Excelente administración y gestión de cada una de las redes previstas, garantizan de forma inmediata, el cumplimiento de las políticas de seguridad de la información establecidas por parte de la gerencia de cada una de las empresas, magnificando el rendimiento de cada uno de los dispositivos de ruteo en pro de garantizar la agilidad de los datos al transitar por la red.

En pro de garantizar la seguridad, conectividad y eficiencia de las redes de datos establecidas en los escenarios 1 y 2, se va a cumplir con los protocolos de enrutamiento (EIGRP), direccionamiento IP, listas de control de acceso, autenticación local con AAA, además de dar cumplimiento a protocolos no mencionados que garanticen la satisfacción de los distintos puntos requeridos en los escenarios propuestos.

En si el desarrollo de las directrices establecidas en cada uno de los escenarios traería en términos generales la tranquilidad de los gerentes y trabajadores de cada una de las empresas, siendo de vital importancia el cumplimiento de las políticas de seguridad de la información en el marco de su compartimentación en aras de mantener el acceso a la información solamente necesaria para el cumplimiento de las funciones otorgadas.

Por otra parte, la forma de abordaje de la solución de este problema basado en la práctica y la repetición de Las actividades dispuestas en los ejercicios de las unidades vistas durante el desarrollo de la diplomado de profundización de cisco, otorga a los estudiantes el conocimiento necesario para el soluciona miento de las directrices de cada uno de los escenarios, otorgándoles la seguridad y experticia al momento de enfrentarse a este tipo de eventualidades durante su vida laboral.

4. MARCO TEÓRICO

4.1 Red de datos.

Son todas aquellas que fueron creadas para el envío y recepción de información utilizando conmutación de paquetes, siendo sujeta a la cobertura y capacidad física de su red.[2]

Los principales elementos de una red de datos son: Hubs, pach panels, servidores y Cables.

Estas se clasifican en: LAN (red de área local), MAN (red de área metropolitana), WAN (red de área extensas) y PAN (red de área personal).

A su vez se pueden presentar estas topologías acuerdo los requerimientos del momento así: Malla, estrella, Estrella extendida y anillo.

En términos generales las redes de datos es todo aquello que se requiere para la interconexión de los dispositivos de una red de datos siendo estos últimos partes primordial para el intercambio de la información.

Hoy día es inconcebible coexistir en una sociedad sin estar conectado a una red de datos como tal, ya que para poder comunicarse o interactuar con otras personas en todos los casos debemos utilizar una red de datos para lograr efectuar esta.

4.2 Protocolos de enrutamiento de Red.

En si este está encargado de que los paquetes de información lleguen al destino indicado, para tal efecto se establecen dos tipos de ruteo que son el ruteo interno y el ruteo externo.[3]

4.2.1 Tipos de protocolos de enrutamiento de red.

Hay dos tipos de ruteo que son el interno y el externo.

[2] Fuente: (www.universidadviu.com, 2019)
[3] Fuente: (www.ecured.cu, 2019)

Del interno podemos encontrar los RIP (Routing Iformation Protocol), el cual solo tiene en cuenta los dispositivos que pasara utilizando el puerto 520 y el OSPF (Open shortest Path Firts) utilizado en redes mayores esta basado en el algoritmo “Dijkstra” y el cual tiene la particularidad de establecerse en redes mas pequeñas para facilitar su utilización. [4]

En el externo encontramos el protocolo de ruteo BGP (border Gateway Protocol), este es utilizado por los vecinos exteriores con el solo propósito de difundir información de accesibilidad, una de sus ventajas es lograr el intercambio de información entre los dispositivos de ruteo con el solo propósito de permitir el intercambio de información. [5]

Siendo uno de los temas más importantes de los que nos convocan este día, los protocolos de enrutamiento, garantizan de forma eficaz el intercambio de los paquetes de información entre los diferentes dispositivos de la red, siendo de gran ayuda al momento de presentase fallas en el funcionamiento de la red, ya que de acuerdo la configuración de enrutamiento utilizada esta estaría en la capacidad de responder a dicho fallo, enrutando su trafico por otra ruta de mayor costo en pro de entregar los datos al destino indicado.

4.3 Listas de control de acceso.

Es un método utilizado para la separación de privilegios que mejora la seguridad de la red, esta funciona por medio de filtros del trafico de la red que otorgan o no privilegios de ingreso y/o salida a un dispositivo y/o recurso en particular.[6]

4.3.1 Tipo de listas de control de acceso

Lista de control de acceso estándar.
Es sencilla, solo se especifica la ip de host origen

Lista de control de acceso extendida.
Se utiliza el protocolo, la dirección de origen y destino. [7]

[4] Fuente: (www.ecured.cu, 2019)
[5] Fuente: (www.ecured.cu/Protocolos_de_ruteo, 2019)
[6] Fuente: (recursostic.educacion.es, 2019)
[7] Fuente: (recursostic.educacion.es, 2019)

Las listas de control de acceso nos permiten acercarnos cada vez mas a el cumplimiento de las políticas de seguridad de la información que establezca los dirigentes de cada organización, promoviendo en todo caso el acceso a recursos autorizados que pueda brindar la red, o denegando el ingreso a usuario que no tengan permiso de acceso a dichos recursos.

5. MATERIALES Y MÉTODOS

5.1 MATERIALES

Materiales utilizados para cada uno del os escenarios dispuestos fueron:

Para el desarrollo del escenario 1

No	Cantidad	Elemento
01	03	Router cisco 1941
02	03	Switch cisco 2960
03	05	Computadoras de escritorio
04	01	servidor
05	02	Cables de interconexión serial
06	09	Cables de interconexión gigabiteEthernet.

Tabla 3 Elementos escenario 1

Para el desarrollo del escenario 2

No	Cantidad	Elemento
01	04	Router cisco 1941
02	04	Switch cisco 2960
03	06	Computadoras de escritorio
04	02	servidor
05	02	Cables de interconexión serial
06	13	Cables de interconexión gigabiteEthernet.
07	01	emulador de internet

Tabla 4 Elementos escenario 2

5.2 METODOLOGÍA

La metodología a utilizar para el desarrollo de esta actividad es la Analítica, ya que abordaremos todos y cada uno de los dispositivos de forma independiente con el fin de establecer un comportamiento general de cada una de las redes de los escenarios propuestos.

6 DESARROLLO DEL PROYECTO

6.1 Escenario 1

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

6.1.2 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.

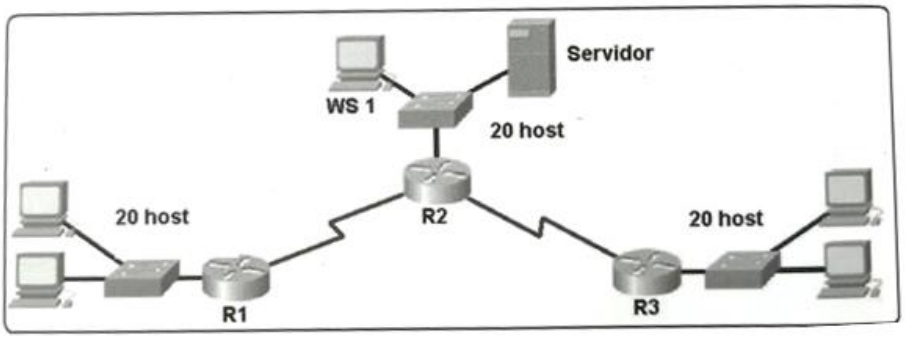


Figura 3 Esquema de Red "Host"

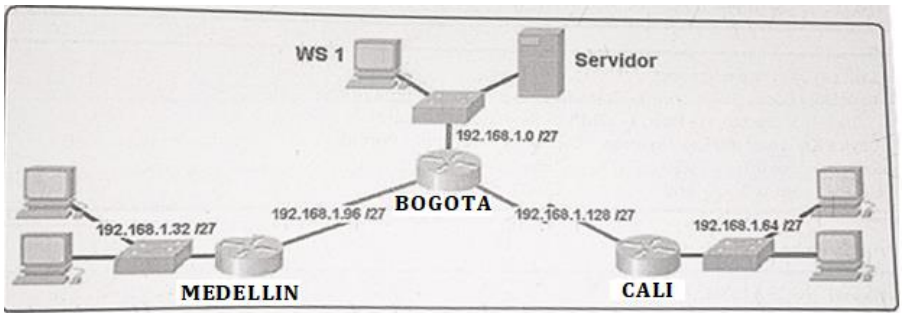


Figura 4 Esquema de la Red

6.1.3 Desarrollo de la actividad

Como trabajo inicial se debe realizar lo siguiente.

- Realizar las rutinas de diagnóstico y dejar los equipos listos para su configuración (asignar nombres de equipos, asignar claves de seguridad, etc).
- Realizar la conexión fisica de los equipos con base en la topología de red

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

6.1.3.1 Parte 1: Asignación de direcciones IP:

a. Se debe dividir (subnetear) la red creando una segmentación en ocho partes, para permitir creciemiento futuro de la red corporativa.

Dividir la red en 8 partes

Relizamos el calculo acuerdo lo indicado

2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
128	64	32	16	8	4	2	1

Tabla 5 Base de cálculo.

$2^n \geq C\ ; 8$
$2^3 = 8$

11111111.11111111.11111111.00000000→11111111.11111111.11111111.11100000
/24 → /27
Host
2^n-2=H $\rightarrow 2^5 - 2 = 32 - 2 = 30$

Saltos de red 256-224 = 32

b. Asignar una dirección IP a la red

192.168.1.0

Redes Subneteadas.

No	Subred	Primera ip utilizable	Ultima direccion Utilizable	broadcast
0	192.168.1.0	192.168.1.1	192.168.1.30	192.168.1.31
1	192.168.1.32	192.168.1.33	192.168.1.62	192.168.1.63
2	192.168.1.64	192.168.1.65	192.168.1.94	192.168.1.95
3	192.168.1.96	192.168.1.95	192.168.1.126	192.168.1.127
4	192.168.1.128	192.168.1.129	192.168.1.158	192.168.1.159
5	192.168.1.160	192.168.1.161	192.168.1.190	192.168.1.191
6	192.168.1.192	192.168.1.193	192.168.1.222	192.168.1.223
7	192.168.1.224	192.168.1.225	192.168.1.254	192.168.1.255

Tabla 6 Redes Subnetedas

6.1.3.2 Parte 2: Configuración Básica.

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

	R1	R2	R3
Nombre de Host	**MEDELLIN**	**BOGOTA**	**CALI**
Dirección de Ip en interfaz Serial 0/0	192.168.1.99	192.168.1.98	192.168.1.131
Dirección de Ip en interfaz Serial 0/1		192.168.1.130	
Dirección de Ip en interfaz GA 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

Tabla 7 Redes Utilizadas

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.

Commando utilizado show ip route
Router medellin

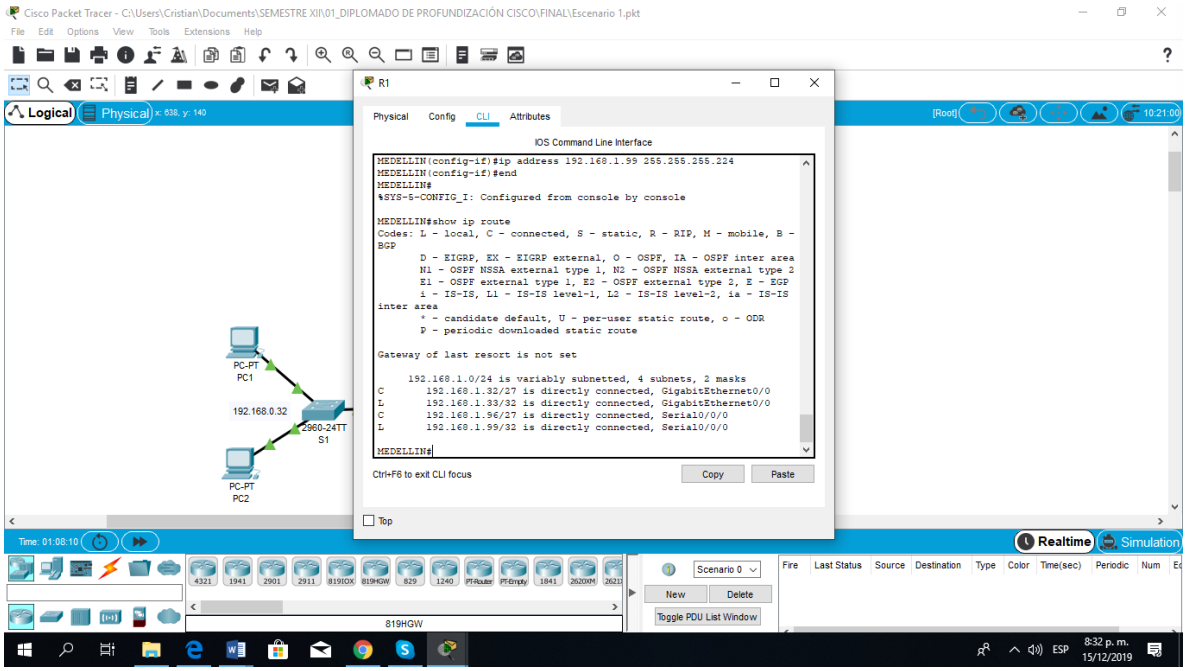


Figura 5 Comando Show Ip route en R1

Router Bogota

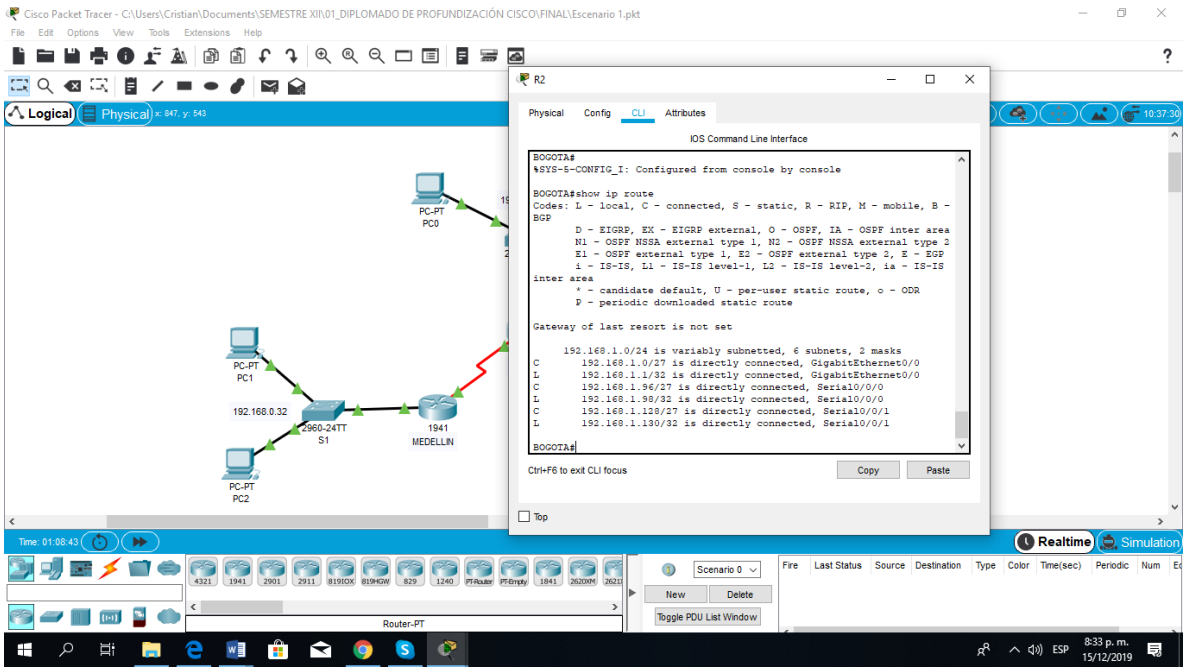


Figura 6 Comando Show Ip route en R2

Router cali

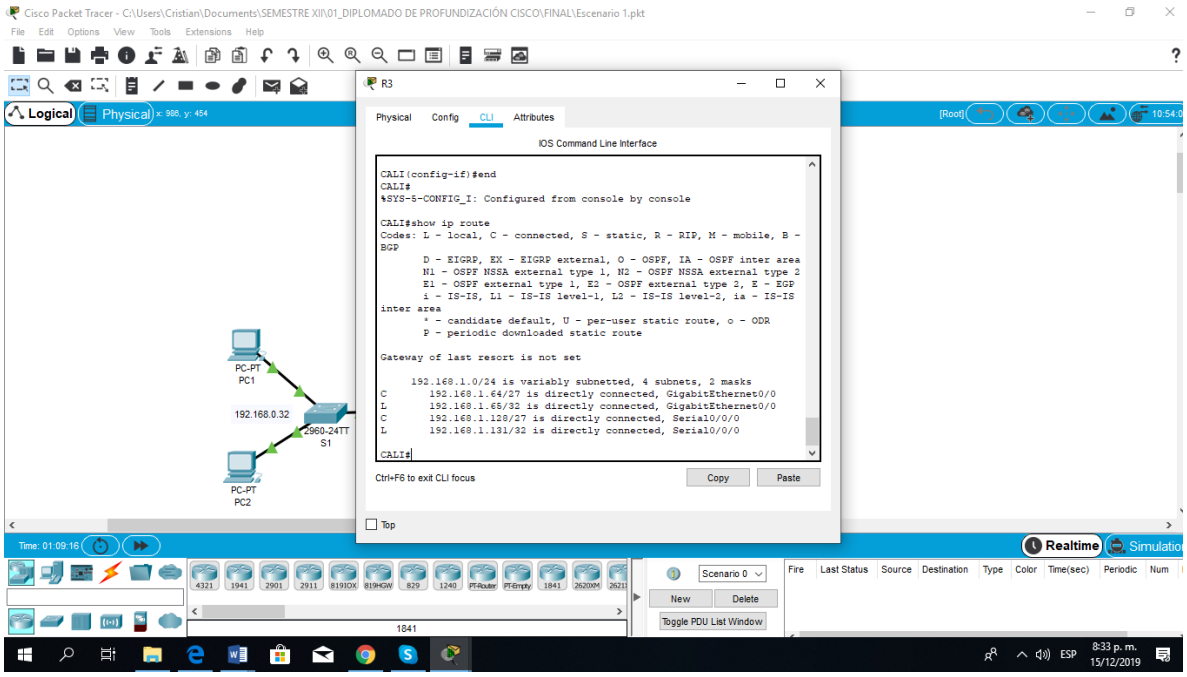


Figura 7 Comando Show Ip route en R3

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

Aun el router no tiene rutas establecidas, por ende no va a mostrar un balanceo de cargas, siendo toda vez que utilicemos el comando show ip route las mismas imágenes colodas para ver la tabla de enrutamiento.

Commando utilizado show ip route

Router medellin

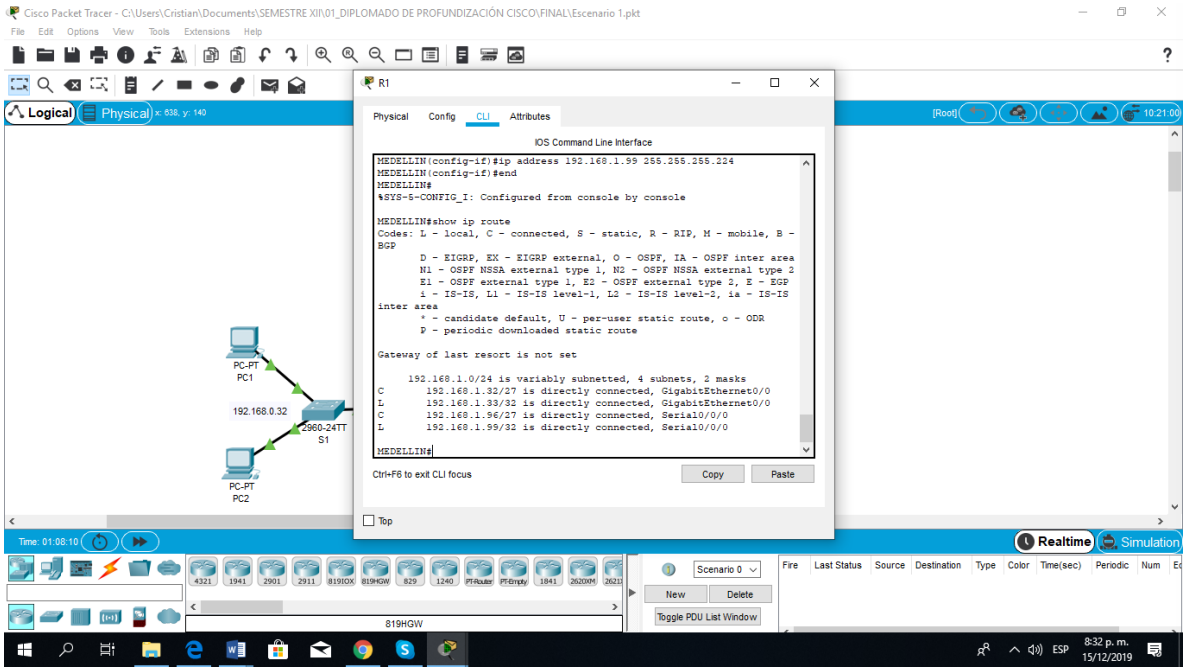


Figura 8 Comando Show Ip route en R1

Router Bogota

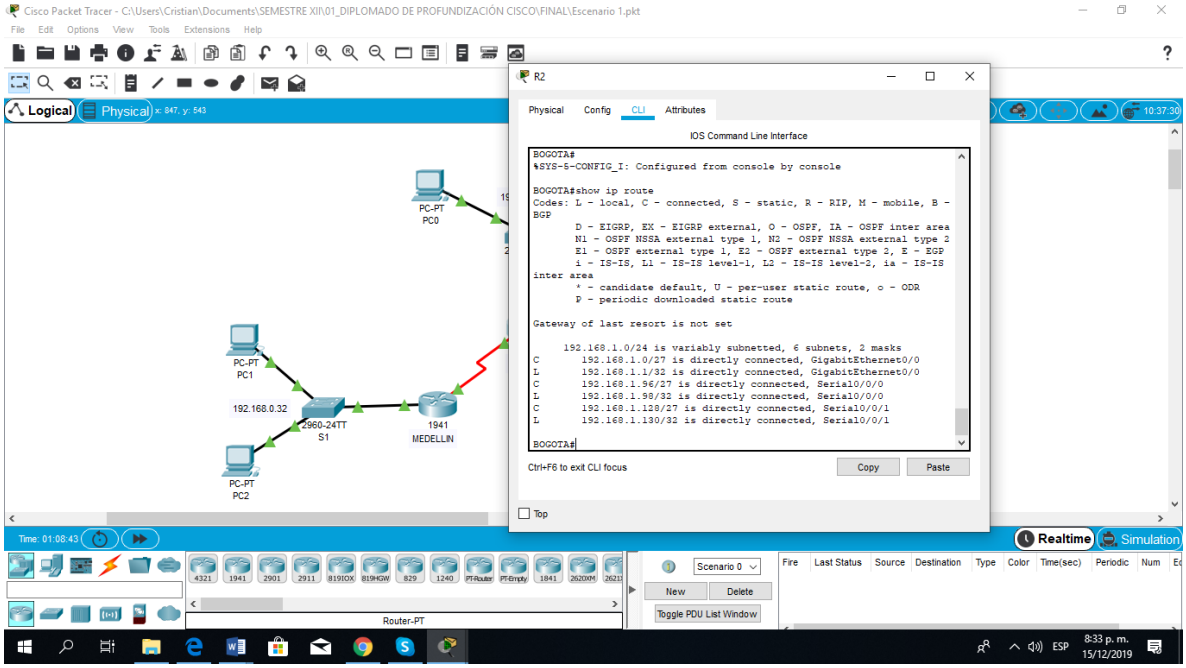


Figura 9 Comando Show Ip route en R2

Router cali

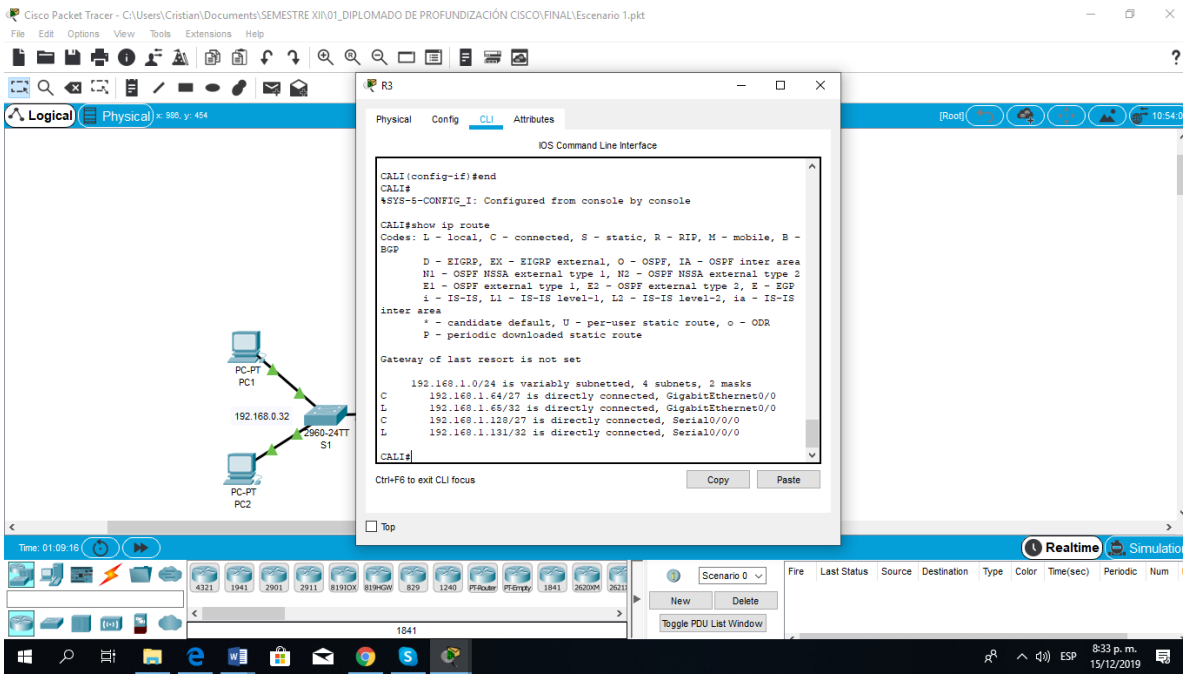


Figura 10 Comando Show Ip route en R3

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

Debemos habilitar el cdp primero

Conf t

Cdp run

Corremos el cdp

Enable

Conf t

Show cdp neighbors

Otros comando que podemos utilizar

Show cdp

Show cdp entry “dispositivo”

