

DIPLOMADO DE PROFUNDIZACIÓN CISCO
DISEÑO E IMPLEMENTACIÓN DE SOLUCIONES INTEGRADAS LAN / WAN

PRESENTADO POR
JAVIER RAMÍREZ CASTILLO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
ESCUELA DE CIENCIAS BASICAS TECNOLOGIA E INGENIERÍA
INGENIERIA DE SISTEMAS
ZIQUAIRA
2020

DIPLOMADO DE PROFUNDIZACIÓN CISCO

JAVIER RAMÍREZ CASTILLO

TRABAJO EVALUATIVO DEL DIPLOMADO DE PROFUNDIZACIÓN
CISCO COMO OPCIÓN DE GRADO

Tutor

GIOVANNI ALBERTO BRACHO

Director

JUAN CARLOS VESGA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
ESCUELA DE CIENCIAS BASICAS TECNOLOGIA E INGENIERÍA
INGENIERIA DE SISTEMAS

ZIPAQUIRA

2020

NOTA DE ACEPTACIÓN

Presidente del jurado

Jurado

Jurado

Zipaquirá, 30 de enero de 2020

DEDICATORIA

Dedico este título especialmente a mi madre Aura María Castillo quien siempre me ha apoyado y confiado en mis capacidades; Ruego a Dios por su salud, y que, con su santa bondad, ella pueda verme recibir el título de Ingeniería de Sistemas.

Igualmente, a todas y cada una de aquellas personas que me ayudaron en mi proceso académico de una u otra manera, pues cada instrucción, cada palabra, cada consejo, inclusive, cada crítica, fue un granito de arena que me aportaron para lograr este objetivo.

AGRADECIMIENTOS

Primero que todo agradezco al todo poderoso en quien siempre encomiendo y confié todas mis acciones, por haberme regalado vida y licencia poder llevar a feliz término la culminación de la carrera. Y reitero mis agradecimientos a cada una de las personas que a lo largo de estos años mantuvo su disposición y paciencia para responderme de la mejor manera, ante cualquier requerimiento, necesidad e inquietud que tuve.



CONTENIDO

	Pág.
Glosario	7
Resumen	10
Abstract.	11
Introducción	12
Objetivos.....	13
Planteamiento escenario 1	14
1. Desarrollo escenario 1	15
1.1 Asignacion de direccion IP	16
a. Configuracion Basica (Puertos Bogota, Cali y Medellin)	17
b. Tabla de enrutamiento.....	17
c. Balanceo de carga Routers.....	19
d. Diagnostico de Vecinos mediante comando cdp	21
e. Prueba de Conectividad	21
1.2 Configuracion de Enrutamiento	22
a. Protocolo de enrutamiento EIGRP	22
b. Vecindad con Routers.....	25
c. Comprobación de las tablas de enrutamiento.....	23
d. Diagnostico de conectividad.....	23
1.3 Configuración de las listas de Control de Acceso	24
1.3.1 Prueba de Servidor a Cualquier dispositivo de red.....	25



1.3.2 Prueba entre otros dispositivos de la red	25
1.4 Comprobacion de la red Instalada (Comandos Ping – Telnet)	26
2. Desarrollo escenario 2	34
2.1 Autenticación local con AAA	35
2.2 Verificación de Autenticación de Acceso a Routers	35
2.3 VLANS.....	36
2.4 Cifrado de Contraseñas.....	37
2.5 Máximo de internos para acceder al router	38
2.6 Configuraciones de DHCP	38
2.7 Configuraciones NAT Estático y de Sobrecarga.....	39
2.8 Listas de Control de Acceso	42
Conclusiones	45
Referencias Bibliograficas	46



LISTA DE TABLAS

	Pág.
Tabla 1. Configuración Básica de Routers.....	17
Tabla 2. Pruebas Conectividad	27



LISTA DE FIGURAS

	Pág.
Figura 1. Topología de Red Dispuesta Escenario 1	17
Figura 2. Conectividad Escenario 1	15
Figura 3. B.C. Router Medellín.....	19
Figura 4. B.C. Router Bogotá.....	20
Figura 5. B.C. Router Cali	20
Figura 6. Ping Successful Bog- Med	33
Figura 7. Topología de Red Dispuesta Escenario 2.....	34
Figura 8. Conectividad Escenario	24



