Solución de dos estudios de caso soportados en Tecnología CISCO

PRESENTADO POR:

JULIO ANDRES SILVA ARAGON

PRESENTADO A:

JUAN CARLOS VESGA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD

ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA

DIPLOMADO DE PROFUNDIZACIÓN CISCO

DISEÑO E IMPLEMENTACIÓN DE SOLUCIONES INTEGRADAS LAN / WAN

2019

Resumen

El propósito del programa de FORMACIÓN (Básica e Intermedia) EN REDES DE COMUNICACIÓN, es facilitar la Certificación de CCENT (Cisco Certified Entry Network Technician) la cual es otorgada por el proveedor tecnológico CISCO, se incluye el currículo de CISCO CCNA (Cisco Certified Network Associate), el cual está conformado por sus 2 primeros módulos (CCNA1 y CCNA2), que proveen bases necesarias para realizar las tareas básicas del trabajo en redes como son instalación de cableado, mantenimiento, configuración de dispositivos, entre otras.

Hoy en día las redes empresariales están pasando por una serie de transformaciones como consecuencia de los avances tecnológicos y del cambio en el enfoque de las TI, que las acerca cada vez más a ser las verdaderas impulsoras de los objetivos del negocio, teniendo la Red como interconexión física o inalámbrica que vincula varios dispositivos informáticos (servidores, computadoras, teléfonos móviles, periféricos, entre otros) para que se comuniquen entre sí, con la finalidad de compartir datos y ofrecer servicios.

Las redes hoy más que nunca, son necesarias para ofrecer la mejor conectividad para los usuarios, de forma confiable y segura, al tiempo en que se permite obtener la información necesaria para tomar decisiones y hacer crecer los negocio, teniendo en cuenta estas características a la hora de elegir la infraestructura de red para su PyME las redes son definidas por software, o SDN, son una manera de abordar la gestión de redes, en ellas, el control se desvincula totalmente del hardware y se le da a una aplicación de software llamada controlador, esto es especialmente útil en ambientes distribuidos y de nube, porque le permite al administrador manejar cargas de tráfico de manera flexible y más eficiente.

Abstract

The purpose of the TRAINING program (Basic and Intermediate) in COMMUNICATION NETWORKS, is to facilitate the Certification of CCENT (Cisco Certified Entry Network Technician) which is granted by the technology provider CISCO, including the CISCO CCNA (Cisco Certified Network) curriculum Associate), which is made up of its first 2 modules (CCNA1 and CCNA2), which provide the necessary bases to perform the basic tasks of networking, such as wiring installation, maintenance, configuration of devices, among others.

Today, business networks are going through a series of transformations as a result of technological advances and the change in the IT approach, which increasingly brings them closer to being the true drivers of business objectives, with the Network as physical or wireless interconnection that links several computing devices (servers, computers, mobile phones, peripherals, among others) to communicate with each other, in order to share data and offer services.

Networks today more than ever, are necessary to offer the best connectivity for users, in a reliable and secure way, while allowing the necessary information to make decisions and grow business, taking these characteristics into account When choosing the network infrastructure for your SME, the networks are defined by software, or SDN, they are a way of approaching network management, in them, the control is completely disconnected from the hardware and is given to a software application called controller, this is especially useful in distributed and cloud environments, because it allows the administrator to handle traffic loads flexibly and more efficiently.

Introducción

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.

En el mundo actual, las redes conectan todo, desde los usuarios y dispositivos en un campus o sucursal hasta una aplicación en el centro de datos o la nube, la red tiene el potencial de adaptar, proteger e informar constantemente a todos los procesos empresariales y de TI, teniendo en cuenta siempre las políticas de seguridad y la segmentación de aplicaciones combinadas en el acceso, la WAN y el centro de datos o la nube para cumplir un objetivo empresarial, que es la conectividad integrada y la seguridad entregada en la nube proporcionando acceso seguro a Internet y aplicaciones SaaS y escalas para el crecimiento futuro del tráfico.

Cisco ofrece soluciones, independientemente de su prioridad sea obtener una visibilidad completa de la red o simplificar su red WAN, de sucursal o de acceso por cable o inalámbrico con redes definidas por software o si necesita optimizar su infraestructura para el acceso a aplicaciones en la nube, una fuerza de trabajo móvil, Internet de las cosas (IdC), o las tres cosas juntas, las soluciones están diseñadas para satisfacer todo tipo de necesidad, además, son escalables, de las implementaciones más pequeñas a las más grandes, siempre hay soluciones que se incluyen para encontrar las que mejor responden a las exigencias de las organizaciones sin dejar a lado que el éxito de la transformación digital depende de una implementación exitosa.

Objetivos

- Enlazar dos o más dispositivos para que exista comunicación entre ellos o para compartir información

- proporcionar una alta fiabilidad, al contar con fuentes alternativas de suministro.

- proporcionar una forma económica de aumentar el número de computadoras de una organización o institución, al permitir la conexión de estaciones de trabajo que dan paso al intercambio de información y optimizan el desarrollo de las diferentes actividades de la empresa.

- intercambiar información que permitan la comunicación entre una empresa y sus clientes.

Desarrollo de los dos escenarios

Escenario 1

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

Topología de red Los requerimientos solicitados son los siguientes:

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

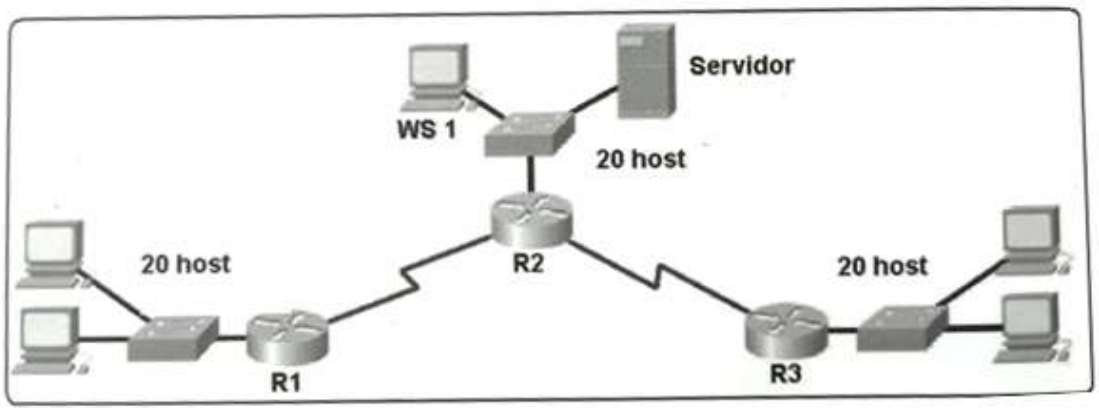


Figura 1: esquema escenario 1

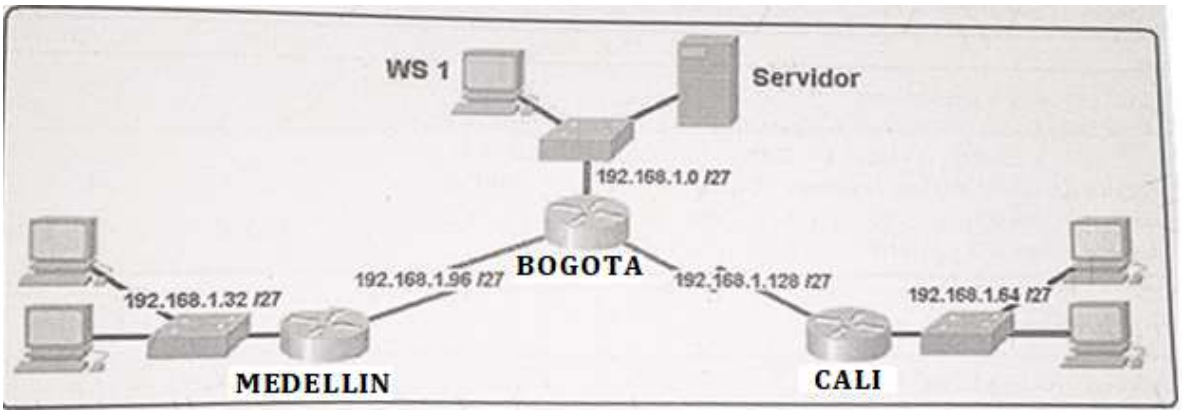


Figura 2: esquema escenario 1

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

Como trabajo inicial se debe realizar lo siguiente.

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

• Realizar la conexión física de los equipos con base en la topología de red Configurar la topología de red, de acuerdo con las siguientes especificaciones.

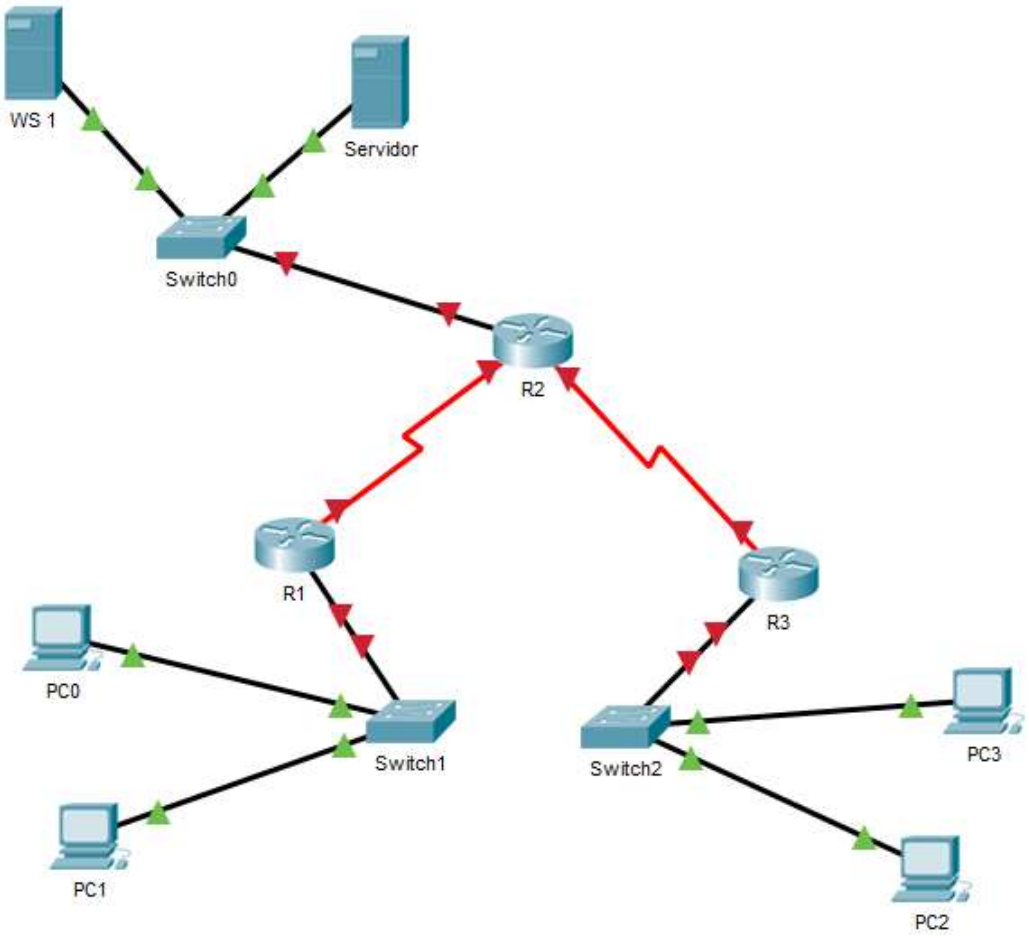


Figura 3: esquema escenario 1 en packet tracer

Parte 2: Configuración Básica.

a. Configure la dirección IP que se indica en la tabla 1, de direccionamiento para todas las interfaces.
b. Establezca la frecuencia de reloj para todas las interfaces seriales DCE en **128000**.
c. Copie la configuración en ejecución en la configuración de inicio

	R1	R2	R3
Nombre de Host	**MEDELLIN**	**BOGOTA**	**CALI**
Dirección de Ip en interfaz Serial 0/0	192.168.1.99	192.168.1.98	192.168.1.131
Dirección de Ip en interfaz Serial 0/1		192.168.1.130	
Dirección de Ip en interfaz FA 0/0	192.168.1.33	192.168.1.1	192.168.1.65
Protocolo de enrutamiento	**Eigrp**	**Eigrp**	**Eigrp**
Sistema Autónomo	200	200	200
Afirmaciones de red	192.168.1.0	192.168.1.0	192.168.1.0

Tabla 1: Protocolo de enrutamiento

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.

R1 - Medellin

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname R1-Medellin
R1-Medellin(config)#no ip domain-lookup
R1-Medellin(config)#int S0/0/0
R1-Medellin(config-if)#ip address 192.168.1.99 255.255.255.224
This command applies only to DCE interfaces
R1-Medellin(config-if)#no shutdown
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to down

R1-Medellin(config)#int g0/0
R1-Medellin(config-if)#ip address 192.168.1.33 255.255.255.224
R1-Medellin(config-if)#no shutdown
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up

R1-Medellin#copy running-config startup-config
```

R2 - Bogota

```
Router>enable
```

```
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname R2-Bogota
R2-Bogota(config)#no ip domain-lookup
R2-Bogota(config)#int S0/1
R2-Bogota (config-if)#ip address 192.168.1.130 255.255.255.224
R2-Bogota(config-if)#clock rate 128000
This command applies only to DCE interfaces
R2-Bogota(config-if)#no shutdown
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to down

R2-Bogota(config)#int S0/0
R2-Bogota (config-if)#ip address 192.168.1.98 255.255.255.224
R2-Bogota(config-if)#clock rate 128000
This command applies only to DCE interfaces
R2-Bogota(config-if)#no shutdown
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to down

R2-Bogota (config)#int g0/0
R2-Bogota (config-if)#ip address 192.168.1.1 255.255.255.224
R2-Bogota (config-if)#no shutdown
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up

R2-Bogota#copy running-config startup-config
```

R3 - Cali

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname R3-Cali
R3-Cali(config)#no ip domain-lookup
R3-Cali(config)#int S0/0/0
R3-Cali (config-if)#ip address 192.168.1.131 255.255.255.224
This command applies only to DCE interfaces
R3-Cali (config-if)#no shutdown
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to down

R3-Cali (config)#int g0/0
R3-Cali (config-if)#ip address 192.168.1.65 255.255.255.224
R3-Cali (config-if)#no shutdown
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up

R3-Cali#copy running-config startup-config
```