Show cdp entry “interface”

Router Medellin

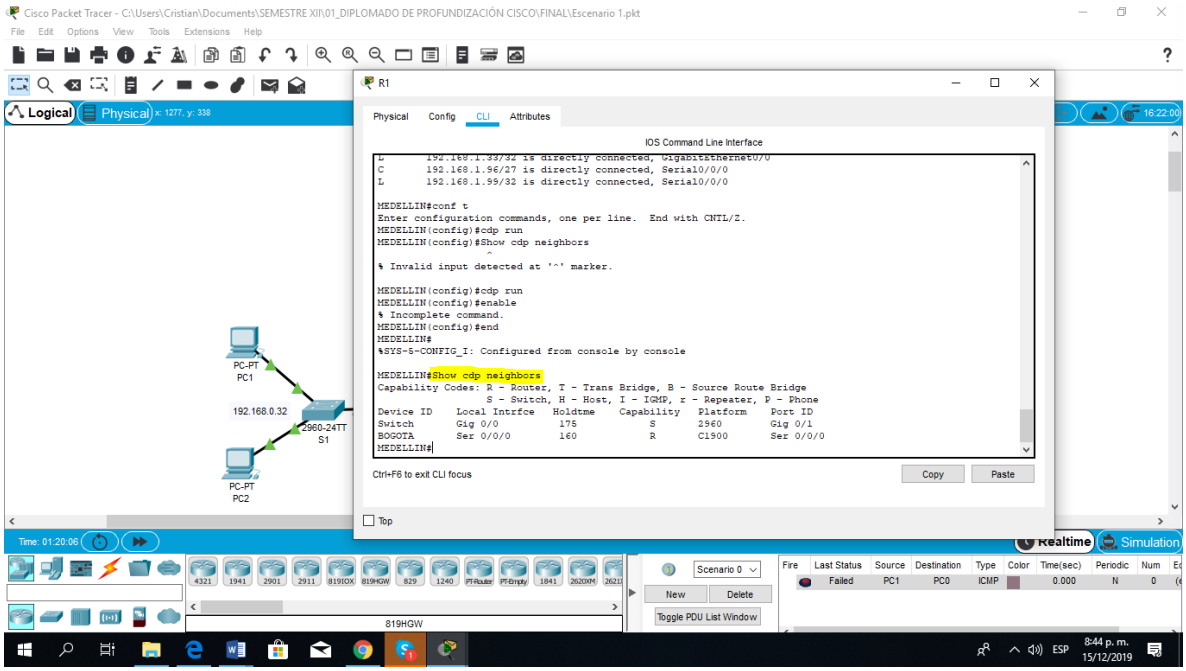


Figura 11 Comando Show cdp neighbors En R1

Router Bogota

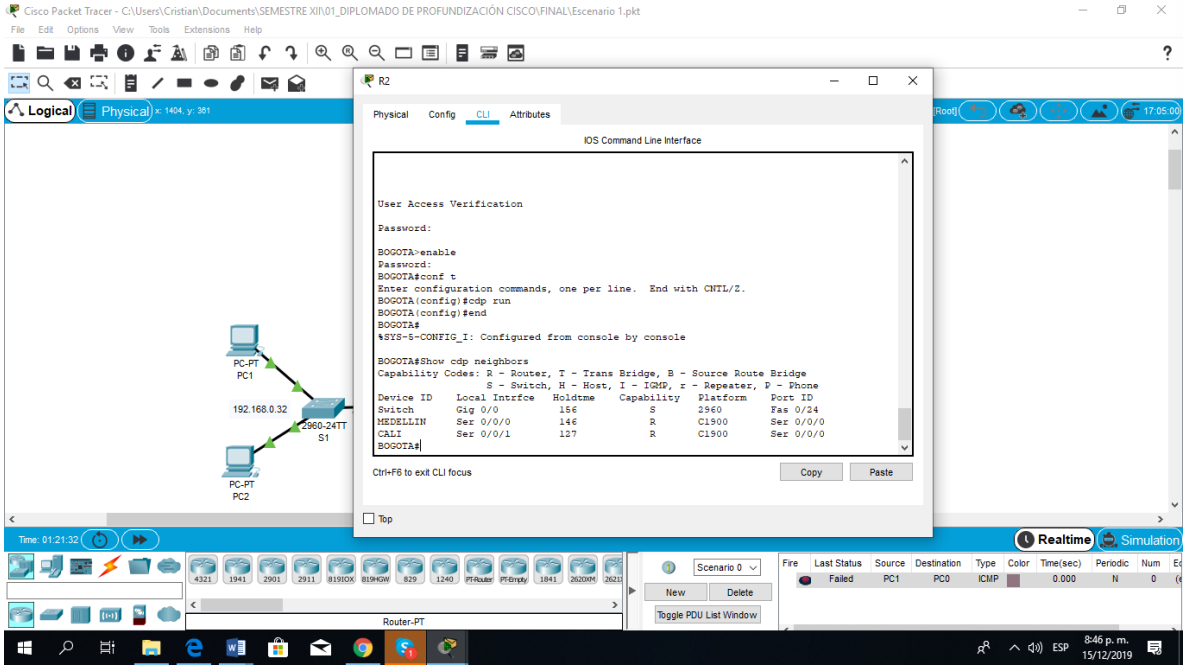


Figura 12 Comando Show cdp neighbors En R2

Router Cali

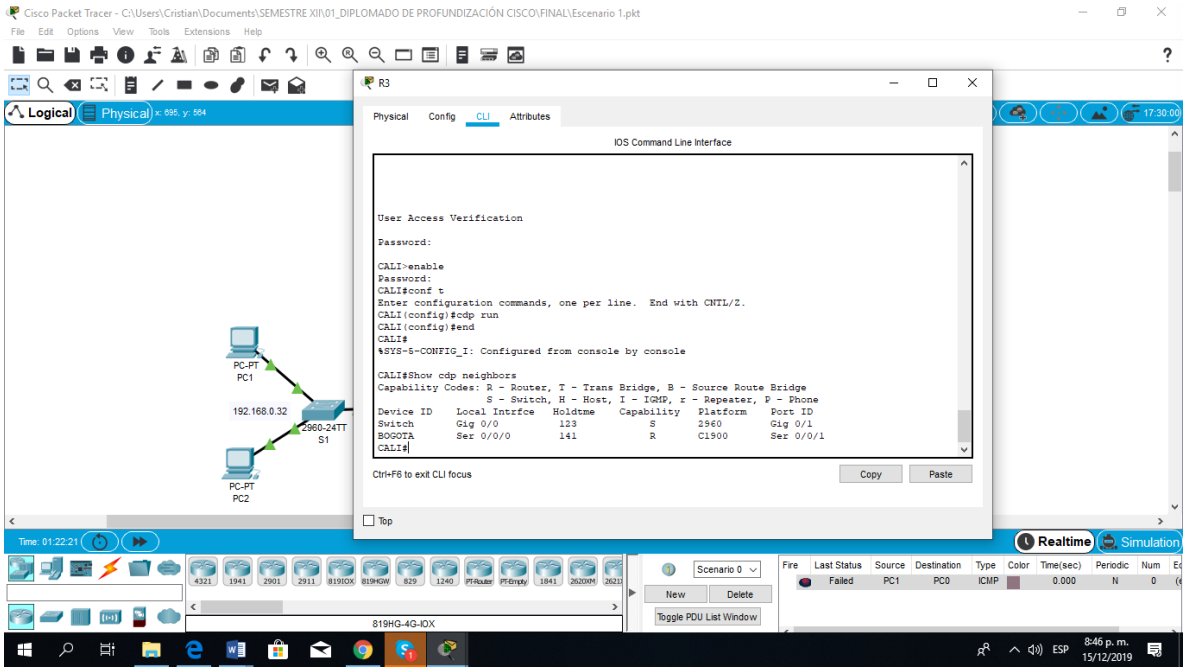


Figura 13 Comando Show cdp neighbors En R3

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

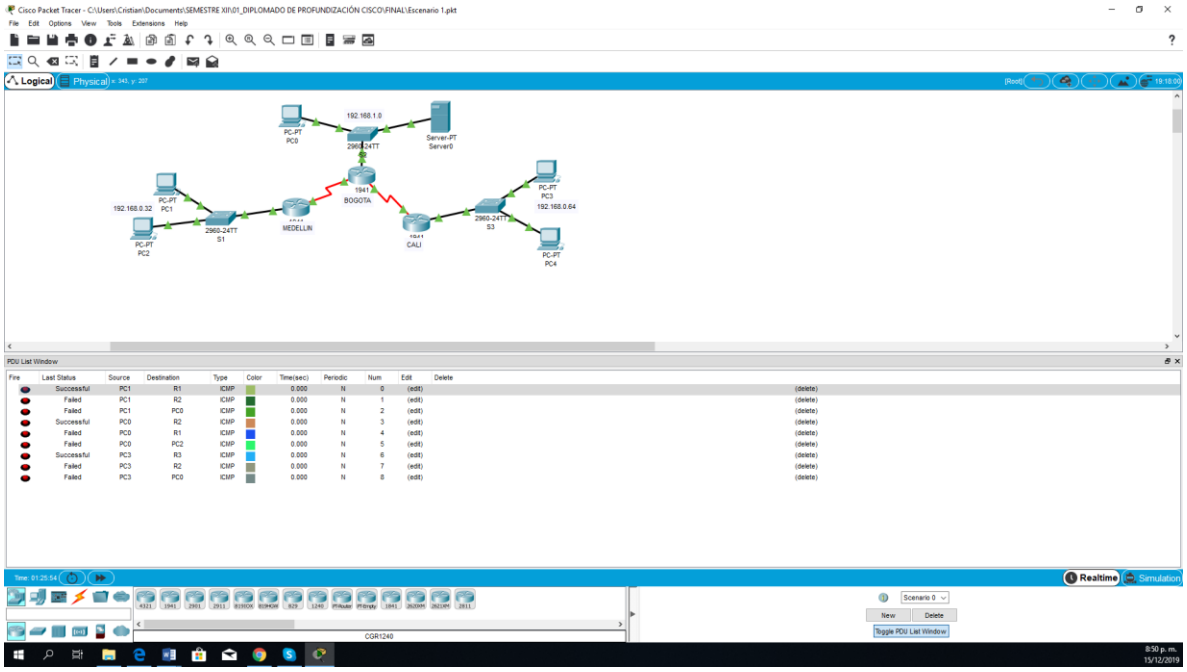


Figura 14 Comando Ping Prueba conectividad red

6.1.3.3 Parte 3: Configuración de Enrutamiento.

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

Router Medellin

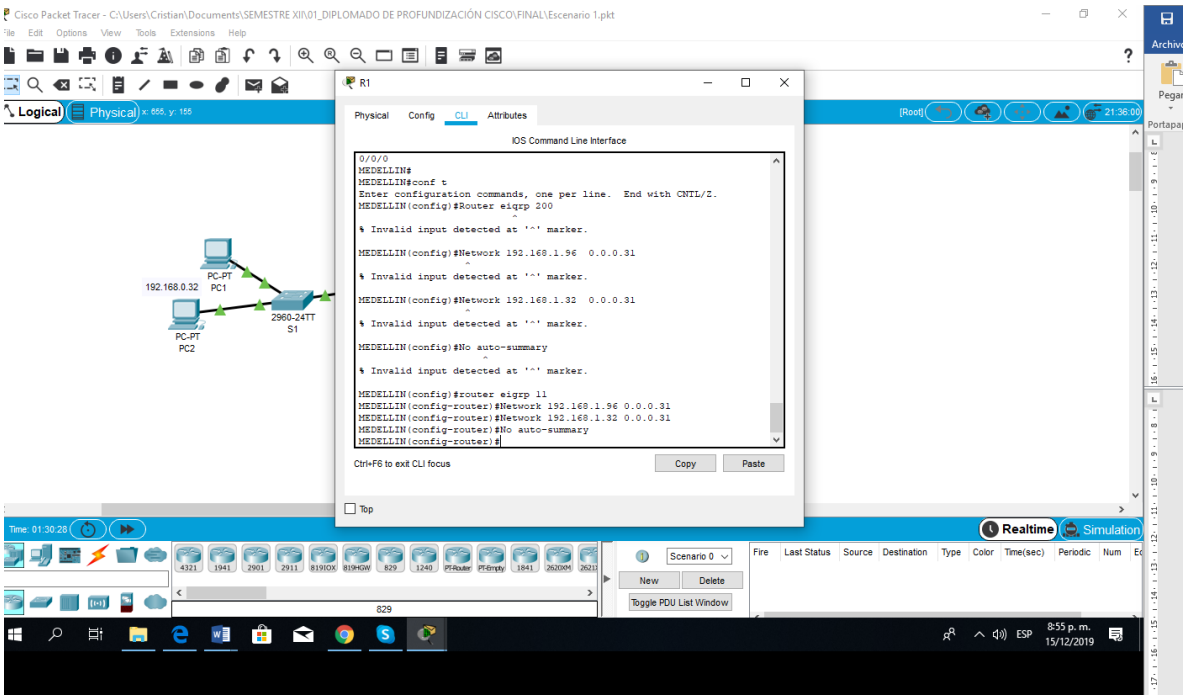


Figura 15 Comando eigrp 11 En R1 Medellín

Router Bogotá

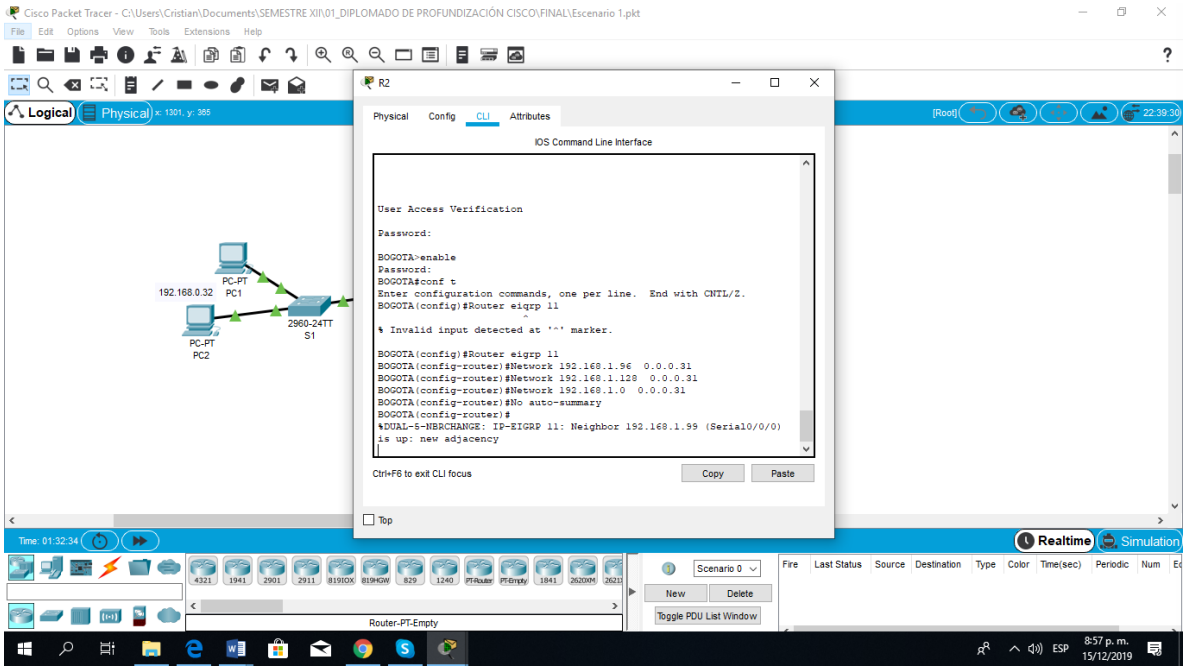


Figura 16 Comando eigrp 11 En R2 Bogotá

Router Cali

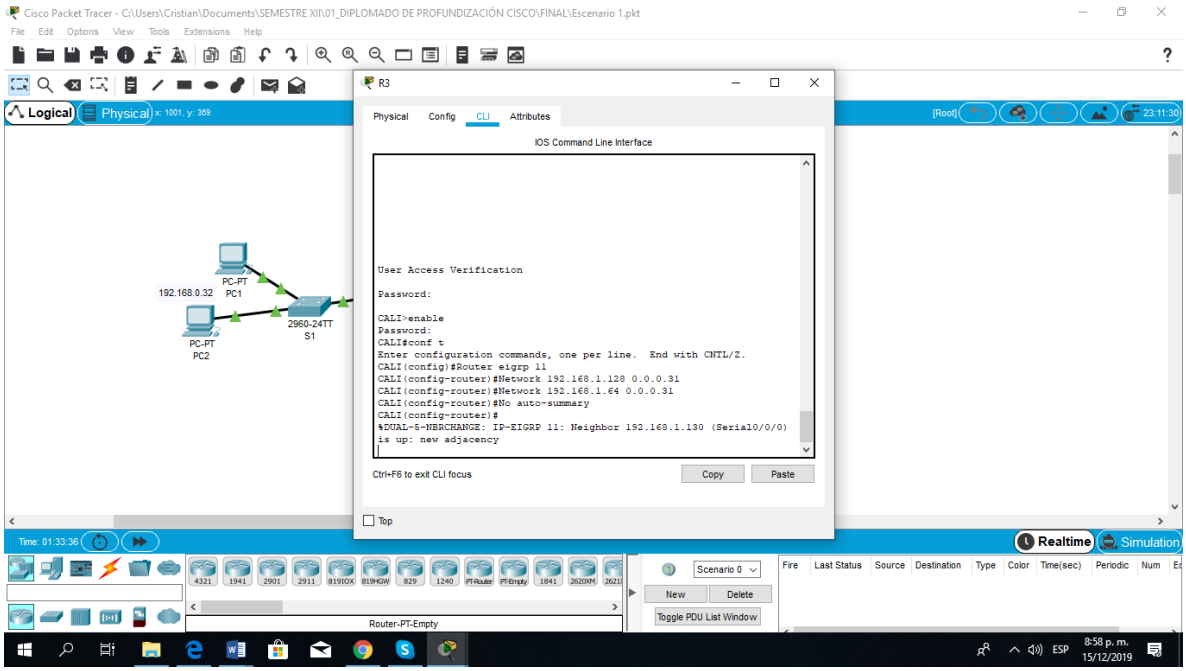


Figura 17 Comando eigrp 11 En R3 Cali

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

Router Cali

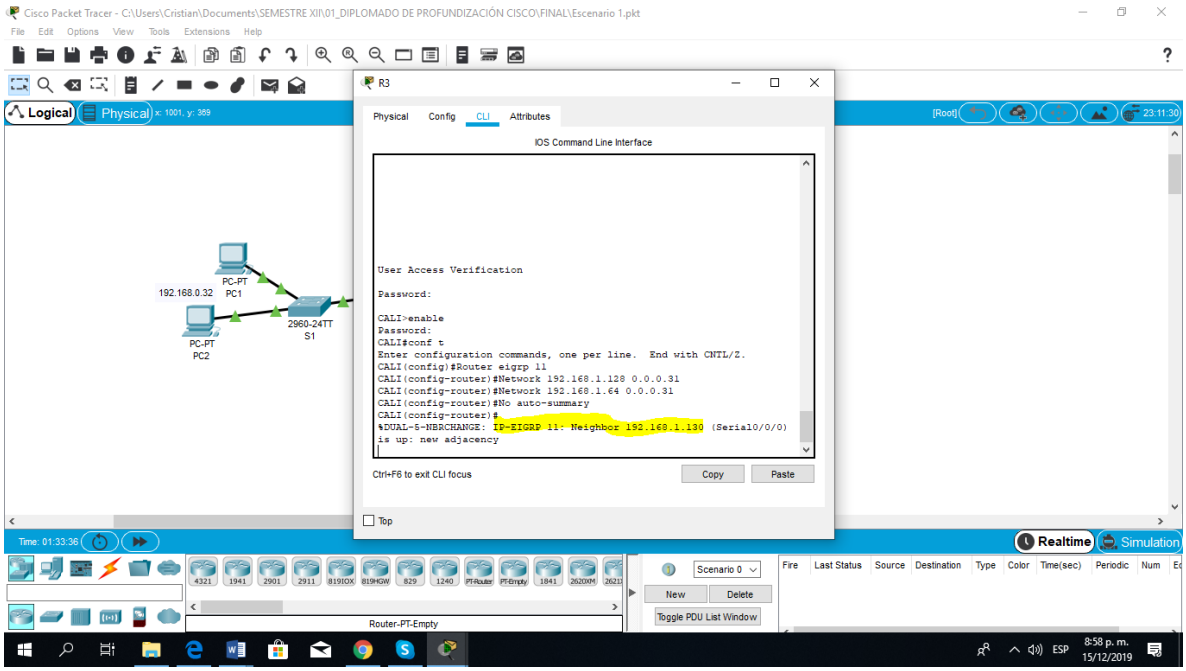


Figura 18 Verificación Comando eigrp 11 En R3 Cali

Router Medellin

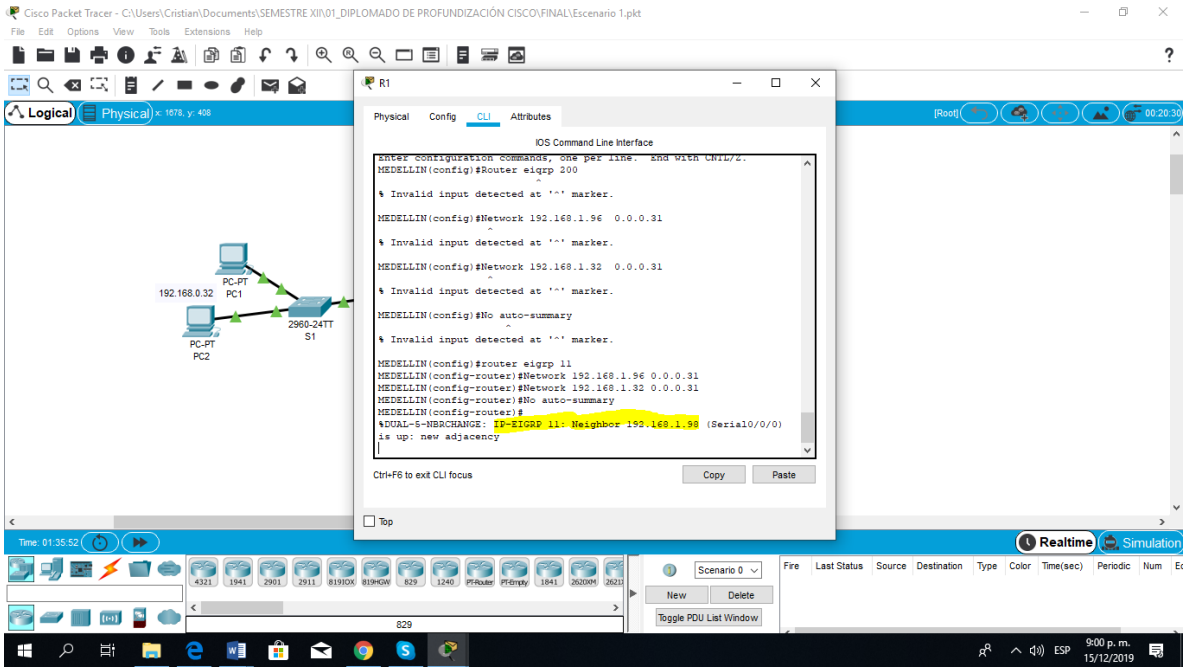


Figura 19 Verificación Comando eigrp 11 En R1 Medellín

Router Bogota

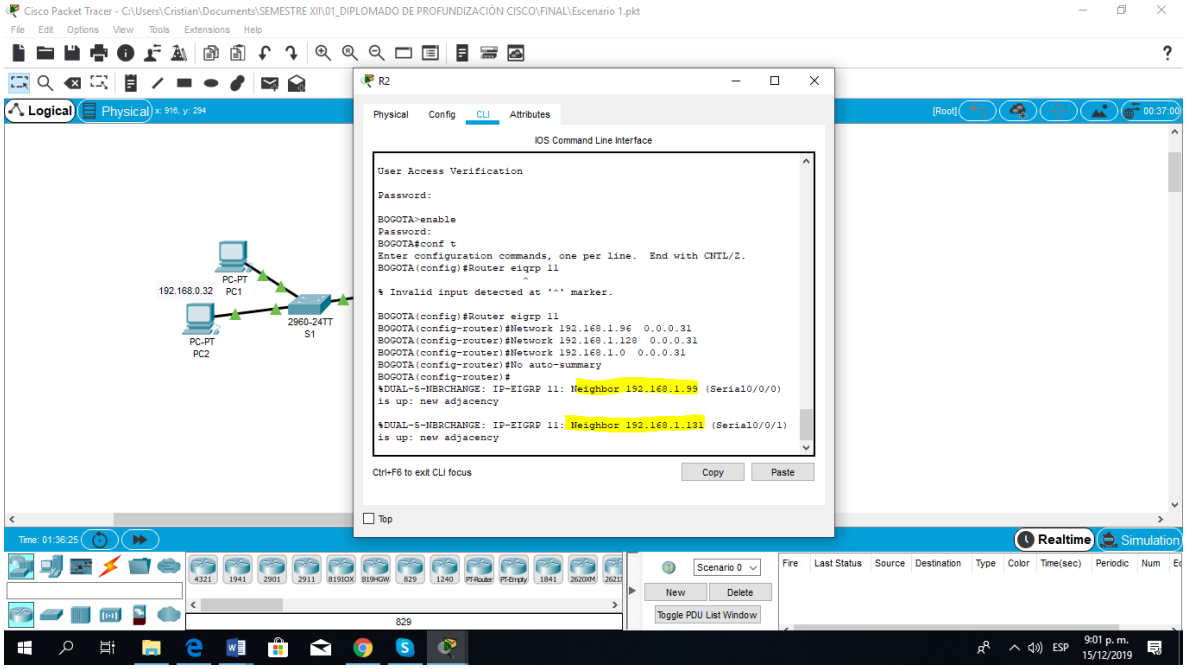


Figura 20 Verificación Comando eigrp 11 En R2 Bogotá

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
Router Medellín

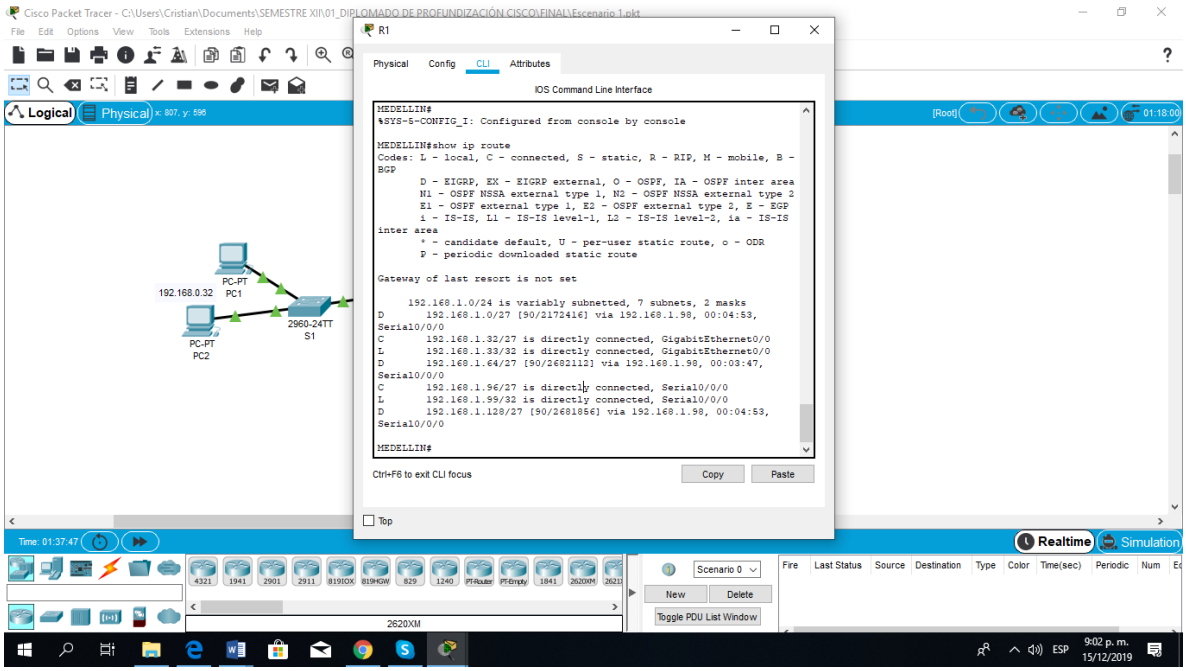


Figura 21 Comando Show Ip Router en R1 Medellín

Router Bogota

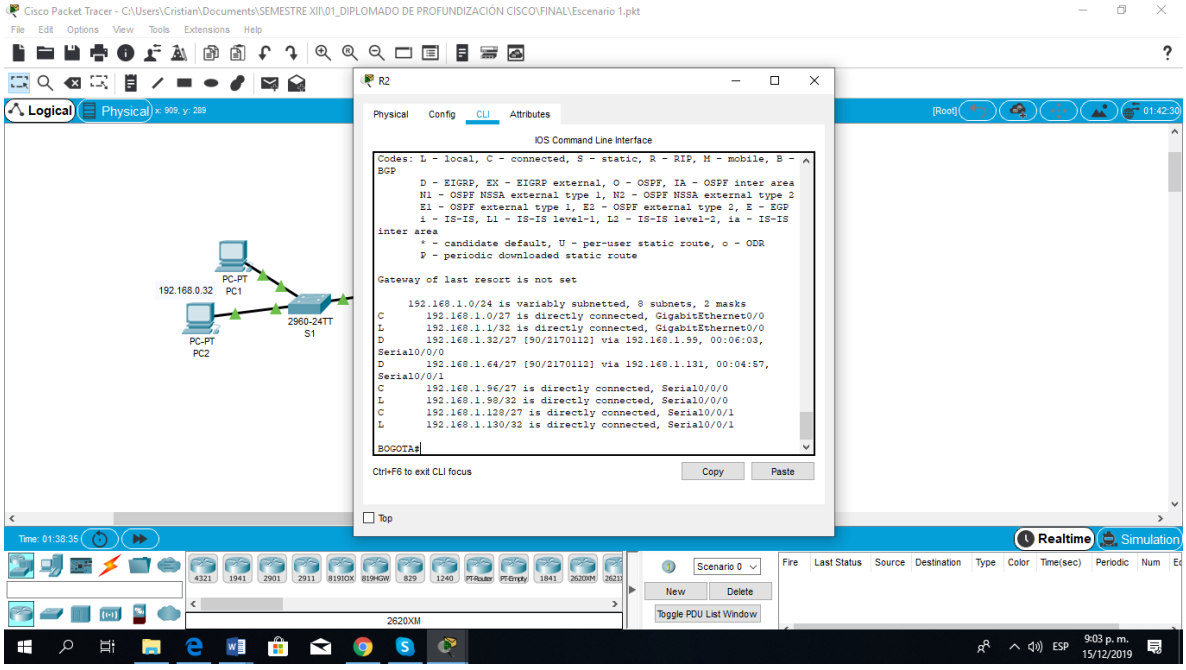


Figura 22 Comando Show Ip Router en R2 Bogotá

Router Cali

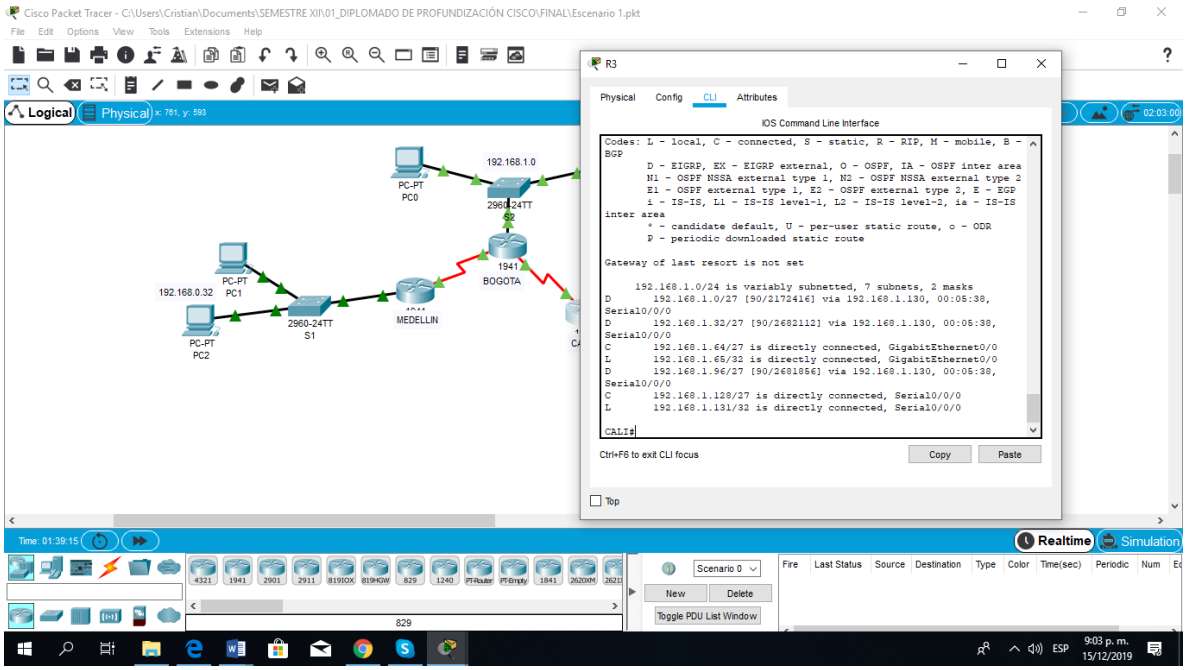


Figura 23 Comando Show Ip Router en R3 Cali

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.

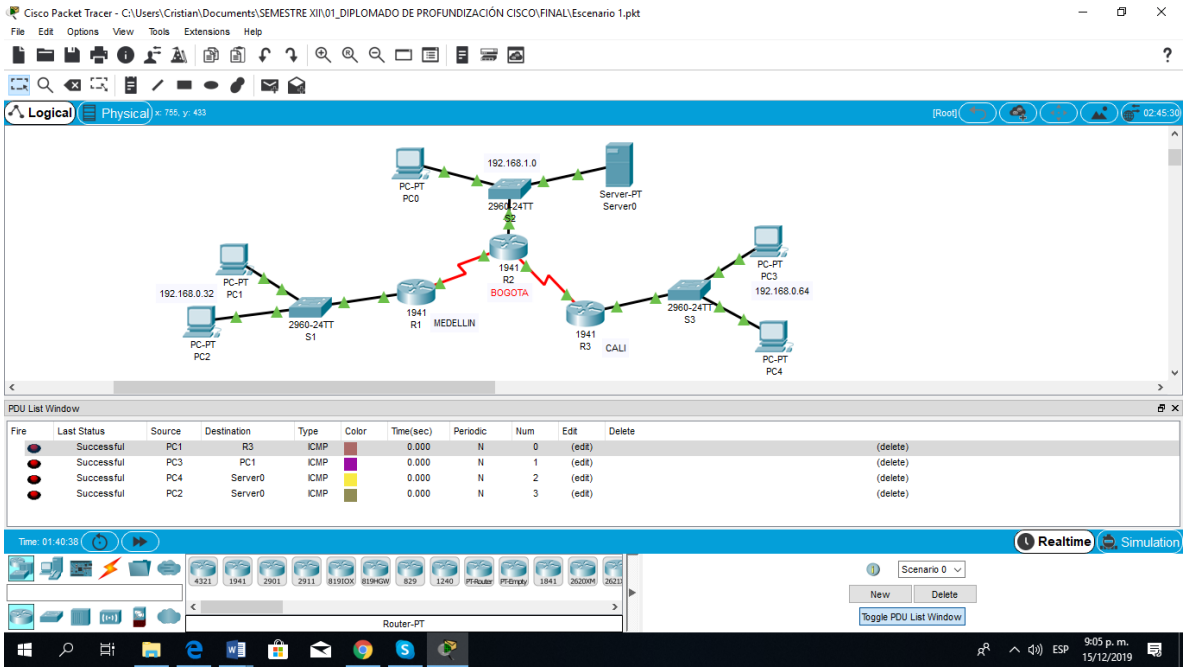


Figura 24 Prueba de ping host de la red LAN del router CALI, primero a la red de MEDELLIN y luego al servidor

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

