

Escuela de ciencias básicas, tecnología e ingeniería
Diplomado de profundización cisco (diseño e implementación de soluciones
integradas lan / wan) (opci - (203092a_614)

Tarea 11. Prueba de habilidades cisco.

Por:

FREYDY GERMAN PINZÓN SOLANO.

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
DICIEMBRE DE 2019

Escuela de ciencias básicas, tecnología e ingeniería
Diplomado de profundización cisco (diseño e implementación de soluciones
integradas lan / wan) (opci - (203092a_614)

Tarea 11. Prueba de habilidades cisco.

Por:

FREYDY GERMAN PINZÓN SOLANO.

Código: 203092a_614

Presentado a:

Diego Édison Ramírez

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
DICIEMBRE DE 2019

CONTENIDO

| | |
|---|----|
| RESUMEN | 4 |
| Abstract | 4 |
| INTRODUCCION | 5 |
| OBJETIVOS | 6 |
| 1. DESCRIPCIÓN GENERAL DE LA PRUEBA DE HABILIDADES | 7 |
| 1.1 Escenario 1. | 9 |
| 1.2 Topología de red | 9 |
| 1.3 Temática y desarrollo | 10 |
| 2. 1 Escenario 2 | 48 |
| 2.1.1 topología de la red | 49 |
| 2.1.3 Temática y desarrollo | 49 |
| ENLACE EXTERNO | 82 |
| CONCLUSIONES | 83 |
| REFERENCIAS BIBLIOGRÁFICAS | 84 |

RESUMEN

El presente documento, contiene detalladamente los pasos a seguir para el análisis y la construcción del modelado en la conexión de una red y sus respectivas configuraciones, para una empresa que cuenta con tres sucursales en diferentes lugares del país (Bogotá, Medellín y Cali), se partirá desde la obtención de las conexiones, cableado de la red, direccionamiento ip de cada elemento del diagrama y su respectiva modificación de seguridad, posteriormente se aplicará la solución de registros a los router , con sus respectivos eigrp y su acceso de lista para verificar todos sus valores de estado en función de la red con sus respectivas restricciones a los dispositivos de la subred. Teniendo en cuenta las condiciones iniciales y direcciones, se representarán las pruebas de cada ítem de la actividad como objeto de veracidad del tema, en la ejecución de simulador PACKET TRACER.

ABSTRACT

This document contains in detail the steps to follow for the analysis and construction of the modeling in the connection of a network and its respective configurations, for a company that has three branches in different parts of the country (Bogotá, Medellín and Cali), It will start from the obtaining of the connections, wiring of the network, IP address of each element of the diagram and its respective security modification, later the solution of registers will be applied to the routers, with their respects eigrp and their access of list to verify all its status values depending on the network with their respective restrictions on the devices of the subnet. Taking into account the initial conditions and directions, the tests of each item of the activity will be represented as an object of veracity of the topic, in the execution of PACKET TRACER simulator.

INTRODUCCION

De acuerdo a lo establecido en el diplomado de profundización de Cisco para la evaluación de adquisición en conocimientos sobre el contenido del curso y con base en un caso de estudio, se sigue un paso a paso, lo que implica las temáticas de Switching y Routing, configuración de una red que abarca un escenario de tres ciudades.

En el desarrollo de esta actividad, se utiliza la herramienta software Packet Trace donde se implementa la topología y se realizan las configuraciones. Como paso inicial se realiza una configuración básica de los dispositivos en donde se les asigna el nombre, la seguridad de acceso a los modos exec y el acceso remoto. A continuación y siguiendo la guía se realiza el direccionamiento IP, configuración del protocolo EIGRP, configuración de las listas de acceso en cada uno de los dispositivos donde aplique la respectiva configuración.

La idea fundamental es aplicar Networking a la topología presentada, haciendo el uso de dispositivos Cisco y por ende del sistema operativo IOS implementado en los routers y switches de esta tecnología, usando los conocimientos y habilidades adquiridas a lo largo del curso, con el propósito de valorar las destrezas a la hora de implementar dispositivos Cisco para conformar y administrar redes.

OBJETIVOS

Objetivos General:

Profundizar el tema del curso mediante la solución de un escenario, solicitado por la guía de actividades durante el proceso de formación del Diplomado en Cisco.

Objetivos Específicos:

- Realizar la implementación de una topología de red conectando tres routers para realizar el direccionamiento IP y las respectivas configuraciones utilizando tecnología Cisco.
- Aplicar los conocimientos y destrezas adquiridos con el estudio de las temáticas de CCNA para realizar Internetworking.
- Configurar los diferentes dispositivos presentados en el escenario aplicando los protocolos y procedimientos necesarios para la optimización de la red.
- Autoevaluar la adquisición de conocimientos adquiridos en el desarrollo del curso, estableciendo falencias a la hora de administrar una red de datos.

1. DESCRIPCIÓN GENERAL DE LA PRUEBA DE HABILIDADES

La evaluación denominada “Prueba de habilidades prácticas”, forma parte de las actividades evaluativas del Diplomado de Profundización CCNA, y busca identificar el grado de desarrollo de competencias y habilidades que fueron adquiridas a lo largo del diplomado. Lo esencial es poner a prueba los niveles de comprensión y solución de problemas relacionados con diversos aspectos de Networking.

Para esta actividad, el estudiante dispone de cerca de dos semanas para realizar las tareas asignadas en cada uno de los dos (2) escenarios propuestos, acompañado de los respectivos procesos de documentación de la solución, correspondientes al registro de la configuración de cada uno de los dispositivos, la descripción detallada del paso a paso de cada una de las etapas realizadas durante su desarrollo, el registro de los procesos de verificación de conectividad mediante el uso de comandos ping, traceroute, show ip route, entre otros.

Teniendo en cuenta que la Prueba de habilidades está conformada por dos (2) escenarios, el estudiante deberá realizar el proceso de configuración de usando cualquiera de las siguientes herramientas: Packet Tracer o GNS3.

Es muy importante mencionar que esta actividad es de carácter **INDIVIDUAL y OBLIGATORIA**.

Toda evidencia de copy-paste o plagio (de la web o de otros informes) será penalizada con severidad.

Lineamientos para la elaboración del Informe

Finalmente, el informe a presentar deberá cumplir con las normas ICONTEC 1486 para la presentación de trabajos escritos e incluir los siguientes elementos en su contenido:

Portada (no registre su número de identificación)

Tabla de contenido

Resumen

Abstract

Introducción

Objetivos

Desarrollo de los dos escenarios

IMPORTANTE: Para cada uno de los escenarios se debe describir el paso a paso de cada punto realizado y deben digitar el código de configuración aplicado (no incluir imágenes ni capturas de pantalla). Las imágenes o capturas de pantalla sólo serán usadas para evidenciar los resultados de comandos como ping, traceroute, show ip route, entre otros.

Conclusiones

Bibliografía

El informe deberá estar acompañado de las respectivas evidencias de configuración de los dispositivos (Packet Tracer ó GNS3), las cuales generarán veracidad al trabajo realizado. El informe deberá ser entregado en el espacio creado para tal fin en el Campus Virtual de la UNAD.

IMPORTANTE: Teniendo en cuenta que este documento deberá ser entregado al final del curso en el Repositorio Institucional, acorde con los lineamientos institucionales para grado. El procedimiento será socializado al finalizar el curso,

pero puede ir revisando este link. ([Lineamientos para el estudiante que carga trabajo de grado](#))

Descripción de escenarios propuestos para la prueba de habilidades

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.

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.

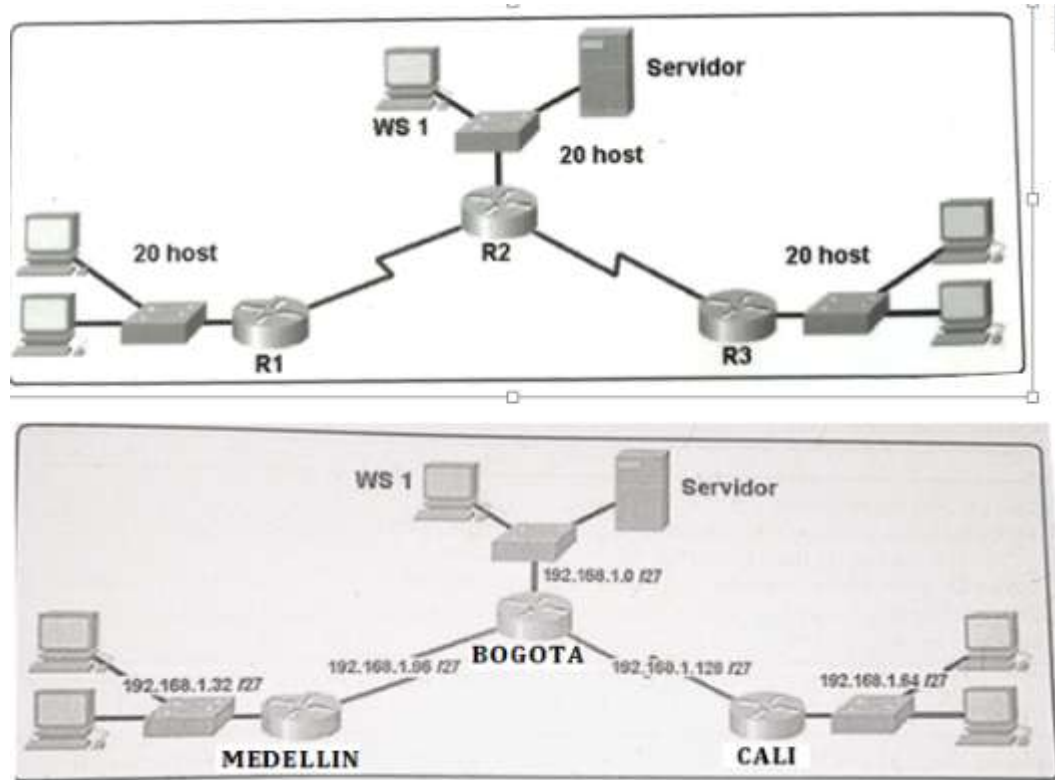


Ilustración 1 red establecida por la guía.

1.3 Temática y 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

En primera instancia se verifica la guía del trabajo, teniendo presente el diagrama se procede a implementar la asignación y cableado de los equipos en el programa PACKET TRACER.

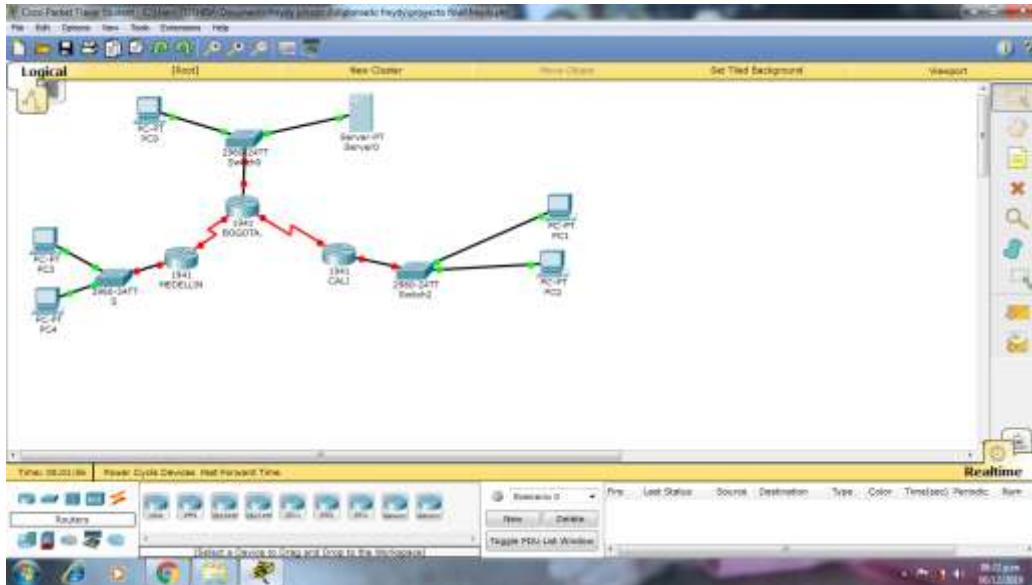


Ilustración 2 equipos de la red.

Fuente: freydy, p. (8 de diciembre de 2019). Aplicación de asignación del entorno principal. Obtenido de packet tracer autoría propia.

Al tener los equipos conectados se verifican y se les asigna la seguridad, implementando la siguiente configuración para todos los equipos.

En el programa PACKET TRACER damos click en el equipo a configurar, se abre la ventana y se escribe la palabra ENABLE, con el fin de habilitar la opción de configurar el dispositivo.

- Configuramos terminal
- Cambiamos nombre con la palabra hostname

- Enable secret UNAD utilizaremos la palabra unad en mayúscula para no tener problemas.
- Seleccionamos exit.
- Configure terminal
- Line console 0
- Password UNAD. Asignamos la clave
- Login iniciamos la configuración
- Exit salimos de la programación de la cosola 0
- Line vty 0 15
- Password UNAD. Asignamos la clave
- Login iniciamos la configuración
- Exit salimos de la programación
- Service password-encryption se habilita para la encriptación de la clave.
- Banner # se asigna un texto dentro los símbolos para que sea visualizado por todos.#
- Exit
- Copy running-config startup-config.

Comprobación de la configuración observar la ilustración 3 y 4.

```
Router>
Router>enable
Router>conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname BOGOTA
BOGOTA(config)#enable secret UNAD
BOGOTA(config)#exit
BOGOTA#
%SYS-5-CONFIG_I: Configured from console by console

BOGOTA#conf t
Enter configuration commands, one per line. End with CNTL/Z.
BOGOTA(config)#line console 0
BOGOTA(config-line)#password UNAD
BOGOTA(config-line)#login
BOGOTA(config-line)#exit
BOGOTA(config)#line vty 0 15
BOGOTA(config-line)#password UNAD
BOGOTA(config-line)#login
BOGOTA(config-line)#exit
BOGOTA(config)#service password-encryption
BOGOTA(config)#banner motd # EXCLUSIVO TUTOR CCNA#
BOGOTA(config)#Exit
BOGOTA#
%SYS-5-CONFIG_I: Configured from console by console

BOGOTA#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
BOGOTA#
```

Ilustración 3 configuración de seguridad.

Fuente: freydy, p. (8 de diciembre de 2019). Aplicación de la configuración de seguridad Obtenido de packet tracer autoría propia.

```
Press RETURN to get started!

solo tutores cna

User Access Verification

Password:
Password:

BOGOTA>ENABLE
Password:
BOGOTA#
BOGOTA#
BOGOTA#
BOGOTA#
BOGOTA#
BOGOTA#
BOGOTA#
BOGOTA#
BOGOTA#
BOGOTA#
```

Ilustración 4 prueba de configuración de seguridad.

Fuente: freydy, p. (8 de diciembre de 2019). Prueba de configuración de la seguridad con sus respectiva clave. Obtenido de packet tracer autoría propia.

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 |

Teniendo presente la tabla de configuración y los equipos conectados procedemos en la verificación de las direcciones IP. Los resultados se pueden ver en la (ilustración 5,6 y 7).

| Router 1 | Router 2 | Router 3. |
|---|--|---|
| UNAD = clave asignada Enable. UNAD. Medellin# configure terminal. Medellin(config)# int g0/0. Medellin(config-if)# ip address 192.168.1.33 255.255.255.224 Medellin(config-if)# no shutdown. Medellin(config-if)#exit Medellin(config)#exit Medellin# UNAD = clave asignada | UNAD = clave asignada Enable. UNAD. bogota# configure terminal. bogota(config)# int g0/0. bogota(config-if)# ip address 192.168.1.1 255.255.255.224 bogota(config-if)# no shutdown. bogota(config-if)#exit bogota(config)#exit bogota# UNAD = clave asignada | UNAD = clave asignada Enable. UNAD. cali# configure terminal. cali(config)# int g0/0. cali(config-if)# ip address 192.168.1.65 255.255.255.224 cali(config-if)# no shutdown. cali(config-if)#exit cali(config)#exit cali# UNAD = clave asignada |

| | | |
|--|--|---|
| <pre> Enable. UNAD. Medellin# configure terminal. 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)#exit Medellin(config)#exit Medellin# </pre> | <pre> Enable. UNAD. bogota# configure terminal. bogota(config)# int g0/0. bogota(config-if)# ip address 192.168.1.98 255.255.255.224 bogota(config-if)# no shutdown. bogota(config-if)#exit bogota(config)#exit bogota# </pre> | <pre> Enable. UNAD. cali# configure terminal. cali(config)# int g0/0. cali(config-if)# ip address 192.168.1.131 255.255.255.224 cali(config-if)# no shutdown. cali(config-if)#exit cali(config)#exit cali# </pre> |
| | <pre> UNAD = clave asignada Enable. UNAD. bogota# configure terminal. bogota(config)# int g0/0. bogota(config-if)# ip address 192.168.1.130 255.255.255.224 bogota(config-if)# no shutdown. bogota(config-if)#exit bogota(config)#exit bogota# </pre> | |

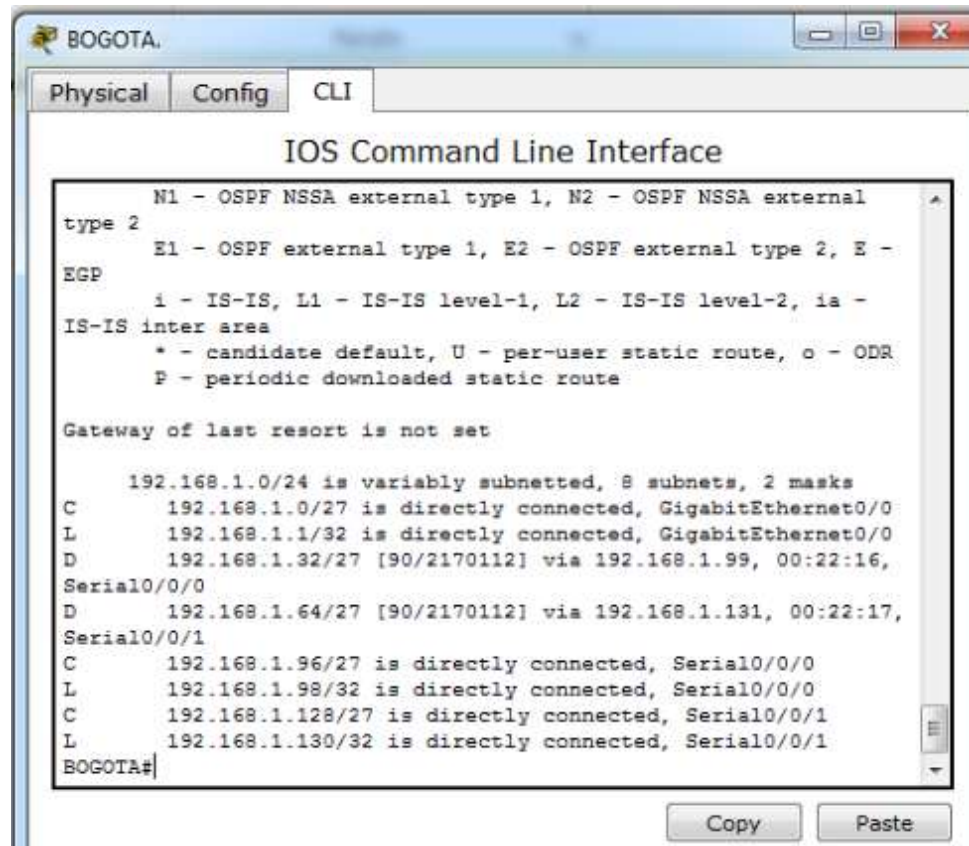


Ilustración 5 ip Bogotá

Fuente: freydy, p. (8 de diciembre de 2019). Prueba de configuración de la seguridad con sus respectiva clave y direcciones ip configuradas.. Obtenido de packet tracer autoría propia.

```
MEDELLIN
Physical Config CLI
IOS Command Line Interface

User Access Verification
Password:
Password:

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

Gateway of last resort is not set

      192.168.1.0/24 is variably subnetted, 7 subnets, 2 masks
D       192.168.1.0/27 [90/2170112] via 192.168.1.98, 00:24:32, Serial0/0/0
C       192.168.1.32/27 is directly connected, GigabitEthernet0/0
L       192.168.1.33/32 is directly connected, GigabitEthernet0/0
D       192.168.1.64/27 [90/2682112] via 192.168.1.98, 00:24:32, Serial0/0/0
C       192.168.1.96/27 is directly connected, Serial0/0/0
L       192.168.1.99/32 is directly connected, Serial0/0/0
D       192.168.1.128/27 [90/2681856] via 192.168.1.98, 00:24:32, Serial0/0/0
MEDELLIN#
```

Ilustración 6 ip medellin

Fuente: freydy, p. (8 de diciembre de 2019). Prueba de configuración de la seguridad con sus respectiva clave y direcciones ip configuradas.. Obtenido de packet tracer autoría propia.

```

CALI
Physical Config CLI
IOS Command Line Interface

User Access Verification

Password:
Password:
Password:

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

Gateway of last resort is not set

    192.168.1.0/24 is variably subnetted, 7 subnets, 2 masks
D:   192.168.1.0/27 [90/21701121] via 192.168.1.130, 00:26:48, Serial0/0/1
D:   192.168.1.32/27 [90/2682112] via 192.168.1.130, 00:26:42, Serial0/0/1
C:   192.168.1.64/27 is directly connected, GigabitEthernet0/0
L:   192.168.1.65/32 is directly connected, GigabitEthernet0/0
D:   192.168.1.96/27 [90/2681856] via 192.168.1.130, 00:26:43, Serial0/0/1
C:   192.168.1.128/27 is directly connected, Serial0/0/1
L:   192.168.1.131/32 is directly connected, Serial0/0/1
CALI#

```

Ilustración 7 ip cali

Fuente: freydy, p. (8 de diciembre de 2019). Prueba de configuración de la seguridad con sus respectiva clave y direcciones ip configuradas.. Obtenido de packet tracer autoría propia.

a. 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. Ver ilustracion 8 y 9 onde la conexión de las redes ip fueron exitosas.