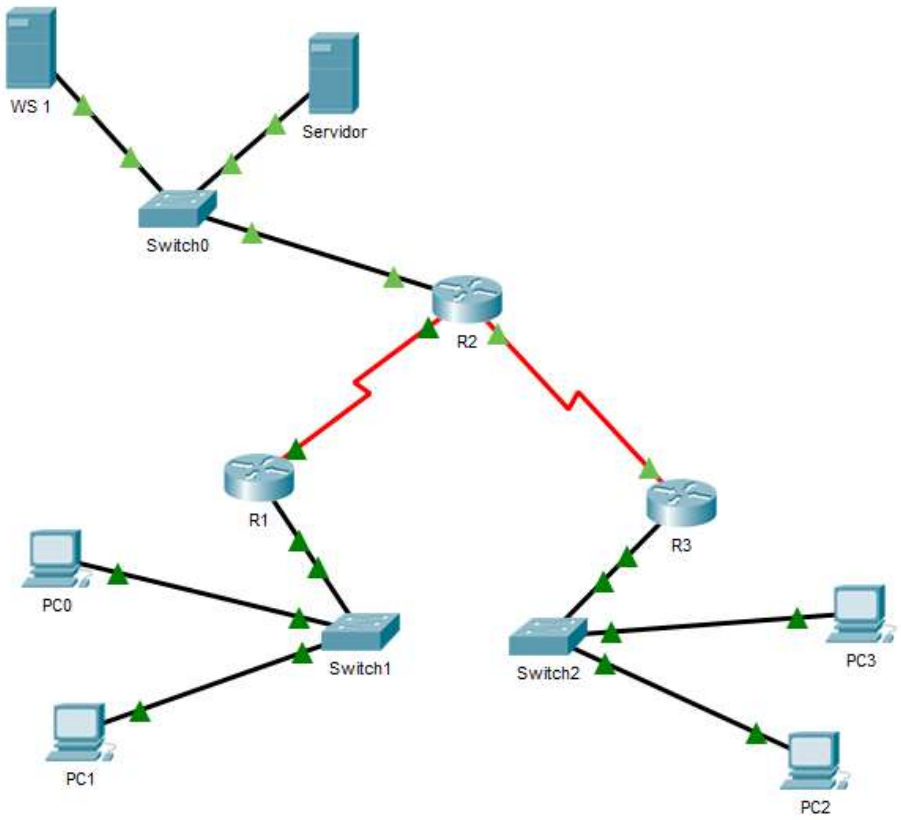


Figura 4: esquema con configuraciones según requerimiento

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.

Parte 3: Configuración de Enrutamiento.

a. Asignar el protocolo de enrutamiento EIGRP a los routers considerando el direccionamiento diseñado.
b. Verificar si existe vecindad con los routers configurados con EIGRP.
c. Realizar la comprobación de las tablas de enrutamiento en cada uno de los routers para verificar cada una de las rutas establecidas.
d. Realizar un diagnóstico para comprobar que cada uno de los puntos de la red se puedan ver y tengan conectividad entre sí. Realizar esta prueba desde un host de la red LAN del router CALI, primero a la red de MEDELLIN y luego al servidor.

R1 – Medellin

R1-Medellin>enable
R1-Medellin#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R1-Medellin(config)#router eigrp 200
R1-Medellin(config-router)#network 192.168.1.99 0.0.0.0
R1-Medellin(config-router)#network 192.168.1.33 0.0.0.0
R1-Medellin(config-router)#no auto-summary

```
R1-Medellin#show ip eigrp neighbors
IP-EIGRP neighbors for process 200
H   Address         Interface      Hold Uptime    SRTT   RTO   Q
Seq
                                   (sec)          (ms)        Cnt
Num
0   192.168.1.98    Se0/0/0        14   00:07:22  40     1000  0   7
```

Figura 5: evidencia Route Medellin

```
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 [90/2172416] via 192.168.1.98, 00:07:23,
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 [90/2684416] via 192.168.1.98, 00:07:18,
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, 00:07:20,
Serial0/0/0
```

Figura 6: evidencia Route Medellin

R2 – Bogota

R2-Bogota>enable
R2-Bogota#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R2-Bogota(config)#router eigrp 200
R2-Bogota(config-router)#network 192.168.1.98 0.0.0.0
R2-Bogota(config-router)#network 192.168.1.130 0.0.0.0
R2-Bogota(config-router)#network 192.168.1.1 0.0.0.0
R2-Bogota(config-router)#no auto-summary

```
R2-Bogota#show ip eigrp neighbors
IP-EIGRP neighbors for process 200
H   Address         Interface      Hold Uptime    SRTT   RTO   Q
Seq
                                   (sec)          (ms)       Cnt
Num
0   192.168.1.99    Se0/0/0        10   00:07:22  40     1000  0   7
1   192.168.1.131   Se0/0/1        11   00:07:18  40     1000  0   7
```

Figura 7: evidencia Route Bogota

```
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 [90/2172416] via 192.168.1.99, 00:07:23,
Serial0/0/0
D       192.168.1.64/27 [90/2172416] via 192.168.1.131, 00:07:18,
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
```

Figura 8: evidencia Route Bogota

R3 - Cali

R3-Cali>enable
R3-Cali#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R3-Cali(config)#router eigrp 200
R3-Cali(config-router)#network 192.168.1.131 0.0.0.0
R3-Cali(config-router)#network 192.168.1.65 0.0.0.0
R3-Cali(config-router)#no auto-summary

```
R3-Cali#show ip eigrp neighbors
IP-EIGRP neighbors for process 200
H   Address         Interface      Hold Uptime    SRTT   RTO   Q
Seq
                                   (sec)          (ms)       Cnt
Num
0   192.168.1.130   Se0/0/0        13   00:07:18  40     1000  0   8
```

Figura 9: evidencia Route Cali

```
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 [90/2172416] via 192.168.1.130, 00:07:18,
Serial0/0/0
D       192.168.1.32/27 [90/2684416] via 192.168.1.130, 00:07:18,
Serial0/0/0
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, 00:07:18,
Serial0/0/0
C       192.168.1.128/27 is directly connected, Serial0/0/0
L       192.168.1.131/32 is directly connected, Serial0/0/0
```