En este momento cualquier usuario de la red tiene acceso a todos sus dispositivos y estaciones de trabajo. El jefe de redes le solicita implementar seguridad en la red. Para esta labor se decide configurar listas de control de acceso (ACL) a los routers.

Las condiciones para crear las ACL son las siguientes:

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

Router Medellín

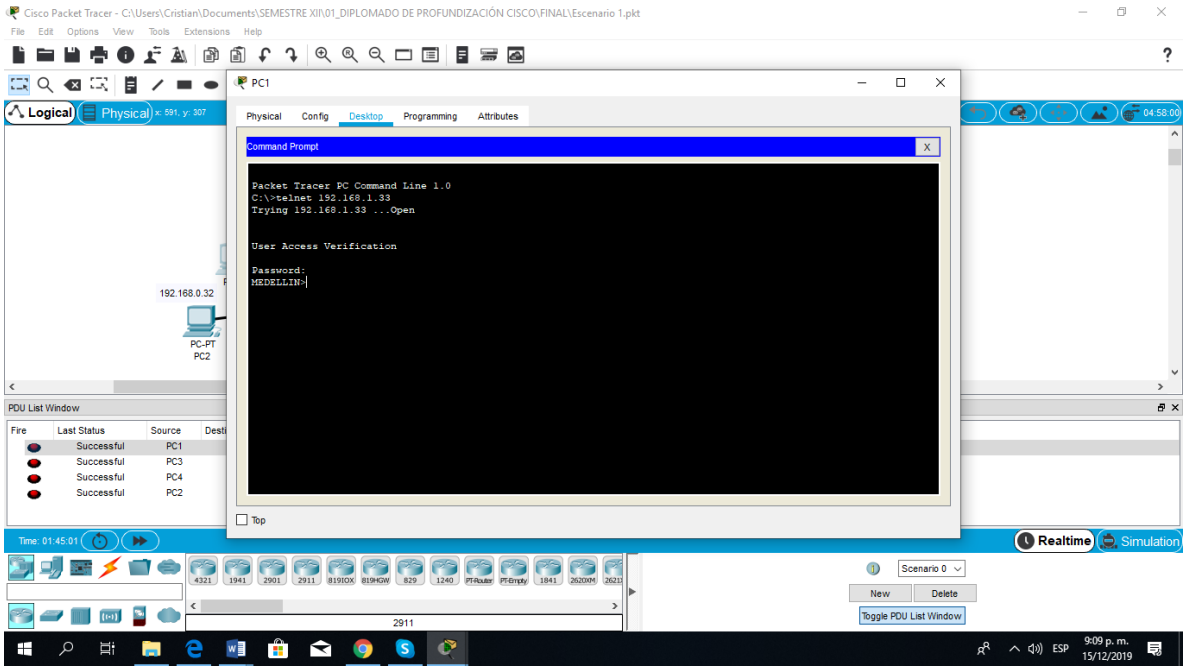


Figura 25 Telnet a router Medellín

Router Bogotá

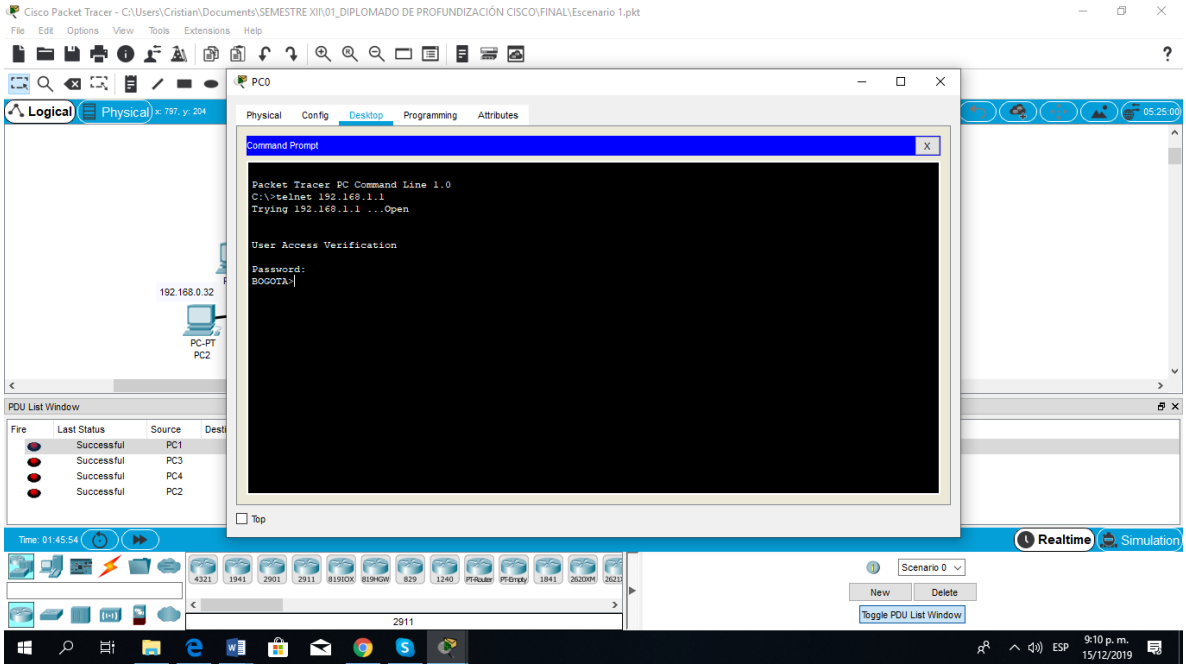


Figura 26 Telnet a router Bogotá

Router Cali

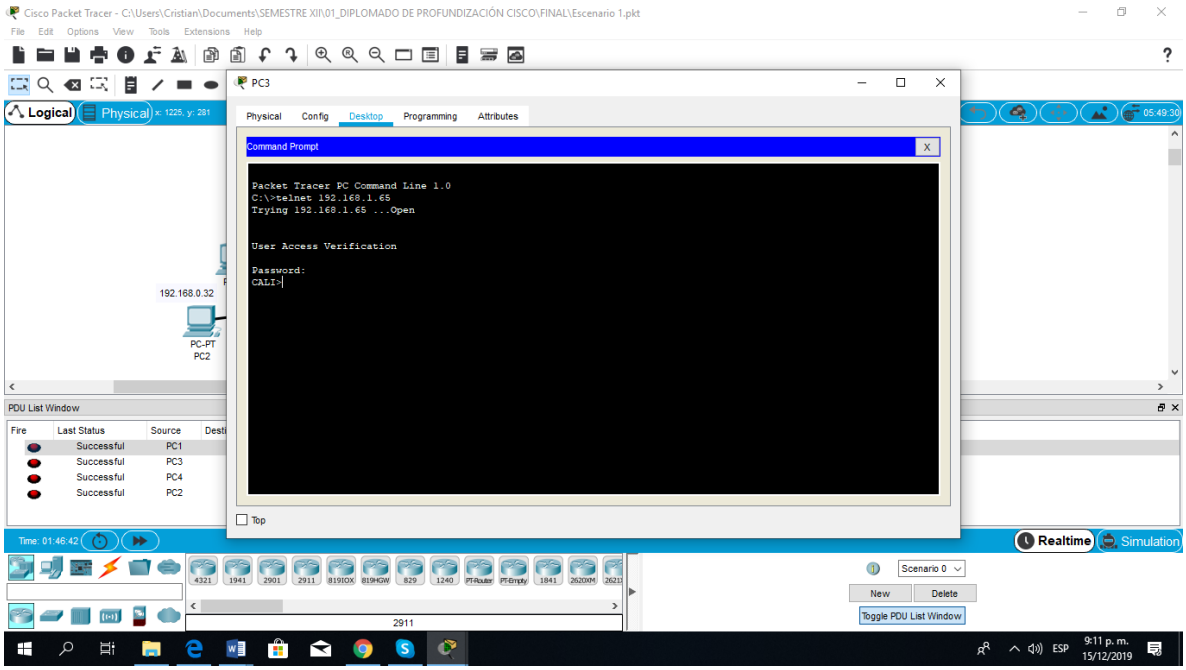


Figura 27 Telnet a router Cali

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

routre Bogotá

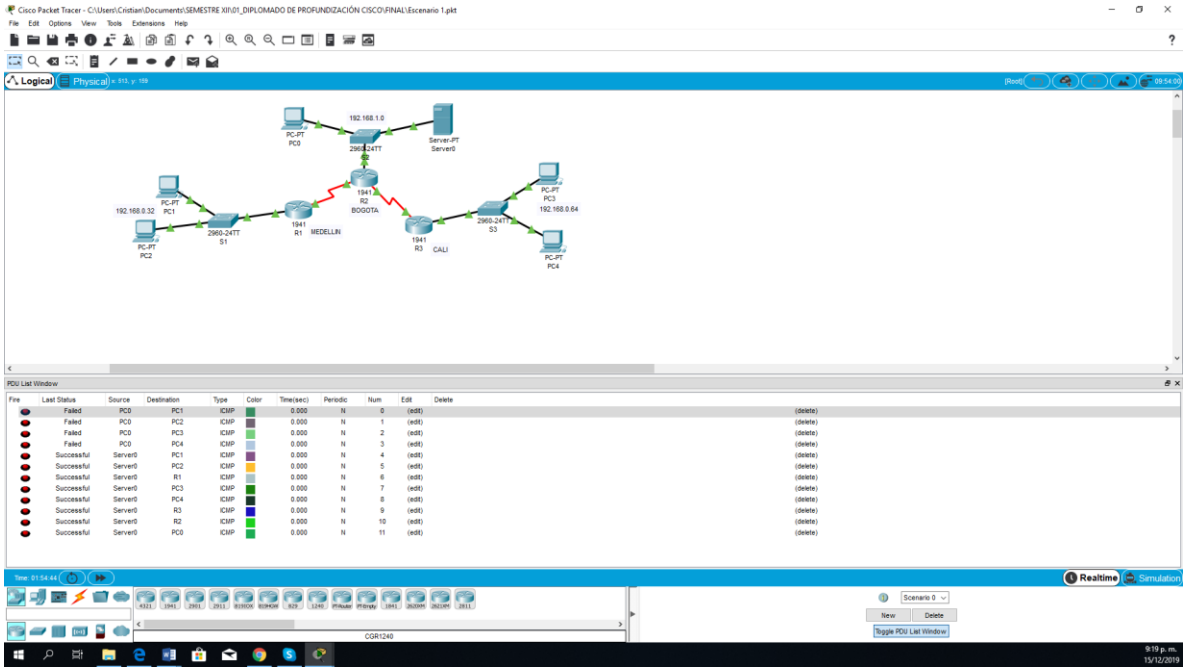


Figura 28 Verificación ACL "A"

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

Vlan Medellín no tiene salía fuera de su red excepto al servidor

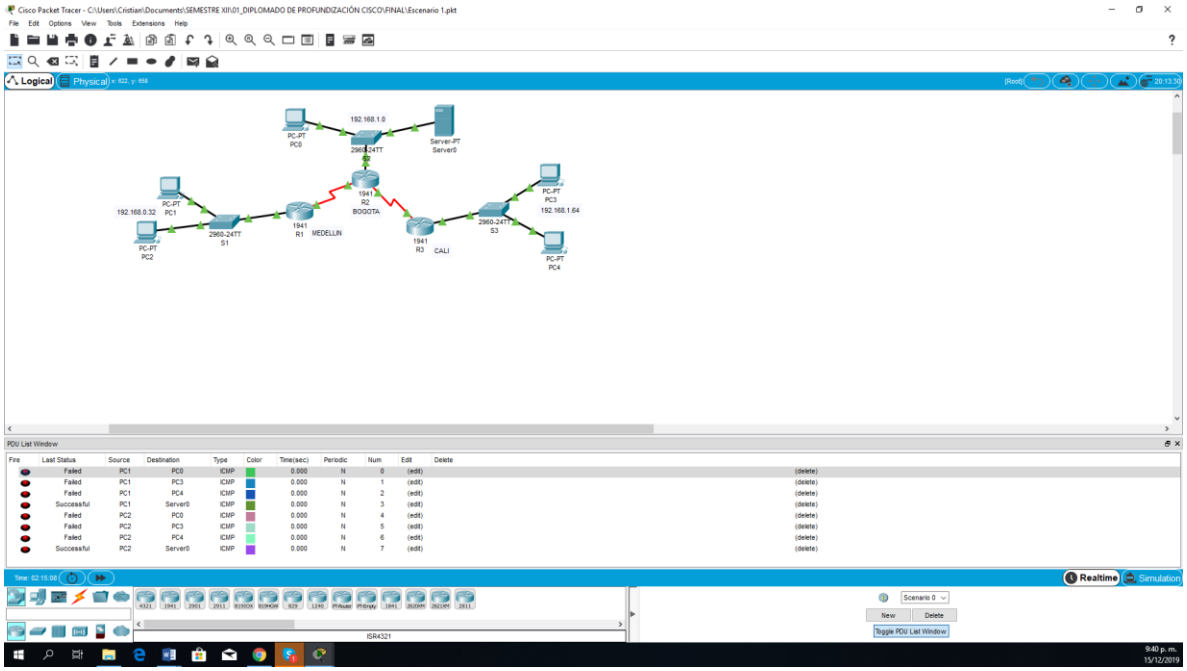


Figura 29 Verificación ACL "B"

Vlan Cali no tiene salía fuera de su red excepto al servidor

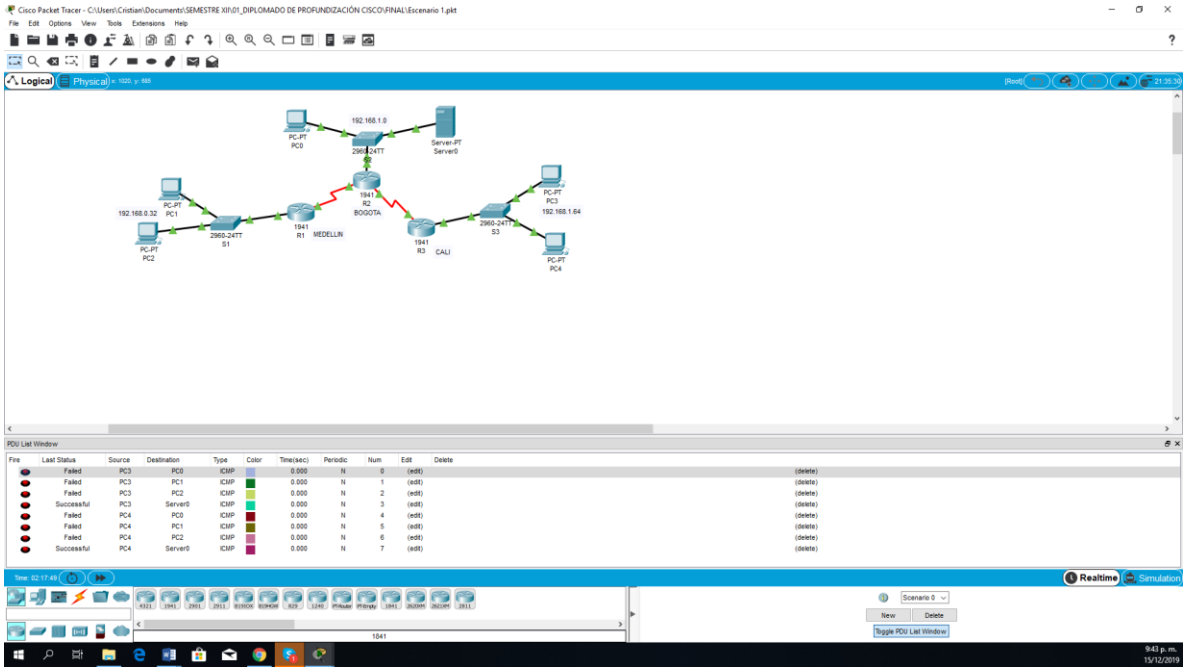


Figura 30 Verificación Vlan Cali no tiene salía fuera de su red excepto al Servidor

6.1.3.5 Parte 5: Comprobación de la red instalada.

c. Se debe probar que la configuración de las listas de acceso fue exitosa.
d. 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**	exitoso
	WS_1	**Router BOGOTA**	Fallido
	Servidor	**Router CALI**	exitoso
	Servidor	**Router MEDELLIN**	exitoso
TELNET	**LAN del Router MEDELLIN**	**Router CALI**	exitoso
	LAN del Router CALI	**Router CALI**	exitoso
	LAN del Router MEDELLIN	**Router MEDELLIN**	exitoso
	LAN del Router CALI	**Router MEDELLIN**	Exitoso
PING	**LAN del Router CALI**	**WS_1**	fallido
	LAN del Router MEDELLIN	**WS_1**	fallido
	LAN del Router MEDELLIN	**LAN del Router CALI**	fallido
PING	**LAN del Router CALI**	**Servidor**	Exitoso
	LAN del Router MEDELLIN	**Servidor**	Exitoso
	Servidor	**LAN del Router MEDELLIN**	Exitoso
	Servidor	**LAN del Router CALI**	Exitoso
	Router CALI	**LAN del Router MEDELLIN**	Exitoso
	Router MEDELLIN	**LAN del Router CALI**	Exitoso