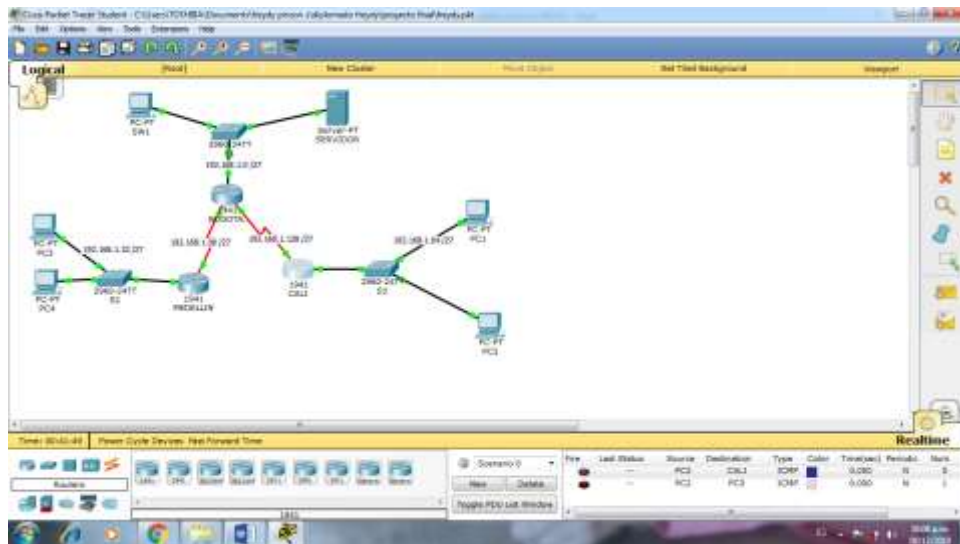


Ilustración 8 configuracion de ip

Fuente: freddy, p. (8 de diciembre de 2019). Prueba de configuración de la seguridad con sus respectiva clave y direcciones ip configuradas en la topología. Obtenido de packet tracer autoría propia.

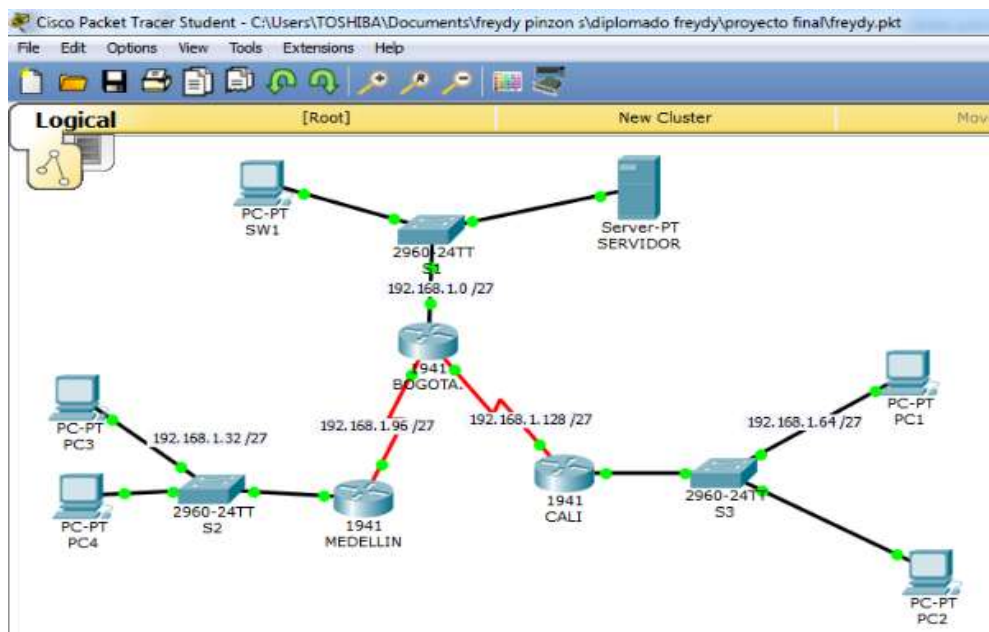
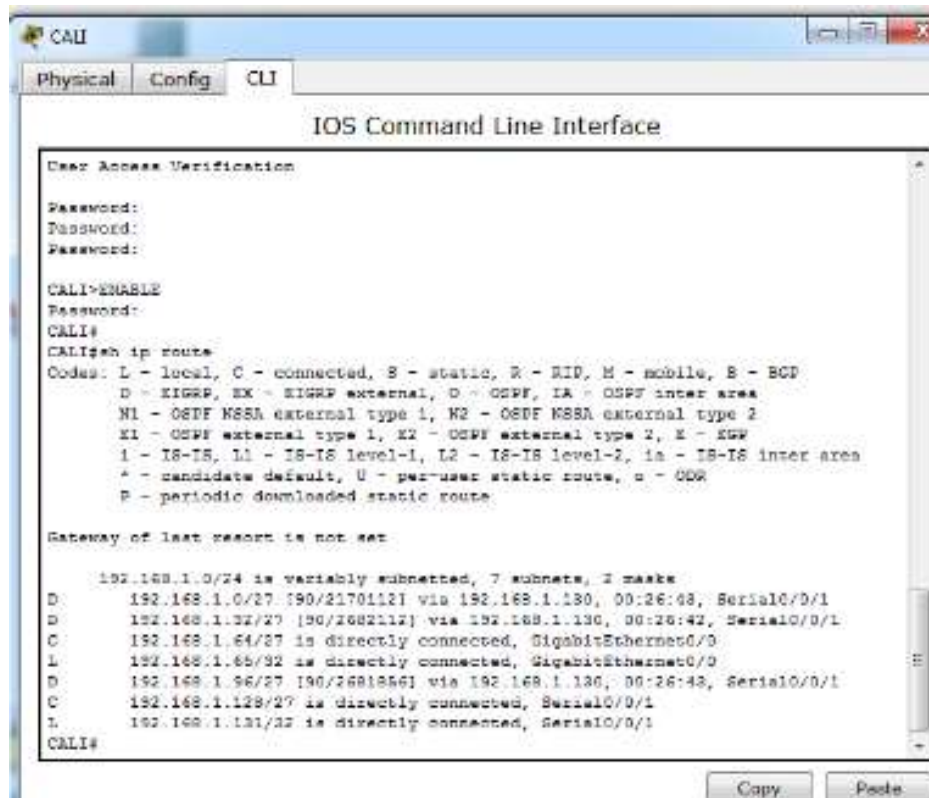


Ilustración 9 conexion de equipos.

Fuente: freydy, p. (8 de diciembre de 2019). Prueba de configuración de la seguridad con sus respectiva clave y direcciones ip configuradas en la topología. Obtenido de packet tracer autoría propia.

b. Verificar el balanceo de carga que presentan los routers. Ver ilustracion 10



```

CALI
Physical Config CLI
IOS Command Line Interface
User Access Verification
Password:
Password:
Password:
CALI>ENABLE
Password:
CALI#
CALI#sh ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
I - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default, U - per-user static route, s - ODR
P - periodic downloaded static route

Gateway of last resort is not set

192.168.1.0/24 is variably subnetted, 7 subnets, 2 masks
D    192.168.1.0/27 [90/2170112] via 192.168.1.130, 00:26:48, Serial0/0/1
D    192.168.1.32/27 [90/2682112] via 192.168.1.130, 00:26:42, Serial0/0/1
C    192.168.1.64/27 is directly connected, GigabitEthernet0/0
L    192.168.1.65/32 is directly connected, GigabitEthernet0/0
D    192.168.1.96/27 [90/2681856] via 192.168.1.130, 00:26:43, Serial0/0/1
C    192.168.1.128/27 is directly connected, Serial0/0/1
L    192.168.1.131/32 is directly connected, Serial0/0/1
CALI#
Copy Paste

```

Ilustración 10 balanceo de carga

c. Realizar un diagnóstico de vecinos usando el comando cdp. En el router se asigna la palabra show cdp neighbors. Ver resultados ilustracion. 11, 12, y 13.



```
BOGOTA
Physical Config CLI
IOS Command Line Interface

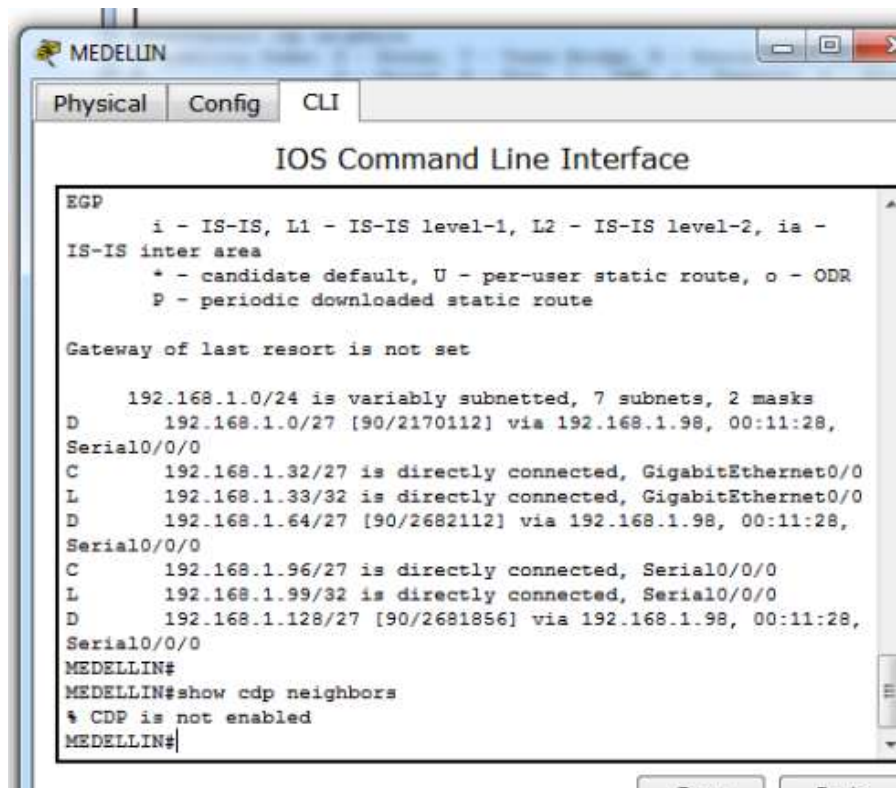
% Invalid input detected at ... marker.
BOGOTA#sh cdp neighbors
% Invalid input detected at ... marker.

BOGOTA#
BOGOTA#
BOGOTA#
BOGOTA#
BOGOTA#
BOGOTA#
BOGOTA#
BOGOTA#show cdp neighbors
% Invalid input detected at ... marker.

BOGOTA#show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, S - Source Route Bridge
                  B - Switch, H - Host, I - IGMP, s - Repeater, P - Phone
Device ID      Local Interface  Holdtime  Capability  Platform  Port ID
-----
BOGOTA#
```

Ilustración 11 cdp bogota.

Fuente: freydy, p. (8 de diciembre de 2019). Prueba de configuración del cdp en Bogotá. Tiene un vecino Obtenido de packet tracer autoría propia.



```
MEDELLIN
Physical Config CLI
IOS Command Line Interface

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

  192.168.1.0/24 is variably subnetted, 7 subnets, 2 masks
D    192.168.1.0/27 [90/2170112] via 192.168.1.98, 00:11:28,
Serial0/0/0
C    192.168.1.32/27 is directly connected, GigabitEthernet0/0
L    192.168.1.33/32 is directly connected, GigabitEthernet0/0
D    192.168.1.64/27 [90/2682112] via 192.168.1.98, 00:11:28,
Serial0/0/0
C    192.168.1.96/27 is directly connected, Serial0/0/0
L    192.168.1.99/32 is directly connected, Serial0/0/0
D    192.168.1.128/27 [90/2681856] via 192.168.1.98, 00:11:28,
Serial0/0/0
MEDELLIN#
MEDELLIN#show cdp neighbors
% CDP is not enabled
MEDELLIN#
```

Ilustración 12 cdp medellin.

Fuente: freydy, p. (8 de diciembre de 2019). Prueba de configuración del cdp en medellin. No tiene vecino Obtenido de packet tracer autoría propia.

```
172.168.1.101/24 is directly connected, Serial0/0/1
CALI#
CALI#
CALI#
CALI#
CALI#
CALI#
CALI#sh cdp neighbors
% CDP is not enabled
CALI#
CALI#
```

Ilustración 13 cdp cali

Fuente: freydy, p. (8 de diciembre de 2019). Prueba de configuración del cdp en cali. No tiene vecino Obtenido de packet tracer autoría propia.

d. Realizar una prueba de conectividad en cada tramo de la ruta usando Ping.ver ilustracion (14 y 15.) donde e evidencia la conexión de todos los dispositivos de la red.

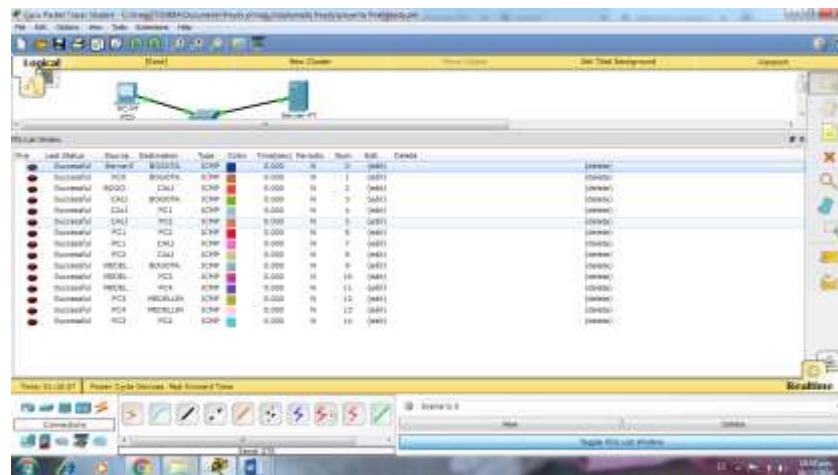


Ilustración 14 conectividad de los equipos.

Fuente: freydy, p. (8 de diciembre de 2019). Prueba de configuración y de conectividad mediante un ping en los dispositivos de la red.. No tiene vecino Obtenido de packet tracer autoría propia.

| Fire | Last Status | Source | Destination | Type | Color | Time(sec) | Periodic | Num | Edit | Delete |
|------|-------------|----------|-------------|------|-------|-----------|----------|-----|--------|--------|
| | Successful | Server0 | BOGOTA. | ICMP | | 0.000 | N | 0 | (edit) | |
| | Successful | PC0 | BOGOTA. | ICMP | | 0.000 | N | 1 | (edit) | |
| | Successful | BOGO... | CALI | ICMP | | 0.000 | N | 2 | (edit) | |
| | Successful | CALI | BOGOTA. | ICMP | | 0.000 | N | 3 | (edit) | |
| | Successful | CALI | PC1 | ICMP | | 0.000 | N | 4 | (edit) | |
| | Successful | CALI | PC2 | ICMP | | 0.000 | N | 5 | (edit) | |
| | Successful | PC1 | PC2 | ICMP | | 0.000 | N | 6 | (edit) | |
| | Successful | PC1 | CALI | ICMP | | 0.000 | N | 7 | (edit) | |
| | Successful | PC2 | CALI | ICMP | | 0.000 | N | 8 | (edit) | |
| | Successful | MEDEL... | BOGOTA. | ICMP | | 0.000 | N | 9 | (edit) | |
| | Successful | MEDEL... | PC3 | ICMP | | 0.000 | N | 10 | (edit) | |
| | Successful | MEDEL... | PC4 | ICMP | | 0.000 | N | 11 | (edit) | |
| | Successful | PC3 | MEDELLIN | ICMP | | 0.000 | N | 12 | (edit) | |
| | Successful | PC4 | MEDELLIN | ICMP | | 0.000 | N | 13 | (edit) | |
| | Successful | PC3 | PC4 | ICMP | | 0.000 | N | 14 | (edit) | |

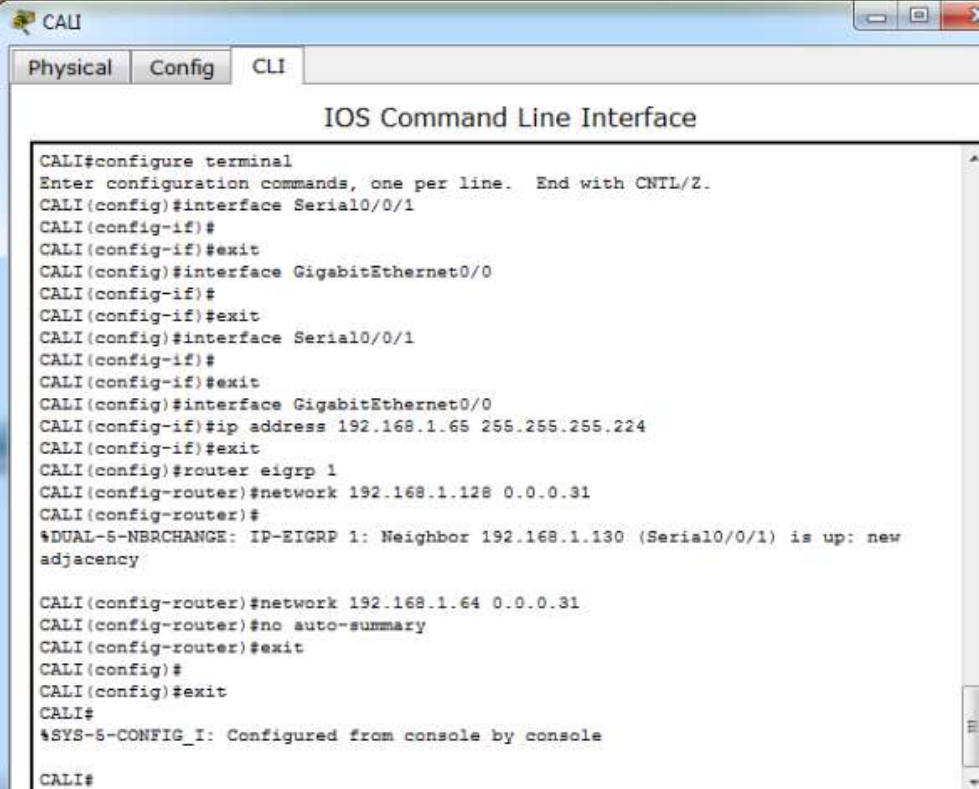
Ilustración 15 conectividad de los equipos.

Fuente: freydy, p. (8 de diciembre de 2019). Prueba de configuración y de conectividad mediante un ping en los dispositivos de la red.. No tiene vecino Obtenido de packet tracer autoría propia.

Parte 3: Configuración de Enrutamiento.

a. Asignar el protocolo de enrutamiento EIGRP a los routers considerando el direccionamiento diseñado. Para designar el eigrp se configura directamente del router y se tiene en cuenta las direcciones ip que implican a ese router , además se le asigna la wirecard.en este caso es de 0.0.0.31 (ver ilustración 16.)

| BOGOTÁ | MEDELLÍN | CALI. |
|--|--|---|
| <pre> UNAD = clave asignada Enable. UNAD. bogota# configure terminal. bogota(config)# router eigrp 1 bogota(config-router)# network 192.168.1.128 0.0.0.31 bogota(config-router)# network 192.168.1.96 0.0.0.31 bogota(config-router)# network 192.168.1.0 0.0.0.31 bogota(config-router)#no auto-sumary bogota(config-router)#exit bogota(config)#exit bogota# </pre> | <pre> UNAD = clave asignada Enable. UNAD. medellin# configure terminal. medellin(config)# router eigrp 1 medellin(config-router)# network 192.168.1.32 0.0.0.31 medellin(config-router)# network 192.168.1.96 0.0.0.31 medellin(config-router)#no auto-sumary medellin(config-router)#exit medellin(config)#exit medellin# </pre> | <pre> UNAD = clave asignada Enable. UNAD. cali# configure terminal. cali(config)# router eigrp 1 cali(config-router)# network 192.168.1.128 0.0.0.31 cali(config-router)# network 192.168.1.64 0.0.0.31 cali(config-router)#no auto-sumary cali(config-router)#exit cali(config)#exit cali# </pre> |



```
CALI
Physical Config CLI
IOS Command Line Interface
CALI#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
CALI(config)#interface Serial0/0/1
CALI(config-if)#
CALI(config-if)#exit
CALI(config)#interface GigabitEthernet0/0
CALI(config-if)#
CALI(config-if)#exit
CALI(config)#interface Serial0/0/1
CALI(config-if)#
CALI(config-if)#exit
CALI(config)#interface GigabitEthernet0/0
CALI(config-if)#ip address 192.168.1.65 255.255.255.224
CALI(config-if)#exit
CALI(config)#router eigrp 1
CALI(config-router)#network 192.168.1.128 0.0.0.31
CALI(config-router)#
%DUAL-5-NBRCHANGE: IP-EIGRP 1: Neighbor 192.168.1.130 (Serial0/0/1) is up: new adjacency
CALI(config-router)#network 192.168.1.64 0.0.0.31
CALI(config-router)#no auto-summary
CALI(config-router)#exit
CALI(config)#
CALI(config)#exit
CALI#
%SYS-5-CONFIG_I: Configured from console by console
CALI#
```

Ilustración 16 verificación del eigrp

Fuente: freydy, p. (8 de diciembre de 2019). Prueba de configuración y de conectividad de los eigrp Obtenido de packet tracer autoría propia.

b. Realizar la comprobación de las tablas de enrutamiento en cada uno de los routers para verificar cada una de las rutas establecidas. Ver ilustración 17,18 y 19

```
BOGOTA
Physical Config CLI
IOS Command Line Interface
Password:
BOGOTA>ENAB
Password:
BOGOTA#SH IP ROUTER
^
% Invalid input detected at '^' marker.
BOGOTA#sh ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
        D - EIGRP, EK - 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

192.168.1.0/24 is variably subnetted, 8 subnets, 2 masks
C       192.168.1.0/27 is directly connected, GigabitEthernet0/0
L       192.168.1.1/32 is directly connected, GigabitEthernet0/0
D       192.168.1.32/27 [90/2170112] via 192.168.1.99, 00:09:39, Serial0/0/0
D       192.168.1.64/27 [90/2170112] via 192.168.1.131, 00:09:37, Serial0/0/1
C       192.168.1.96/27 is directly connected, Serial0/0/0
L       192.168.1.98/32 is directly connected, Serial0/0/0
C       192.168.1.128/27 is directly connected, Serial0/0/1
L       192.168.1.130/32 is directly connected, Serial0/0/1
BOGOTA#
```

Ilustración 17 enrutamiento router bogota.