Figura 10: evidencia Route Cali

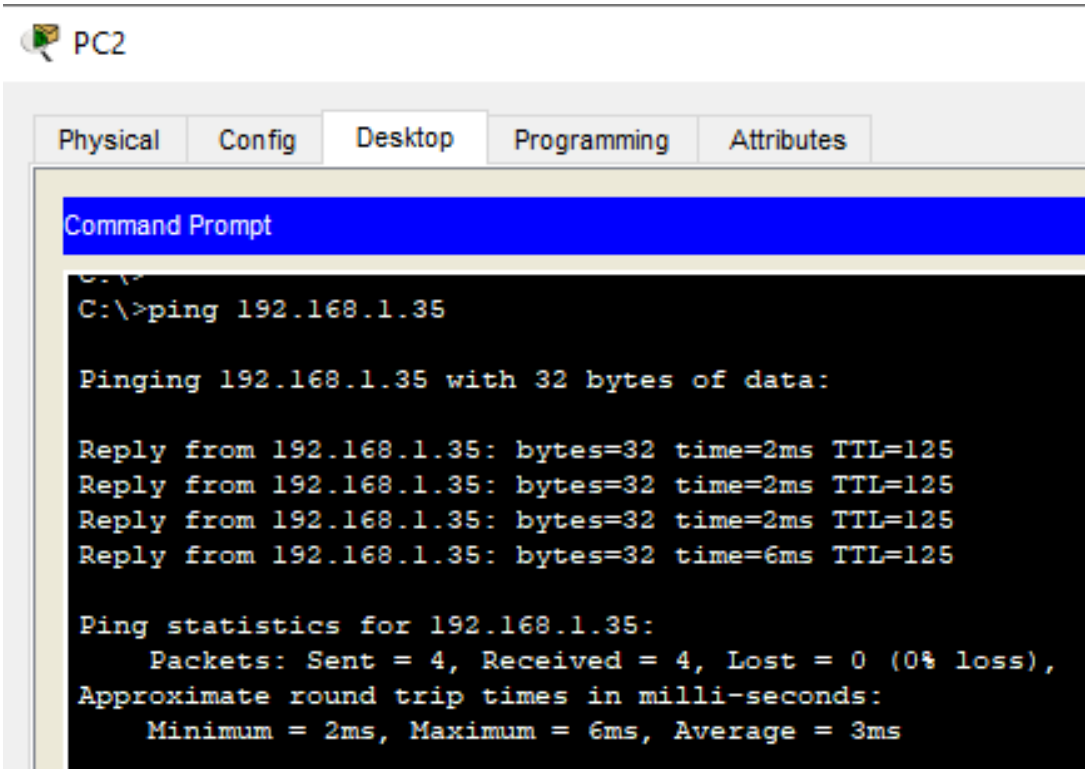


Figura 11: Ping 192.168.1.35

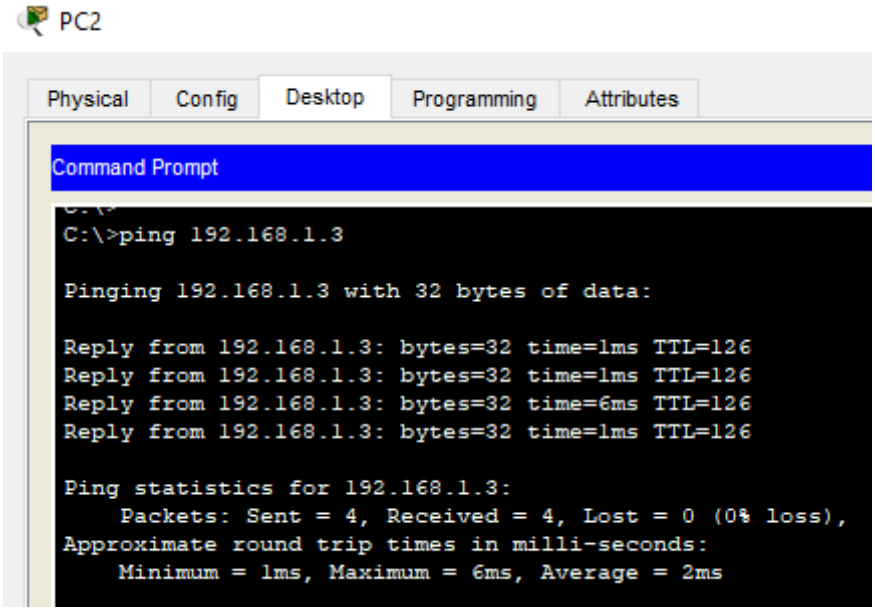


Figura 12: Ping 192.168.1.3

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

En este momento cualquier usuario de la red tiene acceso a todos sus dispositivos y estaciones de trabajo. El jefe de redes le solicita implementar seguridad en la red.

Para esta labor se decide configurar listas de control de acceso (ACL) a los routers.

Las condiciones para crear las ACL son las siguientes:

a. Cada router debe estar habilitado para establecer conexiones Telnet con los demás routers y tener acceso a cualquier dispositivo en la red.
b. El equipo WS1 y el servidor se encuentran en la subred de administración. Solo el servidor de la subred de administración debe tener acceso a cualquier otro dispositivo en cualquier parte de la red.
c. Las estaciones de trabajo en las LAN de MEDELLIN y CALI no deben tener acceso a ningún dispositivo fuera de su subred, excepto para interconectar con el servidor.

R1 – Medellin

```
R1-Medellin>enable
R1-Medellin#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R1-Medellin(config)#line vty 0 4
R1-Medellin(config-line)#password cisco
R1-Medellin(config-line)#login
R1-Medellin(config-line)#exit
R1-Medellin(config)#
```

R2 – Bogota

```
R2-Bogota>enable
R2-Bogota#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R2-Bogota(config)#line vty 0 4
R2-Bogota(config-line)#password cisco
R2-Bogota(config-line)#login
R2-Bogota(config-line)#exit
R2-Bogota(config)#
```

R3 - Cali

```
R3-Cali>enable
R3-Cali#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
```

```
R3-Cali(config)#line vty 0 4
R3-Cali(config-line)#password cisco
R3-Cali(config-line)#login
R3-Cali(config-line)#exit
R3-Cali(config)#
```

Parte 5: Comprobación de la red instalada.

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

	ORIGEN	DESTINO	RESULTADO
TELNET	**Router MEDELLIN**	**Router CALI**	Ok
	WS_1	**Router BOGOTA**	Ok
	Servidor	**Router CALI**	Ok
	Servidor	**Router MEDELLIN**	Ok
TELNET	**LAN del Router MEDELLIN**	**Router CALI**	Denegado
	LAN del Router CALI	**Router CALI**	Denegado
	LAN del Router MEDELLIN	**Router MEDELLIN**	Denegado
	LAN del Router CALI	**Router MEDELLIN**	Denegado
PING	**LAN del Router CALI**	**WS_1**	Denegado
	LAN del Router MEDELLIN	**WS_1**	Denegado
	LAN del Router MEDELLIN	**LAN del Router CALI**	Denegado
PING	**LAN del Router CALI**	**Servidor**	Denegado
	LAN del Router MEDELLIN	**Servidor**	Denegado
	Servidor	**LAN del Router MEDELLIN**	Ok
	Servidor	**LAN del Router CALI**	Ok
	Router CALI	**LAN del Router MEDELLIN**	Denegado
	Router MEDELLIN	**LAN del Router CALI**	Ok