Tabla 8 Verificación lista de accesos

Router MEDELLIN	Router CALI	**exitoso**

Tabla 9 Verificación router Medellín - Cali

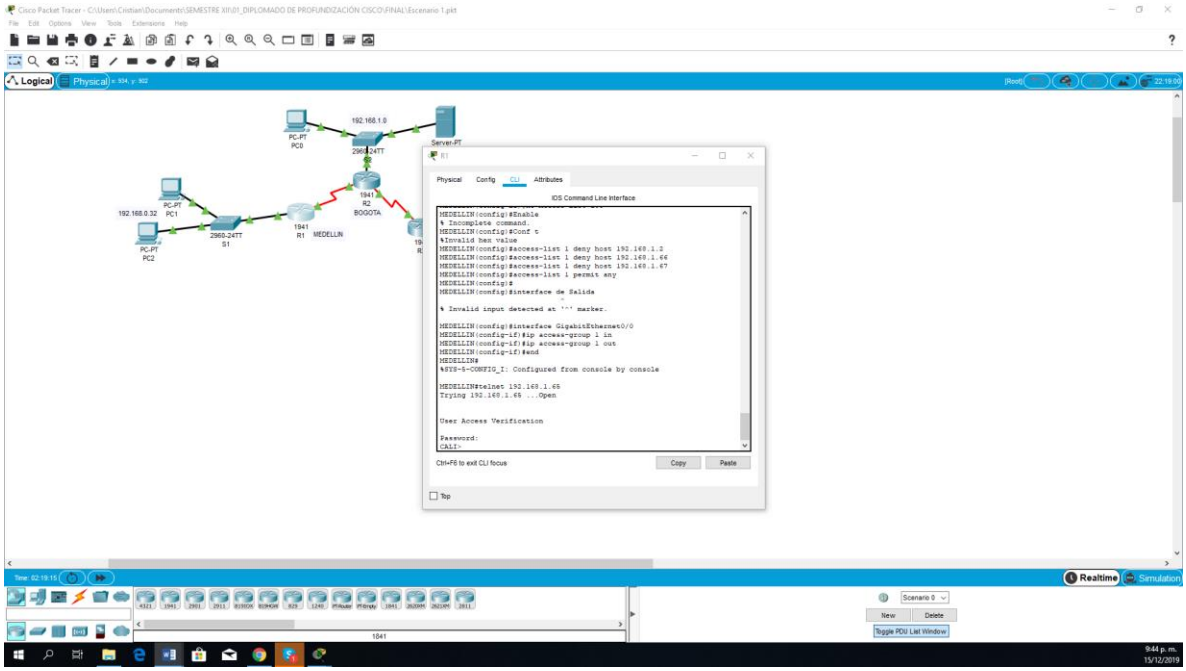


Figura 31 Verificación router Medellín – Cali

WS_1	Router BOGOTA	**Fallido**

Tabla 10 Verificación WS_1 router Bogotá

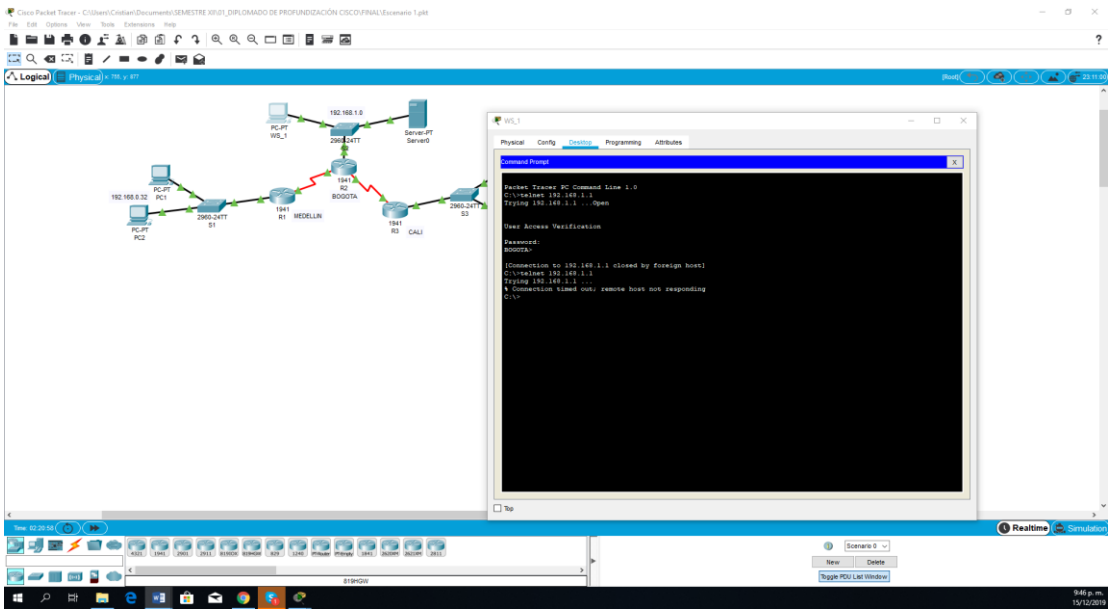


Figura 32 Verificación WS_1 router Bogotá

Servidor	Router CALI	**exitoso**

Tabla 11 Verificación Servidor router Cali

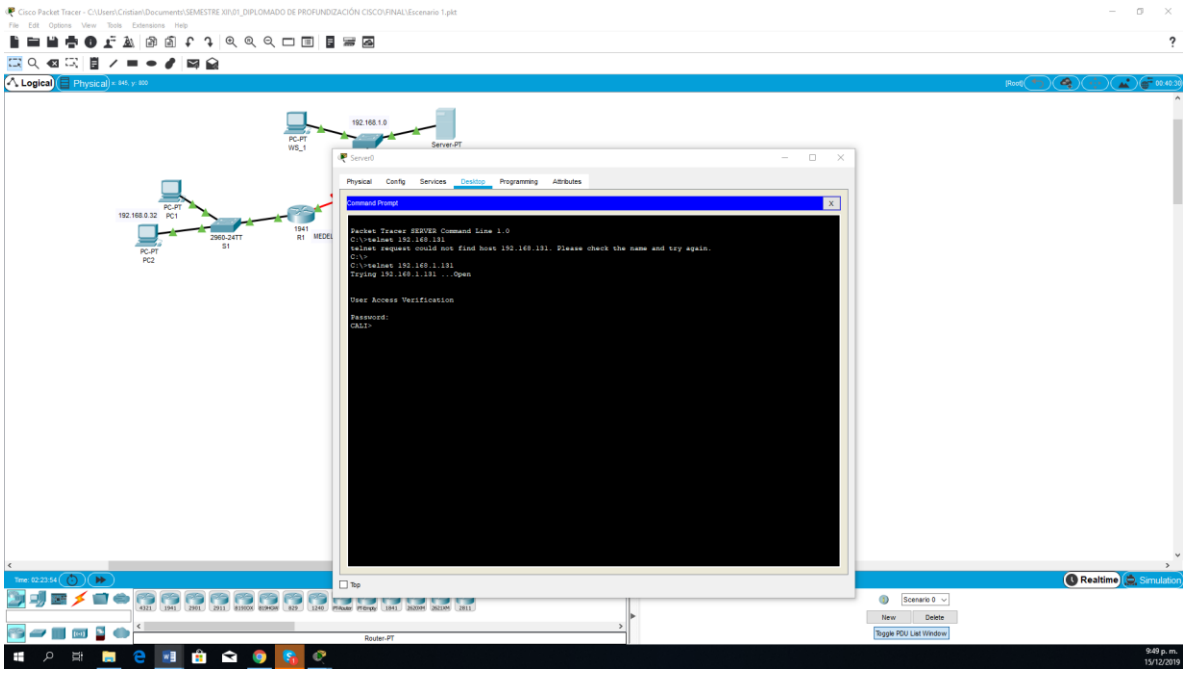


Figura 33 Verificación Servidor router Cali

Servidor	Router MEDELLIN	**exitoso**

Tabla 12 Verificación Servidor router Medellín

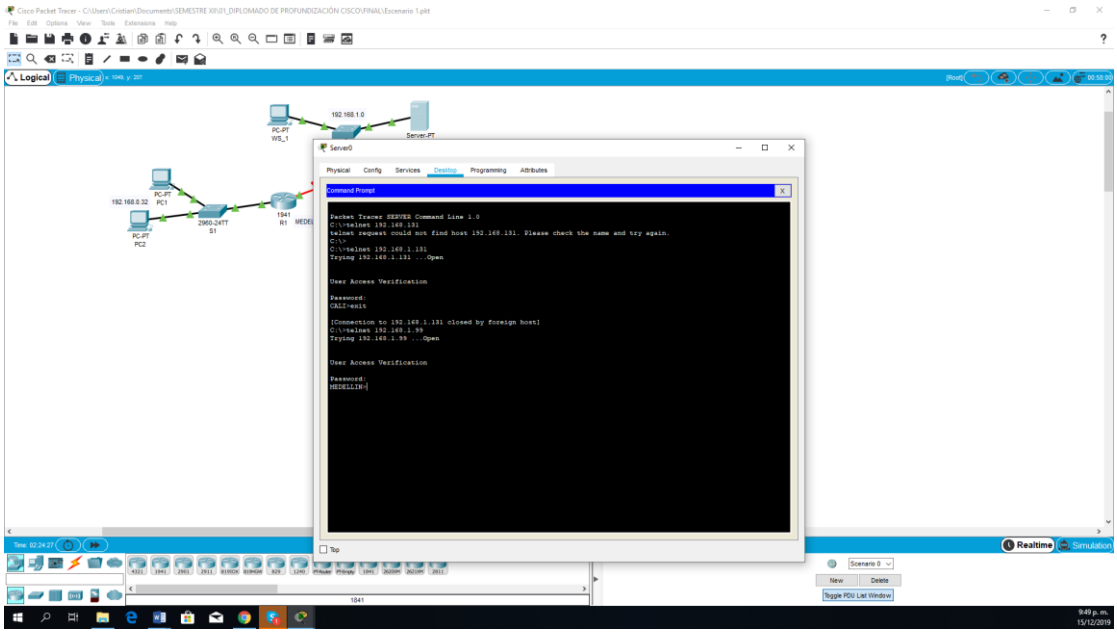


Figura 34 Verificación Servidor router Medellín

LAN del Router CALI	Router CALI	**exitoso**

Tabla 13 Verificación LAN router Cali router Medellín

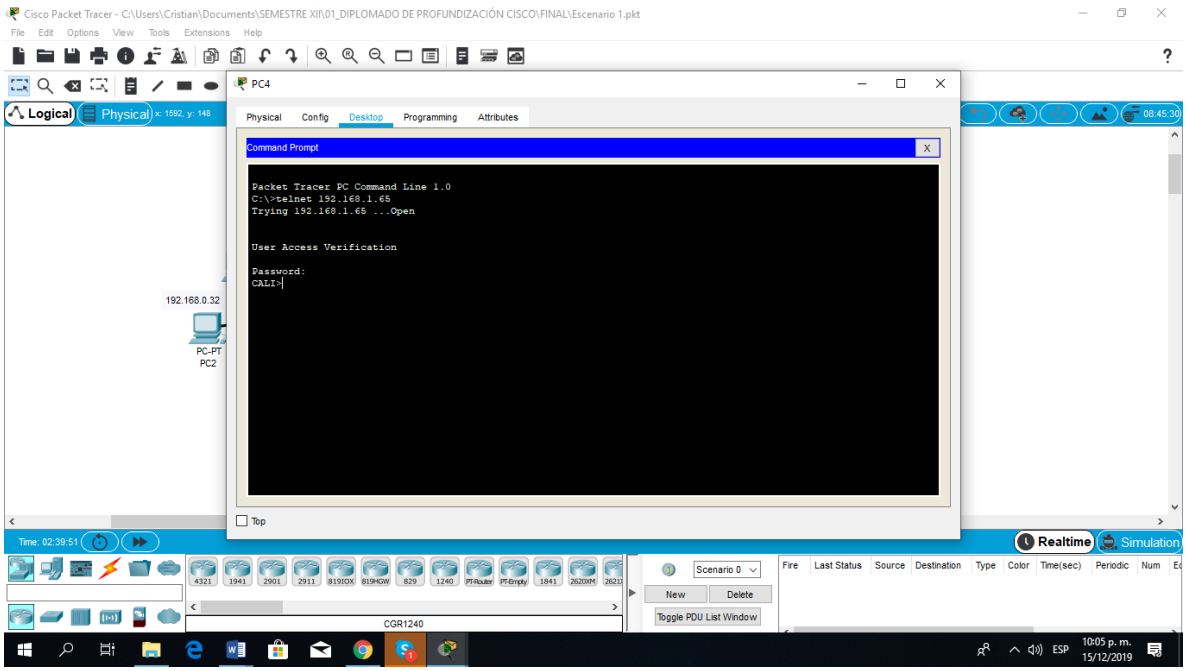


Figura 35 Verificación LAN router Cali router Medellín

LAN del Router MEDELLIN	Router MEDELLIN	**exitoso**

Tabla 14 Verificación LAN router Medellín router Medellín

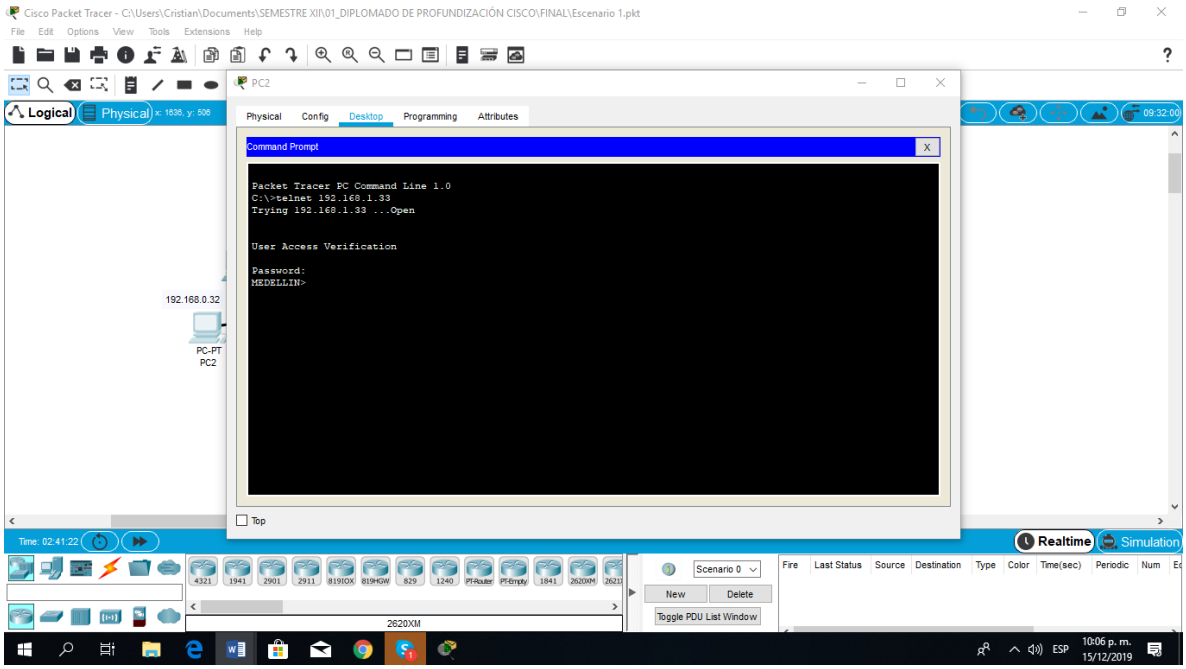


Figura 36 Verificación LAN router Medellín router Medellín

LAN del Router CALI	Router MEDELLIN	**Exitoso**

Tabla 15 Verificación LAN router Cali router Medellín

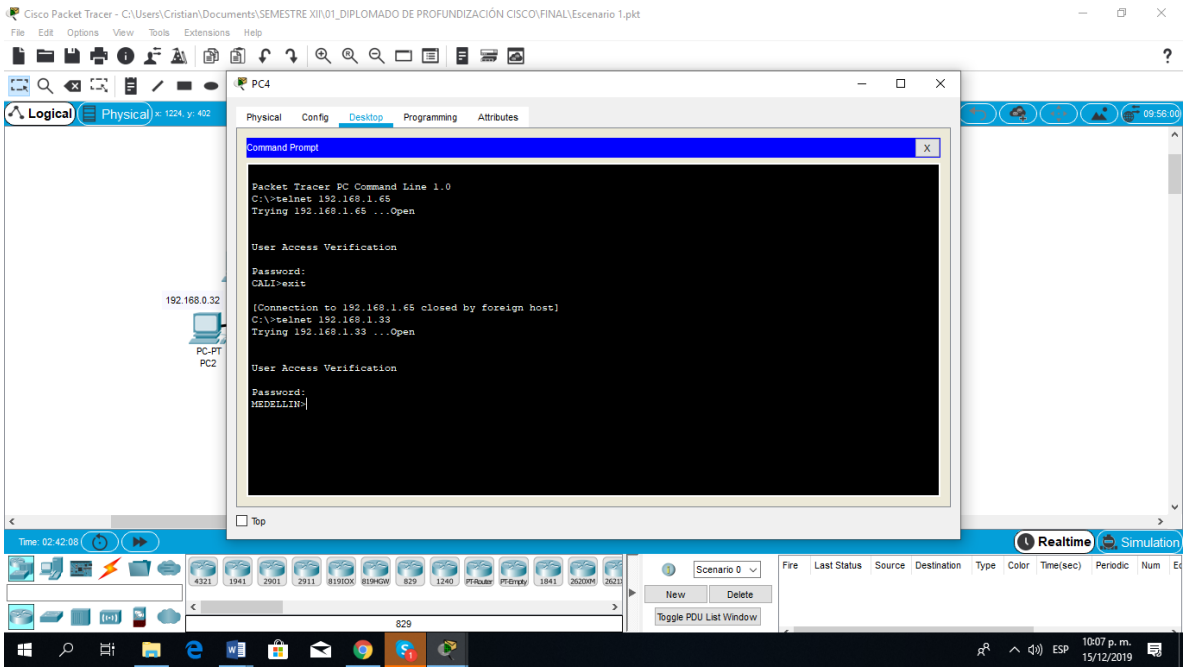


Figura 37 Verificación LAN router Cali router Medellín

LAN del Router CALI	WS_1	**fallido**

Tabla 16 Verificación LAN router Cali WS_1

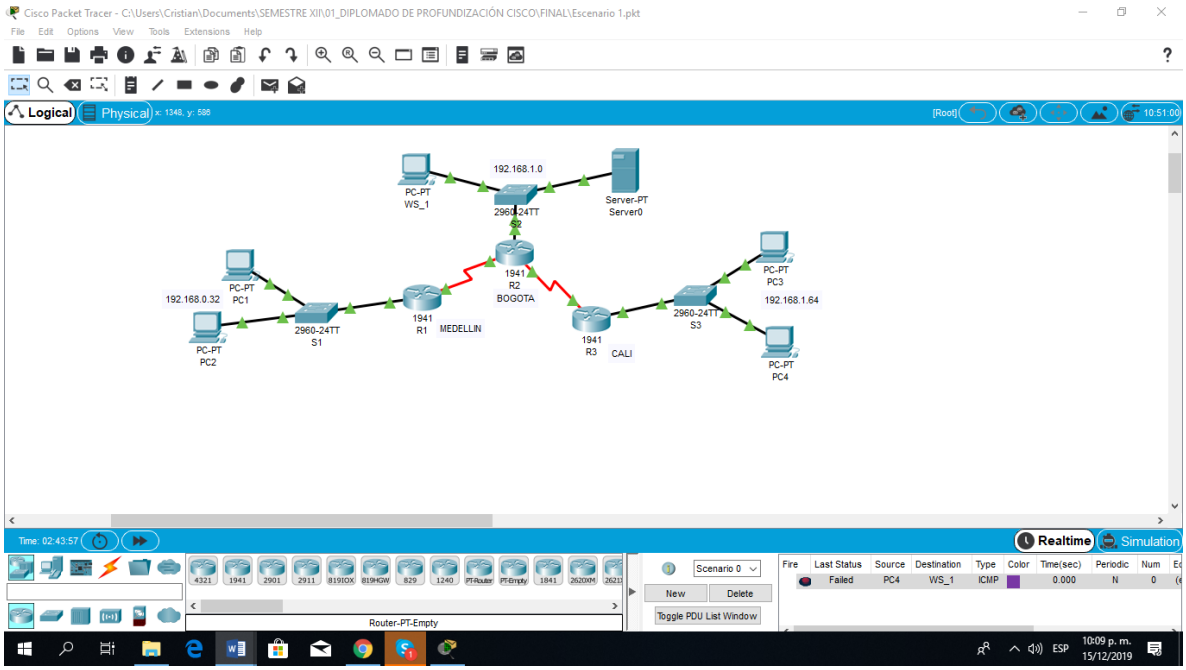


Figura 38 Verificación LAN router Cali WS_1

LAN del Router MEDELLIN	WS_1	**fallido**

Tabla 17 Verificación LAN router Medellín WS_1

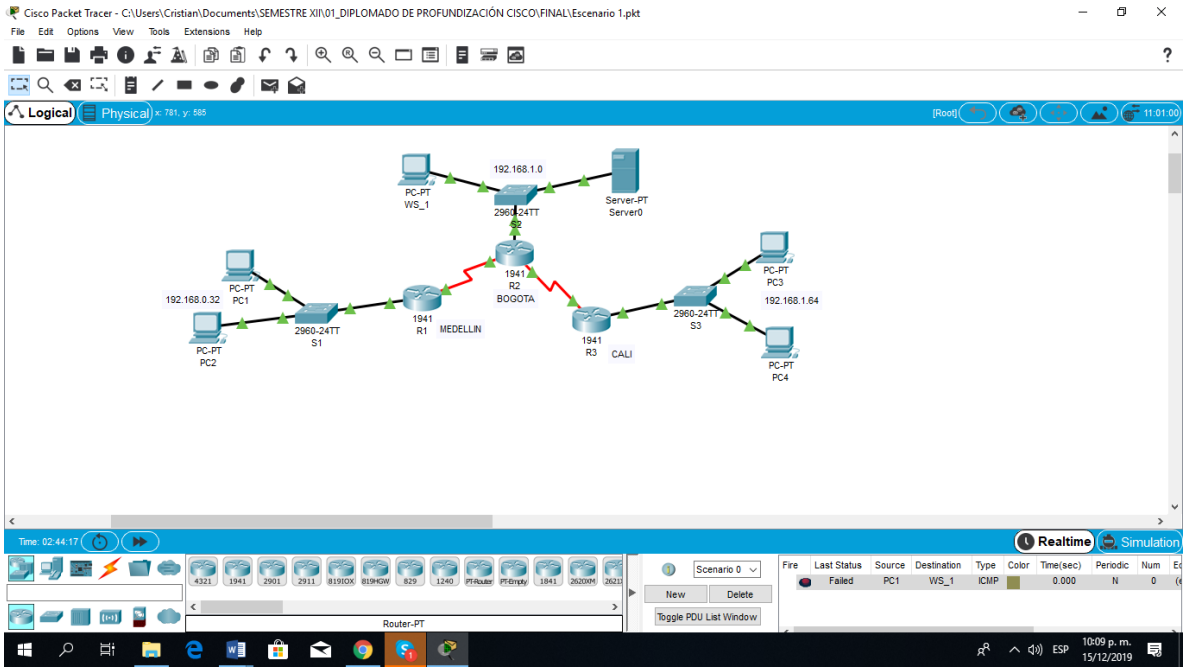


Figura 39 Verificación LAN router Medellín WS_1

LAN del Router MEDELLIN	LAN del Router CALI	**fallido**

Tabla 18 Verificación LAN router Medellín LAN router Cali

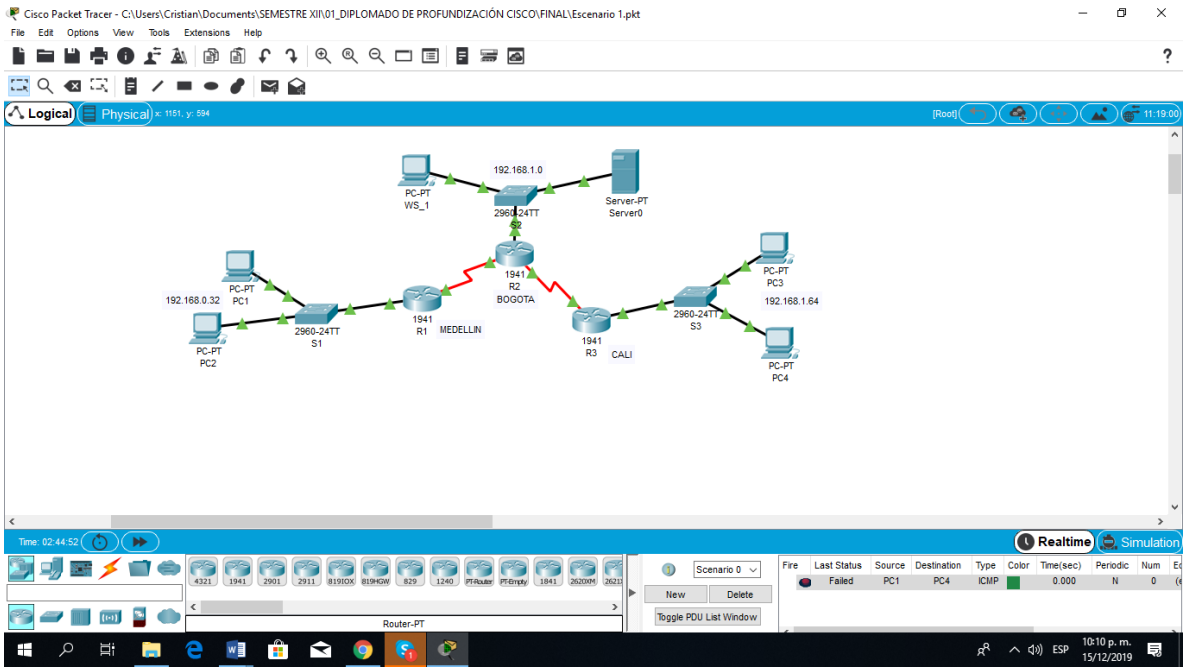


Figura 40 Verificación LAN router Medellín LAN router Cali

LAN del Router CALI	Servidor	**Exitoso**

Tabla 19 Verificación LAN router Cali Servidor

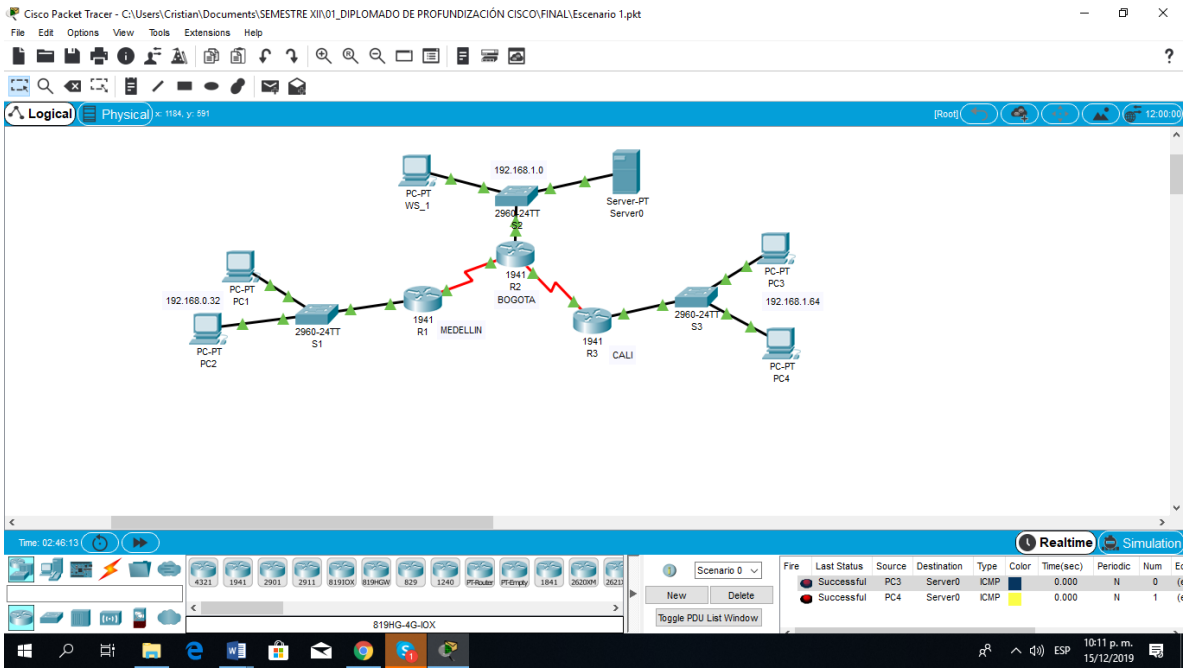


Figura 41 Verificación LAN router Cali Servidor

LAN del Router MEDELLIN	Servidor	**Exitoso**

Tabla 20 Verificación LAN router Medellín Servidor

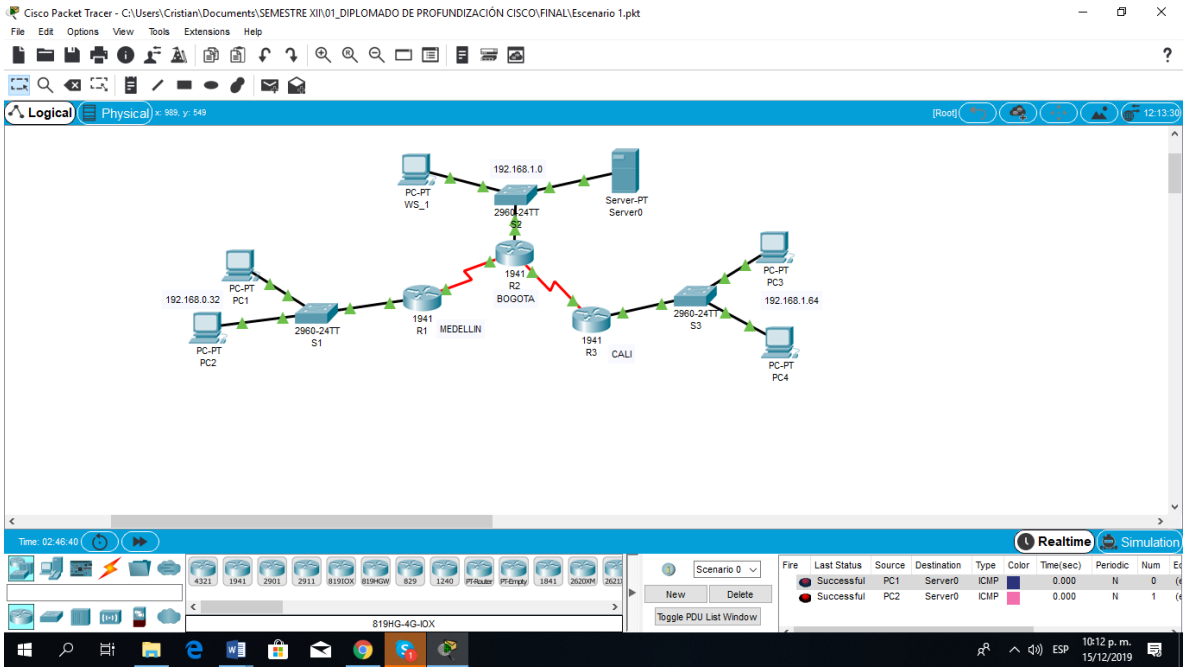


Figura 42 Verificación LAN router Medellín Servidor

Servidor	LAN del Router MEDELLIN	**Exitoso**

Tabla 21 Verificación Servidor LAN router Medellín

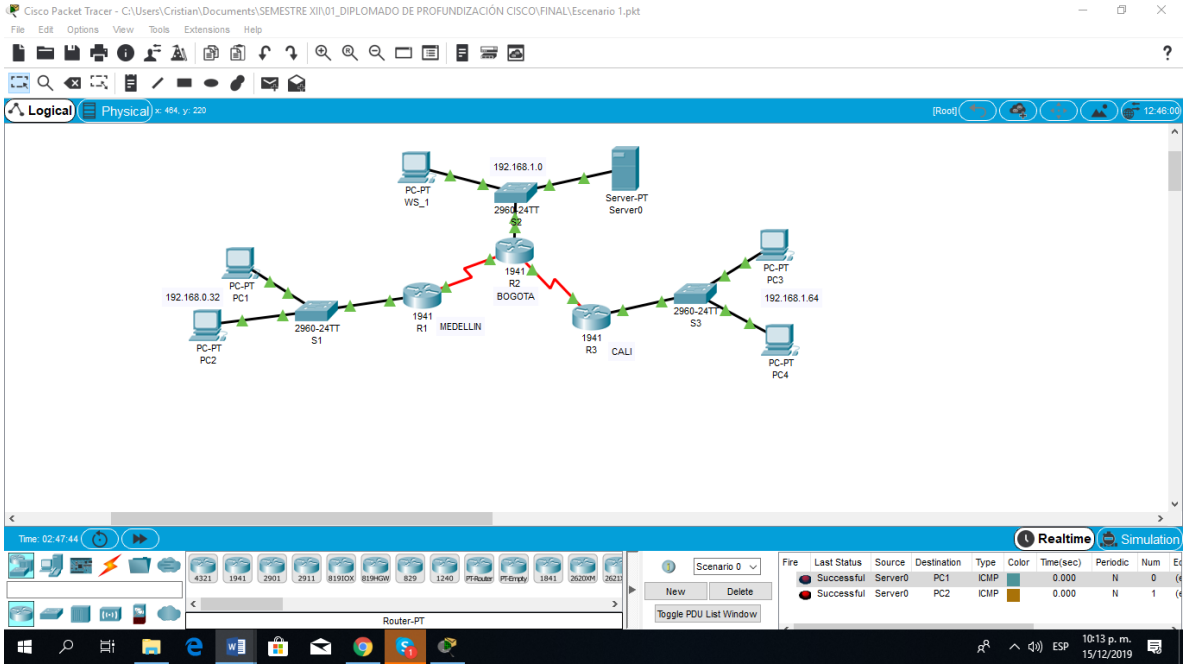


Figura 43 Verificación Servidor LAN router Medellín

Servidor	LAN del Router CALI	**Exitoso**

Tabla 22 Verificación Servidor LAN router Cali

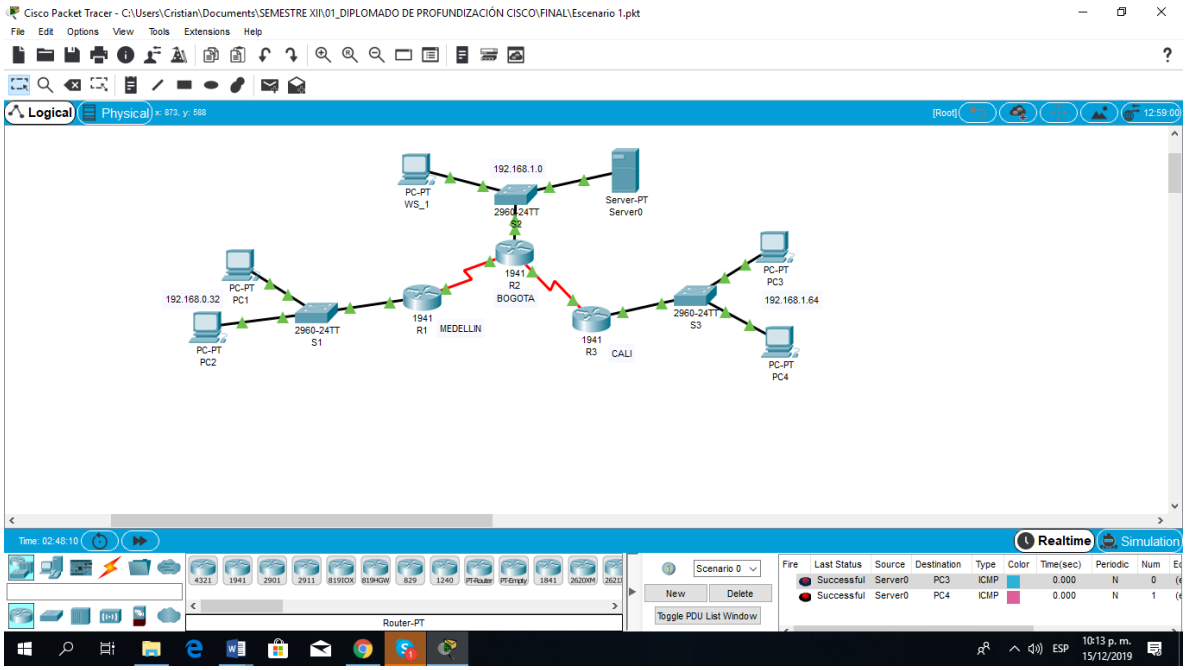


Figura 44 Verificación Servidor LAN router Cali

Router CALI	LAN del Router MEDELLIN	**Exitoso**

Tabla 23 Verificación router Cali LAN router Medellín

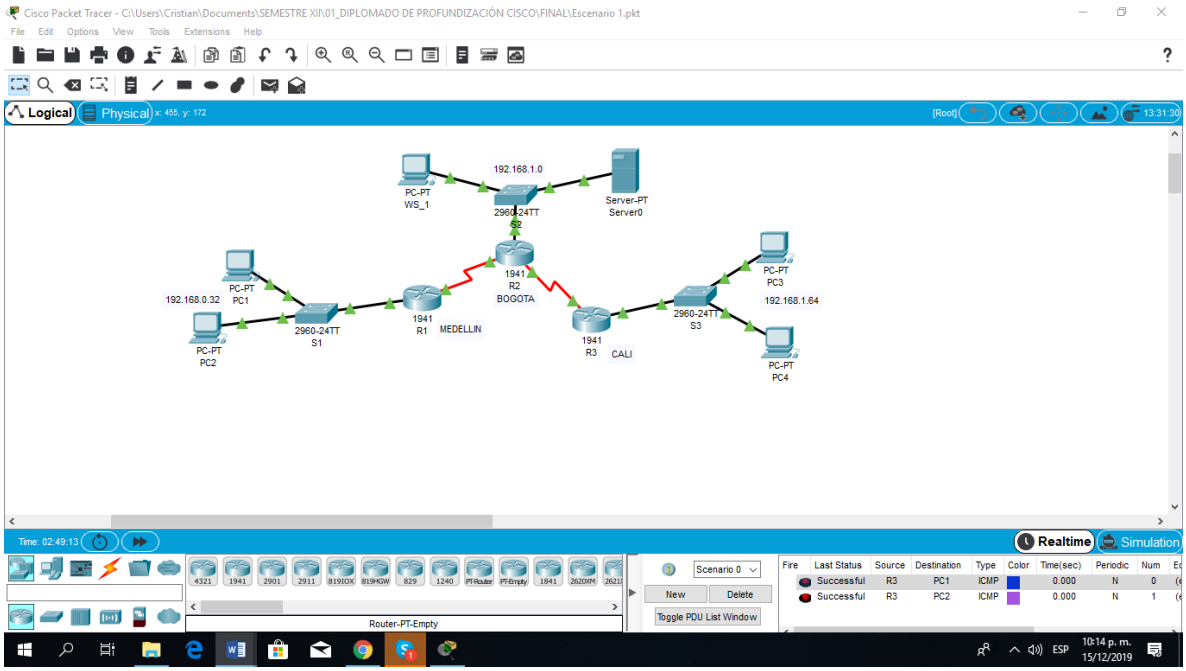


Figura 45 Verificación router Cali LAN router Medellín

Router MEDELLIN	LAN del Router CALI	**Exitoso**

Tabla 24 Verificación router Medellín LAN router Cali

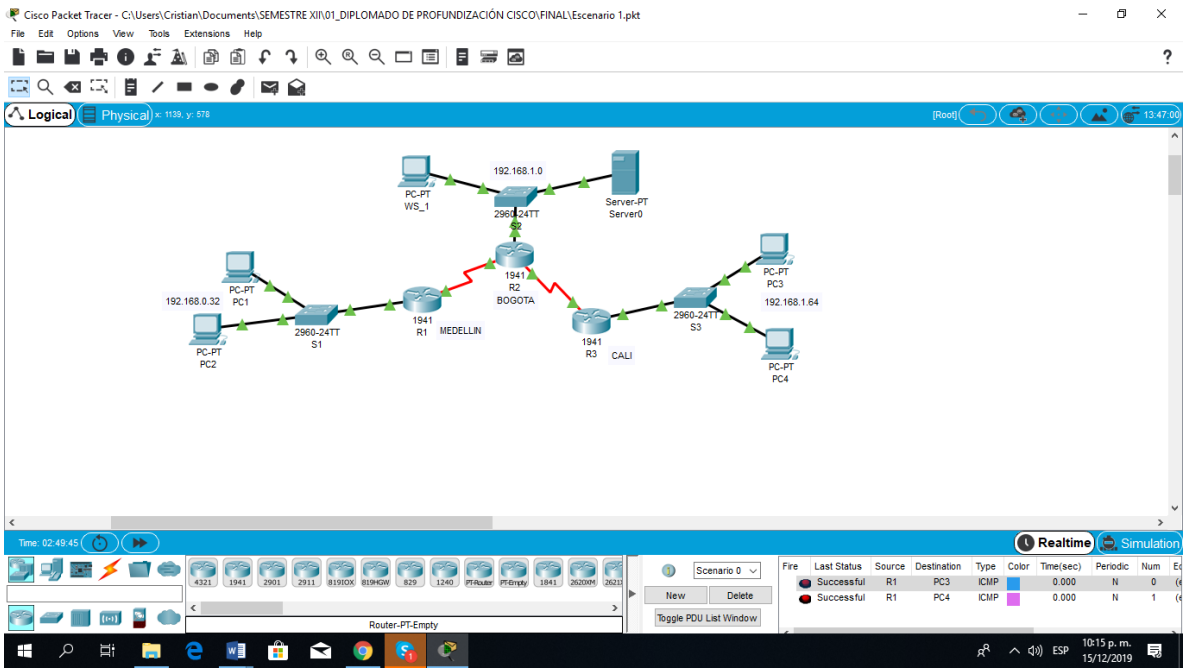


Figura 46 Verificación router Medellín LAN router Cali

6.1.4 CONFIGURACIÓN UTILIZADA