Fuente: freydy, p. (8 de diciembre de 2019). Prueba de configuración y de conectividad de las rutas de los routers. Obtenido de packet tracer autoría propia.

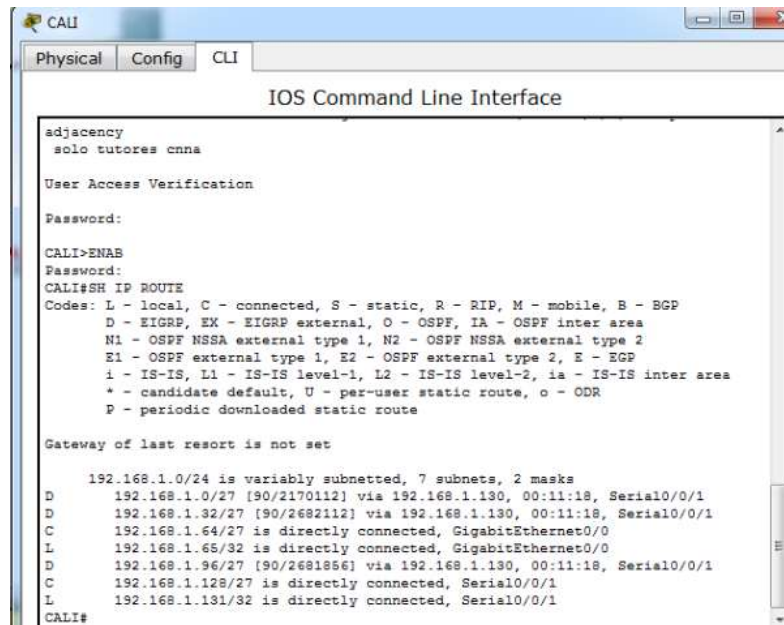
```
MEDELLIN
Physical Config CLI
IOS Command Line Interface
sujelemmy
solo tutores cmts
User Access Verification
Password:
MEDELLIN>ENAB
Password:
MEDELLIN#sh ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
        D - EIGRP, EK - EIGRP external, O - OSPF, IA - OSPF 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

192.168.1.0/24 is variably subnetted, 7 subnets, 2 masks
D       192.168.1.0/27 [90/2170112] via 192.168.1.99, 00:10:47, Serial0/0/0
C       192.168.1.32/27 is directly connected, GigabitEthernet0/0
L       192.168.1.33/32 is directly connected, GigabitEthernet0/0
D       192.168.1.64/27 [90/2682112] via 192.168.1.99, 00:10:44, Serial0/0/0
C       192.168.1.96/27 is directly connected, Serial0/0/0
L       192.168.1.99/32 is directly connected, Serial0/0/0
D       192.168.1.128/27 [90/2681856] via 192.168.1.99, 00:10:47, Serial0/0/0
MEDELLIN#
```

Ilustración 18 enrutamiento de medellin.

Fuente: freydy, p. (8 de diciembre de 2019). Prueba de configuración y de conectividad de las rutas de los routers. Obtenido de packet tracer autoría propia.



```
adjacency
solo tutores cnna

User Access Verification

Password:

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

Gateway of last resort is not set

      192.168.1.0/24 is variably subnetted, 7 subnets, 2 masks
D       192.168.1.0/27 [90/2170112] via 192.168.1.130, 00:11:18, Serial0/0/1
D       192.168.1.32/27 [90/2682112] via 192.168.1.130, 00:11:18, Serial0/0/1
C       192.168.1.64/27 is directly connected, GigabitEthernet0/0
L       192.168.1.65/32 is directly connected, GigabitEthernet0/0
D       192.168.1.96/27 [90/2681856] via 192.168.1.130, 00:11:18, Serial0/0/1
C       192.168.1.128/27 is directly connected, Serial0/0/1
L       192.168.1.131/32 is directly connected, Serial0/0/1
CALI#
```

Ilustración 19 enrutamiento de cali

Fuente: freydy, p. (8 de diciembre de 2019). Prueba de configuración y de conectividad de las rutas de los routers. Obtenido de packet tracer autoría propia.

c. 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. Ver ilustración (21.22.23. y 24)

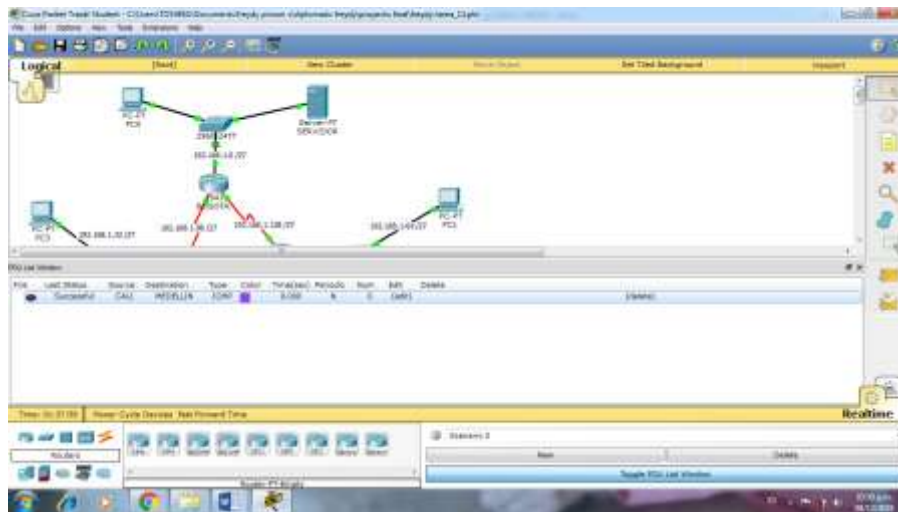


Ilustración 20 conexion de cali medellin.

Fuente: freydy, p. (8 de diciembre de 2019). Prueba de configuración y de conectividad d de Medellín con Cali exitosa. Obtenido de packet tracer autoría propia.

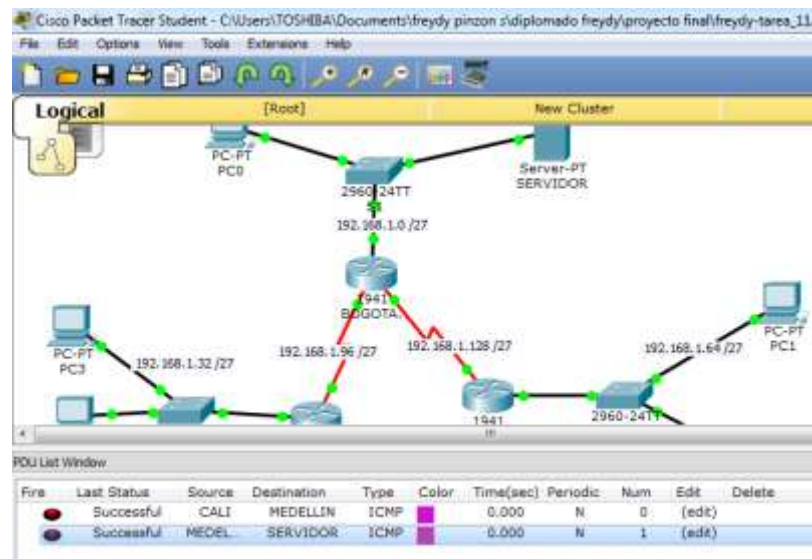


Ilustración 21 medellin - servidor.

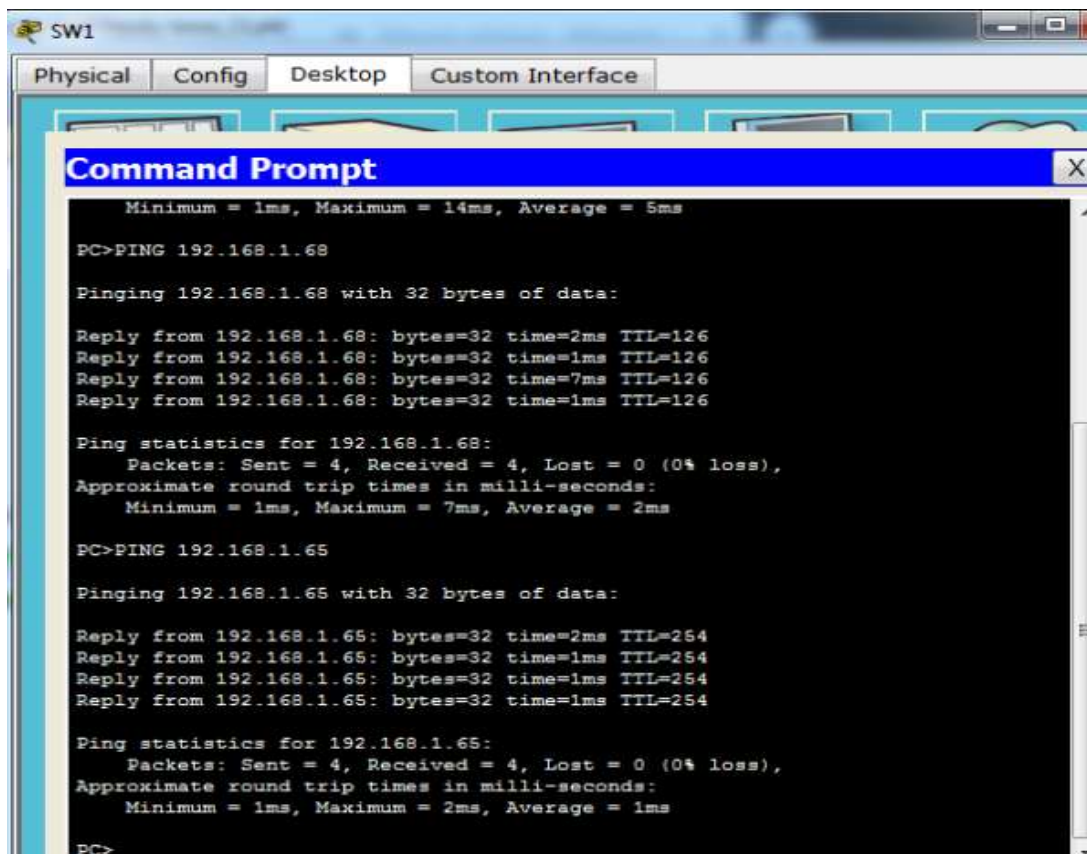
Fuente: freydy, p. (8 de diciembre de 2019). Prueba de configuración y de conectividad d de Medellín con servidor exitosa. Obtenido de packet tracer autoría propia.

En esta imagen cuando se probó la conectividad no se cambió el nombre del computador PC-O por SW-1 por lo tanto PC-0 reemplaza SW-1

| Fire | Last Status | Source | Destination | Type | Color | Time(sec) | Periodic | Num | Edit | Delete |
|------|-------------|----------|-------------|------|-------|-----------|----------|-----|--------|--------|
| | Successful | CALI | MEDELLIN | ICMP | | 0.000 | N | 0 | (edit) | |
| | Successful | MEDEL... | SERVIDOR | ICMP | | 0.000 | N | 1 | (edit) | |
| | Successful | PC0 | PC2 | ICMP | | 0.000 | N | 2 | (edit) | |
| | Successful | PC1 | PC2 | ICMP | | 0.000 | N | 3 | (edit) | |
| | Successful | PC1 | PC3 | ICMP | | 0.000 | N | 4 | (edit) | |
| | Successful | PC1 | PC4 | ICMP | | 0.000 | N | 5 | (edit) | |
| | Successful | PC0 | PC3 | ICMP | | 0.000 | N | 6 | (edit) | |
| | Successful | PC0 | PC4 | ICMP | | 0.000 | N | 7 | (edit) | |
| | Successful | PC2 | CALI | ICMP | | 0.000 | N | 8 | (edit) | |
| | Successful | CALI | BOGOTA. | ICMP | | 0.000 | N | 9 | (edit) | |
| | Successful | BOGO... | MEDELLIN | ICMP | | 0.000 | N | 10 | (edit) | |
| | Successful | MEDEL... | PC4 | ICMP | | 0.000 | N | 11 | (edit) | |
| | Successful | BOGO... | PC2 | ICMP | | 0.000 | N | 12 | (edit) | |
| | Successful | BOGO... | PC4 | ICMP | | 0.000 | N | 13 | (edit) | |
| | Successful | BOGO... | PC3 | ICMP | | 0.000 | N | 14 | (edit) | |

Ilustración 22 conexion de todos los dispositivos.

Fuente: freydy, p. (8 de diciembre de 2019). Prueba de configuración y de conectividad d detodos los elementos .. Obtenido de packet tracer autoría propia.



```
SW1
Physical Config Desktop Custom Interface

Command Prompt
Minimum = 1ms, Maximum = 14ms, Average = 5ms
PC>PING 192.168.1.68
Pinging 192.168.1.68 with 32 bytes of data:
Reply from 192.168.1.68: bytes=32 time=2ms TTL=126
Reply from 192.168.1.68: bytes=32 time=1ms TTL=126
Reply from 192.168.1.68: bytes=32 time=7ms TTL=126
Reply from 192.168.1.68: bytes=32 time=1ms TTL=126
Ping statistics for 192.168.1.68:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 7ms, Average = 2ms
PC>PING 192.168.1.65
Pinging 192.168.1.65 with 32 bytes of data:
Reply from 192.168.1.65: bytes=32 time=2ms TTL=254
Reply from 192.168.1.65: bytes=32 time=1ms TTL=254
Reply from 192.168.1.65: bytes=32 time=1ms TTL=254
Reply from 192.168.1.65: bytes=32 time=1ms TTL=254
Ping statistics for 192.168.1.65:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 2ms, Average = 1ms
PC>
```

Ilustración 23 conexión sw1

Fuente: freydy, p. (8 de diciembre de 2019). Prueba de configuración y de conectividad la computadora SW1 con los equipos que están conectados al router de cali. Obtenido de packet tracer autoría propia.

```
SW1
Physical Config Desktop Custom Interface

Command Prompt
Minimum = 1ms, Maximum = 12ms, Average = 8ms

PC>PING 192.168.1.36

Pinging 192.168.1.36 with 32 bytes of data:

Reply from 192.168.1.36: bytes=32 time=1ms TTL=126
Reply from 192.168.1.36: bytes=32 time=1ms TTL=126
Reply from 192.168.1.36: bytes=32 time=4ms TTL=126
Reply from 192.168.1.36: bytes=32 time=11ms TTL=126

Ping statistics for 192.168.1.36:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 11ms, Average = 4ms

PC>PING 192.168.1.34

Pinging 192.168.1.34 with 32 bytes of data:

Request timed out.
Reply from 192.168.1.34: bytes=32 time=11ms TTL=126
Reply from 192.168.1.34: bytes=32 time=1ms TTL=126
Reply from 192.168.1.34: bytes=32 time=1ms TTL=126

Ping statistics for 192.168.1.34:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 11ms, Average = 4ms

PC>|
```

Ilustración 24 conexión sw1

Fuente: freydy, p. (8 de diciembre de 2019). Prueba de configuración y de conectividad mediante un ping de la computadora SW1 con los equipos que están conectados al router de medellin. Obtenido de packet tracer autoría propia.

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.

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. (Ver ilustración 25 y 26)

UNAD = clave asignada

Enable.

UNAD.

bogota# configure terminal.

bogota(config)# access-list 1 deny 192.168.1.3

bogota(config)# access-list 1 permit any

bogota(config)# int g0/0

bogota(config-if)# ip access-group 1 in

bogota(config-if)#exit

bogota(config)#exit

bogota#

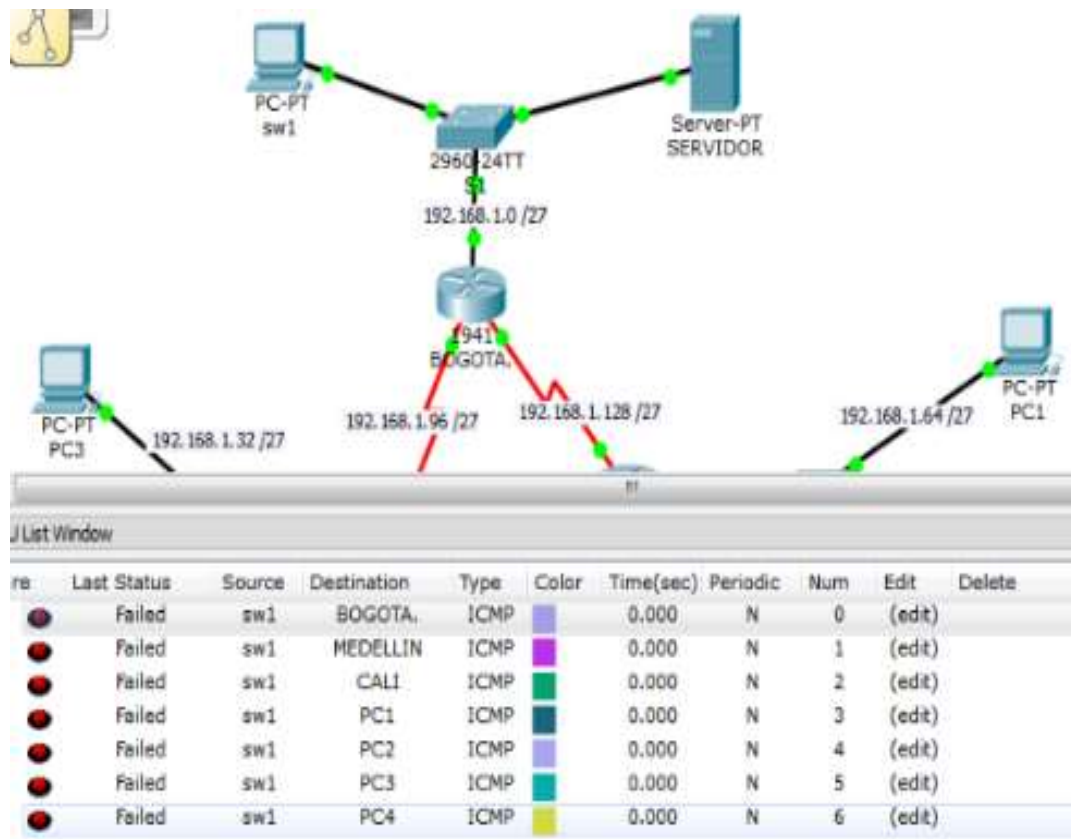


Ilustración 25 sw1 ping a los demas equipos.

Fuente: freydy, p. (8 de diciembre de 2019). Prueba de configuración y de conectividad mediante un ping de la computadora SW1 con los equipos que están conectados donde el acceso de la lista creada funciona exitosamente y no establece conexión con ninguno. Obtenido de packet tracer autoría propia.