Tabla 2: Resultado de las configuraciones y pruebas realizadas

Escenario 2

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

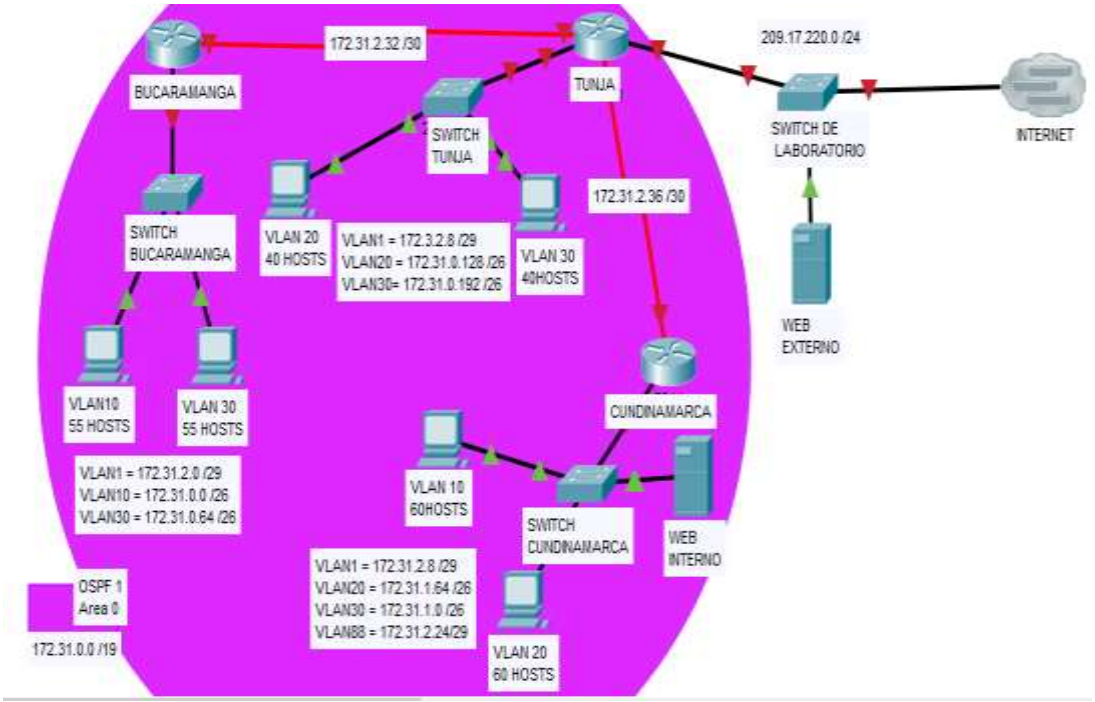


Figura 13: Esquema escenario 2

Desarrollo

Los siguientes son los requerimientos necesarios:

1. **Todos los routers deberán tener los siguiente:**
   - **Configuración básica.**
   - **Autenticación local con AAA.**
   - **Cifrado de contraseñas.**
   - **Un máximo de internos para acceder al router.**
   - **Máximo tiempo de acceso al detectar ataques.**
   - **Establezca un servidor TFTP y almacene todos los archivos necesarios de los routers.**

Router Tunja

```
Building configuration...
Current configuration : 1246 bytes
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
hostname TUNJA
enable secret 5 $1$mERr$hx5rVt7rPNoS4wqbXKX7m0
aaa new-model
aaa authentication login TELNET-LOGIN local
aaa authentication login default local
no ip cef
no ipv6 cef
license udi pid CISCO2901/K9 sn FTX1524ZEH3-
no ip domain-lookup
spanning-tree mode pvst
interface GigabitEthernet0/0
no ip address
duplex auto
speed auto
shutdown
interface GigabitEthernet0/1
no ip address
duplex auto
speed auto
interface GigabitEthernet0/1/0
no ip address
shutdown
interface FastEthernet0/2/0
switchport mode access
interface FastEthernet0/2/1
switchport mode access
interface FastEthernet0/2/2
switchport mode access
interface FastEthernet0/2/3
switchport mode access
interface Serial0/3/0
ip address 172.31.2.34 255.255.255.252
interface Serial0/3/1
ip address 172.31.2.37 255.255.255.252
```

clock rate 2000000
interface Vlan1
no ip address
shutdown
ip classless
ip flow-export version 9
line con 0
password 7 0822455D0A16
line aux 0
line vty 0 4
password 7 0822455D0A16
End

Router Cundinamarca

Current configuration : 1180 bytes
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
hostname CUNDINAMARCA
enable secret 5 1mERr$hx5rVt7rPNoS4wqbXKX7m0
aaa new-model
aaa authentication login TELNET-LOGIN local
aaa authentication login default local
no ip cef
no ipv6 cef
license udi pid CISCO1941/K9 sn FTX1524LTTQ-
no ip domain-lookup
spanning-tree mode pvst
interface GigabitEthernet0/0
no ip address
duplex auto
speed auto
interface GigabitEthernet0/1
no ip address
duplex auto
speed auto
shutdown
interface FastEthernet0/0/0
switchport mode access

```
interface FastEthernet0/0/1
switchport mode access
interface FastEthernet0/0/2
switchport mode access
interface FastEthernet0/0/3
switchport mode access
interface Serial0/1/0
ip address 172.31.2.38 255.255.255.252
interface Serial0/1/1
no ip address
clock rate 2000000
shutdown
interface Vlan1
no ip address
shutdown
ip classless
ip flow-export version 9
line con 0
password 7 0822455D0A16
line aux 0
line vty 0 4
password 7 0822455D0A16
end
```

Router Cundinamarca

```
Current configuration : 1199 bytes
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
hostname BUCARAMANGA
enable secret 5 $1$mERr$hx5rVt7rPNoS4wqbXKX7m0
aaa new-model
aaa authentication login TELNET-LOGIN local
aaa authentication login default local
no ip cef
no ipv6 cef
license udi pid CISCO1941/K9 sn FTX1524EZA2-
no ip domain-lookup
```

```
spanning-tree mode pvst
interface GigabitEthernet0/0
no ip address
duplex auto
speed auto
shutdown
interface GigabitEthernet0/1
no ip address
duplex auto
speed auto
interface FastEthernet0/0/0
switchport mode access
interface FastEthernet0/0/1
switchport mode access
interface FastEthernet0/0/2
switchport mode access
interface FastEthernet0/0/3
switchport mode access
interface Serial0/1/0
ip address 172.31.2.33 255.255.255.252
clock rate 2000000
interface Serial0/1/1
no ip address
clock rate 2000000
shutdown
interface Vlan1
no ip address
shutdown
ip classless
ip flow-export version 9
line con 0
password 7 0822455D0A16
line aux 0
line vty 0 4
password 7 0822455D0A16
end
```