6.1.4.1 Router (Medellín)

Configuramos las interfaces de router, colocando el direccionamiento de forma inmediata

configure terminal

enable secret cisco

line consol 0

password cisco

login

exit

Hostname MEDELLIN

Interface GigabitEthernet 0/0

Ip address 192.168.1.33 255.255.255.224

No shut

Duplex Auto

Speed auto

Interface serial 0/0/0

Ip address 192.168.1.99 255.255.255.224

No shut

Configuramos eigrp como protocolo de enrutamiento

Router eigrp 11

Network 192.168.1.96 0.0.0.31

Network 192.168.1.32 0.0.0.31

No auto-summary

Habilitamos el telnet

Enable

Conf t

Line vty 0 4

Password cisco

Login

Enable secret cisco

exit

configuramos las ACL asi

Enable
Conf t
access-list 1 deny host 192.168.1.2
access-list 1 deny host 192.168.1.66
access-list 1 deny host 192.168.1.67
access-list 1 permit any

interface GigabitEthernet0/0
ip access-group 1 in
ip access-group 1 out

6.1.4.2 Router Bogota

Configuramos las interfaces de router, colocando el direccionamiento de forma inmediata

configure terminal

enable secret cisco

line consol 0

password cisco

login

exit

Hostname BOGOTA

Interface GigabitEthernet 0/0

Ip address 192.168.1.1 255.255.255.224

No shut

Duplex Auto

Speed auto

Interface serial 0/0/0

Ip address 192.168.1.98 255.255.255.224

Clock rate 6400

No shut

Interface serial 0/0/1

Ip address 192.168.1.130 255.255.255.224

Clock rate 6400

No shut

Configuramos eigrp como protocolo de enrutamiento

Router eigrp 11

Network 192.168.1.96 0.0.0.31

Network 192.168.1.128 0.0.0.31

Network 192.168.1.0 0.0.0.31

No auto-summary

Habilitamos el telnet

Enable

Conf t

Line vty 0 4

Password cisco

Login

Enable secret cisco

exit

configuramos las listas de control de acceso

Enable
Conf t
access-list 1 deny host 192.168.1.2
access-list 1 permit host 192.168.1.3

access-list 1 permit any

interface de Salida
interface GigabitEthernet0/0
ip access-group 1 in

6.1.4.3 Router CALI

Configuramos las interfaces de router, colocando el direccionamiento de forma inmediata

configure terminal

enable secret cisco

line consol 0

password cisco

login

exit

Hostname CALI

Interface GigabitEthernet 0/0

Ip address 192.168.1.65 255.255.255.224

No shut

Duplex Auto

Speed auto

Interface serial 0/0/0

Ip address 192.168.1.131 255.255.255.224

Clock rate 6400

No shut

Configuramos eigrp como protocolo de enrutamiento

Router eigrp 11

Network 192.168.1.128 0.0.0.31

Network 192.168.1.64 0.0.0.31

No auto-summary

Habilitamos el telnet

Enable

Conf t

Line vty 0 4

Password cisco

Login

Enable secret cisco

exit

Configuramos las acls asi:

Enable
Conf t
access-list 1 deny host 192.168.1.2
access-list 1 deny host 192.168.1.34
access-list 1 deny host 192.168.1.35
access-list 1 permit any

interface g0/0
ip access-group 1 in
ip access-group 1 out

6.2 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.

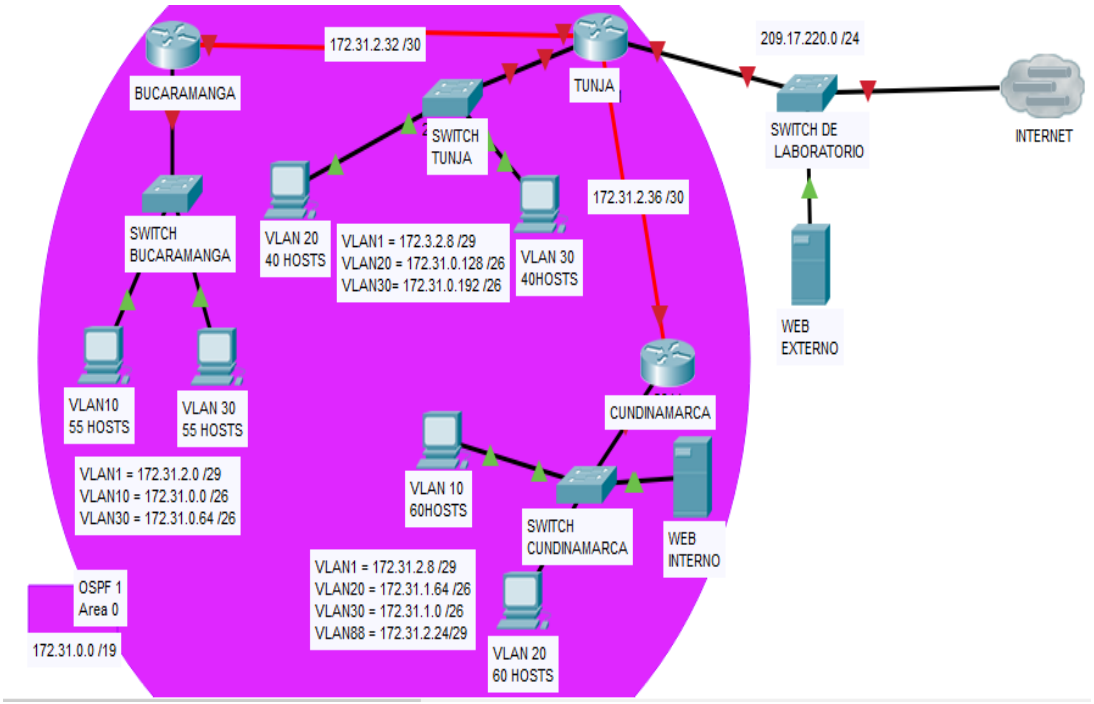


Figura 47 Esquema De la Red Escenario 2

6.2.1 Desarrollo de la actividad

Los siguientes son los requerimientos necesarios:

6.2.1.1 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.