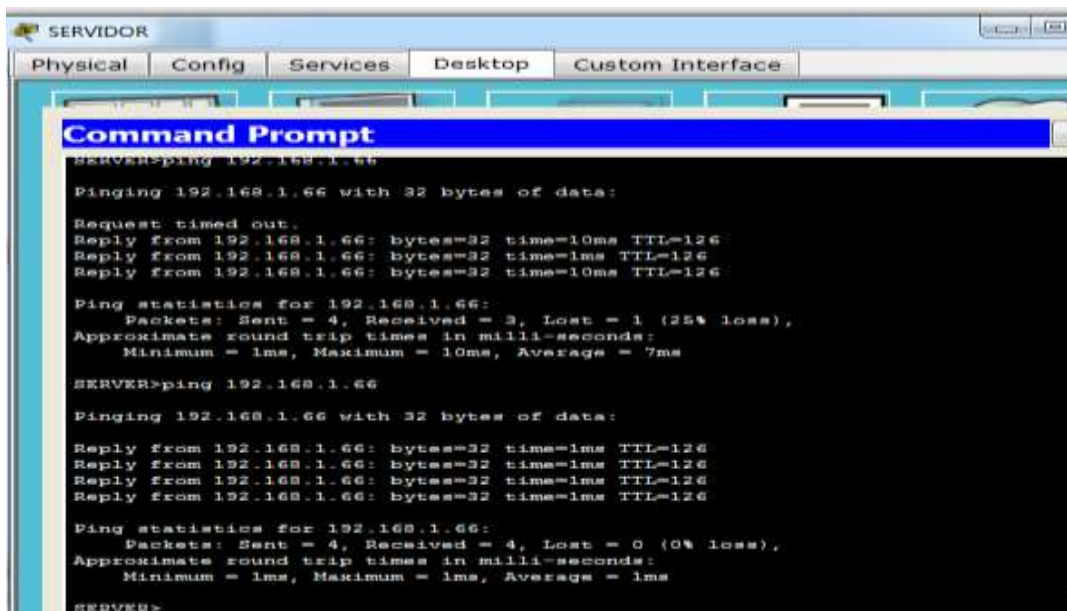
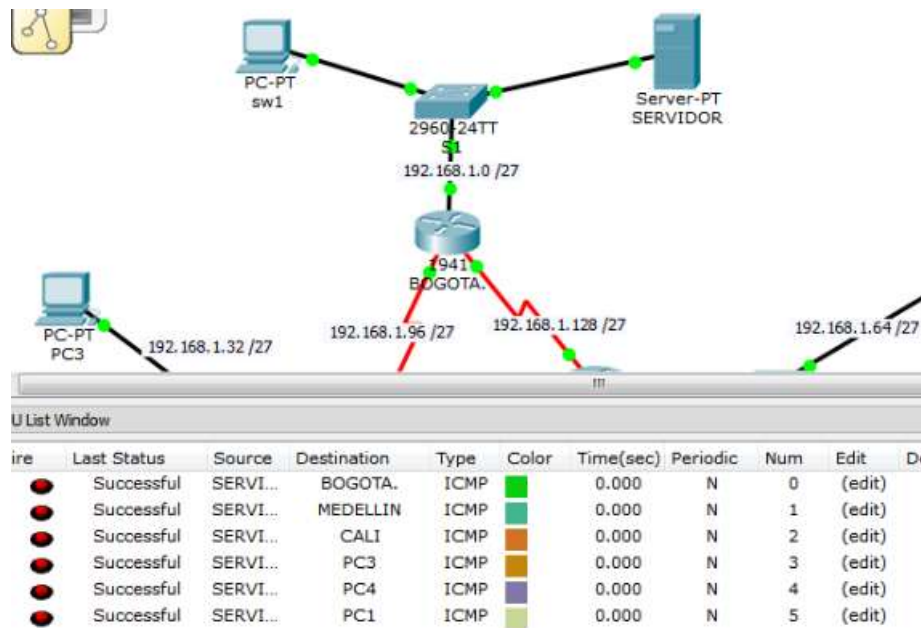


Ilustración 26 conexion servidor.

Fuente: freydy, p. (8 de diciembre de 2019). Prueba de configuración y de conectividad mediante un ping de la computadora servidor con los equipos que están conectados y fue exitoso con la conexión a los demás.. Obtenido de packet tracer autoría propia.

a. 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.

| | | |
|--|--|---|
| <pre> UNAD = clave asignada Enable. UNAD. bogota# configure terminal. bogota(config)# access-list 1 deny 192.168.1.68 bogota(config)# access-list 1 permit any bogota(config)# int s0/0/0 bogota(config-if)# ip access-group 1 out bogota(config-if)#exit bogota(config)#exit </pre> | <pre> UNAD = clave asignada Enable. UNAD. medellin# configure terminal. medellin(config)# access-list 1 deny 192.168.1.66 medellin(config)# access-list 1 permit any medellin(config)# int s0/0/0 medellin(config-if)# ip access-group 1 in medellin(config-if)#exit medellin(config)#exit medellin # </pre> | <pre> UNAD = clave asignada Enable. UNAD. cali# configure terminal. cali(config)# access-list 1 deny 192.168.1.36 cali(config)# access-list 1 permit any cali(config)# int s0/0/1 cali(config-if)# ip access-group 1 in cali(config-if)#exit cali(config)#exit </pre> |
|--|--|---|

| | | |
|--|--|--------------|
| bogota# UNAD = clave asignada Enable. UNAD. bogota# configure terminal. bogota(config)# access-list 78 deny 192.168.1.34 bogota(config)# access-list 78 permit any bogota(config)# int s0/0/1 bogota(config-if)# ip access-group 78 out bogota(config-if)#exit bogota(config)#exit bogota# | | cali# |
|--|--|--------------|

Parte 5: Comprobación de la red instalada.

a. Se debe probar que la configuración de las listas de acceso fue exitosa. Se comprueba que los router Medellín y Cali solo pueden acceder a sus equipos de su misma red pero no a los demás. (Ver ilustración 27 y 28.)

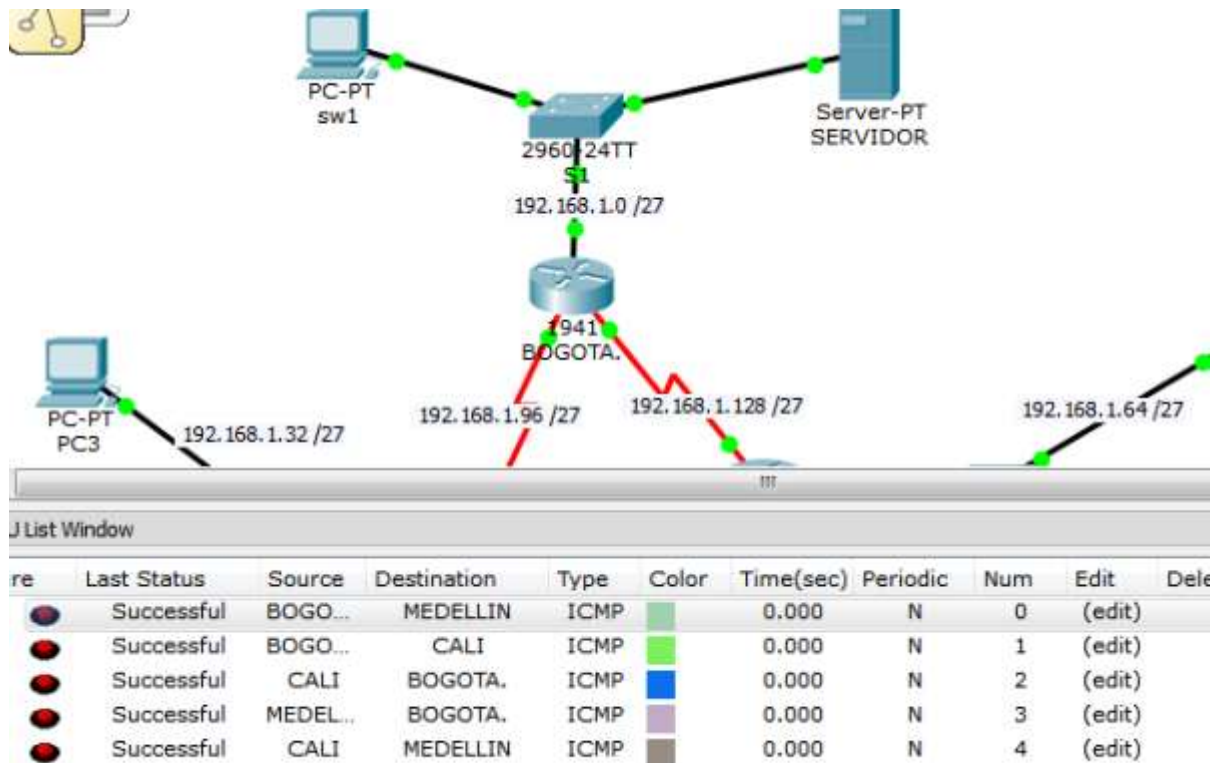


Ilustración 27 conexión router.

Fuente: freydy, p. (8 de diciembre de 2019). Prueba de configuración y de conectividad mediante un ping de los router fue exitoso con la conexión..
Obtenido de packet tracer autoría propia.

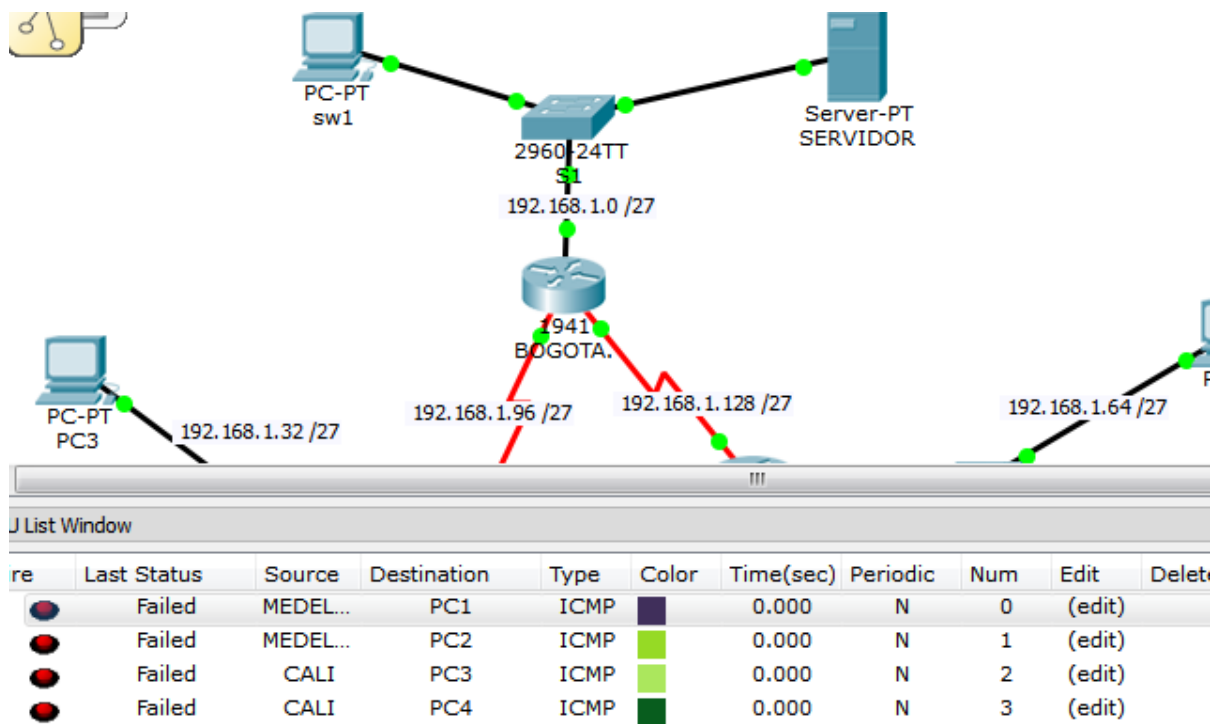


Ilustración 28 equipo de los router.

Fuente: freydy, p. (8 de diciembre de 2019). Prueba de configuración y de conectividad mediante un ping de los router fue exitoso con la conexión pero los router no pueden conectarse a los equipos que no pertenece a su subred.. Obtenido de packet tracer autoría propia.

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 | exitoso |
| | WS_1 | Router BOGOTA | fallo |
| | Servidor | Router CALI | EXITOSO |
| | Servidor | Router MEDELLIN | EXITOSO |

| | | | |
|---------------|------------------------------------|------------------------------------|-----------------------------|
| TELNET | LAN del Router MEDELLIN | Router CALI | RESPONDE |
| | LAN del Router CALI | Router CALI | RESPONDE |
| | LAN del Router MEDELLIN | Router MEDELLIN | EXITOSO |
| | LAN del Router CALI | Router MEDELLIN | EXITOSO |
| PING | LAN del Router CALI | WS_1 | fallo |
| | LAN del Router MEDELLIN | WS_1 | fallo |
| | LAN del Router MEDELLIN | LAN del Router CALI | Conexión estable |
| PING | LAN del Router CALI | Servidor | Conexión estable |
| | LAN del Router MEDELLIN | Servidor | Conexión estable |
| | Servidor | LAN del Router MEDELLIN | Conexión estable |
| | Servidor | LAN del Router CALI | Conexión estable |
| | Router CALI | LAN del Router MEDELLIN | Conexión estable |
| | Router MEDELLIN | LAN del Router CALI | Conexión estable |

Comprobacion e las telnet.

```
MEDELLIN
Physical Config CLI
IOS Command Line Interface

Password:
MEDELLIN#PING 192.168.1.96

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.96, timeout is 2 seconds:
.
Reply to request 0 from 192.168.1.98, 18 ms
Reply to request 1 from 192.168.1.98, 34 ms
Reply to request 2 from 192.168.1.98, 1 ms
Reply to request 3 from 192.168.1.98, 1 ms
Reply to request 4 from 192.168.1.98, 16 ms

MEDELLIN#TELNET 192.168.1.65
Trying 192.168.1.65 ...Open solo tutores cnna

User Access Verification

Password:
CALI>ENABLE
Password:
CALI#
CALI#
```

Ilustración 29 Medellín- Cali

Fuente: freydy, p. (8 de diciembre de 2019). Prueba de configuración y de conectividad mediante un ping de los router fue exitoso .Obtenido de packet tracer autoría propia.

```
sw1
Physical Config Desktop Custom Interface

Command Prompt

Packet Tracer PC Command Line 1.0
PC>telnet 192.168.1.1
Trying 192.168.1.1 ...
% Connection timed out; remote host not responding
PC>
```

Ilustración 30 sw-1 – Bogotá

Fuente: freydy, p. (8 de diciembre de 2019). Prueba de configuración y de conectividad mediante un ping de los router presenta falla.Obtenido de packet tracer autoría propia.

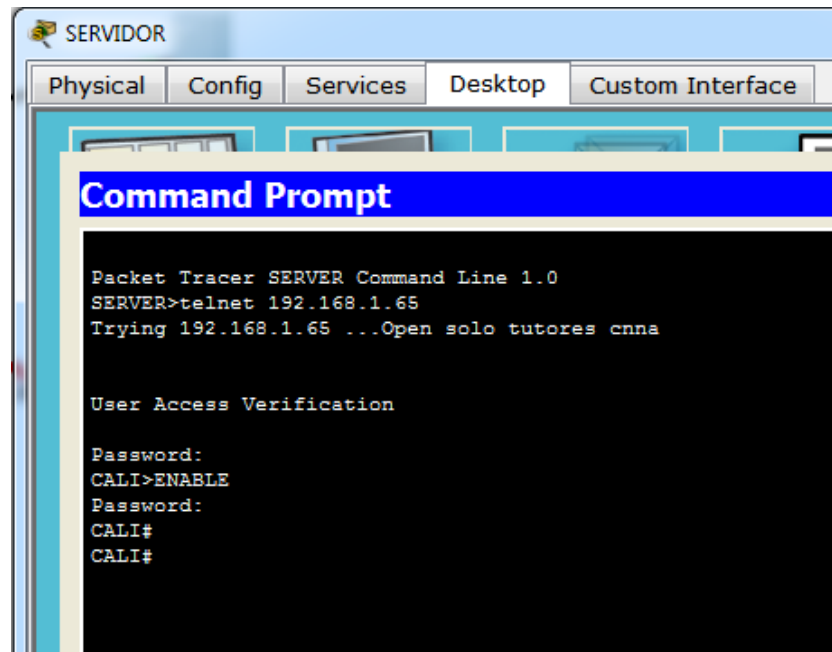


Ilustración 31 servidor –Cali

Fuente: freydy, p. (8 de diciembre de 2019). Prueba de configuración y de conectividad mediante un ping de los router fue exitoso .Obtenido de packet tracer autoría propia.

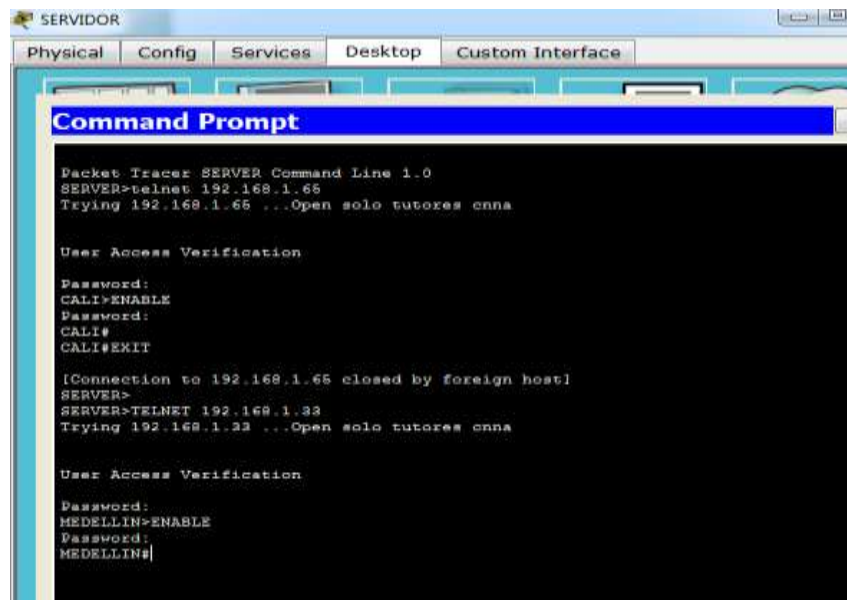


Ilustración 32 servidor- Medellín.

Fuente: freydy, p. (8 de diciembre de 2019). Prueba de configuración y de conectividad mediante un ping de los router fue exitoso. Obtenido de packet tracer autoría propia.

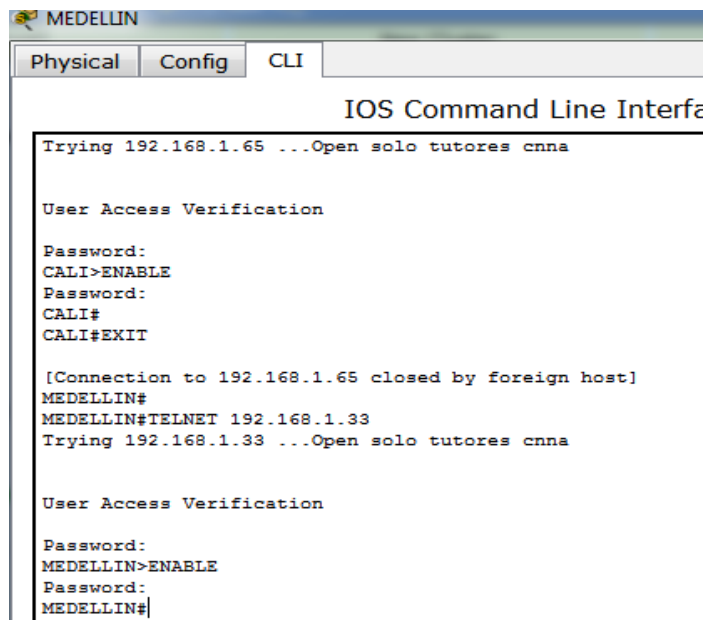
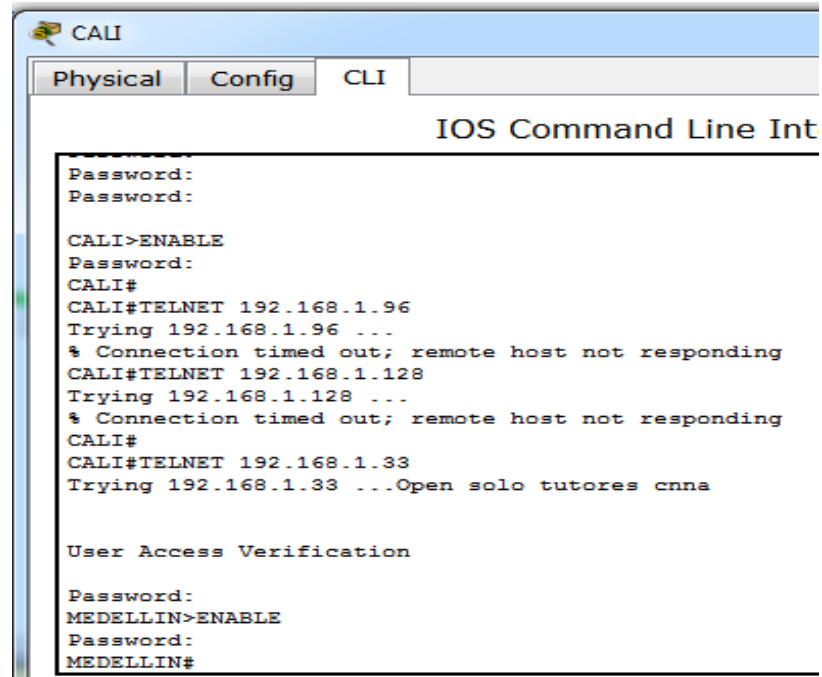


Ilustración 33 medellin-medellin.