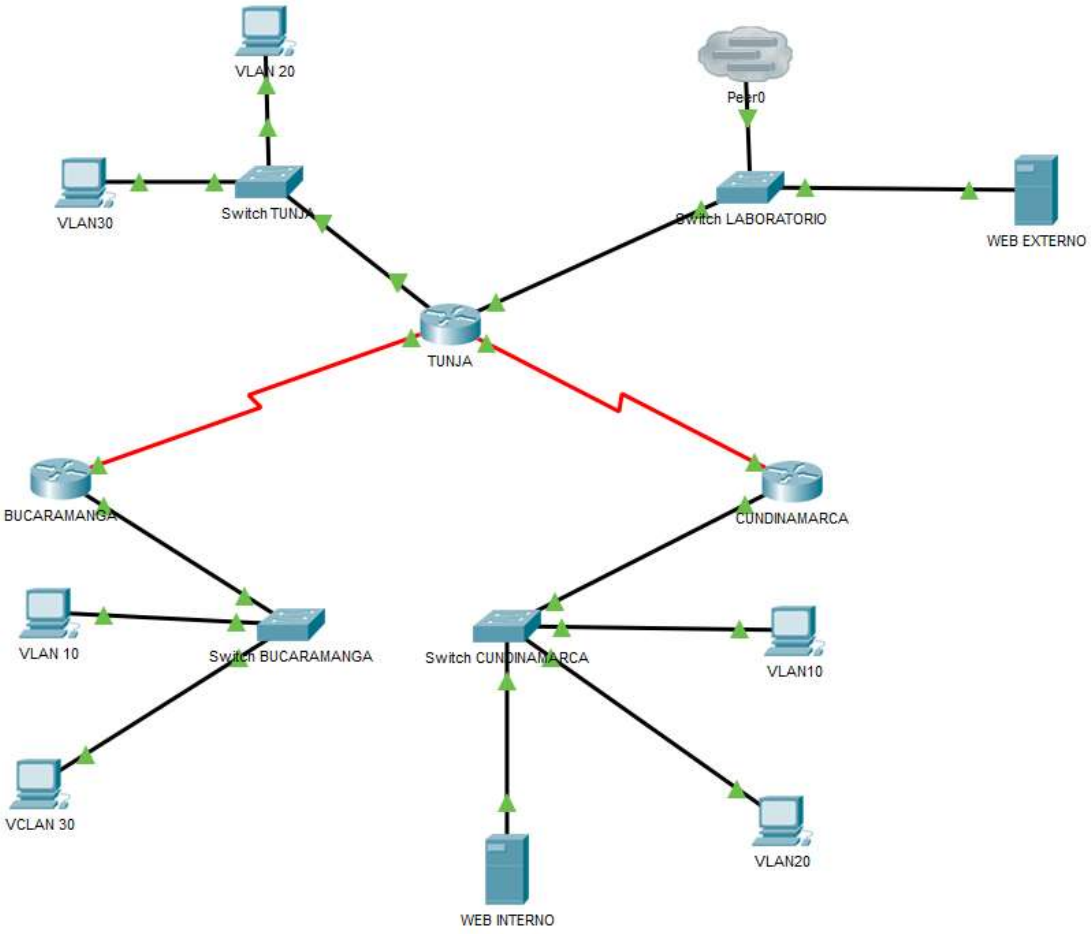


Figura 14: evidencia de esquema funcionando en packet tracert

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

DHCP Tunja:

TUNJA>enable
Password:
Password:
TUNJA#conf terminal
Enter configuration commands, one per line. End with CNTL/Z.
TUNJA(config)#ip dhcp excluded-address 172.31.2.1 172.31.2.2
TUNJA(config)#ip dhcp excluded-address 172.31.0.1 172.31.0.2

TUNJA(config)#ip dhcp excluded-address 172.31.0.65 172.31.0.66
TUNJA(config)#ip dhcp excluded-address 172.31.2.9 172.31.2.10
TUNJA(config)#ip dhcp excluded-address 172.31.1.65 172.31.1.66
TUNJA(config)#ip dhcp excluded-address 172.31.1.1 172.31.1.2
TUNJA(config)#ip dhcp excluded-address 172.31.2.25 172.31.2.26
TUNJA(config)#ip dhcp excluded-address 172.31.2.11
TUNJA(config)#ip dhcp pool BucaramangaV1
TUNJA(dhcp-config)#network 172.31.2.0 255.255.255.248
TUNJA(dhcp-config)#default-router 172.31.2.1
TUNJA(dhcp-config)#ip dhcp pool BucaramangaV10
TUNJA(dhcp-config)#network 172.31.0.0 255.255.255.192
TUNJA(dhcp-config)#default-router 172.31.0.1
TUNJA(dhcp-config)#ip dhcp pool BucaramangaV30
TUNJA(dhcp-config)#network 172.31.0.64 255.255.255.192
TUNJA(dhcp-config)#default-router 172.31.0.65
TUNJA(dhcp-config)#ip dhcp pool CundinamarcaV1
TUNJA(dhcp-config)#network 172.31.2.8 255.255.255.248
TUNJA(dhcp-config)#default-router 172.31.2.9
TUNJA(dhcp-config)#ip dhcp pool CundinamarcaV20
TUNJA(dhcp-config)#network 172.31.1.64 255.255.255.192
TUNJA(dhcp-config)#default-router 172.31.1.65
TUNJA(dhcp-config)#ip dhcp pool CundinamarcaV30
TUNJA(dhcp-config)#network 172.31.1.0 255.255.255.192
TUNJA(dhcp-config)#default-router 172.31.1.1
TUNJA(dhcp-config)#ip dhcp pool CundinamarcaV88
TUNJA(dhcp-config)#network 172.31.2.24 255.255.255.248
TUNJA(dhcp-config)#default-router 172.31.2.25
TUNJA(dhcp-config)#end
TUNJA#
%SYS-5-CONFIG_I: Configured from console by console
TUNJA#copy run start
Destination filename [startup-config]?

DHCP Bucaramanga:

BUCARAMANGA>enable
Password:
Password:
BUCARAMANGA#conf t
Enter configuration commands, one per line. End with CNTL/Z.
BUCARAMANGA(config)#int g0/1.1

```
BUCARAMANGA(config-subif)#ip helper-address 172.31.2.34
BUCARAMANGA(config-subif)#int g0/1.10
BUCARAMANGA(config-subif)#ip helper-address 172.31.2.34
BUCARAMANGA(config-subif)#int g0/1.30
BUCARAMANGA(config-subif)#ip helper-address 172.31.2.34
BUCARAMANGA(config-subif)#end
BUCARAMANGA#
%SYS-5-CONFIG_I: Configured from console by console
BUCARAMANGA#copy run start
Destination filename [startup-config]?
```