Router Cundinamarca

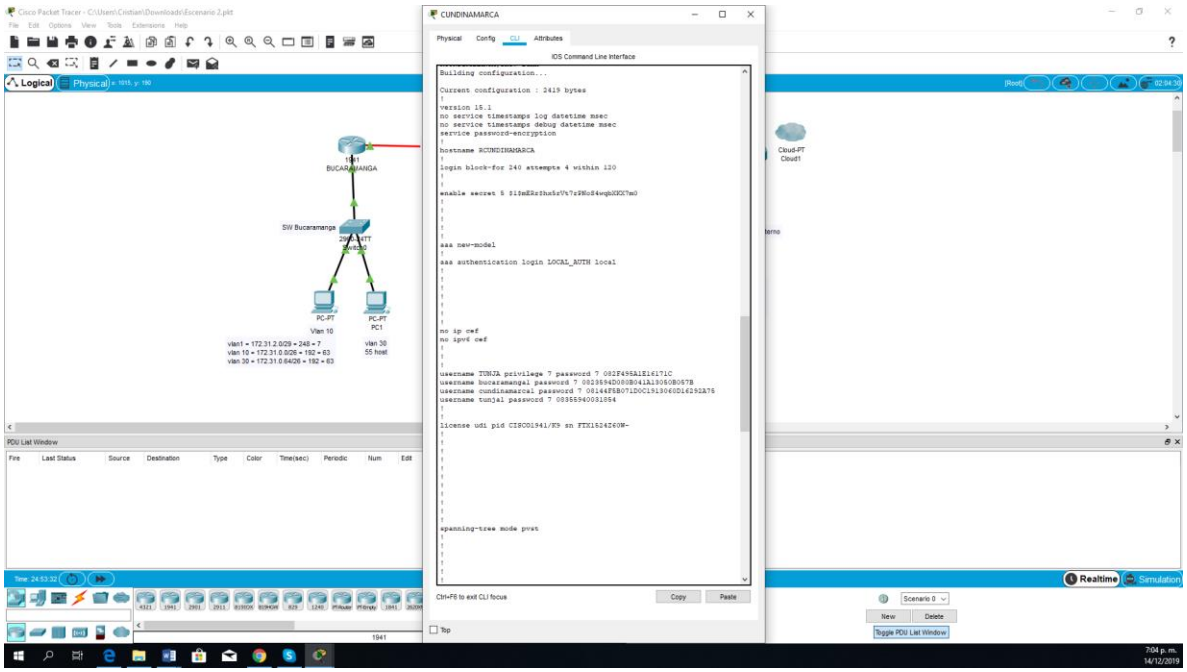


Figura 48 Configuración básica Router Cundinamarca

Router Tunja

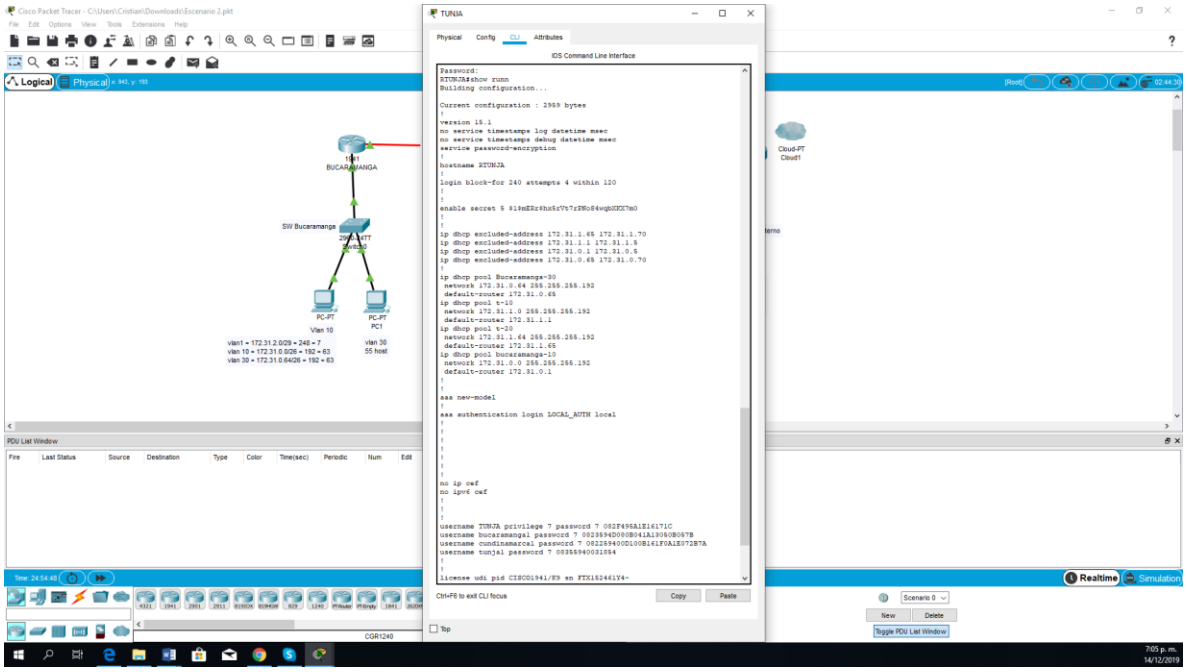


Figura 49 Configuración básica Router Tunja

Router Bucaramanga

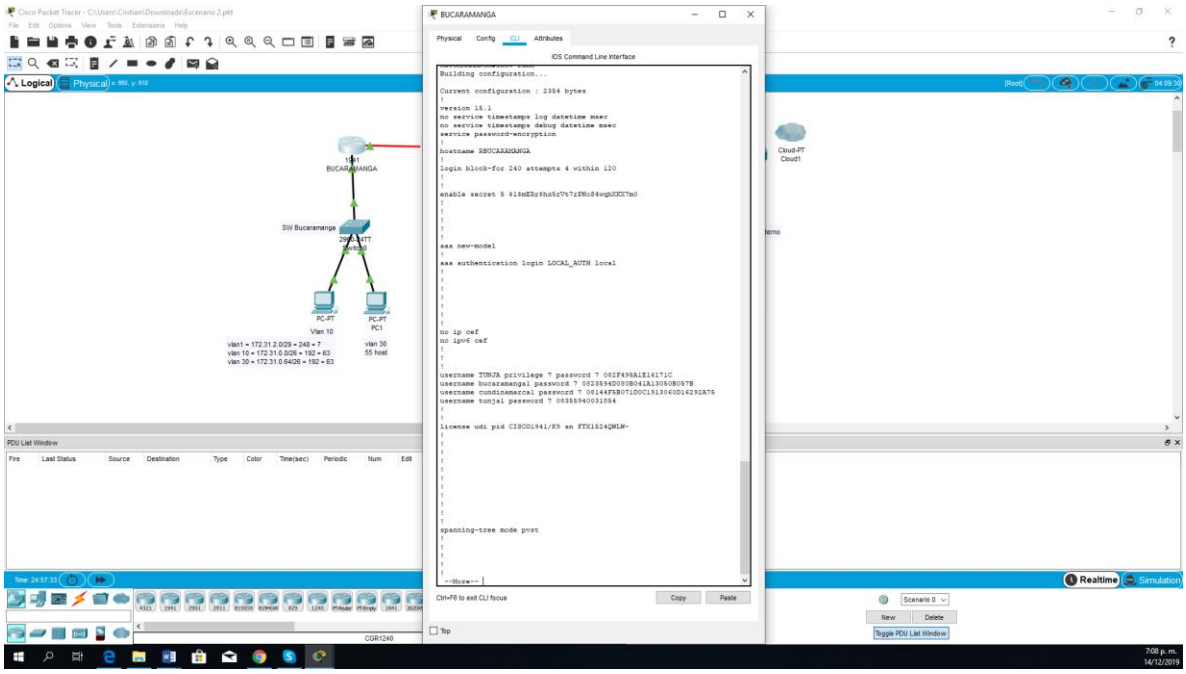


Figura 50 Configuración básica Router Bucaramanga

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

Router Bucaramanga

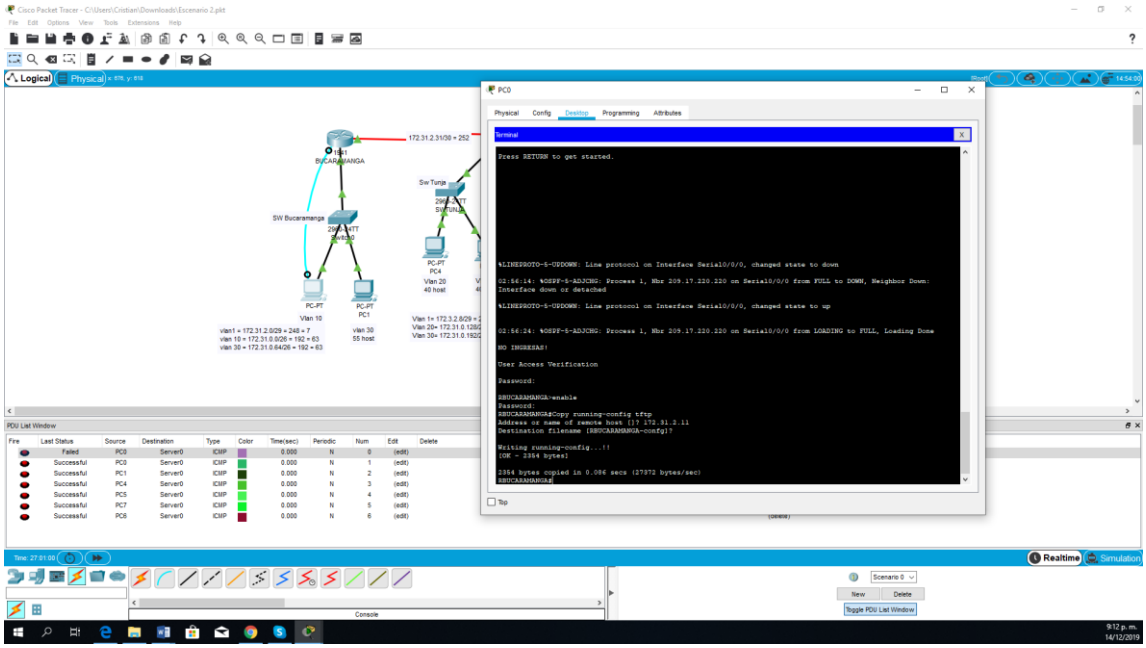


Figura 51 Servidor TFTP router Bucaramanga

Router Tunja

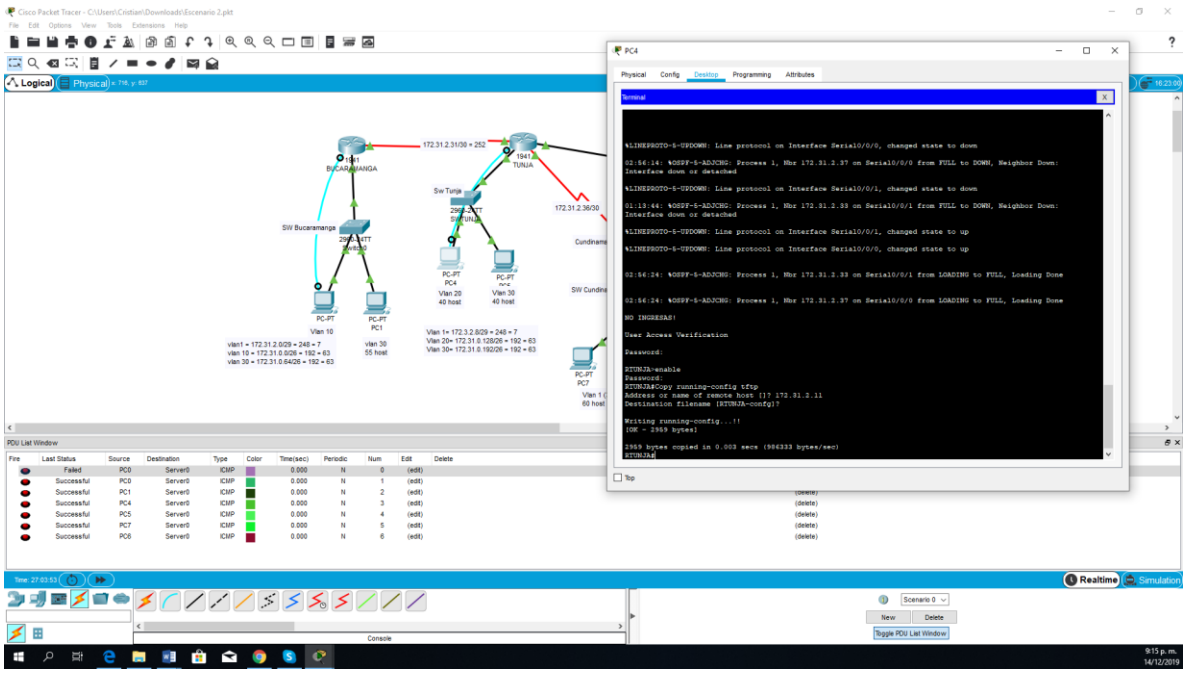


Figura 52 Servidor TFTP router Tunja

Router Cundinamarca

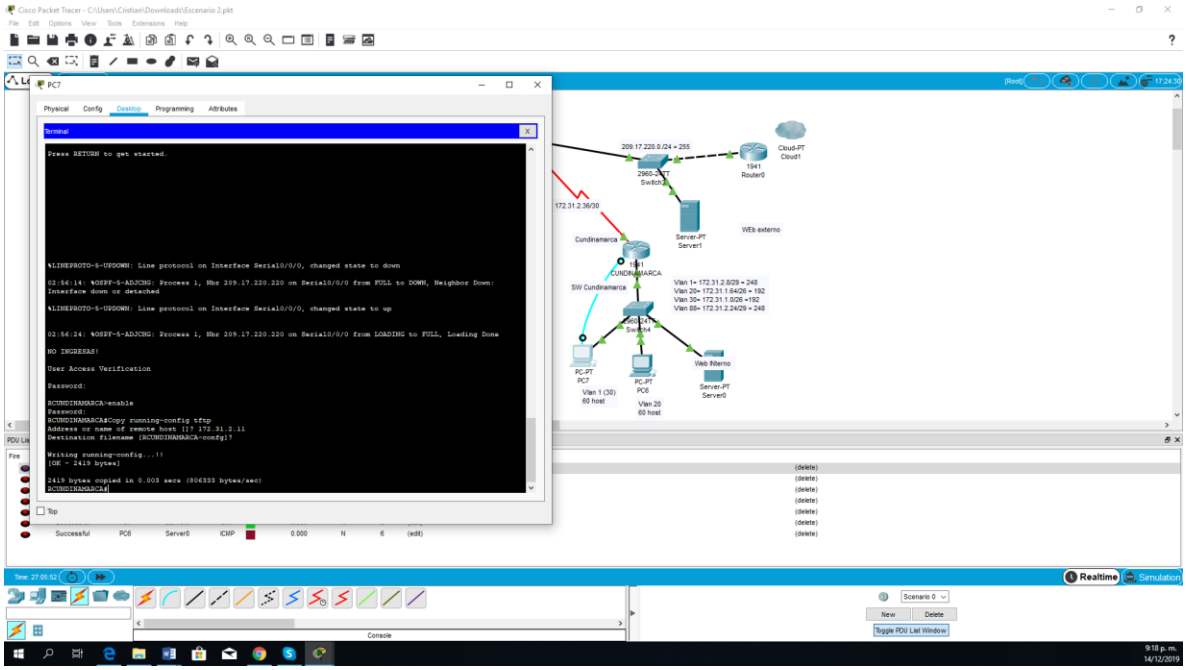


Figura 53 Servidor TFTP router Cundinamarca

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

Configuración router Tunja

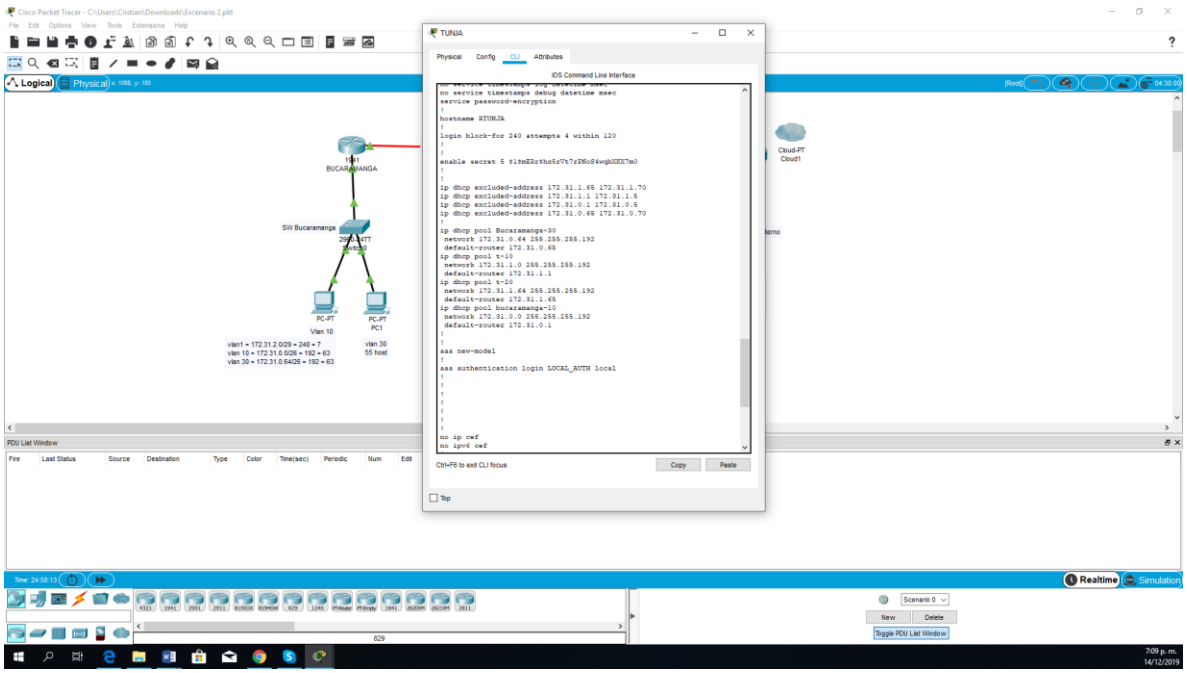


Figura 54 DHCP Router Tunja

Computadores red de Bucaramanga

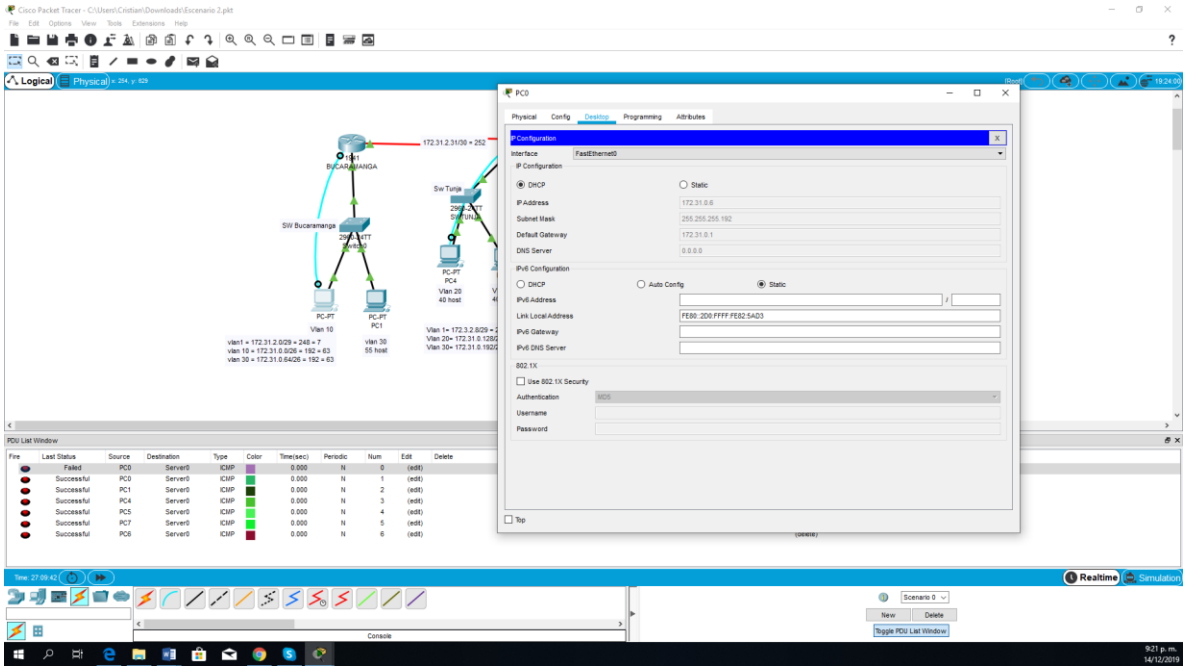


Figura 55 DHCP red LAN Bucaramanga

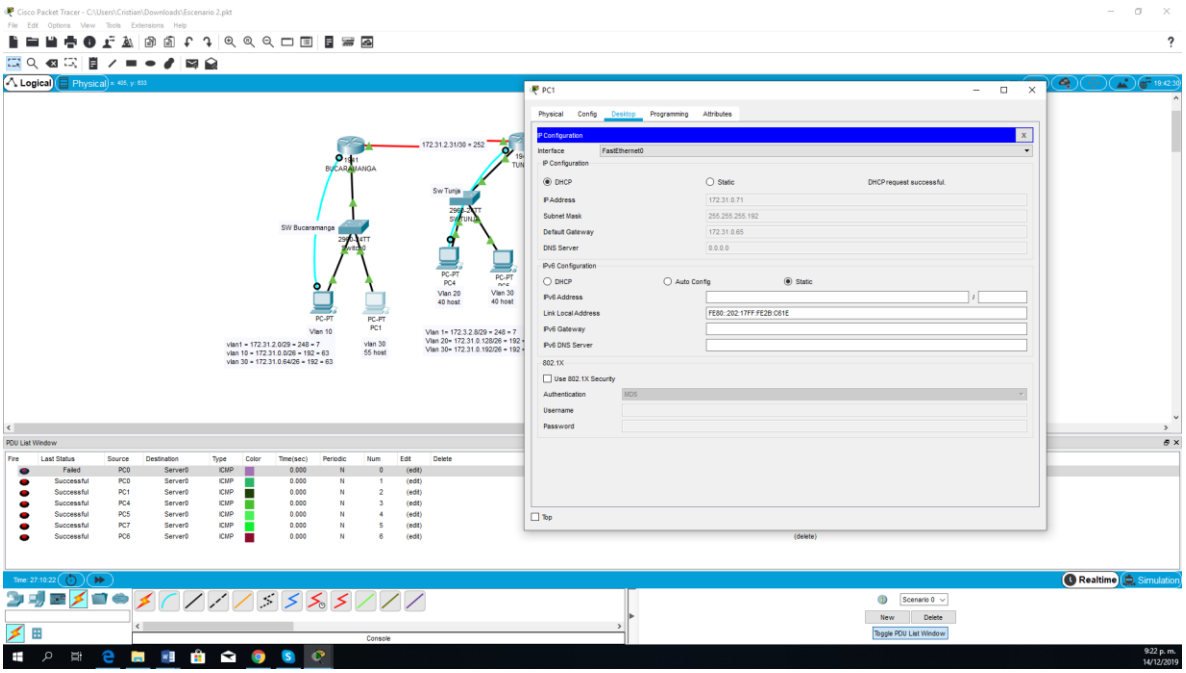


Figura 56 DHCP red LAN Bucaramanga

Computadores red de Cundinamarca

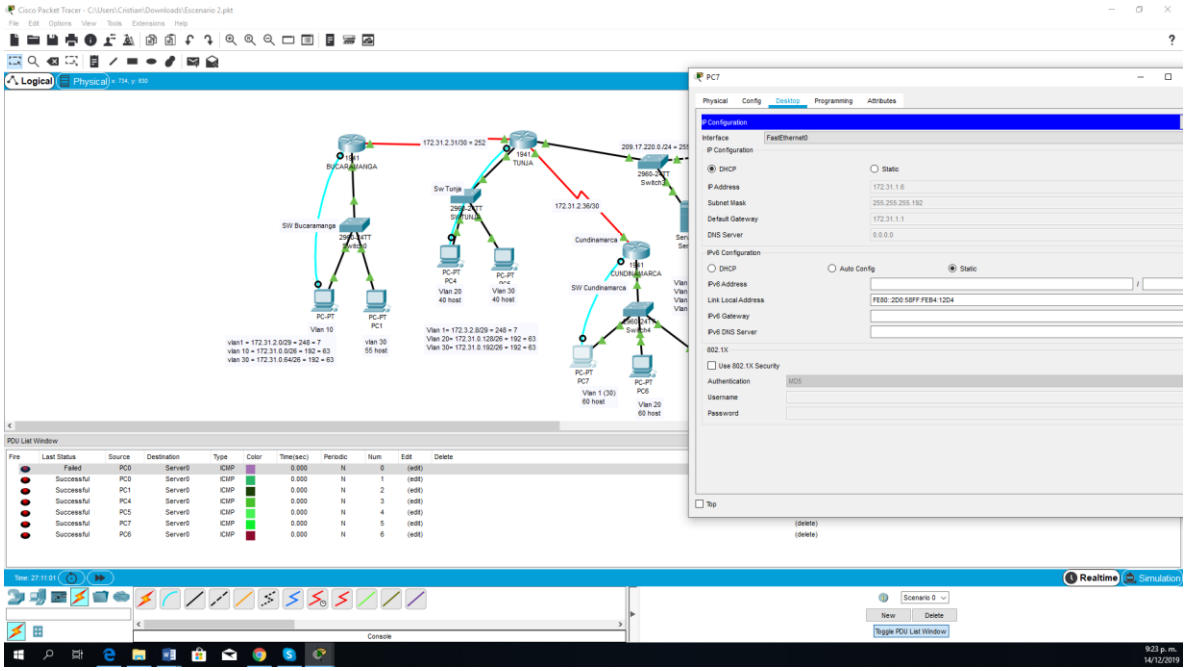


Figura 57 DHCP red LAN Cundinamarca

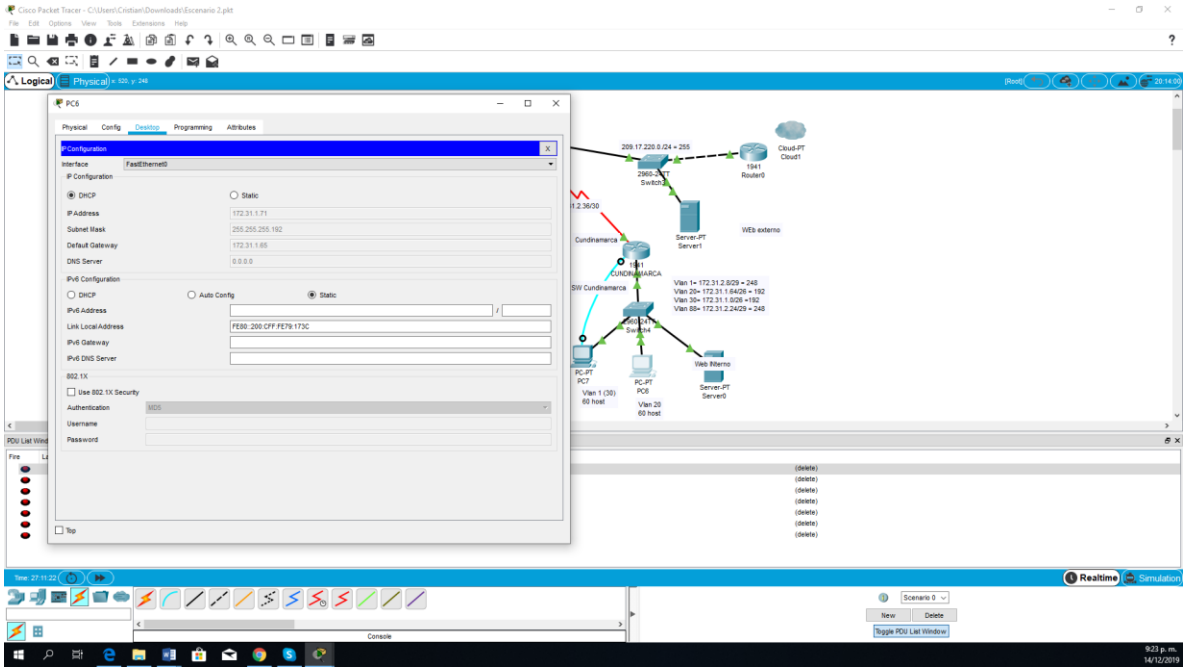


Figura 58 DHCP red LAN Cundinamarca

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

Nat estatico

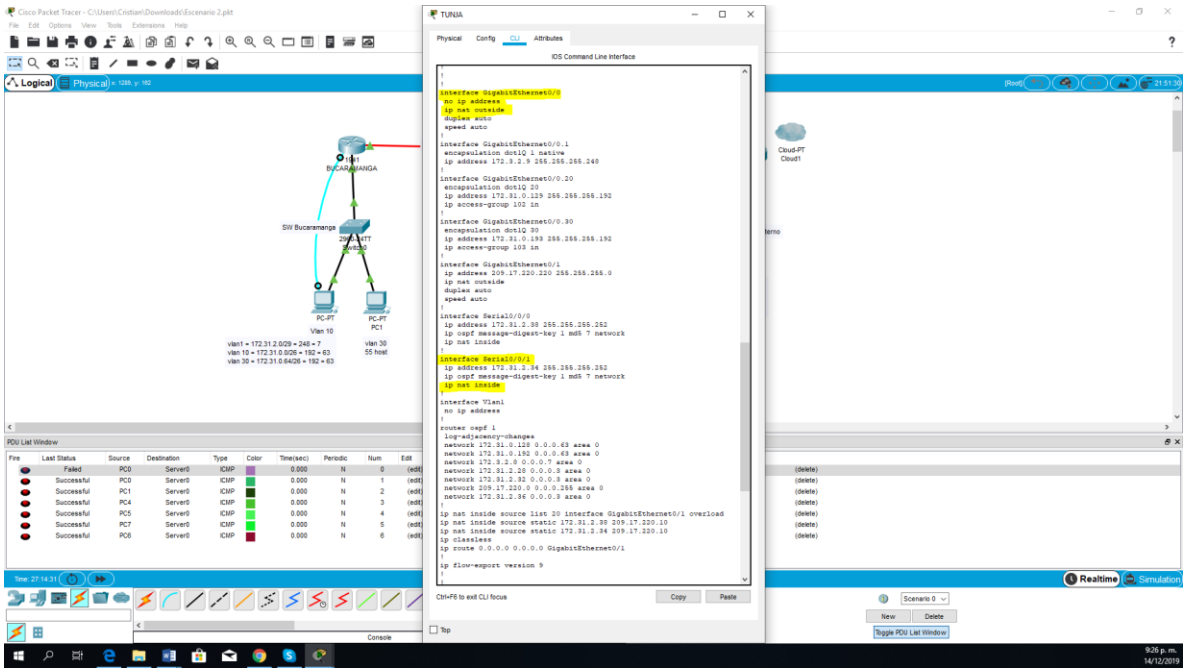


Figura 59 NAT estatico Router Tunja

De sobrecarga (PAT).