Fuente: freydy, p. (8 de diciembre de 2019). Prueba de configuración y de conectividad mediante un ping de los router fue exitoso .Obtenido de packet tracer autoría propia.



```

CALI
Physical Config CLI
IOS Command Line Int
Password:
Password:
CALI>ENABLE
Password:
CALI#
CALI#TELNET 192.168.1.96
Trying 192.168.1.96 ...
% Connection timed out; remote host not responding
CALI#TELNET 192.168.1.128
Trying 192.168.1.128 ...
% Connection timed out; remote host not responding
CALI#
CALI#TELNET 192.168.1.33
Trying 192.168.1.33 ...Open solo tutores cnna

User Access Verification
Password:
MEDELLIN>ENABLE
Password:
MEDELLIN#

```

Ilustración 34 cali- medellin

Fuente: freydy, p. (8 de diciembre de 2019). Prueba de configuración y de conectividad mediante un ping de los router fue exitoso .Obtenido de packet tracer autoría propia.

```
CALI
Physical Config CLI
IOS Command Line Interface
CALI#TELNET 192.168.1.128
Trying 192.168.1.128 ...
% Connection timed out; remote host not responding
CALI#
CALI#TELNET 192.168.1.33
Trying 192.168.1.33 ...Open solo tutores cnaa

User Access Verification

Password:
MEDELLIN>ENABLE
Password:
MEDELLIN#TELNET 192.168.1.65
Trying 192.168.1.65 ...Open solo tutores cnaa

User Access Verification

Password:
CALI>ENABLE
Password:
CALI#
```

Ilustración 35 cali – cali

Fuente: freydy, p. (8 de diciembre de 2019). Prueba de configuración y de conectividad mediante un ping de los router fue exitoso .Obtenido de packet tracer autoría propia.

```
MEDELLIN
Physical Config CLI
IOS Command Line Int
[Connection to 192.168.1.65 closed by foreign host]
MEDELLIN#
MEDELLIN#TELNET 192.168.1.33
Trying 192.168.1.33 ...Open solo tutores cnaa

User Access Verification

Password:
MEDELLIN>ENABLE
Password:
MEDELLIN#TELNET 192.168.1.65
Trying 192.168.1.65 ...Open solo tutores cnaa

User Access Verification

Password:
Password:
Password:
CALI>ENABLE
Password:
CALI#
```

Ilustración 36 medellin – cali

Fuente: freydy, p. (8 de diciembre de 2019). Prueba de configuración y de conectividad mediante un ping de los router fue exitoso .Obtenido de packet tracer autoría propia.

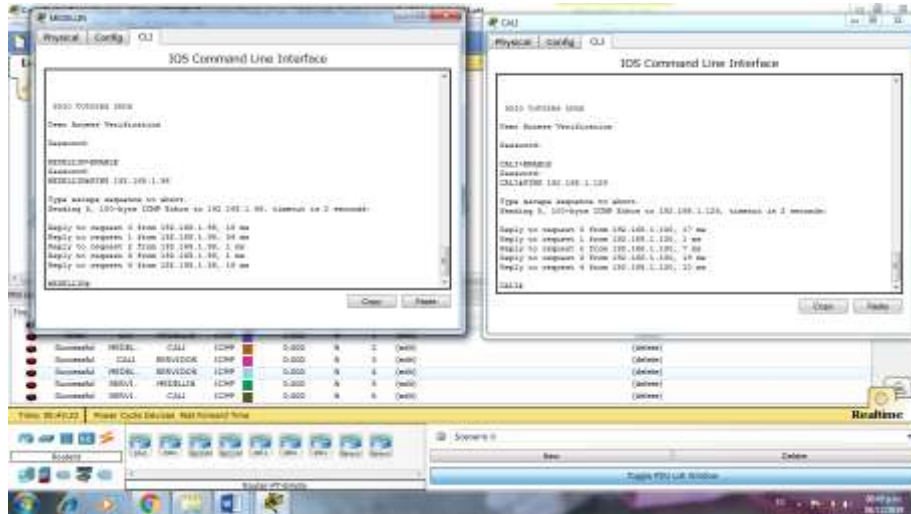


Ilustración 37 ping a lo equipo.

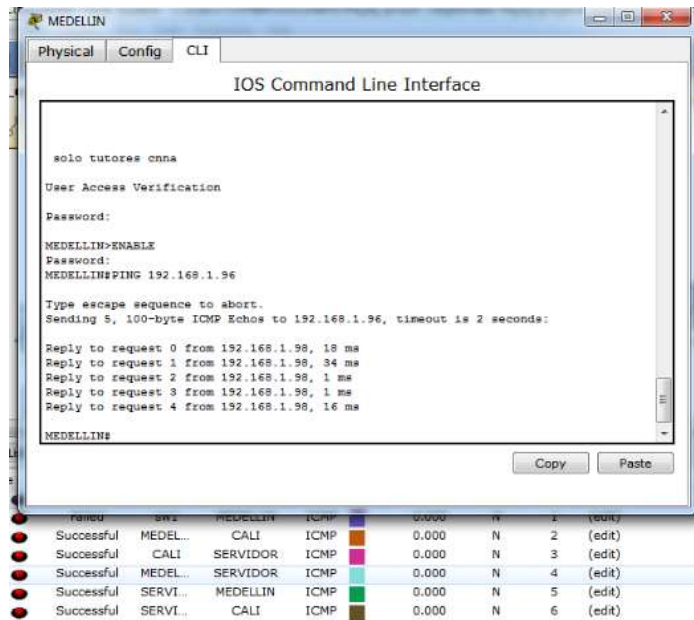
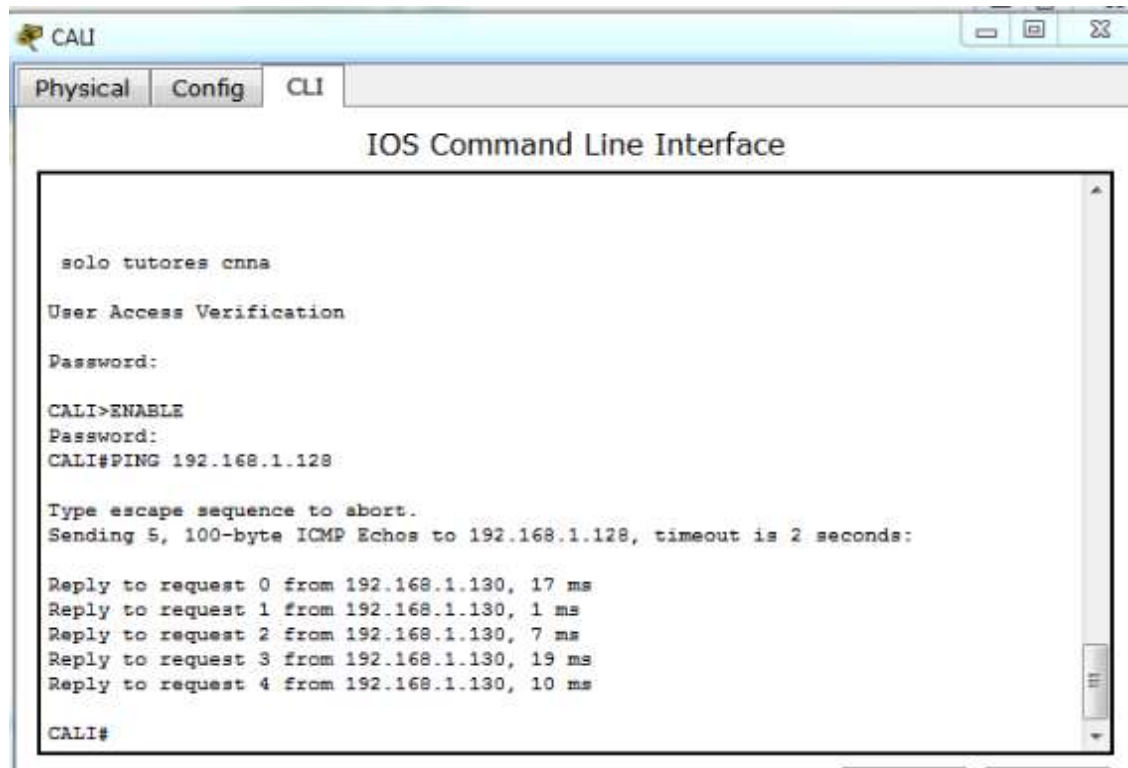


Ilustración 38 ping medellin



The screenshot shows a window titled "CALI" with three tabs: "Physical", "Config", and "CLI". The "CLI" tab is active, displaying the "IOS Command Line Interface". The terminal output is as follows:

```
solo tutores cnna
User Access Verification
Password:
CALI>ENABLE
Password:
CALI#PING 192.168.1.128

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.128, timeout is 2 seconds:

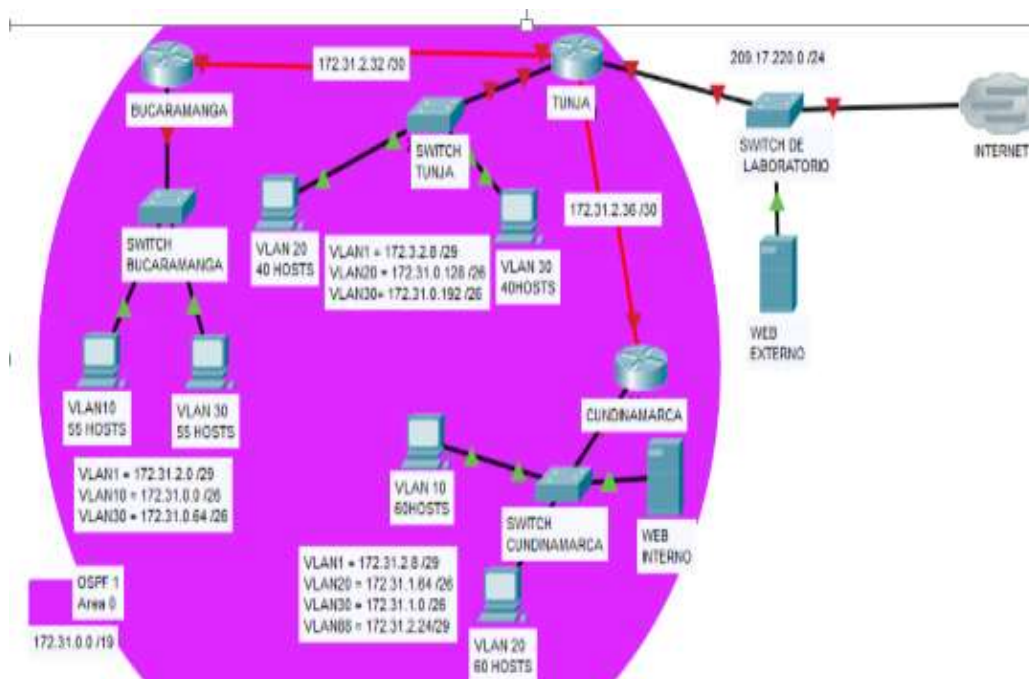
Reply to request 0 from 192.168.1.130, 17 ms
Reply to request 1 from 192.168.1.130, 1 ms
Reply to request 2 from 192.168.1.130, 7 ms
Reply to request 3 from 192.168.1.130, 19 ms
Reply to request 4 from 192.168.1.130, 10 ms

CALI#
```

Ilustración 39ping cali.

2. 1 Escenario 2

- 1 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.



- Password UNAD. Asignamos la clave
- Login iniciamos la configuración
- Exit salimos de la programación de la cosola 0
- Line vty 0 15
- Password UNAD. Asignamos la clave
- Login iniciamos la configuración
- Exit salimos de la programación
- Service password-encryption se habilita para la encriptación de la clave.
- Banner # se asigna un texto dentro los símbolos para que sea visualizado por todos.#
- Exit
- Copy running-config startup-config.

```

TUNJA
Physical Config CLI
IOS Command Line Interface

TUNJA(config)#enable secret UNAD
TUNJA(config)#exit
TUNJA#
%SYS-5-CONFIG_I: Configured from console by console

TUNJA#conf t
Enter configuration commands, one per line. End with CNTL/Z.
TUNJA(config)#line console 0
TUNJA(config-line)#password UNAD
TUNJA(config-line)#login
TUNJA(config-line)#exit
TUNJA(config)#line vty 0 15
TUNJA(config-line)#password UNAD
TUNJA(config-line)#login
~
% Invalid input detected at '^' marker.

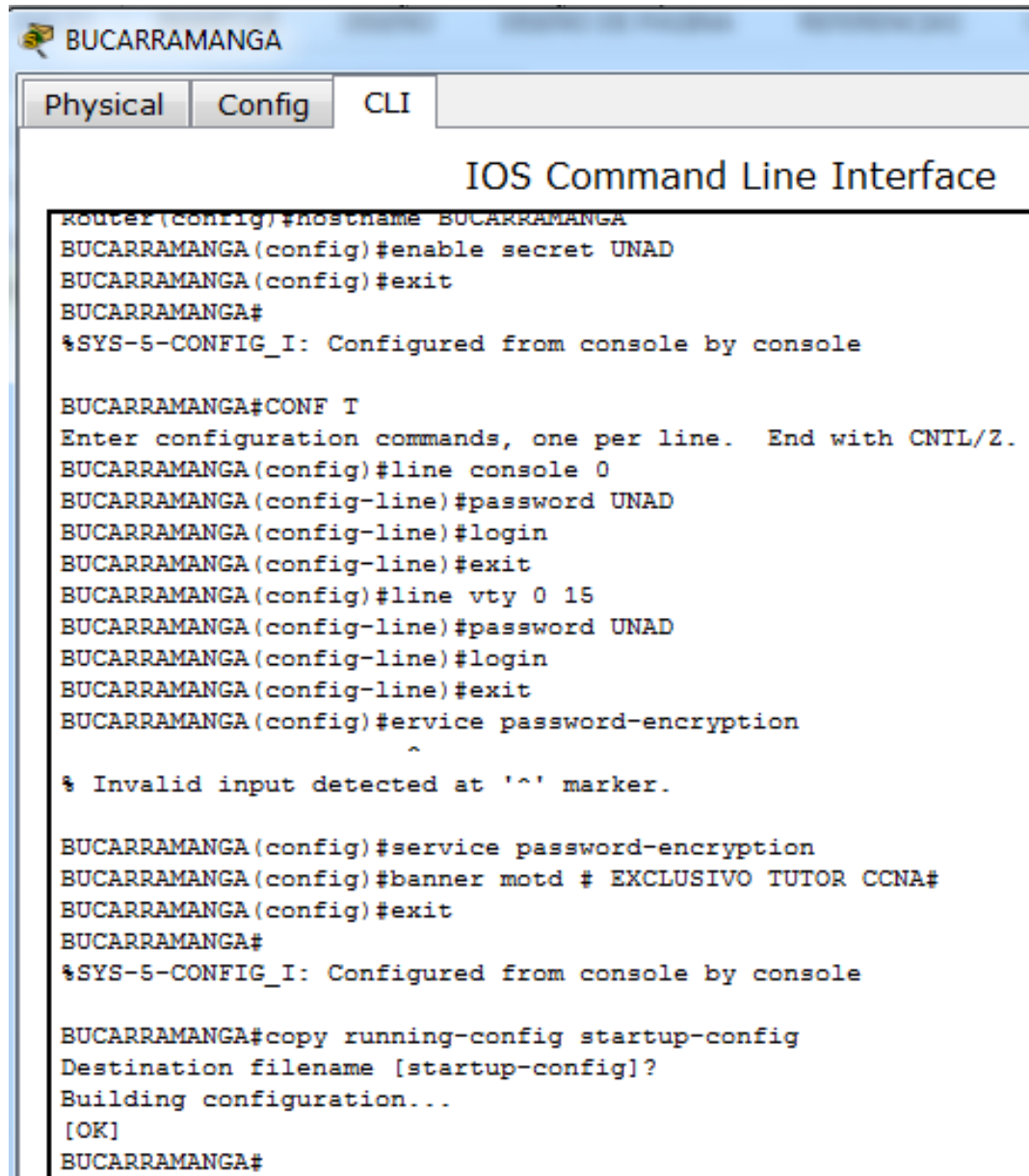
TUNJA(config-line)#login
TUNJA(config-line)#exit
TUNJA(config)#service password-encryption
TUNJA(config)#banner motd # EXCLUSIVO TUTOR CCNA#
TUNJA(config)#exit
TUNJA#
%SYS-5-CONFIG_I: Configured from console by console

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

```

Ilustración 41 configuración de seguridad

Fuente: freydy, p. (20 de diciembre de 2019). Aplicación de la configuración De seguridad Obtenido de packet tracer autoría propia.



```
Router (config)#hostname BUCARRAMANGA
BUCARRAMANGA (config)#enable secret UNAD
BUCARRAMANGA (config)#exit
BUCARRAMANGA#
%SYS-5-CONFIG_I: Configured from console by console

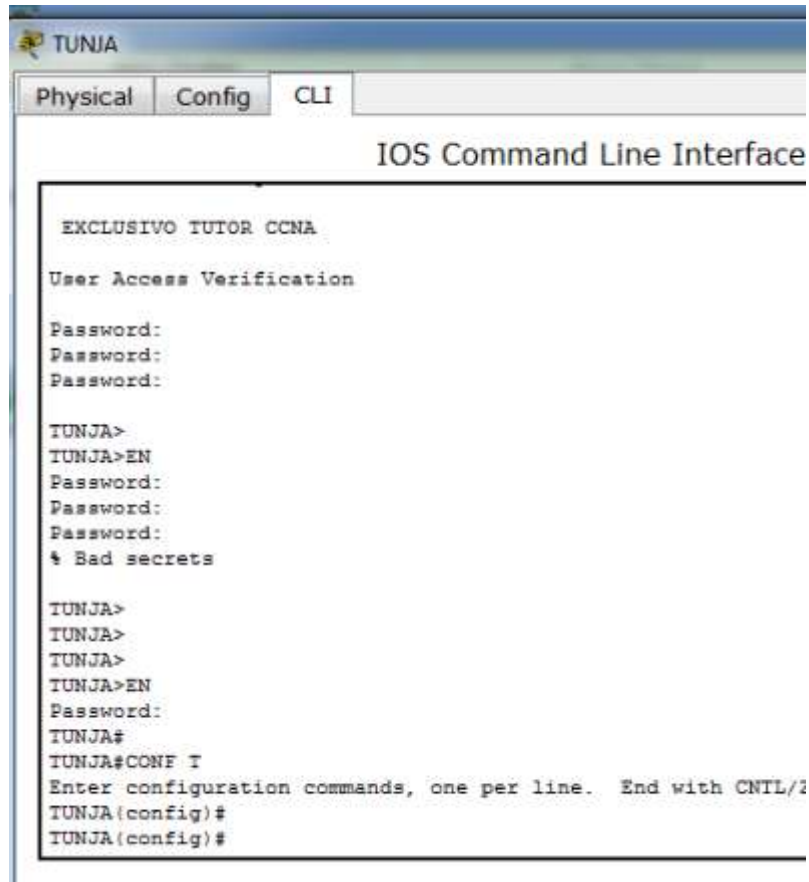
BUCARRAMANGA#CONF T
Enter configuration commands, one per line. End with CNTL/Z.
BUCARRAMANGA (config)#line console 0
BUCARRAMANGA (config-line)#password UNAD
BUCARRAMANGA (config-line)#login
BUCARRAMANGA (config-line)#exit
BUCARRAMANGA (config)#line vty 0 15
BUCARRAMANGA (config-line)#password UNAD
BUCARRAMANGA (config-line)#login
BUCARRAMANGA (config-line)#exit
BUCARRAMANGA (config)#service password-encryption
^
% Invalid input detected at '^' marker.

BUCARRAMANGA (config)#service password-encryption
BUCARRAMANGA (config)#banner motd # EXCLUSIVO TUTOR CCNA#
BUCARRAMANGA (config)#exit
BUCARRAMANGA#
%SYS-5-CONFIG_I: Configured from console by console

BUCARRAMANGA#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
BUCARRAMANGA#
```

Ilustración 42 configuración de seguridad

Fuente: freydy, p. (20 de diciembre de 2019). Aplicación de la configuración De seguridad Obtenido de packet tracer autoría propia.



```
TUNJA
Physical Config CLI
IOS Command Line Interface

EXCLUSIVO TUTOR CCNA
User Access Verification
Password:
Password:
Password:

TUNJA>
TUNJA>EN
Password:
Password:
Password:
* Bad secrets

TUNJA>
TUNJA>
TUNJA>
TUNJA>EN
Password:
TUNJA#
TUNJA#CONF T
Enter configuration commands, one per line. End with CNTL/Z
TUNJA(config)#
TUNJA(config)#
```

Ilustración 43 prueba de configuración de seguridad.

Fuente: freydy, p. (20 de diciembre de 2019). Prueba de configuración de la Seguridad con su respectiva clave. Obtenido de packet tracer autoría Propia.