Se utiliza el DHCP pool. LAN Bucaramanga

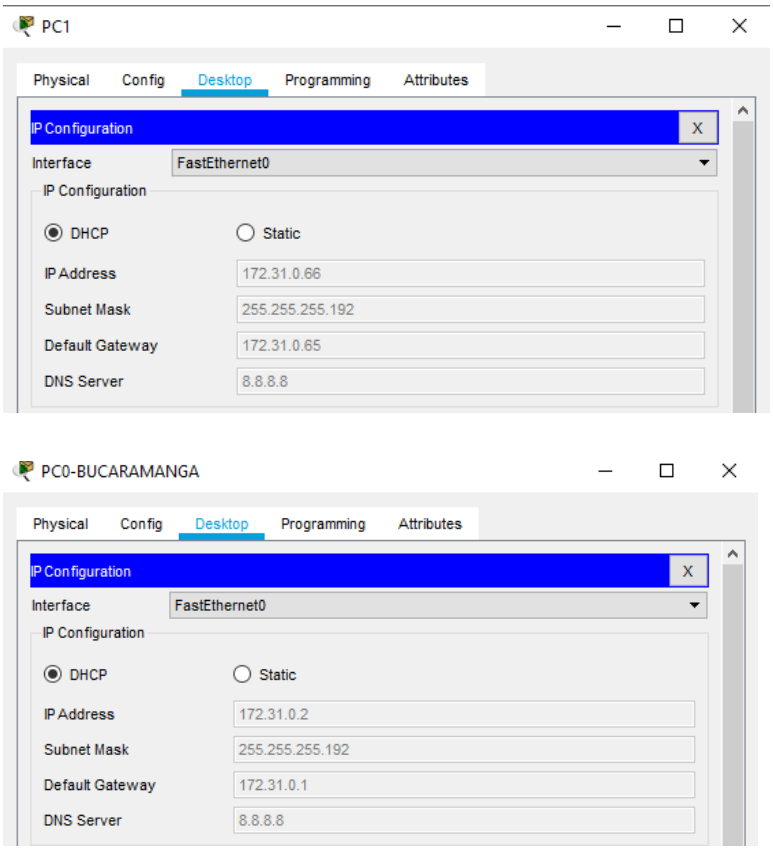


Figura 15: evidencia de configuración DHCP A PC DE Bucaramanga

DHCP Cundinamarca:

```
CUNDINAMARCA>enable
```

```
Password:
Password:
CUNDINAMARCA#conf t
Enter configuration commands, one per line. End with CNTL/Z.
CUNDINAMARCA(config)#int g0/1.1
CUNDINAMARCA(config-subif)#ip helper-address 172.31.2.37
CUNDINAMARCA(config-subif)#int g0/1.20
CUNDINAMARCA(config-subif)#ip helper-address 172.31.2.37
CUNDINAMARCA(config-subif)#int g0/1.30
CUNDINAMARCA(config-subif)#ip helper-address 172.31.2.37
CUNDINAMARCA(config-subif)#int g0/1.88
CUNDINAMARCA(config-subif)#ip helper-address 172.31.2.37
CUNDINAMARCA(config-subif)#end
CUNDINAMARCA#
%SYS-5-CONFIG_I: Configured from console by console
CUNDINAMARCA#copy run start
Destination filename [startup-config]?
```

Se utiliza el DHCP pool. LAN Cundinamarca

Figura 15: evidencia de configuración DHCP A PC DE Cundinamarca

3. **El enrutamiento deberá tener autenticación.**

```
TUNJA(config)#ip nat inside source static 172.31.1.67
209.17.220.2 TUNJA(config)#interface fa0/1
TUNJA(config-if)#ip nat
outside TUNJA(config-
if)#interface se 0/0/1
TUNJA(config-if)#ip nat
inside TUNJA(config-
if)#exit
TUNJA(config)#ip nat inside source static 172.31.1.67
209.17.220.1 TUNJA(config)#interface fa0/1
TUNJA(config-if)#ip nat
outside TUNJA(config-
if)#interface se 0/0/1
TUNJA(config-if)#ip nat
inside TUNJA(config-
if)#exit
```

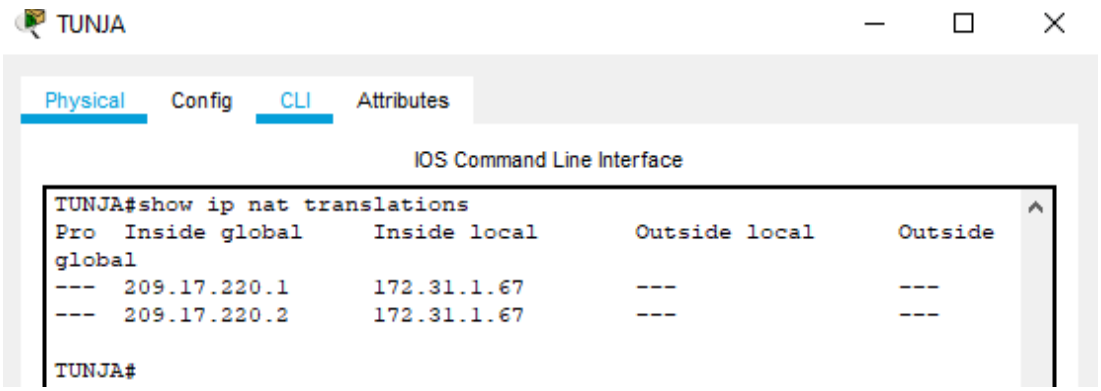


Figura 16: evidencia de configuración NAT Route tunja

4. **Listas de control de acceso:**
   - **Los hosts de VLAN 20 en Cundinamarca no acceden a internet, solo a la red interna de Tunja.**
   - **Los hosts de VLAN 10 en Cundinamarca si acceden a internet y no a la red interna de Tunja.**

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

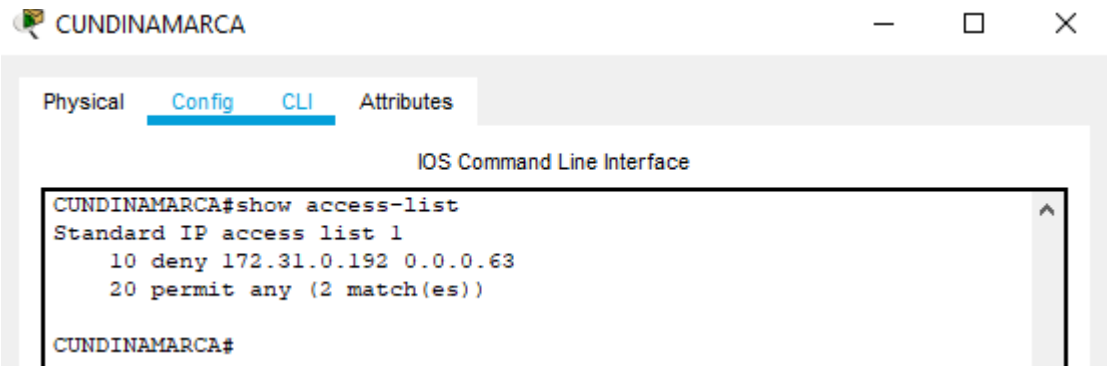
- Los hosts de VLAN 20 en Cundinamarca no acceden a internet, solo a la red interna de Tunja.

```
Username: NOMBRE60
Password:
CUNDINAMARCA>enable
Password:
CUNDINAMARCA#conf t
Enter configuration commands, one per line. End with CNTL/Z.
CUNDINAMARCA(config)#ip access-list extended LANCV30
CUNDINAMARCA(config-ext-nacl)#permit ip 172.31.1.0 0.0.0.63 172.31.2.16
0.0.0.7
CUNDINAMARCA(config-ext-nacl)#permit ip 172.31.1.0 0.0.0.63 172.31.0.128
0.0.0.63
CUNDINAMARCA(config-ext-nacl)#permit ip 172.31.1.0 0.0.0.63 172.31.0.192
0.0.0.63
CUNDINAMARCA(config-ext-nacl)#exit
CUNDINAMARCA(config)#int g0/1.30
CUNDINAMARCA(config-subif)#ip access-group LANCV30 in
CUNDINAMARCA(config-subif)#end
CUNDINAMARCA#
%SYS-5-CONFIG_I: Configured from console by console
```

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

```
CUNDINAMARCA(config)#access-list 1 deny 172.31.0.192 0.0.0.63
CUNDINAMARCA(config)#access-list 1 permit any
```

CUNDINAMARCA(config)#interface fa0/0
CUNDINAMARCA(config-if)#ip access-group 1 out