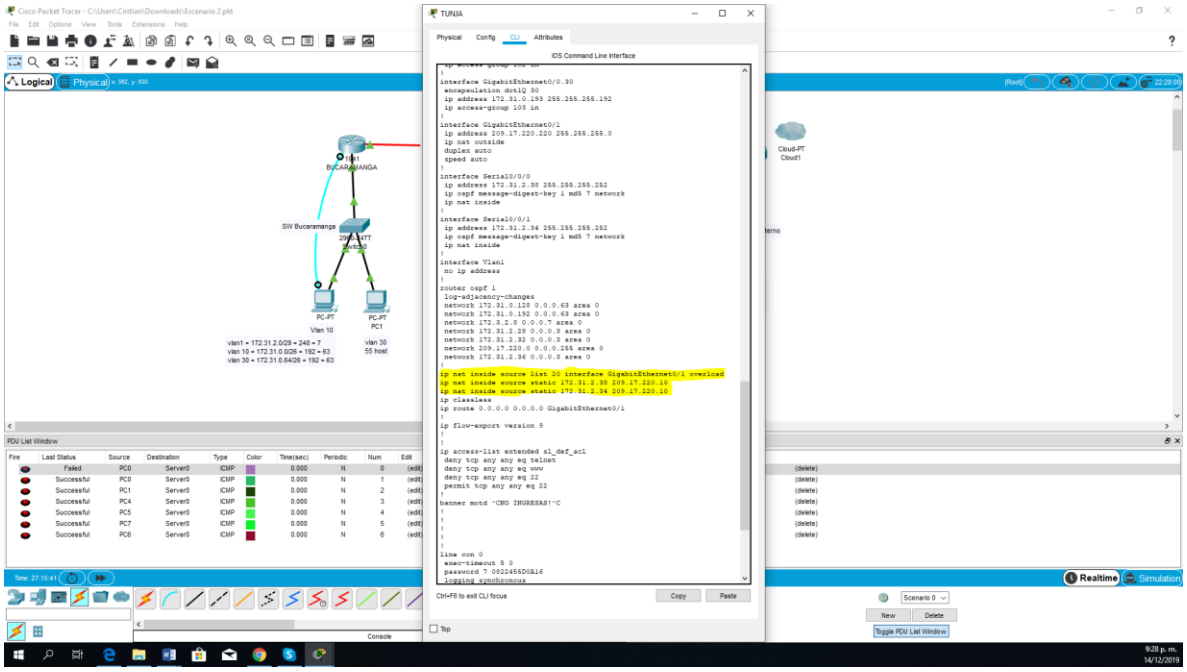


Figura 60 PAT router Tunja

6.2.1.5 El enrutamiento deberá tener autenticación.

Router Bucaramanga

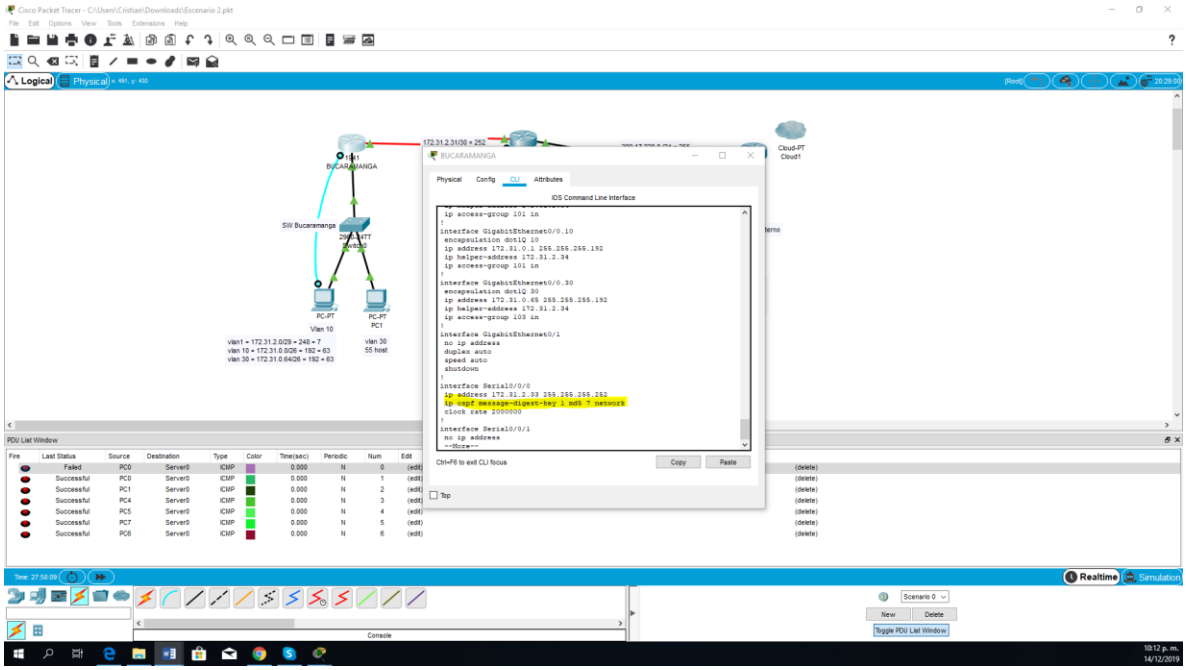


Figura 61 Autenticación de enrutamiento router Bucaramanga

Router Tunja

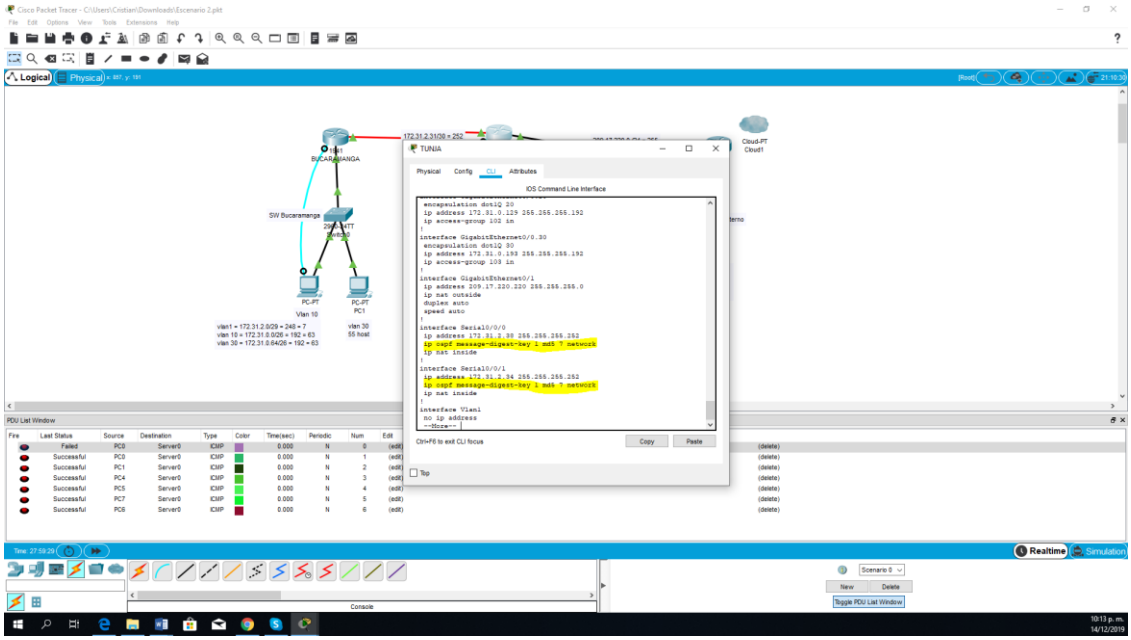


Figura 62 Autenticación de enrutamiento router Tunja

Router Cundinamarca

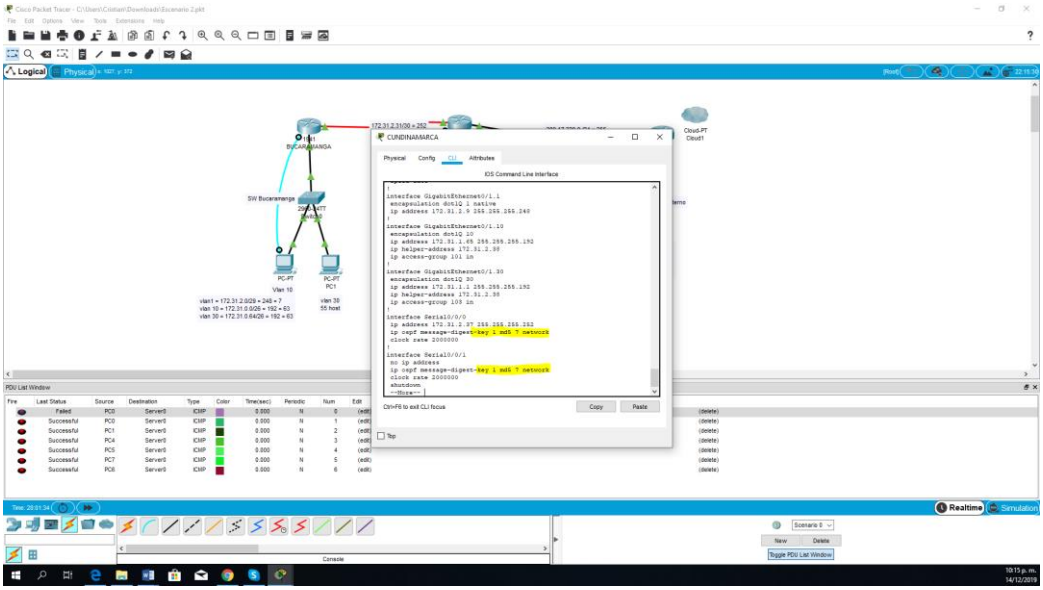


Figura 63 Autenticación de enrutamiento router Cundinamarca

6.2.1.6 Listas de control de acceso:

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

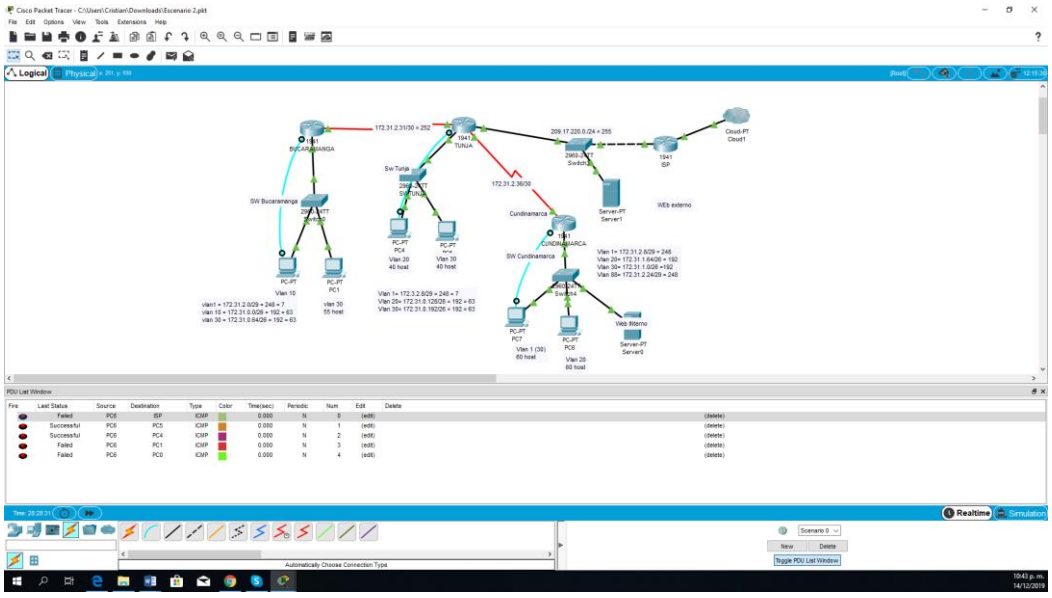


Figura 64 Verificación "Los hosts de VLAN 20 en Cundinamarca no acceden a internet, solo a la red interna de Tunja"

- Los hosts de VLAN 10 (30) en Cundinamarca si acceden a internet y no a la red interna de Tunja.

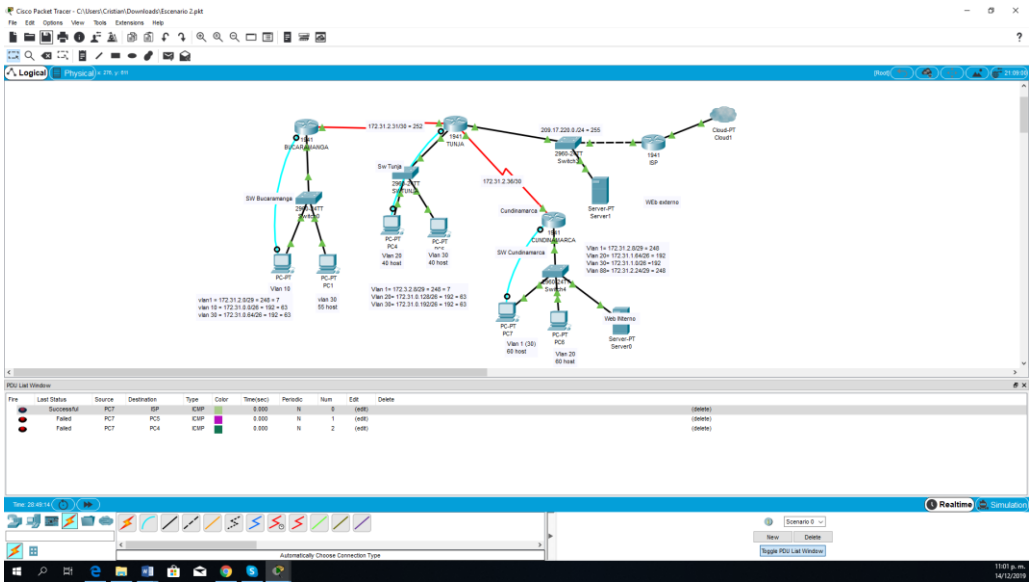


Figura 65 Verificación "Los hosts de VLAN 10 (30) en Cundinamarca si acceden a internet y no a la red interna de Tunja"

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

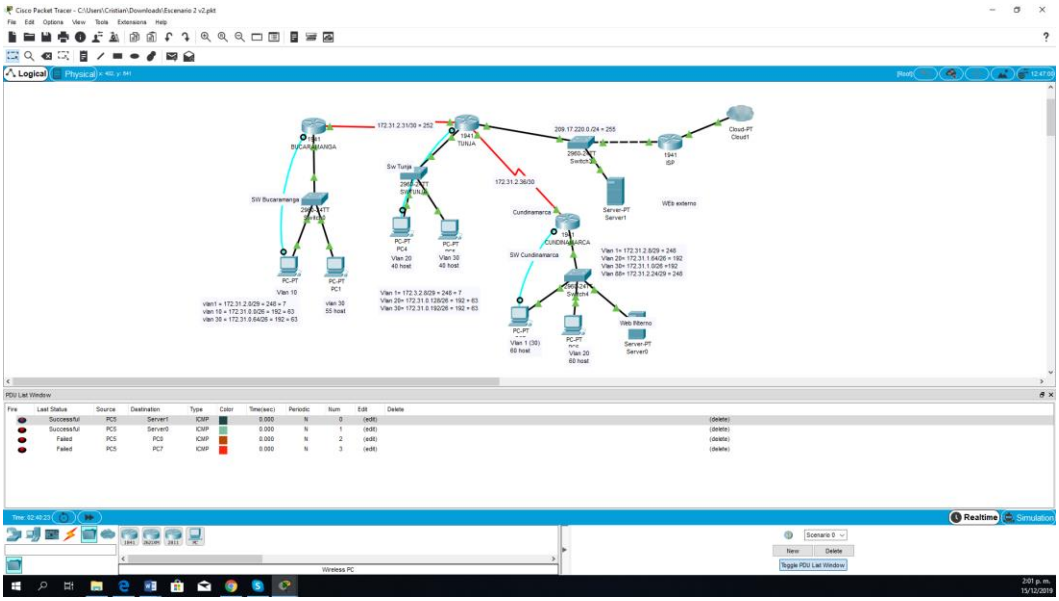


Figura 66 Verificación "Los hosts de VLAN 30 en Tunja solo acceden a servidores web y ftp de internet"

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

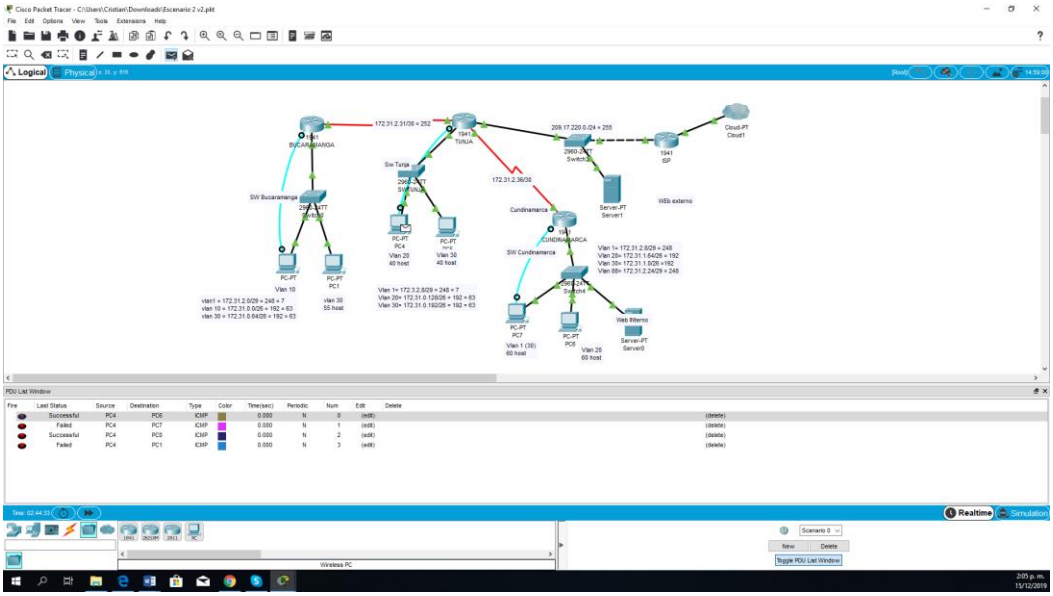


Figura 67 Verificación "Los hosts de VLAN 20 en Tunja solo acceden a la VLAN 20 de Cundinamarca y VLAN 10 de Bucaramanga"

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

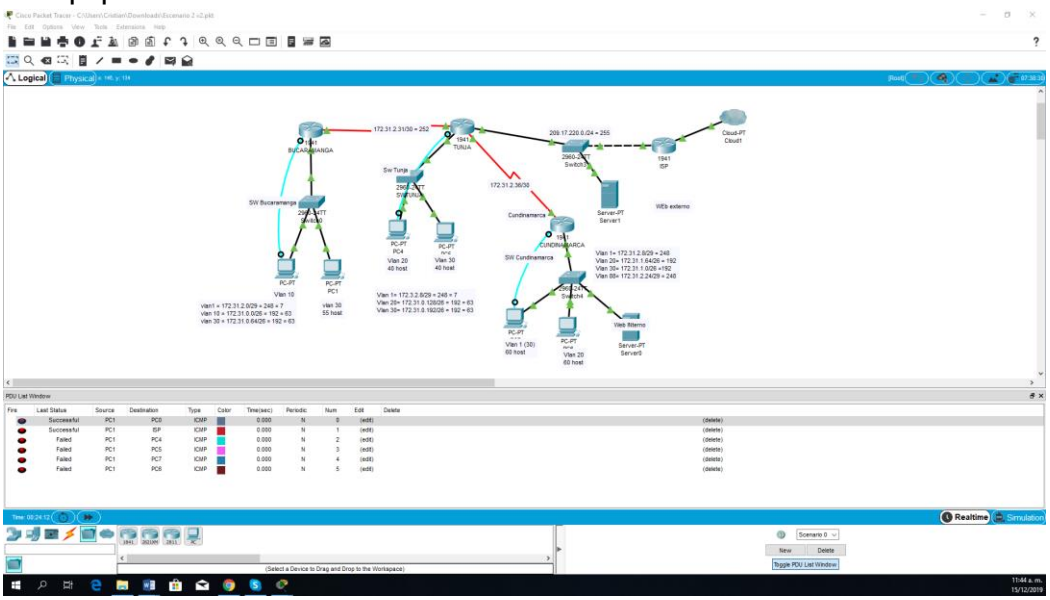


Figura 68 Verificación "Los hosts de VLAN 30 de Bucaramanga acceden a internet y a cualquier equipo de VLAN 10."

- Los hosts de VLAN 10 en Bucaramanga acceden a la red de Cundinamarca (VLAN 20) y Tunja (VLAN 20), no internet.

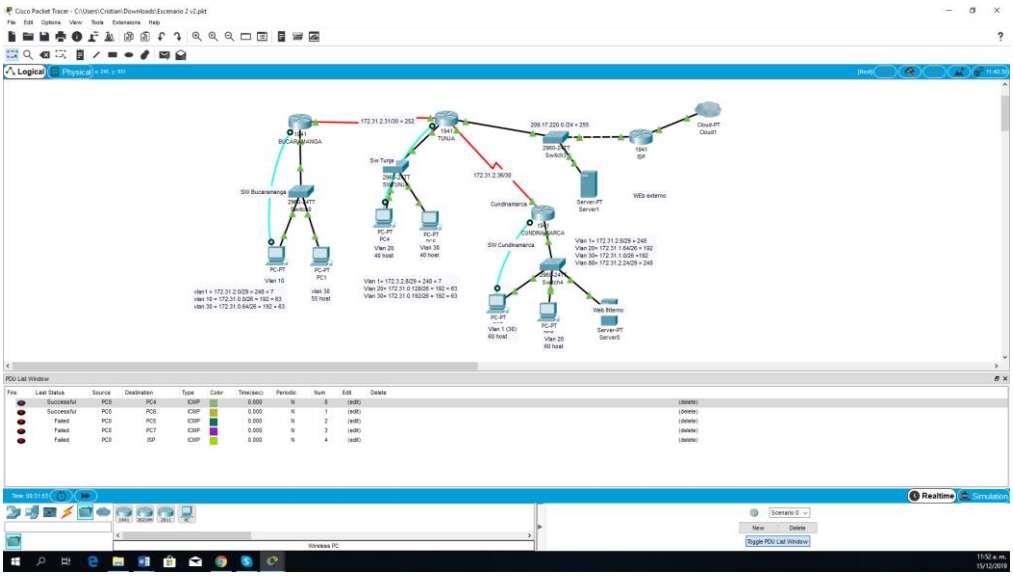


Figura 69 Verificación "• Los hosts de VLAN 10 en Bucaramanga acceden a la red de Cundinamarca (VLAN 20) y Tunja (VLAN 20), no internet"

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

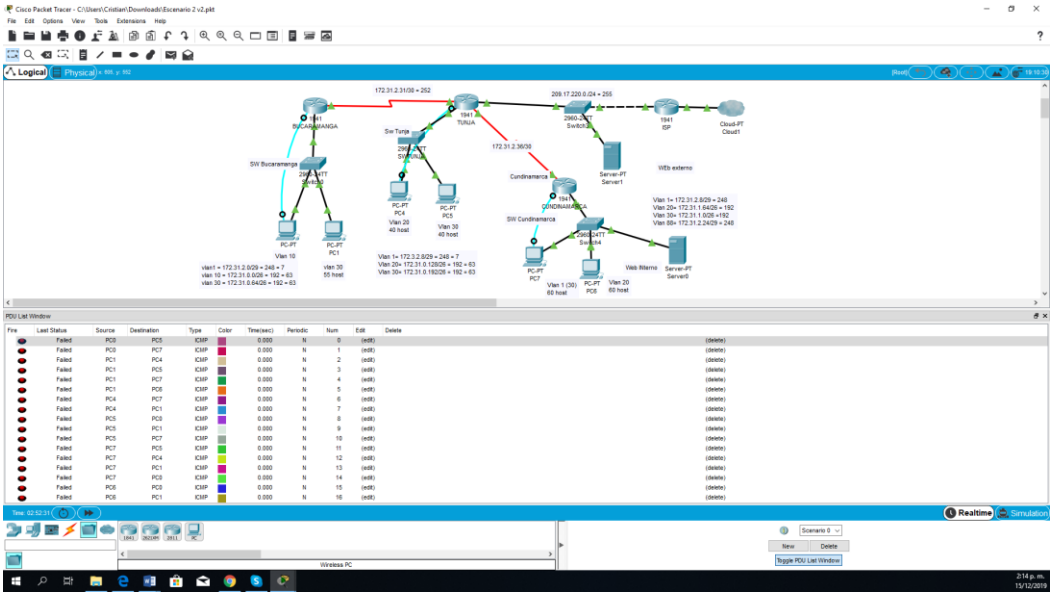


Figura 70 Verificación "Los hosts de una VLAN no pueden acceder a los de otra VLAN en una ciudad"

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

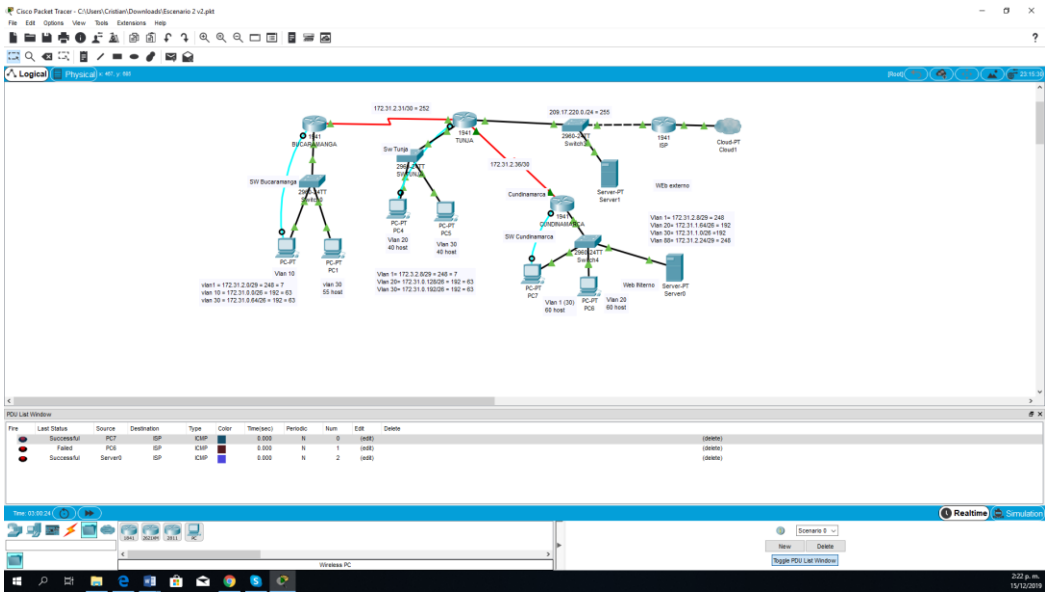


Figura 71 Verificación "Solo los hosts de las VLAN administrativas y de la VLAN de servidores tienen accedo a los routers e internet

En este caso los hosts de la vlan 20 de Cundinamarca no acceden a internet por que estarían violando una regla establecida anteriormente.