Configuraciones ip

BUCARRAMANGA(config)#

BUCARRAMANGA(config)#int g0/0.30

BUCARRAMANGA(config-subif)#encapsulation dot1q 30

BUCARRAMANGA(config-subif)#ip address 172.31.0.65 255.255.255.192

```
BUCARRAMANGA(config-subif)#int g0/0.10
BUCARRAMANGA(config-subif)#encapsulation dot1q 10
BUCARRAMANGA(config-subif)#ip address 172.31.0.1 255.255.255.192
BUCARRAMANGA(config-subif)#int g0/0.1
BUCARRAMANGA(config-subif)#encapsulation dot1q 1
BUCARRAMANGA(config-subif)#ip address 172.31.2.1 255.255.255.248
BUCARRAMANGA(config-subif)#int g0/0
BUCARRAMANGA(config-if)#no shutdown
```

```
BUCARRAMANGA(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0,
changed state to up

%LINK-5-CHANGED: Interface GigabitEthernet0/0.1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0.1,
changed state to up

%LINK-5-CHANGED: Interface GigabitEthernet0/0.10, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0.10,
changed state to up

%LINK-5-CHANGED: Interface GigabitEthernet0/0.30, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0.30,
changed state to up
```

```
BUCARRAMANGA(config-if)#
BUCARRAMANGA(config-if)#int s0/0/0
BUCARRAMANGA(config-if)#ip address 172.31.2.34 255.255.255.252
```

```

BUCARRAMANGA(config-if)#no shutdown
BUCARRAMANGA(config-if)#router ospf 1
BUCARRAMANGA(config-router)#network 172.31.0.0 0.0.0.63 area 0
BUCARRAMANGA(config-router)#network 172.31.0.64 0.0.0.63 area 0
BUCARRAMANGA(config-router)#network 172.31.2.0 0.0.0.63 area 0
BUCARRAMANGA(config-router)#network 172.31.2.0 0.0.0.7 area 0
BUCARRAMANGA(config-router)#network 172.31.2.32 0.0.0.3 area 0
BUCARRAMANGA(config-router)#end

```

```

BUCARRAMANGA#
BUCARRAMANGA#show ip
% Incomplete command.
BUCARRAMANGA#
BUCARRAMANGA#
BUCARRAMANGA#do show ip interface brief
^
% Invalid input detected at '^' marker.

BUCARRAMANGA#show ip interface brief
Interface                IP-Address      OK? Method Status        Protocol
GigabitEthernet0/0       unassigned      YES unset  up            up
GigabitEthernet0/0.1     172.31.2.1     YES manual  up            up
GigabitEthernet0/0.10    172.31.0.1     YES manual  up            up
GigabitEthernet0/0.30    172.31.0.65    YES manual  up            up
GigabitEthernet0/1       unassigned      YES unset  administratively down down
Serial10/0/0              172.31.2.34    YES manual  up            up
Serial10/0/1              unassigned      YES unset  administratively down down
Vlan1                     unassigned      YES unset  administratively down down
BUCARRAMANGA#

```

Ilustración 44 ip configuradas

Fuente: freydy, p. (20 de diciembre de 2019).equipo conectados y con su respectiva configuración. Obtenido de packet tracer autoría propia.

TUNJA.

TUNJA>EN

Password:

TUNJA#

TUNJA#CONF T

Enter configuration commands, one per line. End with CNTL/Z.

TUNJA(config)#

TUNJA(config)#int g0/0.1

TUNJA(config-subif)#encapsulation dot1q 1

TUNJA(config-subif)#ip address 172.3.2.9 255.255.255.248

TUNJA(config-subif)#int g0/0.20

TUNJA(config-subif)#encapsulation dot1q 20

TUNJA(config-subif)#ip address 172.31.0.129 255.255.255.192

TUNJA(config-subif)#int g0/0.30

TUNJA(config-subif)#encapsulation dot1q 30

TUNJA(config-subif)#ip address 172.31.0.193 255.255.255.192

TUNJA(config-subif)#int g0/0

TUNJA(config-if)#no shutdown

TUNJA(config-if)#

%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up

**%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0,
changed state to up**

%LINK-5-CHANGED: Interface GigabitEthernet0/0.1, changed state to up

**%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0.1,
changed state to up**

%LINK-5-CHANGED: Interface GigabitEthernet0/0.20, changed state to up

**%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0.20,
changed state to up**

%LINK-5-CHANGED: Interface GigabitEthernet0/0.30, changed state to up

**%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0.30,
changed state to up**

TUNJA(config-if)#

TUNJA#

%SYS-5-CONFIG_I: Configured from console by console

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 g0/1

TUNJA(config-if)#ip address 209.165.220.1 255.255.255.0

TUNJA(config-if)#no shutdown 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

```
TUNJA
Physical Config CLI
IOS Command Line Interface
TUNJA(config)#exit
TUNJA#
%SYS-5-CONFIG_I: Configured from console by console
TUNJA#
TUNJA#
TUNJA#
TUNJA#
TUNJA#
TUNJA#
TUNJA#show ip interface brief
Interface                IP-Address      OK? Method Status          Protocol
GigabitEthernet0/0      unassigned      YES unset  up              up
GigabitEthernet0/0.1    172.31.2.9      YES manual  up              up
GigabitEthernet0/0.20   172.31.0.129    YES manual  up              up
GigabitEthernet0/0.30   172.31.0.193    YES manual  up              up
GigabitEthernet0/1      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#
```

Ilustración 45 ip configuradas

Fuente: freydy, p. (20 de diciembre de 2019).equipo conectados y con su respectiva configuración. Obtenido de packet tracer autoría propia.

CUNDINAMARCA

CUNDINAMARCA#CONF T

Enter configuration commands, one per line. End with CNTL/Z.

CUNDINAMARCA(config)#

CUNDINAMARCA(config)#int g0/0.1

CUNDINAMARCA(config-subif)#encapsulation dot1q 1

CUNDINAMARCA(config-subif)#ip address 172.31.2.9 255.255.255.248

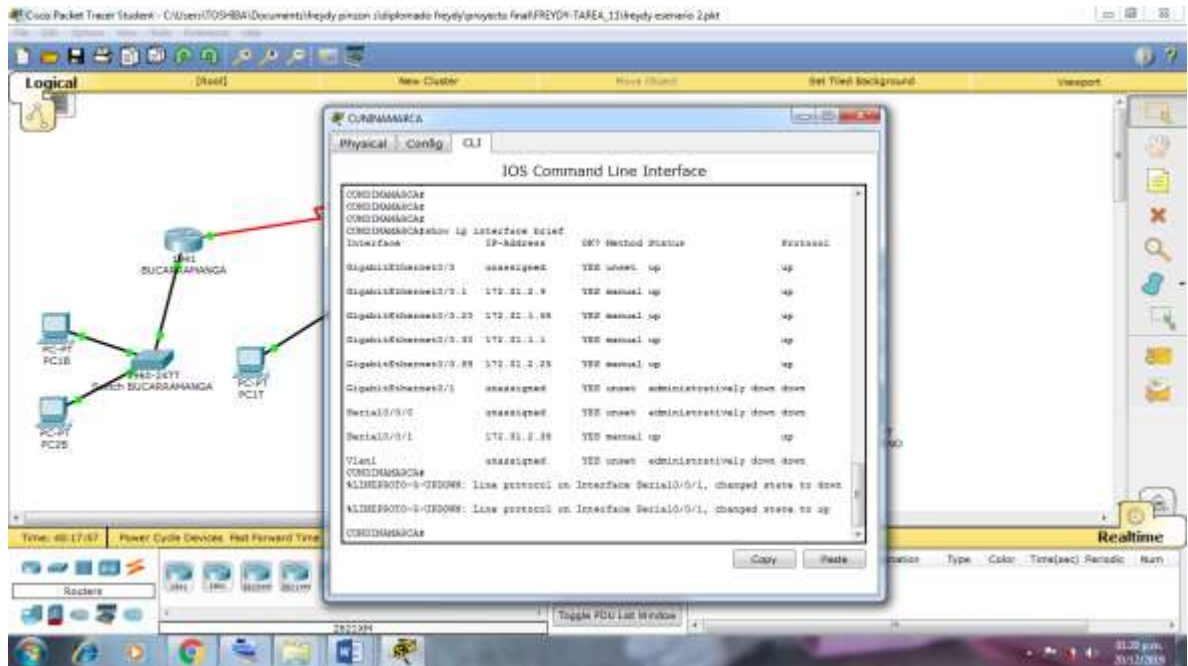
CUNDINAMARCA(config-subif)#int g0/0.20

CUNDINAMARCA(config-subif)#encapsulation dot1q 20

```

CUNDINAMARCA(config-subif)#ip address 172.31.1.65 255.255.255.192
CUNDINAMARCA(config-subif)#int g0/0.30
CUNDINAMARCA(config-subif)#encapsulation dot1q 30
CUNDINAMARCA(config-subif)#ip address 172.31.1.1 255.255.255.192
CUNDINAMARCA(config-subif)#int g0/0.88
CUNDINAMARCA(config-subif)#encapsulation dot1q 88
CUNDINAMARCA(config-subif)#ip address 172.31.2.25 255.255.255.248
CUNDINAMARCA(config-subif)#int g0/0
CUNDINAMARCA(config-if)#no shutdown
CUNDINAMARCA(config-if)#int s0/0/1
CUNDINAMARCA(config-if)#ip address 172.31.2.38 255.255.255.252
CUNDINAMARCA(config-if)#no shutdown
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)#en

```



```
CUNDINAMARCA#
CUNDINAMARCA#
CUNDINAMARCA#
CUNDINAMARCA#show ip interface brief
Interface                IP-Address      OK? Method Status      Protocol
GigabitEthernet0/0       unassigned      YES unset    up          up
GigabitEthernet0/0.1     172.31.2.9      YES manual   up          up
GigabitEthernet0/0.20    172.31.1.65     YES manual   up          up
GigabitEthernet0/0.30    172.31.1.1      YES manual   up          up
GigabitEthernet0/0.88    172.31.2.25     YES manual   up          up
GigabitEthernet0/1       unassigned      YES unset    administratively down down
Serial0/0/0              unassigned      YES unset    administratively down down
Serial0/0/1              172.31.2.38     YES manual   up          up
Vlan1                    unassigned      YES unset    administratively down down
CUNDINAMARCA#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1, changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1, changed state to up
CUNDINAMARCA#
```

Ilustración 46p configuradas

Fuente: freydy, p. (20 de diciembre de 2019).equipo conectados y con su respectiva configuración. Obtenido de packet tracer autoría propia

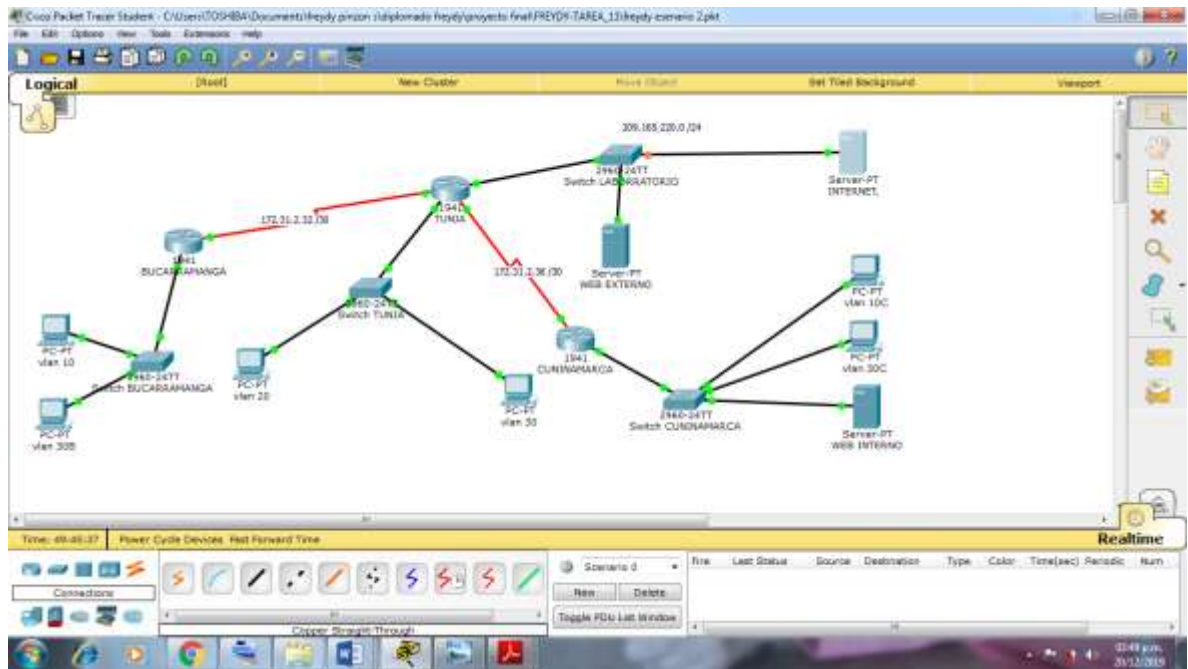


Ilustración 47 Configuraciones ip

Fuente: freydy, p. (20 de diciembre de 2019). Prueba de configuración de la Seguridad con sus respectiva clave y direcciones ip configuradas en la Topología. Obtenido de packet tracer autoría propia.

Configuraciones Switch

| BUCARAMANGA | TUNJA | CUNDINAMARCA |
|--|---|---|
| <pre>Switch>en Switch#conf t Enter configuration commands, one per line. End with CNTL/Z. Switch(config)#hostname BUCARAMANGAFREYDY BUCARAMANGAFREYDY(config) #vlan 1 BUCARAMANGAFREYDY(config- vlan)#vlan 10 BUCARAMANGAFREYDY(config- vlan)#vlan 30 BUCARAMANGAFREYDY(config- vlan)#int f0/12</pre> | <pre>Switch(config)# Switch(config)# Switch(config)#hostname TUNJAFREYDY TUNJAFREYDY(config)#vlan 1 TUNJAFREYDY(config- vlan)#vlan 20 TUNJAFREYDY(config- vlan)#vlan 30 TUNJAFREYDY(config-vlan)#int f0/12 TUNJAFREYDY(config- if)#switchport mode access TUNJAFREYDY(config- if)#switchport access vlan 20</pre> | <pre>Switch#CONF T Enter configuration commands, one per line. End with CNTL/Z. Switch(config)# Switch(config)#hostna me CUNDINAMARCAFREY DY CUNDINAMARCAFREY DY(config)#vlan 1 CUNDINAMARCAFREY DY(config-vlan)#</pre> |

| | | |
|---|--|--|
| <pre> BUCARAMANGAFREYDY(config-if)#switchport mode access BUCARAMANGAFREYDY(config-if)#switchport access vlan 10 BUCARAMANGAFREYDY(config-if)#int f0/24 BUCARAMANGAFREYDY(config-if)#switchport mode access BUCARAMANGAFREYDY(config-if)#switchport access vlan 30 BUCARAMANGAFREYDY(config-if)#int f0/1 BUCARAMANGAFREYDY(config-if)#switchport mode trunk BUCARAMANGAFREYDY(config-if)#int vlan 1 BUCARAMANGAFREYDY(config-if)#ip address 172.31.2.3 255.255.255.248 BUCARAMANGAFREYDY(config-if)#no shutdown BUCARAMANGAFREYDY(config-if)# %LINK-5-CHANGED: Interface Vlan1, changed state to up %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up BUCARAMANGAFREYDY(config-if)#ip default-gateway 172.31.2.1 BUCARAMANGAFREYDY(config) # BUCARAMANGAFREYDY(config) # BUCARAMANGAFREYDY(config) # </pre> | <pre> TUNJAFREYDY(config-if)#int f0/24 TUNJAFREYDY(config-if)#switchport mode access TUNJAFREYDY(config-if)#switchport access vlan 30 TUNJAFREYDY(config-if)#int f0/1 TUNJAFREYDY(config-if)#switchport mode trunk TUNJAFREYDY(config-if)#int vlan 1 TUNJAFREYDY(config-if)#ip address 172.3.2.11 255.255.255.248 TUNJAFREYDY(config-if)#no shutdown TUNJAFREYDY(config-vlan)#int f0/12 TUNJAFREYDY(config-if)#switchport mode access TUNJAFREYDY(config-if)#switchport access vlan 20 TUNJAFREYDY(config-if)#int f0/24 TUNJAFREYDY(config-if)#switchport mode access TUNJAFREYDY(config-if)#switchport access vlan 30 TUNJAFREYDY(config-if)#int f0/1 TUNJAFREYDY(config-if)#switchport mode trunk TUNJAFREYDY(config-if)#int vlan 1 TUNJAFREYDY(config-if)#ip address 172.3.2.11 255.255.255.248 TUNJAFREYDY(config-if)#no shutdown </pre> | <pre> CUNDINAMARCAFREY DY(config-vlan)#vlan 20 CUNDINAMARCAFREY DY(config-vlan)#vlan 30 CUNDINAMARCAFREY DY(config-vlan)#vlan 88 CUNDINAMARCAFREY DY(config-vlan)#exit CUNDINAMARCAFREY DY(config)# CUNDINAMARCAFREY DY(config)#int f0/12 CUNDINAMARCAFREY DY(config-if)#switchport mode access CUNDINAMARCAFREY DY(config-if)#switchport access vlan 20 CUNDINAMARCAFREY DY(config-if)#int f0/24 CUNDINAMARCAFREY DY(config-if)#switchport mode access CUNDINAMARCAFREY DY(config-if)#switchport access vlan 30 CUNDINAMARCAFREY DY(config-if)#int f0/10 CUNDINAMARCAFREY DY(config-if)#switchport mode access CUNDINAMARCAFREY DY(config-if)#switchport access vlan 88 CUNDINAMARCAFREY DY(config-if)#int f0/1 CUNDINAMARCAFREY DY(config-if)#switchport mode trunk CUNDINAMARCAFREY DY(config-if)#int vlan 1 CUNDINAMARCAFREY DY(config- </pre> |
|---|--|--|

| | | |
|--|--|--|
| | | <pre> if)#ip address 172.31.2.11 255.255.255.248 CUNDINAMARCAFREY DY(config-if)#no shutdown CUNDINAMARCAFREY DY(config-if)#ip default-gateway 172.31.2.9 CUNDINAMARCAFREY DY(config)# CUNDINAMARCAFREY DY(config)# </pre> |
|--|--|--|

Switch BUCARRAMANGA

Physical Config CLI

IOS Command Line Interface

| | | | | | |
|--------------------|------------|-----|--------|------|------|
| FastEthernet0/10 | unassigned | YES | manual | down | down |
| FastEthernet0/11 | unassigned | YES | manual | down | down |
| FastEthernet0/12 | unassigned | YES | manual | up | up |
| FastEthernet0/13 | unassigned | YES | manual | down | down |
| FastEthernet0/14 | unassigned | YES | manual | down | down |
| FastEthernet0/15 | unassigned | YES | manual | down | down |
| FastEthernet0/16 | unassigned | YES | manual | down | down |
| FastEthernet0/17 | unassigned | YES | manual | down | down |
| FastEthernet0/18 | unassigned | YES | manual | down | down |
| FastEthernet0/19 | unassigned | YES | manual | down | down |
| FastEthernet0/20 | unassigned | YES | manual | down | down |
| FastEthernet0/21 | unassigned | YES | manual | down | down |
| FastEthernet0/22 | unassigned | YES | manual | down | down |
| FastEthernet0/23 | unassigned | YES | manual | down | down |
| FastEthernet0/24 | unassigned | YES | manual | up | up |
| GigabitEthernet0/1 | unassigned | YES | manual | up | up |

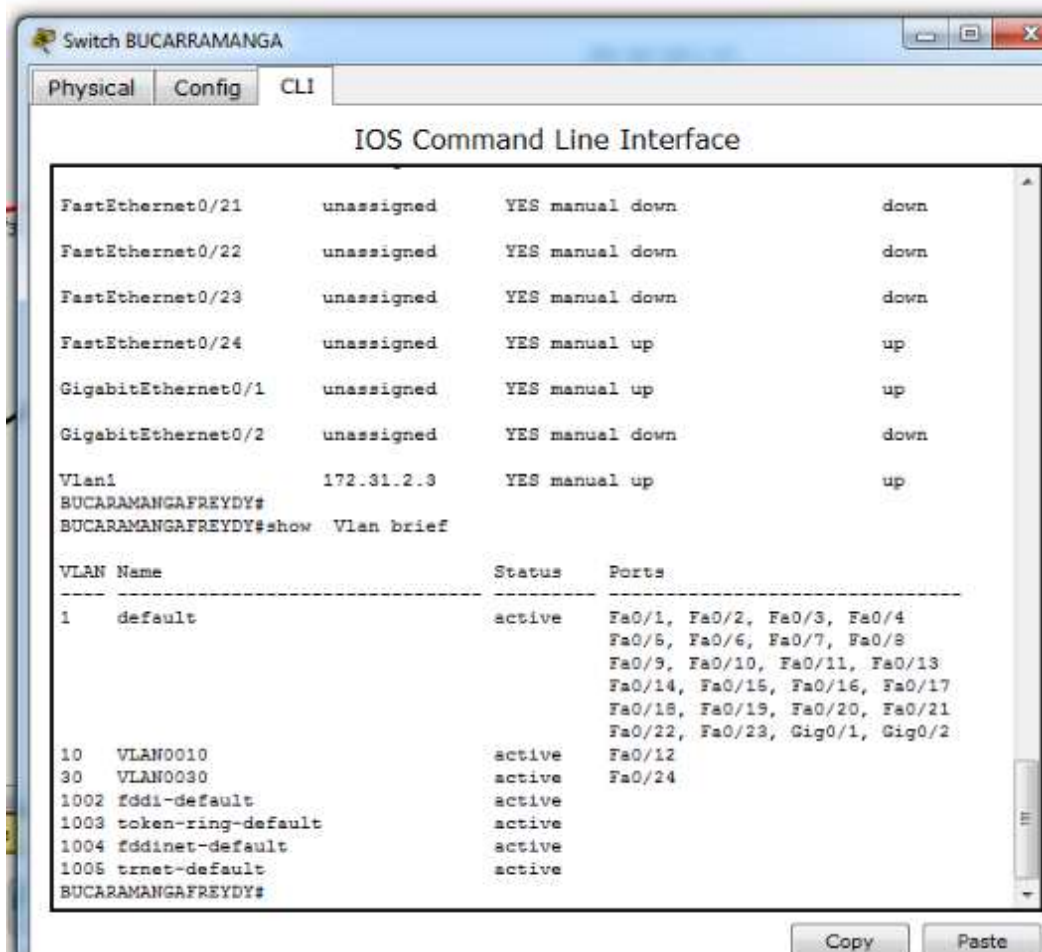


Ilustración 48 vlan de Bucaramanga

Fuente: freydy, p. (20 de diciembre de 2019).equipo conectados y con su respectiva configuración vlan 10 y 30. Obtenido de packet tracer autoría propia