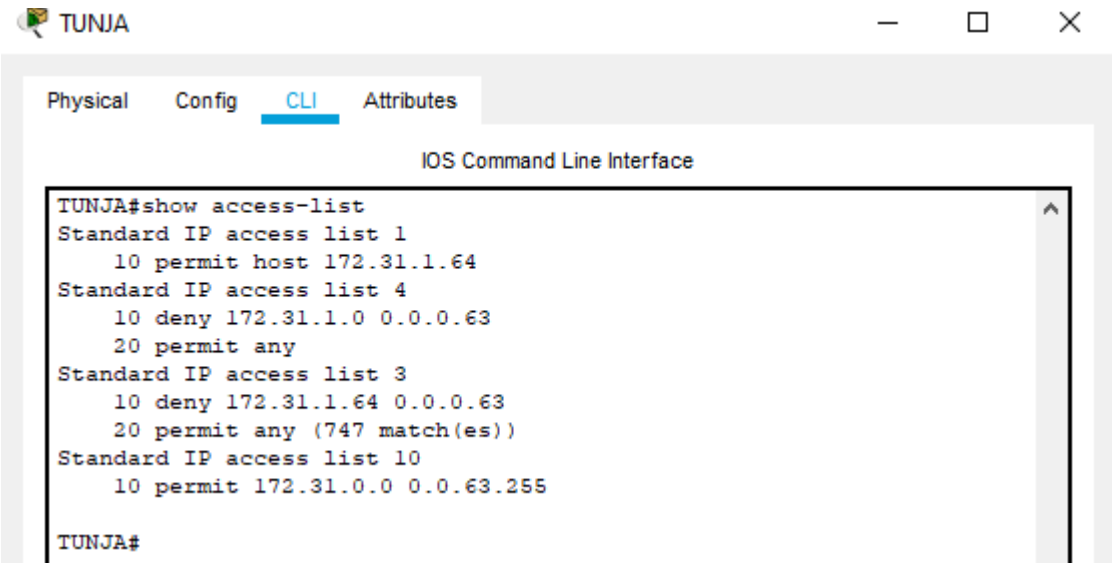


- Los hosts de VLAN 30 en Tunja solo acceden a servidores web y ftp de internet.

CUNDINAMARCA(config)#access-list 1 deny 172.31.0.192 0.0.0.63 CUNDINAMARCA(config)#access-list 1 permit any
CUNDINAMARCA(config)#interface fa0/0
CUNDINAMARCA(config-if)#ip access-group 1 out

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

CUNDINAMARCA(config)#access-list 1 deny 172.31.0.192 0.0.0.63
CUNDINAMARCA(config)#access-list 1 permit any
CUNDINAMARCA(config)#interface fa0/0
CUNDINAMARCA(config-if)#ip access-group 1 out



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

BUCARAMANGA(config)#access-list 2 permit 209.17.220.0
BUCARAMANGA (config)#access-list 2 permit host 172.31.0.0
BUCARAMANGA (config)#access-list 2 deny any
BUCARAMANGA (config)#interface fa0/0
BUCARAMANGA (config-if)#ip access-group 2 out

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

TUNJA(config)#access-list 3 permit 172.31.0.0
TUNJA(config)#interface fa0/0
TUNJA(config-if)#ip access-group 3 in
TUNJA(config-if)#

CUNDINAMARCA>en
Password:
CUNDINAMARCA#conf term
Enter configuration commands, one per line. End with CNTL/Z. CUNDINAMARCA(config)#access-list 3 permit 172.31.0.0 CUNDINAMARCA(config)#interface se0/0/0 CUNDINAMARCA(config-if)#ip access-group 3 in CUNDINAMARCA(config-if)#

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

Id	Host	Host encontrados	Direccion de red	Mascara de Sub red
1	55	62	172.31.0.0	255.255.255.192
2	55	62	172.31.0.64	255.255.255.192
3	40	62	172.31.0.128	255.255.255.192
4	40	62	172.31.0.192	255.255.255.192
5	60	62	172.31.1.0	255.255.255.192
6	60	62	172.31.1.64	255.255.255.192
7			172.31.1.128	
8			172.31.1.192	
9	6	6	172.31.2.0	255.255.255.248
10	6	6	172.31.2.8	255.255.255.248
11	6	6	172.31.2.16	255.255.255.248
12			172.31.2.24	
13	2	2	172.31.2.32	255.255.255.252
14	2	2	172.31.2.36	255.255.255.252

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

Conclusiones

- El Proceso de intercambio de información que permite la comunicación entre una empresa y sus clientes. Se utiliza ampliamente y forma la base en gran medida del uso de redes. Es aplicable cuando el cliente y el servidor están en el mismo edificio, pero también cuando están bastante retirados uno del otro y, por otra parte, el proceso se da, cuando el cliente envía una solicitud a través de la red al servidor de una empresa y espera una respuesta. Cuando el servidor recibe la solicitud, realiza el trabajo que se le pide o busca los datos solicitados y devuelve una respuesta.

- Los routers analizan los datos que se van a enviar a través de una red, los empaquetan de forma diferente y los envían a otra red o a través de un tipo de red distinto. Conectan su negocio con el mundo exterior, protegen la información de amenazas a la seguridad e, incluso, pueden decidir qué computadoras tienen prioridad sobre las demás.

- Las tecnologías de routing y switching pueden tener un impacto positivo en la base de su negocio. Puede ahorrar gastos mediante el uso compartido de aplicaciones, como impresoras y servidores, y servicios, como acceso a Internet. Además, una red conable puede crecer también al ritmo de su negocio, evitando el tener que reemplazarla conforme crecen sus necesidades.

- La globalización ha cambiado nuestra forma de trabajar. Los equipos virtuales, los trabajadores móviles y los teletrabajadores domésticos necesitan compartir información en todo momento. Las empresas modernas necesitan redes capaces de conectar empleados, proveedores, Socio de Negocioss y clientes, independientemente de su ubicación, de si se encuentran en la misma ciudad o al otro lado del mundo. Con la conectividad remota a través de una VPN, los empleados pueden acceder de

Bibliografía

- Redes basadas en intención. (2019, 7 agosto). Recuperado 12 diciembre, 2019, de https://www.cisco.com/c/es_co/solutions/intent-based-networking.html

- Soluciones de TI a la medida. (2019, 12 julio). Recuperado 12 diciembre, 2019, de https://www.cisco.com/c/es_pr/solutions/smb.html

- Diplomado preparación para la Certificación CISCO CCNP - Universidad Nacional Abierta y a Distancia UNAD - Educación Virtual. (s.f.). Recuperado 12 diciembre, 2019, de https://estudios.unad.edu.co/diplomado-preparacion-para-la-certificacion-cisco-ccnp

- Cisco SD-WAN Security. (2019, 28 noviembre). Recuperado 12 diciembre, 2019, de https://www.cisco.com/c/en/us/solutions/enterprise-networks/sd-wan/sd-wan-security.html

- Soluciones de redes empresariales de Cisco. (2019, 5 abril). Recuperado 12 diciembre, 2019, de https://www.cisco.com/c/es_bz/solutions/enterprise-networks/solution-listing.html

- Conceptos sobre tecnología de redes. (2019, 18 abril). Recuperado 12 diciembre, 2019, de https://www.cisco.com/c/es_co/solutions/smb/networks/infographic-basic-concepts.html