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

Network	First	Last	Broadcast	Mascara	
172.31.0.0	172.31.0.1	172.31.0.254	172.31.0.255	/ 24	255.255.255.0
172.31.1.0	172.31.1.1	172.31.1.62	172.31.1.63	/ 26	255.255.255.192
172.31.1.64	172.31.1.65	172.31.1.126	172.31.1.127	/ 26	255.255.255.192
172.31.1.128	172.31.1.129	172.31.1.190	172.31.1.191	/ 26	255.255.255.192
172.31.1.192	172.31.1.193	172.31.1.254	172.31.1.255	/ 26	255.255.255.192
172.31.2.0	172.31.2.1	172.31.2.62	172.31.2.63	/ 26	255.255.255.192
172.31.2.64	172.31.2.65	172.31.2.126	172.31.2.127	/ 26	255.255.255.192
172.31.2.128	172.31.2.129	172.31.2.134	172.31.2.135	/ 29	255.255.255.248

172.31.2.136	172.31.2.137	172.31.2.142	172.31.2.143	/ 29	255.255.255.248
172.31.2.144	172.31.2.145	172.31.2.150	172.31.2.151	/ 29	255.255.255.248
172.31.2.152	172.31.2.153	172.31.2.158	172.31.2.159	/ 29	255.255.255.248
172.31.2.160	172.31.2.161	172.31.2.162	172.31.2.163	/ 30	255.255.255.252
172.31.2.164	172.31.2.165	172.31.2.166	172.31.2.167	/ 30	255.255.255.252

Tabla 25 Redes VLSM

6.2.2 CONFIGURACIÓN UTILIZADA EN EL ESCENARIO 2.

6.2.2.1 Router Bucaramanga

Elaboramos las configuraciones básicas del Router

```
Config terminal
Hostname RBUCARAMANGA
Login block-for 240 attempts 4 within 120
Enable secret cisco
service password-encryption

line con 0
password cisco

exec-timeout 5 0
login
logging synchronous
exit

line vty 0 4
password cisco
exec-timeout 5 0
login
logging synchronous
exit

banner motd #NO INGRESAS!#
```

login delay 10

Establecemos la autenticación AAA
Aaa new-model
Aaa authentication login LOCAL_AUTH local

Creamos los usuarios de la autenticación

Username TUNJA privilege 7 password 0 network
Username tunja1 password 0 tunja1
Username bucaramanga1 password 0 bucaramanga1
Username cundinamarca1 password 0 Ucundinamarca1

Iniciamos a configurar las interfaces y sub-interface
Colocamos el comando helper-address para facilitar el DHCP

Interface GigabitEternet0/0
No ip address
duplex Auto
speed auto

interface GigabitEthernet0/0.1
Encapsulation dot1Q 1 native
Ip address 172.31.2.1 255.255.255.248   (VLAN 1)

Interface GigabitEthernet0/0.10
Encapsulation dot1Q 10
Ip address 172.31.0.1 255.255.255.192 (VLAN 10)
Ip helper-address 172.31.2.34
Ip Access-group 101 in

Interface gigabitEthernet 0/0.30
Encapsulation dot1Q 30
Ip address 172.31.0.65 255.255.255.192 (VLAN 30)
Ip helper-address 172.31.2.34
Ip Access-group 103 in

Interface serial 0/0/0
Ip address 172.31.2.33 255.255.255.252 (ENLACES)

Ip ospf message-digest-key 1 md5 7 network
exit
exit

establecemos el Servidor tftp

Conectamos cable de consola al router

Copy running-config tftp
Colocamos la ip del servidor de tfpt “172.31.2.11”

Establecemos una ruta estatica

Ip route 172.31.0.64 255.255.255.192 s0/0/0
Ip route 172.31.0.0 255.255.255.192 s0/0/0
Ip route 172.31.1.0 255.255.255.192 s0/0/0
Ip route 172.31.1.64 255.255.255.192 s0/0/0

Guardamos la configuracion
copy running-config startup-config

Configuramos el enrutamiento OSPF

Router ospf 1
Network 172.31.2.0 0.0.0.7 area 0
Network 172.31.0.0 0.0.0.63 area 0
Network 172.31.0.64 0.0.0.63 area 0
Network 172.31.2.31 0.0.0.3 area 0
Network 172.31.2.36 0.0.0.3 area 0

Establecemos las listas de control de acceso acuerdo lo indicado

Access-list 103 permit udp host 0.0.0.0 eq bootpc host 255.255.255.255 eq bootps
Access-list 103 permit ip 172.31.0.64 0.0.0.63 209.17.220.254 0.0.0.255
Access-list 103 permit ip 172.31.0.64 0.0.0.63 209.17.220.10 0.0.0.255
Access-list 103 permit ip 172.31.0.64 0.0.0.63 172.31.0.0 0.0.0.63
Access-list 103 permit ip 172.31.0.0 0.0.0.63 172.31.1.64 0.0.0.63
Access-list 103 permit ip 172.31.0.0 0.0.0.63 172.31.0.128 0.0.0.63
Access-list 103 deny ip 172.31.0.0 0.0.0.63 209.17.220.254 0.0.0.255

Access-list 103 deny ip 172.31.0.0 0.0.0.63 209.17.220.10 0.0.0.255

6.2.2.2 Router Tunja

Elaboramos las configuraciones básicas del Reuter

Config terminal
Hostname RTUNJA
Login block-for 240 attempts 4 within 120
Enable secret cisco
service password-encryption

line con 0
password cisco
exec-timeout 5 0
login
logging synchronous
exit

line vty 0 4
password cisco
exec-timeout 5 0
login
logging synchronous
exit

banner motd #NO INGRESAS!#

Establecemos la autenticación AAA

aaa new-model
aaa authentication login LOCAL_AUTH local

Creamos los usuarios de la autenticación

Username TUNJA privilege 7 password 0 network
Username tunja1 password 0 tunja1

Username bucaramanga1 password 0 bucaramanga1
Username cundinamarca1 password 0 cundinamarca1

Iniciamos a configurar las interfaces y sub-interface

Interface GigabitEthernet 0/1
ip address 209.17.220.220 255.255.255.0 (INTERNET)
ip nat outside
duplex Auto
speed auto

Interface GigabitEthernet 0/0
No ip address
ip nat outside
duplex Auto
speed auto

Interface GigabitEthernet 0/0.1
Encapsulation dot1Q 1 native
ip address 172.3.2.9 255.255.255.248 (VLAN 1)
no shut

Interface GigabitEthernet 0/0.20
Encapsulation dot1Q 20
Ip address 172.31.0.129 255.255.255.192 (VLAN 20)
Ip Access-group 102 in
no shut

Interface GigabitEthernet 0/0.30
Encapsulation dot1Q 30
Ip address 172.31.0.193 255.255.255.192 (VLAN 30)
Ip Access-group 103 in

Interface serial 0/0/1
Ip address 172.31.2.34 255.255.255.252
Ip ospf message-digest-key 1 md5 7 network
Ip nat inside
Clock rate 64000
No shut

Interface serial 0/0/0
Ip address 172.31.2.38 255.255.255.252
Ip ospf message-digest-key 1 md5 7 network
Ip nat inside
Clock rate 64000
no shut

Creamos la vlan 1 y la iniciamos

Interface Vlan1
No ip address
No Shutdown

Configuramos DHCP

Ip dhcp excluded-address 172.31.1.65 172.31.1.70
Ip dhcp excluded-address 172.31.1.1 172.31.1.5
Ip dhcp excluded-address 172.31.0.1 172.31.0.5
Ip dhcp excluded-address 172.31.0.65 172.31.0.70

Establecemos los pools de cada DHCP

Ip dhcp pool Bucaramanga-30
Network 172.31.0.64 255.255.255.192
Default-router 172.31.0.65

Ip dhcp Pool t-10
Network 172.31.1.0 255.255.255.192
Default-router 172.31.1.1

Ip dhcp Pool t-20
Network 172.31.1.64 255.255.255.192
Default-router 172.31.1.65

Ip dhcp Pool bucaramanga-10
Network 172.31.0.0 255.255.255.192
Default-router 172.31.0.1

Configuramos el Servidor tftp

Conectamos cable de consola al router

Copy running-config tftp
Colocamos la ip del servidor de tfpt 172.31.2.11

Guardamos la configuración

copy running-config startup-config

Configuramos el enrutamiento OSPF

Router ospf 1
Network 172.31.0.128 0.0.0.63 area 0
Network 172.31.0.192 0.0.0.63 area 0
Network 172.3.2.8 0.0.0.7 area 0
Network 172.31.2.31 0.0.0.3 area 0
Network 172.31.2.36 0.0.0.3 area 0
Network 209.17.220.0 0.0.0.255 area 0

Establecemos la NAT de sobrecarga PAT

Ip nat inside source list 20 interfase gigabitEthernet 0/1 overload

Establecemos la NAT
Ip nat inside source static 172.31.2.38 209.17.220.10
Ip nat inside source static 172.31.2.34 209.17.220.10

Establecemos la ruta de salida
Ip route 0.0.0.0 0.0.0.0 gigabitEthernet 0/1

Establecemos las listas de control de acceso acuerdo lo indicado

Access-list 105 permit udp host 0.0.0.0 eq bootpc host 255.255.255.255 eq bootps
Access-list 105 permit ip 172.31.0.192 0.0.0.63 209.17.220.10 0.0.0.255
Access-list 105 permit ip 172.31.0.192 0.0.0.63 172.31.2.11 0.0.0.7
Access-list 105 permit tcp 172.31.0.192 0.0.0.63 any eq www
Access-list 105 permit tcp 172.31.0.192 0.0.0.63 any eq ftp
Access-list 108 permit ip 172.31.0.128 0.0.0.63 172.31.1.64 0.0.0.63
Access-list 108 permit ip 172.31.0.128 0.0.0.63 172.31.0.0 0.0.0.63

6.2.2.3 Router Cundinamarca

Elaboramos las configuraciones básicas del Router

Config terminal
Hostname RCUNDINAMARCA
Login block-for 240 attempts 4 within 120

Enable secret cisco
service password-encryption

line con 0
password cisco

exec-timeout 5 0
login
logging synchronous
exit

line vty 0 4
password cisco
exec-timeout 5 0
login
logging synchronous
exit

banner motd #NO INGRESAS!#

Establecemos la autenticación AAA

Aaa new-model
Aaa authentication login LOCAL_AUTH local

Creamos los usuarios de la autenticación

Username bucaramanga1 password 0 bucaramanga1
Username tunja1 password 0 tunja1
Username cundinamarca1 password 0 cundinamarca1

Iniciamos a configurar las interfaces y sub-interface
Configuramos el helper-address para facilitar el dhcp

Interface GigabitEthernet0/1
No ip address
duplex Auto
speed auto

interface GigabitEthernet0/1.1
Encapsulation dot1Q 1 native
Ip address 172.31.2.9 255.255.255.248 (VLAN 1)
No shut

Interface GigabitEthernet0/1.10
Encapsulation dot1Q 10
Ip address 172.31.1.65 255.255.255.192
Ip helper-address 172.31.2.38
Ip Access-group 101 in
No shut

Interface gigabitEthernet 0/1.30
Encapsulation dot1Q 30
Ip address 172.31.1.1 255.255.255.192 (VLAN 30)
Ip helper-address 172.31.2.38
Ip Access-group 103 in
No shut

No Interface gigabitEthernet 0/0.80
Encapsulation dot1Q 80
Ip address 172.31.2.25 255.255.255.248
Ip helper-address 172.31.2.38
Ip Access-group 103 in
No shut

Interface serial 0/0/0
Ip address 172.31.2.37 255.255.255.252
No shut
Ip ospf message-digest-key 1 md5 7 network
exit

exit

Configuramos el servidor TFTP

Conectamos cable de consola al router

Copy running-config tftp
Colocamos la ip del servidor de tfpt 172.31.2.11

Establecemos las rutas estáticas

Ip route 172.31.0.64 255.255.255.192 s0/0/0
Ip route 172.31.0.0 255.255.255.192 s0/0/0
Ip route 172.31.1.0 255.255.255.192 s0/0/0
Ip route 172.31.1.64 255.255.255.192 s0/0/0

Configuramos el enrutamiento OSPF

Router ospf 1
Network 172.31.2.8 0.0.0.7 area 0
Network 172.31.1.64 0.0.0.63 area 0
Network 172.31.1.0 0.0.0.63 area 0
Network 172.31.2.24 0.0.0.7 area 0
Network 172.31.2.31 0.0.0.3 area 0
Network 172.31.2.36 0.0.0.3 area 0
Network 209.17.220.0 0.0.0.255 area 0

Establecemos las listas de control de acceso acuerdo lo indicado

Access-list 101 permit udp host 0.0.0.0 eq bootpc host 255.255.255.255 eq bootps
Access-list 101 permit ip 172.31.1.64 0.0.0.63 172.31.0.128 0.0.0.63
Access-list 101 permit ip 172.31.1.64 0.0.0.63 172.31.0.192 0.0.0.63
Access-list 101 deny ip 172.31.1.64 0.0.0.63 209.17.220.0 0.0.0.255
Access-list 103 permit ip 172.31.1.0 0.0.0.63 209.17.220.0 0.0.0.255
Access-list 103 deny ip 172.31.1.0 0.0.0.63 172.31.0.128 0.0.0.63
Access-list 103 deny ip 172.31.1.0 0.0.0.63 172.31.0.192 0.0.0.63

6.2.2.4 Nat En El Router Tunja

Establecemos el Nat estático.
Ip nat inside source static 172.31.2.38 209.17.220.10
Ip nat inside source static 172.31.2.34 209.17.220.10

Establecemos el Nat de sobrecarga (PAT)
Ip nat inside source list 20 interface GigabitEthernet0/1 overload
Access-list 20 permit 172.31.0.0 0.0.31.255

6.2.2.5 Router Isp

Elaboramos las configuraciones básicas del Router

Hostname RISP
Login block-for 240 attempts 4 within 120
Enable secret cisco
service password-encryption
line con 0
password cisco
exec-timeout 5 0
login
logging synchronous
exit
line vty 0 4
password cisco
exec-timeout 5 0
login
logging synchronous
exit
banner motd #NO INGRESAS!#

Establecemos la autenticación AAA

Aaa new-model
Aaa authentication login LOCAL_AUTH local

Creamos los usuarios de la autenticación

Username TUNJA privilege 7 password 0 network
Username tunja1 password 0 tunja1
Username bucaramanga1 password 0 bucaramanga1
Username cundinamarca1 password 0 Ucundinamarca1

Iniciamos a configurar las interfaces

Interface GigabitEthernet 0/0
ip address 209.17.220.11 255.255.255.0
Duplex Auto
Speed auto

Establecemos ruta estatica
Ip route 172.31.0.0 255.255.224.0 209.17.220.200

6.2.2.6 Switch Cundinamarca

Colocamos la configuración básica

no ip domain-lookup
hostname SWCUNDINAMARCA
enable password cisco
Line console 0
Password cisco
login
Line vty 0 15
Password cisco
login
exit
Line console 0
Logging synchronous
Line 0
password cisco
Exec-timeout 5 0
Logging synchronous
Exit

Line vty 0 4
password cisco
Exec-timeout 5 0
Login
logging synchronous
exit
Creamos y colocamos direccionamiento en las vlans y asignamos puertos

interface VLAN1
Ip address 172.31.2.10 255.255.255.248
Ip default-gateway 172.31.2.9
interface f0/12
switchport mode Access
switchport access vlan 1
No shut
interface VLAN1
no shut
exit

interface VLAN10
Ip address 172.31.1.66 255.255.255.192
Ip default-gateway 172.31.1.65
interface f0/1
switchport mode Access
switchport access VLAN 10
No shut
Int vlan 10
No shut

interface VLAN30
Ip address 172.31.1.2 255.255.255.192
Ip default-gateway 172.31.1.1
interface f0/11
switchport mode Access
switchport access vlan 30
no shut
Int vlan 30
No shut

interface VLAN88
Ip address 172.31.2.26 255.255.255.248
Ip default-gateway 172.31.2.25
interface f0/13
switchport mode Access
switchport access vlan 88
no shut
exit

Colocamos el puerto TRONCAL

interface f0/2
switchport mode trunk

6.2.2.7 Switch Tunja

Colocamos la configuración

no ip domain-lookup
hostname SWTUNJA
enable password cisco

Line console 0
Password cisco
login
Line vty 0 15
Password cisco
login
exit
Line console 0
Logging synchronous

Creamos y colocamos direccionamiento en las vlans y asignamos puertos

interface VLAN1
Ip address 172.3.2.10 255.255.255.248
Ip default-gateway 172.3.2.9
interface f0/12

switchport mode Access
switchport access vlan 1
no shut
exit
interface VLAN1
no shutdown

interface VLAN20
Ip address 172.31.0.130 255.255.255.192
Ip default-gateway 172.31.0.129
interface f0/1
switchport mode Access
switchport access vlan 20
no shut
exit
interface VLAN20
no shutdown

interface VLAN30
Ip address 172.31.0.194 255.255.255.192
Ip default-gateway 172.31.0.193
interface f0/11
switchport mode Access
switchport access vlan 30
no shut
exit

interface VLAN30
no shutdown
exit
exit

asignamos el puerto TRONCAL

interface f0/2
switchport mode trunk

6.2.2.8 Switch Bucaramanga

Realizamos la configuración básica

```
no ip domain-lookup
hostname SWBUCARAMANGA
enable password cisco

Line console 0
Password cisco
login
Line vty 0 15
Password cisco
login
exit
Line console 0
Logging synchronous
```

Creamos y colocamos direccionamiento en las vlans y asignamos puertos

```
interface VLAN1
Ip address 172.31.2.2 255.255.255.248
Ip default-gateway 172.31.2.1
interface f0/12
switchport mode Access
switchport access vlan 1
no shut
exit

interface VLAN1
no shutdown
exit
exit

 interface VLAN10
Ip address 172.31.0.2 255.255.255.192
Ip default-gateway 172.31.0.1
interface f0/1
```

switchport mode Access
switchport access vlan 10
No shut
exit

interface VLAN10
no shutdown
interface VLAN30
Ip address 172.31.0.66 255.255.255.192
Ip default-gateway 172.31.0.65
interface f0/11
switchport mode Access
switchport access vlan 30
no shut
exit

interface VLAN30
no shut

Asigne el puerto TRONCAL
interface f0/2
switchport mode trunk

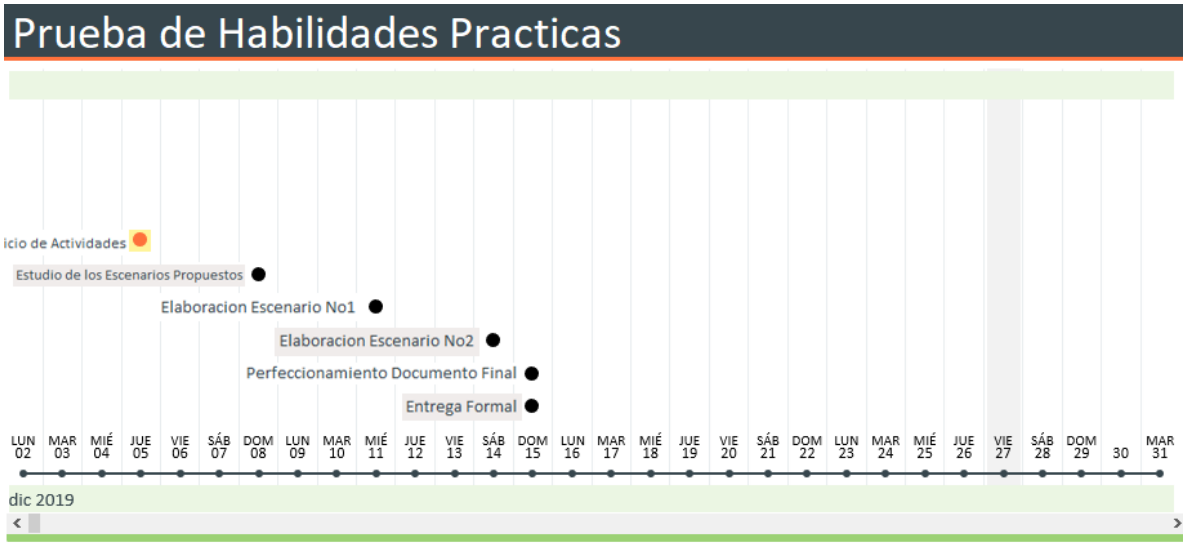
6.3 ANÁLISIS DEL DESARROLLO DEL PROYECTO

El método utilizado del practica y repetición de los ejercicios propuestos en las unidades abordadas en el diplomado de profundización cisco, sirvió de gran ayuda para la culminación de los requerimientos de cada uno de los escenarios.

La correcta compresión de la debida configuración de los protocolos de enrutamiento y las listas de control de acceso has sido de vital ayuda al momento de dar cumplimiento a las pautas establecidas en el desarrollo de las actividades dispuestas.

Dichas configuraciones han servido para dar cumplimiento a las mencionadas directrices establecidas por las gerencias de cada empresa que tenían la necesidad de cumplir con parámetros de seguridad de la información para el correcto funcionamiento de su negocio.

6.4 CRONOGRAMA



ACTIVIDAD	INICIO	FIN	NOTAS
Inicio de Actividades	5/12/2019		Se recibe Por medio de mail interno Prueba de Habilidades
Estudio de los Escenarios Propuestos	6/12/2019	8/12/2019	Se realiza Veriicacion de los escenarios en aras de establecer tran de trabajo a desarrollar
Elaboracion Escenario No1	8/12/2019	11/12/2019	Se inicia Solución del escenario No1
Elaboracion Escenario No2	11/12/2019	14/12/2019	Se inicia Solución del escenario No2
Perfeccionamiento Documento Final	15/12/2019	15/12/2019	Se perfecciona Documento final a Entregar
Entrega Formal	15/12/2019	15/12/2019	Se realiza entrega forma documento En el Link correspondiente

Figura 72 Cronograma de Actividades

CONCLUSIONES

Se logró dar soluciono a los escenarios planteados en la presente actividad de habilidades prácticas, donde los estudiantes retomaron todas las temáticas abordadas en el desarrollo del diplomado de profundización Cisco como enrutamiento OSPF, DHCP, ACL entre otros para dar solución a los puntos establecidos en cada uno de los dos entornos de práctica, todo esto se llevó al programa de simulación de redes cisco packet tracert, el cual permite la creación de evidencias en el desarrollo de las actividades en aras de ser verificadas posteriormente por el tutor.

RECOMENDACIONES

- Realizar entrega de los escenarios que realizan la validación de la prueba de habilidades del diplomado de profundización Cisco al momento de entregar los ejercicios relacionados con la unidad No4, esto con el fin de que los estudiantes tengan el tiempo necesario para el entendimiento de los ejercicios y su desarrollo dentro de los tiempos propuestos por el diplomado.

- Indicar una Canal de comunicación de una vía que funcione de manera informativa acerca de las pautas a seguir en el desarrollo de los escenarios propuestos, estos con el fin de evitar información equivoca que solo hace es desorientar a los estudiantes que cumplen con estrictos horarios laborales.

BIBLIOGRAFÍA

recursostic.educacion.es. (26 de 12 de 2019). Obtenido de recursostic.educacion.es: http://recursostic.educacion.es/observatorio/web/ca/software/servidores/1065-listas-de-control-de-acceso-acl?start=1

recursostic.educacion.es. (26 de 12 de 2019). Obtenido de recursostic.educacion.es: http://recursostic.educacion.es/observatorio/web/ca/software/servidores/1065-listas-de-control-de-acceso-acl?start=1

Universidad Nacional Abierta y a Distancia . (2019). Formato guía de actividades y rúbrica de evaluación Tarea 5 . Obtenido de file:///C:/Users/Cristian/Documents/SEMESTRE%20XII/01_DIPLOMADO%20DE%20PROFUNDIZACIÓN%20CISCO/tarea%205/Guía%20de%20actividades%20y%20rúbrica%20de%20evaluacion%20-%20Tarea%205%20-%20Actividad%20Colaborativa%203.pdf

Universidad Nacional Abierta y a Distancia. (2019). Formato guía de actividades y rúbrica de evaluación Tarea 3 . Obtenido de file:///C:/Users/Cristian/Documents/SEMESTRE%20XII/01_DIPLOMADO%20DE%20PROFUNDIZACIÓN%20CISCO/tarea%203/Guía%20de%20actividades%20y%20rúbrica%20de%20evaluacion%20-%20Tarea%203%20-%20Actividad%20Colaborativa%202.pdf

Universidad Nacional Abierta y a Distancia. (2019). Formato guía de actividades y rúbrica de evaluación Tarea 7. Obtenido de file:///C:/Users/Cristian/Documents/SEMESTRE%20XII/01_DIPLOMADO%20DE%20PROFUNDIZACIÓN%20CISCO/tarea%207/Guía%20de%20actividades%20y%20rúbrica%20de%20evaluacion%20-%20Tarea%207%20-%20Actividad%20Colaborativa%204.pdf

www.ecured.cu. (26 de 12 de 2019). Obtenido de www.ecured.cu: https://www.ecured.cu/Protocolos_de_ruteo

www.ecured.cu. (26 de 12 de 2019). Obtenido de www.ecured.cu: https://www.ecured.cu/Protocolos_de_ruteo

www.ecured.cu/Protocolos_de_ruteo. (26 de 12 de 2019). Obtenido de www.ecured.cu/Protocolos_de_ruteo: https://www.ecured.cu/Protocolos_de_ruteo

www.universidadviu.com. (27 de 12 de 2019). Obtenido de www.universidadviu.com: https://www.universidadviu.com/redes-de-datos-todo-lo-que-hay-que-saber-sobre-ellas/