The screenshot shows a network switch CLI window titled "Switch TUNJA". The window has tabs for "Physical", "Config", and "CLI". The main content is the "IOS Command Line Interface".

```

FastEthernet0/23    unassigned    YES manual down    down
FastEthernet0/24    unassigned    YES manual up      up
GigabitEthernet0/1  unassigned    YES manual down    down
GigabitEthernet0/2  unassigned    YES manual down    down
Vlan1               172.3.2.11    YES manual up      up
TUNJAFREYDY>
TUNJAFREYDY>
TUNJAFREYDY>show Vlan brief

```

| VLAN Name | Status | Ports |
|-------------------------|--------|---|
| 1 default | active | Fa0/1, Fa0/2, Fa0/3, Fa0/4 Fa0/5, Fa0/6, Fa0/7, Fa0/8 Fa0/9, Fa0/10, Fa0/11, Fa0/13 Fa0/14, Fa0/15, Fa0/16, Fa0/17 Fa0/18, Fa0/19, Fa0/20, Fa0/21 Fa0/22, Fa0/23, Gig0/1, Gig0/2 |
| 20 VLAN0020 | active | Fa0/12 |
| 30 VLAN0030 | active | Fa0/24 |
| 1002 fddi-default | active | |
| 1003 token-ring-default | active | |
| 1004 fddinet-default | active | |
| 1005 trnet-default | active | |

```

TUNJAFREYDY>

```

Ilustración 49 vlan tunja

Fuente: freydy, p. (20 de diciembre de 2019).equipo conectados y con su respectiva configuración vlan 20 y 30. Obtenido de packet tracer autoría propia

```

Switch CUNDINAMARCA
Physical Config CLI
IOS Command Line Interface
CUNDINAMARCAFREYDY>
CUNDINAMARCAFREYDY>
CUNDINAMARCAFREYDY>
CUNDINAMARCAFREYDY>
CUNDINAMARCAFREYDY>
CUNDINAMARCAFREYDY>
CUNDINAMARCAFREYDY>enable
Translating "enable"...domain server (255.255.255.255)
% Unknown command or computer name, or unable to find computer address

CUNDINAMARCAFREYDY>en
CUNDINAMARCAFREYDY#show Vlan brief

VLAN Name                Status    Ports
-----
1    default                  active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                           Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                           Fa0/9, Fa0/11, Fa0/13, Fa0/14
                                           Fa0/15, Fa0/16, Fa0/17, Fa0/18
                                           Fa0/19, Fa0/20, Fa0/21, Fa0/22
                                           Fa0/23, Gig0/1, Gig0/2

20   VLAN0020                 active    Fa0/12

30   VLAN0030                 active    Fa0/24

88   VLAN0088                 active    Fa0/10

1002 fddi-default             active

1003 token-ring-default     active

1004 fddinet-default         active

1005 trnet-default          active

CUNDINAMARCAFREYDY#

```

Ilustración 50 vlan Cundinamarca

Fuente: freydy, p. (20 de diciembre de 2019).equipo conectados y con su respectiva configuración vlan 20 ,30, 88. Obtenido de packet tracer autoría propia

Autenticación local con AAA

| BUCARAMANGA | TUNJA | CUNDINAMARCA |
|--------------------------|--------------|--------------|
| User Access Verification | TUNJA#CONF T | |

| | | |
|---|---|--|
| <p> Password: Password: BUCARRAMANGA>EN Password: BUCARRAMANGA#CONF T Enter configuration commands, one per line. End with CNTL/Z. BUCARRAMANGA(config)#aaa new-model BUCARRAMANGA(config)#aaa authentication login AUTH local BUCARRAMANGA(config)#line console 0 BUCARRAMANGA(config-line)#login authentication AUTH BUCARRAMANGA(config-line)#line vty 0 15 BUCARRAMANGA(config-line)#login authentication AUTH BUCARRAMANGA(config-line)#exit BUCARRAMANGA(config)# </p> | <p> Enter configuration commands, one per line. End with CNTL/Z. TUNJA(config)# TUNJA(config)#aaa new-model TUNJA(config)#aaa authentication login AUTH local TUNJA(config)#line console 0 TUNJA(config-line)#login authentication AUTH TUNJA(config-line)#line vty 0 15 TUNJA(config-line)#login authentication AUTH TUNJA(config-line)#EXIT TUNJA(config)# </p> | <p> User Access Verification Password: Password: CUNDINAMARCA>EN CUNDINAMARCA#CONF T Enter configuration commands, one per line. End with CNTL/Z. CUNDINAMARCA(config)# CUNDINAMARCA(config)# CUNDINAMARCA(config)#aaa new-model CUNDINAMARCA(config)#aaa authentication login AUTH local CUNDINAMARCA(config)#line console 0 CUNDINAMARCA(config-line)#login authentication AUTH CUNDINAMARCA(config-line)#line vty 0 15 CUNDINAMARCA(config-line)#login authentication AUTH CUNDINAMARCA(config-line)#EXIT CUNDINAMARCA(config)# CUNDINAMARCA(config)# CUNDINAMARCA# </p> |
|---|---|--|

Cifrado de contraseñas.

| BUCARAMANGA | TUNJA | CUNDINAMARCA |
|---|--|--|
| <p> BUCARAMANGA (config)#service password-encryption TUNJA(config)#EXIT </p> | <p> TUNJA(config)#service password-encryption TUNJA(config)#EXIT </p> | <p> CUNDINAMARCA(config)#service password-encryption CUNDINAMARCA(config)#EXIT </p> |

Un máximo de internos para acceder al router.

| BUCARAMANGA | TUNJA | CUNDINAMARCA |
|---|---|--|
| BUCARAMANGA(config-line)#login block-for 6 attempts 4 within 60 TUNJA(config)# | TUNJA(config-line)#login block-for 6 attempts 4 within 60 TUNJA(config)# | CUNDINAMARCA(config)#login block-for 6 attempts 4 within 60 CUNDINAMARCA(config)#exit |

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

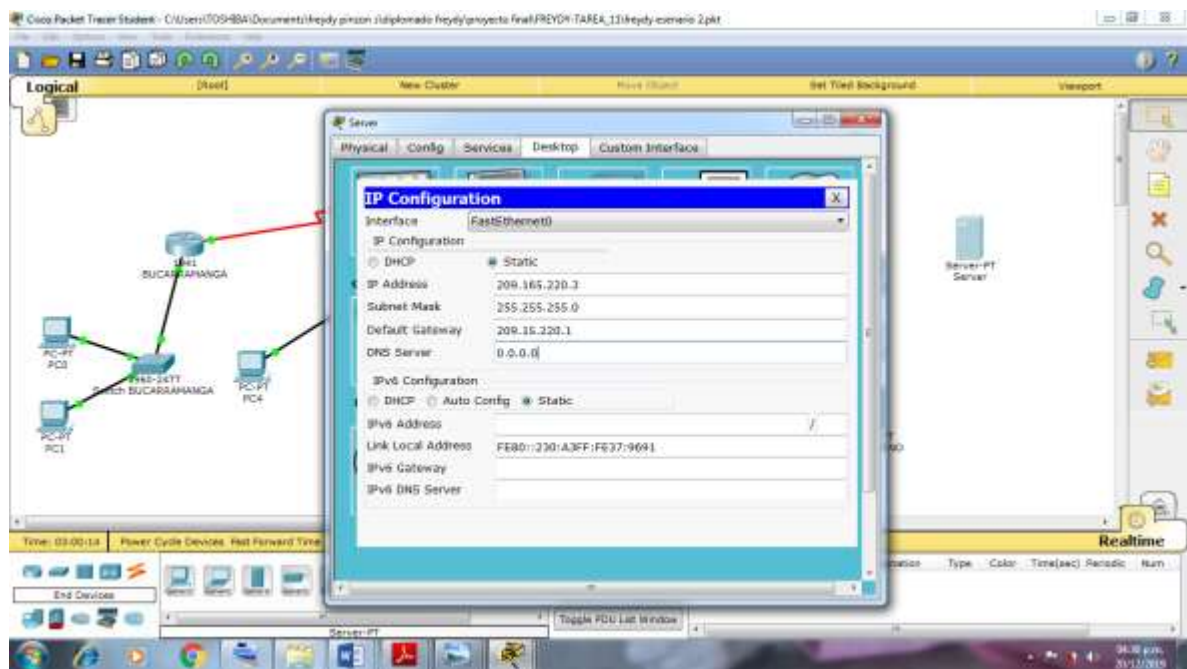


Ilustración 51 TFTP

Fuente: freydy, p. (20 de diciembre de 2019).TFTP. Obtenido de packet tracer autoría propia

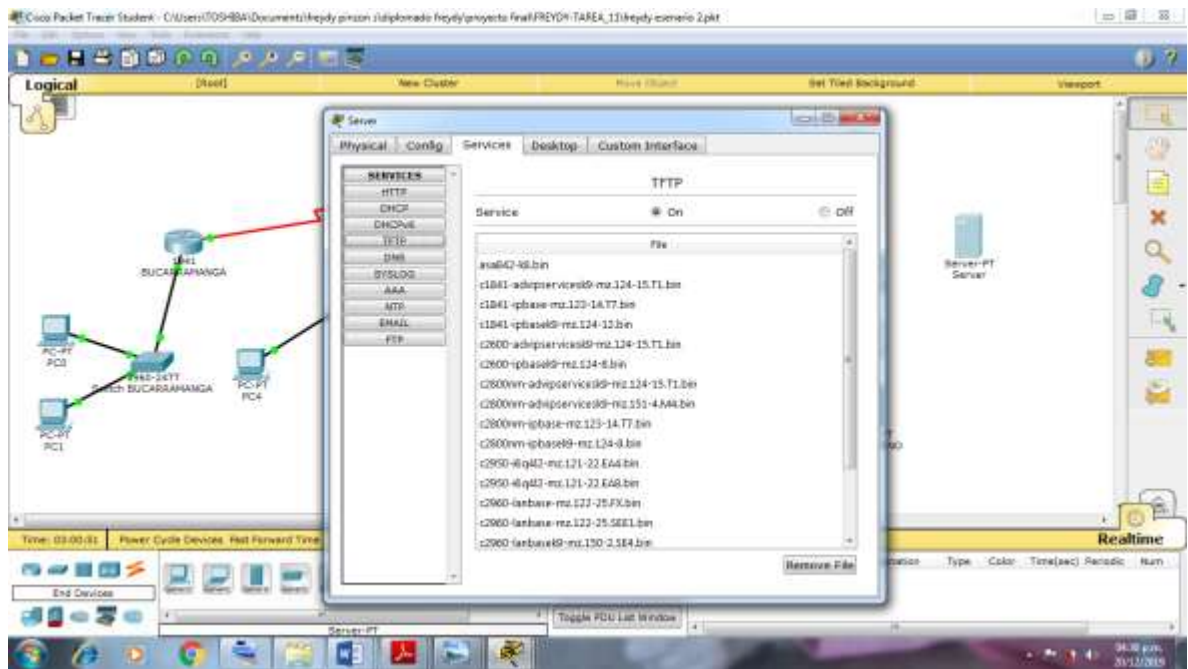


Ilustración 52 diagnóstico del TFTP

Fuente: freydy, p. (20 de diciembre de 2019) diagnóstico del TFTP. Obtenido de packet tracer autoría propia

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

| BUCARAMANGA | TUNJA | CUNDINAMARCA |
|--|---|---|
| BUCARRAMANGA>enable Password: BUCARRAMANGA#configure terminal Enter configuration commands, one per line. End with CNTL/Z. | TUNJA#conf t Enter configuration commands, one per line. End with CNTL/Z. TUNJA(config)#ip dhcp excluded-address 172.31.0.1 | CUNDINAMARCA(config)# CUNDINAMARCA(config)#int g0/0.20 |

| | | | |
|---|---|------|---|
| BUCARRAMANGA(config)#interf ace GigabitEthernet0/0 | TUNJA(config)#ip excluded-address 172.31.0.65 | dhcp | CUNDINAMARCA(confi g-subif)#ip helper- |
| BUCARRAMANGA(config-if)#exit | TUNJA(config)#ip | dhcp | address 172.31.2.37 |
| BUCARRAMANGA(config)# | excluded-address 172.31.1.65 | | CUNDINAMARCA(confi |
| BUCARRAMANGA(config)# | TUNJA(config)#ip | dhcp | g-subif)#int g0/0.30 |
| BUCARRAMANGA(config)# | excluded-address 172.31.1.1 | | CUNDINAMARCA(confi |
| BUCARRAMANGA(config)#int g0/0.10 | TUNJA(config)#ip dhcp pool V10B | | g-subif)#ip helper- |
| BUCARRAMANGA(config- subif)#ip helper-address 172.31.2.33 | TUNJA(dhcp-config)#network 172.31.0.0 255.255.255.192 | | address 172.31.2.37 |
| BUCARRAMANGA(config- subif)#int g0/0.30 | TUNJA(dhcp-config)#default- router 172.31.0.1 | | CUNDINAMARCA(confi |
| BUCARRAMANGA(config- subif)#ip helper-address 172.31.2.33 | TUNJA(dhcp-config)#dns- server 172.31.2.28 | | g-subif)#end |
| BUCARRAMANGA(config- subif)#end | TUNJA(dhcp-config)#ip dhcp pool V30B | | CUNDINAMARCA# |
| BUCARRAMANGA# | 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 172.31.2.28 | | |
| | TUNJA(dhcp-config)#ip dhcp pool V20C | | |
| | 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 172.31.2.28 | | |
| | TUNJA(dhcp-config)#ip dhcp pool V30C | | |
| | TUNJA(dhcp-config)#network 172.31.1.0 255.255.255.192 | | |

| | | |
|--|--|--|
| | <pre>TUNJA(dhcp-config)#default- router 172.31.1.1 TUNJA(dhcp-config)#dns- server 172.31.2.28 TUNJA(dhcp-config)#exit TUNJA(config)#</pre> | |
|--|--|--|

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

```
TUNJA(config)#ip nat inside source static 172.31.2.28 209.165.220.4  
TUNJA(config)#access-list 1 permit 172.0.0.0 0.255.255.255  
TUNJA(config)#ip nat inside source list 1 interface g0/1 overload  
TUNJA(config)#int g0/1  
TUNJA(config-if)#ip nat outside  
TUNJA(config-if)#int g0/0.1  
TUNJA(config-subif)#ip nat inside  
TUNJA(config-subif)#int g0/0.20  
TUNJA(config-subif)#ip nat inside  
TUNJA(config-subif)#int g0/0.30  
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  
TUNJA(config)#ip route 0.0.0.0 0.0.0.0 209.165.220.3  
TUNJA(config)#router ospf 1  
TUNJA(config-router)#default-information originate  
TUNJA(config-router)#exit  
TUNJA(config)#exit  
TUNJA#
```

%SYS-5-CONFIG_I: Configured from console by console

TUNJA#copy run start

Resultado de la configuración mediante el comando show ip route



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

Gateway of last resort is 209.165.220.3 to network 0.0.0.0

    172.31.0.0/16 is variably subnetted, 2 subnets, 2 masks
   C    172.31.2.8/29 is directly connected, GigabitEthernet0/0.1
   L    172.31.2.9/32 is directly connected, GigabitEthernet0/0.1
    172.31.0.0/16 is variably subnetted, 15 subnets, 4 masks
   O    172.31.0.0/26 [110/65] via 172.31.2.34, 01:39:54, Serial0/0/0
   O    172.31.0.64/26 [110/65] via 172.31.2.34, 01:39:54, Serial0/0/0
   C    172.31.0.128/26 is directly connected, GigabitEthernet0/0.20
   L    172.31.0.129/32 is directly connected, GigabitEthernet0/0.20
   C    172.31.0.192/26 is directly connected, GigabitEthernet0/0.30
   L    172.31.0.193/32 is directly connected, GigabitEthernet0/0.30
   O    172.31.1.0/26 [110/65] via 172.31.2.38, 01:39:54, Serial0/0/1
   O    172.31.1.64/26 [110/65] via 172.31.2.38, 01:39:54, Serial0/0/1
   O    172.31.2.0/29 [110/65] via 172.31.2.34, 01:39:54, Serial0/0/0
   O    172.31.2.8/29 [110/65] via 172.31.2.38, 01:39:54, Serial0/0/1
   O    172.31.2.24/29 [110/65] via 172.31.2.38, 01:39:54, Serial0/0/1
   C    172.31.2.32/30 is directly connected, Serial0/0/0
   L    172.31.2.33/32 is directly connected, Serial0/0/0
   C    172.31.2.36/30 is directly connected, Serial0/0/1
   L    172.31.2.37/32 is directly connected, Serial0/0/1
    209.165.220.0/24 is variably subnetted, 2 subnets, 2 masks
   C    209.165.220.0/24 is directly connected, GigabitEthernet0/1
   L    209.165.220.1/32 is directly connected, GigabitEthernet0/1
   S*   0.0.0.0/0 [1/0] via 209.165.220.3
TUNJA#
TUNJA#
```

Ilustración 53 show ip route

Fuente: freydy, p. (20 de diciembre de 2019) Resultado de la configuración mediante el comando show ip route. Obtenido de packet tracer autoría propia

```
BUCARRAMANGA
Physical Config CLI
IOS Command Line Interface
BUCARRAMANGA(Config)#exit
BUCARRAMANGA#
%SYS-5-CONFIG_I: Configured from console by console
BUCARRAMANGA#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
I - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default, U - per-user static route, o - ODR
D - 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 172.3.2.8/29 [110/65] via 172.31.2.33, 01:44:20, Serial0/0/0
172.31.0.0/16 is variably subnetted, 15 subnets, 4 masks
C 172.31.0.0/26 is directly connected, GigabitEthernet0/0.10
L 172.31.0.1/32 is directly connected, GigabitEthernet0/0.10
C 172.31.0.64/26 is directly connected, GigabitEthernet0/0.30
L 172.31.0.65/32 is directly connected, GigabitEthernet0/0.30
O 172.31.0.128/26 [110/65] via 172.31.2.33, 01:44:20, Serial0/0/0
O 172.31.0.192/26 [110/65] via 172.31.2.33, 01:44:20, Serial0/0/0
O 172.31.1.0/26 [110/129] via 172.31.2.33, 01:44:20, Serial0/0/0
O 172.31.1.64/26 [110/129] via 172.31.2.33, 01:44:20, Serial0/0/0
C 172.31.2.0/29 is directly connected, GigabitEthernet0/0.1
L 172.31.2.1/32 is directly connected, GigabitEthernet0/0.1
O 172.31.2.8/29 [110/129] via 172.31.2.33, 01:44:20, Serial0/0/0
O 172.31.2.24/29 [110/129] via 172.31.2.33, 01:44:20, Serial0/0/0
C 172.31.2.32/30 is directly connected, Serial0/0/0
L 172.31.2.34/32 is directly connected, Serial0/0/0
O 172.31.2.36/30 [110/128] via 172.31.2.33, 01:44:20, Serial0/0/0
O*E2 0.0.0.0/0 [110/1] via 172.31.2.33, 00:08:10, Serial0/0/0
BUCARRAMANGA#
BUCARRAMANGA#
```

Ilustración 54 show ip route

Fuente: freydy, p. (20 de diciembre de 2019) Resultado de la configuración mediante el comando show ip route. Obtenido de packet tracer autoría propia

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

Gateway of last resort is 172.31.2.37 to network 0.0.0.0

    172.3.0.0/29 is subnetted, 1 subnets
O       172.3.2.8/29 [110/65] via 172.31.2.37, 01:46:43, Serial0/0/1
    172.31.0.0/16 is variably subnetted, 16 subnets, 4 masks
O       172.31.0.0/26 [110/129] via 172.31.2.37, 01:46:43, Serial0/0/1
O       172.31.0.64/26 [110/129] via 172.31.2.37, 01:46:43, Serial0/0/1
O       172.31.0.128/26 [110/65] via 172.31.2.37, 01:46:43, Serial0/0/1
O       172.31.0.192/26 [110/65] via 172.31.2.37, 01:46:43, Serial0/0/1
C       172.31.1.0/26 is directly connected, GigabitEthernet0/0.30
L       172.31.1.1/32 is directly connected, GigabitEthernet0/0.30
C       172.31.1.64/26 is directly connected, GigabitEthernet0/0.20
L       172.31.1.65/32 is directly connected, GigabitEthernet0/0.20
O       172.31.2.0/29 [110/129] via 172.31.2.37, 01:46:43, Serial0/0/1
C       172.31.2.8/29 is directly connected, GigabitEthernet0/0.1
L       172.31.2.9/32 is directly connected, GigabitEthernet0/0.1
C       172.31.2.24/29 is directly connected, GigabitEthernet0/0.88
L       172.31.2.25/32 is directly connected, GigabitEthernet0/0.88
O       172.31.2.32/30 [110/128] via 172.31.2.37, 01:46:43, Serial0/0/1
C       172.31.2.36/30 is directly connected, Serial0/0/1
L       172.31.2.38/32 is directly connected, Serial0/0/1
O*E2 0.0.0.0/0 [110/1] via 172.31.2.37, 00:10:28, Serial0/0/1
CUNDINAMARCA#
CUNDINAMARCA#
```

Ilustración 55 show ip route

Fuente: freydy, p. (20 de diciembre de 2019) Resultado de la configuración mediante el comando show ip route. Obtenido de packet tracer autoría propia

```

TUNJA
Physical Config CLI
IOS Command Line Interface

Username:
Username:
Username:
TUNJA>enable
Password:
TUNJA#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
TUNJA(config)#interface GigabitEthernet0/0
TUNJA(config-if)#
TUNJA(config-if)#exit
TUNJA(config)#interface GigabitEthernet0/0
TUNJA(config-if)#exit
TUNJA(config)#exit
TUNJA#
%SYS-5-CONFIG_I: Configured from console by console

TUNJA#
TUNJA#show ip nat translation
Pro  Inside global      Inside local      Outside local      Outside global
---  209.165.220.4        172.31.2.28      ---                ---
TUNJA#

```

El enrutamiento deberá tener autenticación.

| BUCARAMANGA | TUNJA | CUNDINAMARCA |
|--|--|--|
| <pre> BUCARRAMANGA(config)# BUCARRAMANGA(config)#int s0/0/0 BUCARRAMANGA(config-if)#ip ospf authentication message- digest BUCARRAMANGA(config-if)#ip ospf message-digest-key 1 md5 UN BUCARRAMANGA(config- if)#EXIT BUCARRAMANGA #copy run start </pre> | <pre> TUNJA#conf t Enter configuration commands, one per line. End with CNTL/Z. TUNJA(config)#int s0/0/0 TUNJA(config-if)#ip ospf authentication message-digest TUNJA(config-if)#ip ospf message-digest-key 1 md5 UN 01:57:41: %OSPF-5-ADJCHG: Process 1, Nbr 172.31.2.34 on Serial0/0/0 from FULL to DOWN, Neighbor Down: Dead timer expired 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 UN </pre> | <pre> CUNDINAMARCA(confi g)# CUNDINAMARCA(confi g)#int s0/0/0 CUNDINAMARCA(confi g-if)#ip ospf authentication message-digest CUNDINAMARCA(confi g-if)#ip ospf message- digest-key 1 md5 UN CUNDINAMARCA(confi g-if)#EXIT CUNDINAMARCA#cop y run start </pre> |

| | | |
|--|--|--|
| | TUNJA(config-if)#EXIT TUNJA #copy run start | |
|--|--|--|

Listas de control de acceso:

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

```
CUNDINAMARCA#  
CUNDINAMARCA#CONF T  
Enter configuration commands, one per line. End with CNTL/Z.  
CUNDINAMARCA(config)#access-list 111 deny ip 172.31.1.64 0.0.0.63  
209.165.220.0 0.0.0.255  
CUNDINAMARCA(config)#access-list 111 permit ip any any  
CUNDINAMARCA(config)#int g0/0.20  
CUNDINAMARCA(config-subif)#ip access-group 111 in  
CUNDINAMARCA(config-subif)#exit  
CUNDINAMARCA(config)#  
CUNDINAMARCA#
```

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

```
CUNDINAMARCA#  
CUNDINAMARCA#conf t  
Enter configuration commands, one per line. End with CNTL/Z.  
CUNDINAMARCA(config)#access-list 112 permit ip 172.31.1.0 0.0.0.63  
209.165.220.0 0.0.0.255  
CUNDINAMARCA(config)#access-list 112 deny ip any any  
CUNDINAMARCA(config)#int g0/0.30  
CUNDINAMARCA(config-subif)#ip access-group 112 in  
CUNDINAMARCA(config-subif)#exit  
CUNDINAMARCA(config)#exit  
CUNDINAMARCA#
```

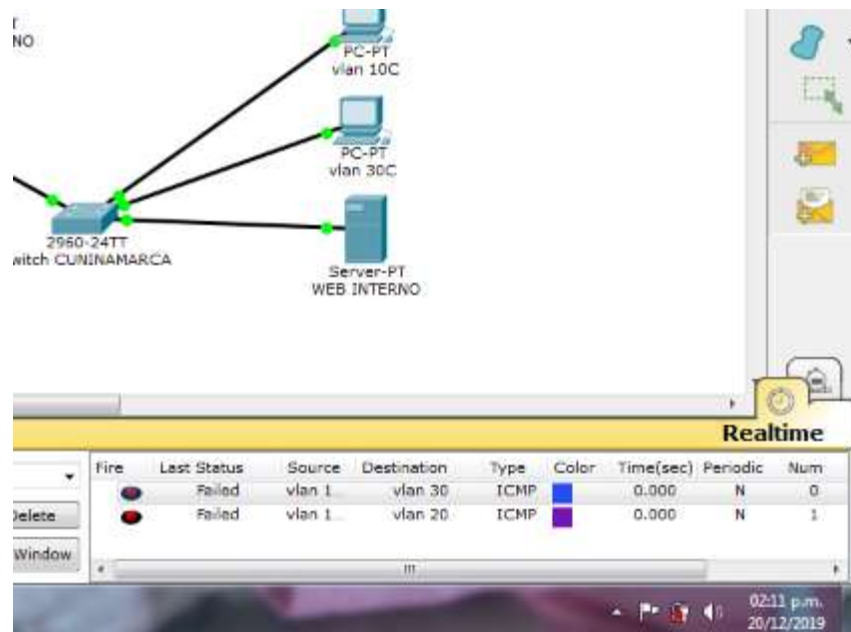


Ilustración 56 resultado mediante ping

Fuente: freydy, p. (20 de diciembre de 2019) Resultado de la configuración mediante el comando ping. Obtenido de packet tracer autoría propia

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

```
TUNJA(config)#
TUNJA(config)#access-list 121 permit tcp 172.31.0.192 0.0.0.63 209.165.220.0
0.0.0.255 eq 80
TUNJA(config)#access-list 121 permit tcp 172.31.0.192 0.0.0.63 209.165.220.0
0.0.0.255 eq 21
TUNJA(config)#access-list 121 permit tcp 172.31.0.192 0.0.0.63 209.165.220.0
0.0.0.255 eq 20
TUNJA(config)#int g0/0.30
TUNJA(config-subif)#ip access-group 121 in
TUNJA(config-subif)#exit
TUNJA(config)#exit
TUNJA#
```

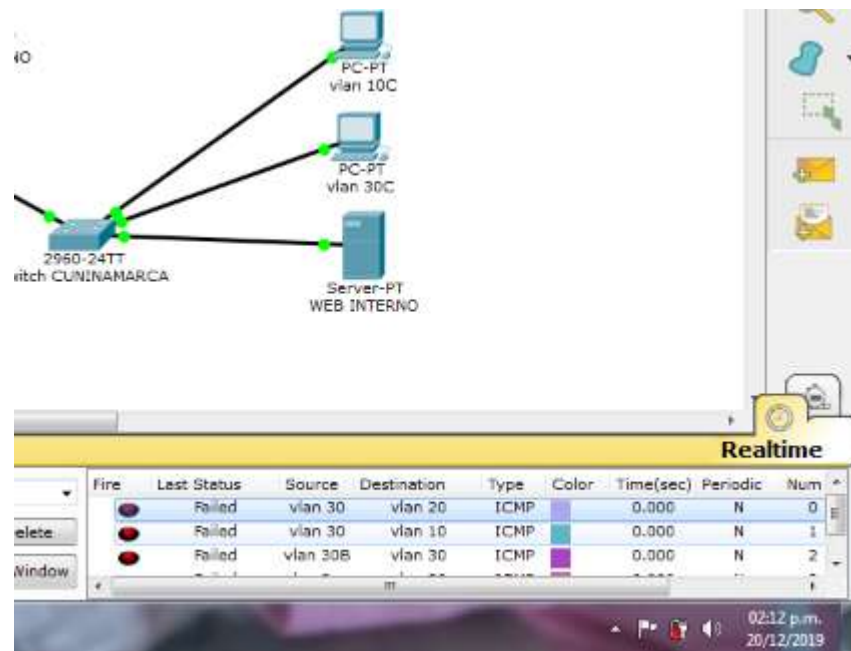


Ilustración 57 resultado mediante ping

Fuente: freydy, p. (20 de diciembre de 2019) Resultado de la configuración mediante el comando ping. Obtenido de packet tracer autoría propia

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

```
TUNJA(config)#
TUNJA(config)#access-list 122 permit ip 172.31.0.128 0.0.0.63 172.31.1.64 0.0.0.63
TUNJA(config)#access-list 122 permit ip 172.31.0.128 0.0.0.63 172.31.0.0 0.0.0.63
TUNJA(config)#int g0/0.20
TUNJA(config-subif)#ip access-group 122 in
TUNJA(config-subif)#exit
TUNJA(config)#
TUNJA(config)
```

| Fire | Last Status | Source | Destination | Type | Color | Time(sec) | Periodic | Num | Edit |
|------|-------------|---------|---------------|------|-------|-----------|----------|-----|--------|
| | Successful | vlan 20 | vlan vlan 20C | ICMP | | 0.000 | N | 0 | (edit) |
| | Successful | vlan 20 | vlan vlan 20C | ICMP | | 0.000 | N | 1 | (edit) |
| | Failed | vlan 20 | vlan 10 | ICMP | | 0.000 | N | 2 | (edit) |
| | Successful | vlan 20 | vlan vlan 20C | ICMP | | 0.000 | N | 3 | (edit) |

Ilustración 58 resultado mediante ping

Fuente: freydy, p. (20 de diciembre de 2019) Resultado de la configuración mediante el comando ping. Obtenido de packet tracer autoría propia

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

```

BUCARRAMANGA(config)#
BUCARRAMANGA(config)#access-list 131 permit ip 172.31.0.64 0.0.0.63
209.165.220.0 0.0.0.255
BUCARRAMANGA(config)#int g0/0.30
BUCARRAMANGA(config-subif)#ip access-group 131 in
BUCARRAMANGA(config-subif)#exit
BUCARRAMANGA(config)#
BUCARRAMANGA(config)#

```

| Fire | Last Status | Source | Destination | Type | Color | Time(sec) | Periodic | Num |
|------|-------------|----------|-------------|------|--------|-----------|----------|-----|
| | Successful | vlan 30B | vlan 10C | ICMP | Green | 0.000 | N | 0 |
| | Successful | vlan 30B | vlan 10C | ICMP | Blue | 0.000 | N | 1 |
| | Successful | vlan 30B | INERTNET, | ICMP | Purple | 0.000 | N | 2 |

Ilustración 59 resultado mediante ping

Fuente: freydy, p. (20 de diciembre de 2019) Resultado de la configuración mediante el comando ping. Obtenido de packet tracer autoría propia

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

```

BUCARRAMANGA(config)#
BUCARRAMANGA(config)#access-list 132 permit ip 172.31.0.0 0.0.0.63
172.31.1.64 0.0.0.63
BUCARRAMANGA(config)#int g0/0.10
BUCARRAMANGA(config-subif)#ip access-group 132 in
BUCARRAMANGA(config-subif)#exit
BUCARRAMANGA(config)#
BUCARRAMANGA(config)#

```

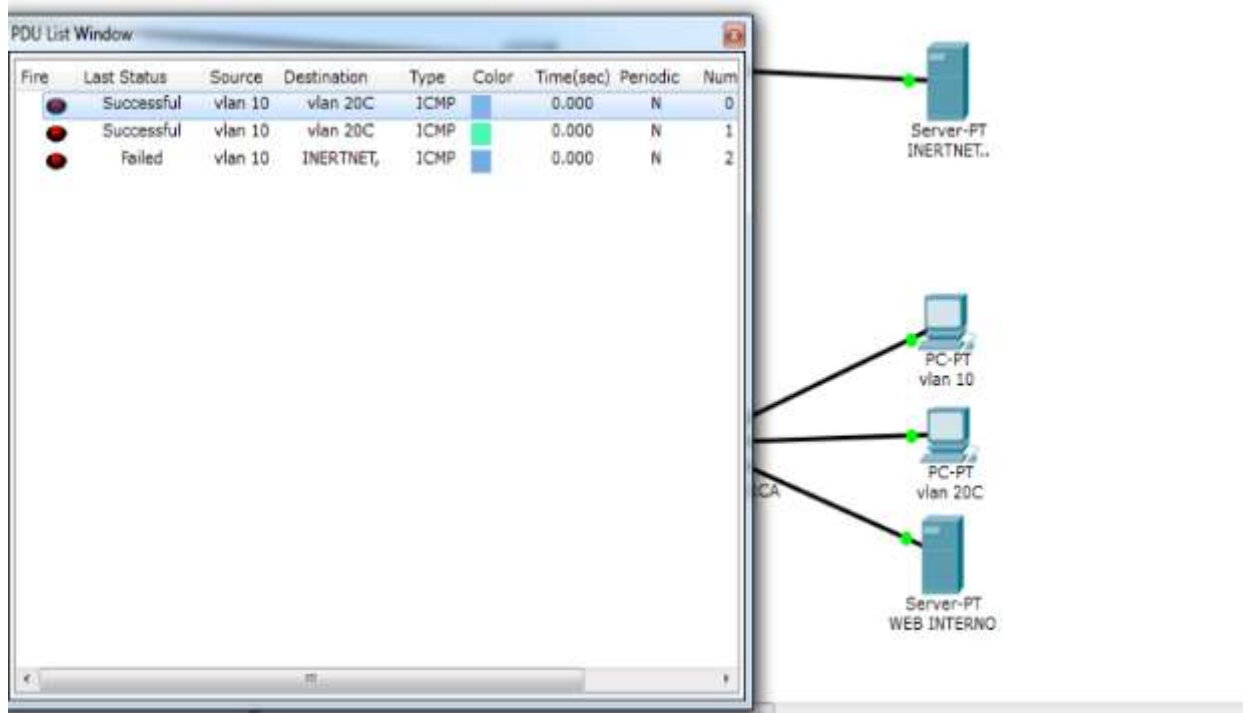


Ilustración 60 resultado mediante ping

Fuente: freydy, p. (20 de diciembre de 2019) Resultado de la configuración mediante el comando ping. Obtenido de packet tracer autoría propia

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

| BUCARAMANGA | TUNJA | CUNDINAMARCA |
|---|--|---|
| <pre> BUCARRAMANGA(config)# BUCARRAMANGA(config)#access-list 133 deny ip 172.31.2.0 0.0.0.7 172.31.0.0 0.0.0.63 BUCARRAMANGA(config)#access-list 133 deny ip 172.31.0.64 0.0.0.63 172.31.0.0 0.0.0.63 BUCARRAMANGA(config)#access-list 133 permit ip any any BUCARRAMANGA(config)#int g0/0.10 BUCARRAMANGA(config-subif)#ip access-group 133 out </pre> | <pre> TUNJA(config)# TUNJA(config)#access-list 133 deny ip 172.3.2.8 0.0.0.7 172.31.0.128 0.0.0.63 TUNJA(config)#access-list 133 deny ip 172.3.0.192 0.0.0.63 172.31.0.128 0.0.0.63 TUNJA(config)#access-list 133 permit ip any any TUNJA(config)#int g0/0.20 TUNJA(config-subif)#ip access-group 133 out TUNJA(config-subif)#exit TUNJA(config)# </pre> | <pre> CUNDINAMARCA(config)# CUNDINAMARCA(config)#access-list 133 deny ip 172.31.2.8 0.0.0.7 172.31.1.64 0.0.0.63 CUNDINAMARCA(config)#access-list 133 deny ip 172.31.1.0 0.0.0.63 172.31.1.64 0.0.0.63 CUNDINAMARCA(config)#access-list 133 deny ip 172.31.2.24 0.0.0.7 172.31.1.64 0.0.0.63 </pre> |

| | | |
|--|--|--|
| BUCARRAMANGA(config-subif)#exit BUCARRAMANGA(config)# | | CUNDINAMARCA(config)#access-list 133 permit ip any any CUNDINAMARCA(config)#int g0/0.20 CUNDINAMARCA(config-subif)#ip access-group 133 out CUNDINAMARCA(config-subif)#exit CUNDINAMARCA(config)# CUNDINAMARCA(config)# |
|--|--|--|

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

| BUCARAMANGA | TUNJA | CUNDINAMARCA |
|--|---|---|
| <pre> BUCARRAMANGA(config)# BUCARRAMANGA(config)#access-list f4 permit 172.31.2.0 0.0.0.7 ^ % Invalid input detected at '^' marker. BUCARRAMANGA(config)#access-list 5 permit 172.31.2.0 0.0.0.7 BUCARRAMANGA(config)#access-list 5 permit 172.3.2.8 0.0.0.7 BUCARRAMANGA(config)#access-list 5 permit 172.31.2.8 0.0.0.7 BUCARRAMANGA(config)#line vty 0 15 BUCARRAMANGA(config-line)#access-class 5 in BUCARRAMANGA(config-line)#exit BUCARRAMANGA(config)# BUCARRAMANGA(config)# BUCARRAMANGA# </pre> | <pre> TUNJA(config)# TUNJA(config)#access-list 5 permit 172.31.2.0 0.0.0.7 TUNJA(config)#access-list 5 permit 172.3.2.8 0.0.0.7 TUNJA(config)#access-list 5 permit 172.31.2.8 0.0.0.7 TUNJA(config)#line vty 0 15 TUNJA(config-line)#access-class 5 in TUNJA(config-line)#exit TUNJA(config)# TUNJA(config)# </pre> | <pre> CUNDINAMARCA(config)# CUNDINAMARCA(config)#access-list 5 permit 172.31.2.0 0.0.0.7 CUNDINAMARCA(config)#access-list 5 permit 172.3.2.8 0.0.0.7 CUNDINAMARCA(config)#access-list 5 permit 172.31.2.8 0.0.0.7 CUNDINAMARCA(config)#line vty 0 15 CUNDINAMARCA(config-line)#access-class 5 in CUNDINAMARCA(config-line)# CUNDINAMARCA(config-line)#exit CUNDINAMARCA(config)# </pre> |

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

ENLACE EXTERNO

Para sustentar la configuración de la topología y el direccionamiento en cada uno

<https://drive.google.com/file/d/1BzD-UOnStE3691BMP3nLR5RQOTXRmohw/view?usp=sharing>

Este enlace direcciona a un documento en Google Drive donde se puede descargar el archivo realizado en Packet Tracer (pkt). No aparece ninguna vista previa pero tiene la opción para descargarlo y a dar click automáticamente descarga el archivo.

CONCLUSIONES

- Durante la realización de la actividad se encuentran fallas en la aplicación práctica de los conceptos adquiridos durante el curso, como concepto personal, porque al principio no podía establecer las direcciones IP ya que estaban contenidas en una sola por lo tanto se opta por investigar en varias páginas para fortalecer y enriquecer el conocimiento y las habilidades.
- Con este diplomado de profundización se adquieren conocimientos sobre el Routing and Switching en la tecnología de redes CISCO, aprendizaje y habilidades necesarias para planificar, implementar, asegurar y solucionar problemas de redes empresariales convergentes, logrando así el desarrollo y cumplimiento de los 2 escenarios propuestos para esta prueba de habilidades, logrando comprender la implementación de protocolos de enrutamiento como lo son EIGRP Y OSPF, DHCP, además se utilizaron VLAN, las cuales son bastante útiles al momento de proteger la red implementada Y mediante los comandos show, se verificó que los protocolos se han realizado correctamente y mediante los comandos ping que tenga conectividad entre los diferentes dispositivos.
- El correcto direccionamiento IP tanto en Switches como en routers ya sea en una herramienta software como packet Tracer o en un laboratorio con equipos reales, permite lograr la correcta comunicación entre dispositivos en una red de datos teniendo presente su funcionamiento el cual está basado

en la implementación de una serie de protocolos que permiten la optimización de la red.

REFERENCIAS BIBLIOGRÁFICAS

- CISCO. (2014). Exploración de la red. Fundamentos de Networking. Recuperado de <https://staticcourse-assets.s3.amazonaws.com/ITN50ES/module1/index.html#1.0.1.1>
- CISCO. (2014). Configuración de un sistema operativo de red. Fundamentos de Networking. Recuperado de <https://static-course-assets.s3.amazonaws.com/ITN50ES/module2/index.html#2.0.1.1>
- CISCO. (2014). Protocolos y comunicaciones de red. Fundamentos de Networking. Recuperado de <https://static-course-assets.s3.amazonaws.com/ITN50ES/module2/index.html#3.0.1.1>
- CISCO. (2014). Acceso a la red. Fundamentos de Networking. Recuperado de <https://static-courseassets.s3.amazonaws.com/ITN50ES/module2/index.html#4.0.1.1>
- Cisco Networking Academy. (2018). CP - CCNA2. Routing y switching de CCNA: Principios básicos de routing y switching. Capítulo 1 al 6. Recuperado de <https://1314297.netacad.com/courses/627676>
- CISCO. (2014). Introducción a redes conmutadas. Principios de Enrutamiento y Conmutación. Recuperado de: <https://static-course-assets.s3.amazonaws.com/RSE50ES/module1/index.html#1.0.1.1>
- CISCO. (2014). Configuración y conceptos básicos de Switching. Principios de Enrutamiento y Conmutación. Recuperado de: <https://static-course-assets.s3.amazonaws.com/RSE50ES/module2/index.html#2.0.1.1>

CISCO. (2014). VLANs. Principios de Enrutamiento y Conmutación. Recuperado de: <https://static-course-assets.s3.amazonaws.com/RSE50ES/module3/index.html#3.0.1.1>

CISCO. (2014). Conceptos de Routing. Principios de Enrutamiento y Conmutación. Recuperado de: <https://static-course-assets.s3.amazonaws.com/RSE50ES/module4/index.html#4.0.1.1>

CISCO. (2014). Enrutamiento entre VLANs. Principios de Enrutamiento y Conmutación. Recuperado de: <https://static-course-assets.s3.amazonaws.com/RSE50ES/module5/index.html#5.0.1.1>