GLOSARIO

- **AAA:** acrónimo, corresponde a un tipo de protocolos que realizan tres funciones: autenticación, autorización y contabilización (en inglés, Authentication, Authorization and Accounting).
- **ACL:** Listas de Control de Acceso en Router Cisco, concepto de seguridad informática usado para fomentar la separación de privilegios.
- **Cisco:** Cisco Systems es una empresa global con sede en San José, California, Estados Unidos, principalmente dedicada a la fabricación, venta, mantenimiento y consultoría de equipos de telecomunicaciones.
- **Configuración:** Forma particular de una cosa, determinada por la disposición de las partes que la componen. Configuración de red permite especificar la forma en que el sistema se conecta a otros equipos y a Internet.
- **DHCP:** Protocolo de configuración dinámica de host (en inglés: Dynamic Host Configuration Protocol, es un protocolo de red de tipo cliente/servidor mediante el cual un servidor DHCP asigna dinámicamente una dirección IP y otros parámetros de configuración de red a cada dispositivo en una red para que puedan comunicarse con otras redes IP.
- **Dispositivo:** Pieza o conjunto de piezas o elementos preparados para realizar una función determinada y que generalmente forman parte de un conjunto más complejo. Los dispositivos electrónicos de interconexión son los que centralizan todo el cableado de una red en estrella o en árbol.
- **Enrutamiento EIGRP:** (Protocolo de **Enrutamiento** de Puerta de enlace Interior Mejorado en español) es un protocolo de encaminamiento de vector distancia, propiedad de Cisco Systems, que ofrece lo mejor de los algoritmos de vector de distancia.
- **Host:** Es un computador que funciona como el punto de inicio y final de las transferencias de datos.
- **Ip:** La dirección IP es un número que identifica, de manera lógica y jerárquica, a una Interfaz en red (elemento de comunicación/conexión) de un dispositivo



(computadora, tableta, portátil, teléfono inteligente) que utilice el protocolo o (Internet Protocol), que corresponde al nivel de red del modelo TCP/IP.

- **Lineamiento:** Tendencia, una dirección o un rasgo característico de algo.
- **NAT:** (Network Address Translation), es un mecanismo utilizado por routers IP para intercambiar paquetes entre dos redes que asignan mutuamente direcciones incompatibles.
- **PAT:** Es una característica del estándar NAT, que traduce conexiones TCP y UDP hechas por un host y un puerto en una red externa a otra dirección y puerto de la red interna.
- **Ping:** es un comando o una herramienta de diagnóstico que permite hacer una verificación del estado de una determinada conexión de un host local con al menos un equipo remoto contemplado en una red de tipo TCP/IP.
- **Protocolo:** Un protocolo de comunicaciones es un conjunto de normas que están obligadas a cumplir todas las máquinas y programas que intervienen en una comunicación de datos entre ordenadores sin las cuales la comunicación resultaría caótica y por tanto imposible.
- **Red:** Una red de comunicaciones es un conjunto de medios técnicos que permiten la comunicación a distancia entre equipos autónomos (no jerárquica -master/slave). Normalmente se trata de transmitir datos, audio y vídeo por ondas electromagnéticas a través de diversos medios de transmisión (aire, vacío, cable de cobre, Cable de fibra óptica).
- **Router:** Un rúter o enrutador, del inglés **router**, es un dispositivo que permite interconectar computadoras que funcionan en el marco de una red. Su función: se encarga de establecer la ruta que destinará a cada paquete de datos dentro de una red informática
- **Switch:** O conmutador es un dispositivo de interconexión utilizado para conectar equipos en red formando lo que se conoce como una red de área local (LAN) y cuyas especificaciones técnicas siguen el estándar conocido como Ethernet (o técnicamente IEEE 802.3).
- **Telnet:** (Telecommunication Network1) es el nombre de un protocolo de red que nos permite acceder a otra máquina para manejarla remotamente como si estuviéramos sentados delante de ella.



- **Topología:** La topología de red se define como el mapa físico o lógico de una red para intercambiar datos. En otras palabras, es la forma en que está diseñada la red, sea en el plano físico o lógico.
- **TFTP:** Son las siglas de Trivial file transfer Protocol (Protocolo de transferencia de archivos trivial) Utiliza UDP (en el puerto 69) como protocolo de transporte (a diferencia de FTP que utiliza los puertos 20 y 21 TCP). No puede listar el contenido de los directorios.
- **VLAN:** Acrónimo de virtual LAN (red de área local virtual), es un método para crear redes lógicas independientes dentro de una misma red física.



RESUMEN

El desarrollo del presente trabajo, pretende abarcar la mayoría de los temas tratados y estudiados durante el curso de diseño e implementación de soluciones integradas lan / wan, bajo la plataforma de Cisco y apoyados con el programa de simulación de redes denominado packet tracer, siguiendo la guía de actividades definida para tal fin. Las principales actividades implementadas en los ejercicios planteados, están basados en direccionamiento IP, subneteo de redes, Enrutamiento, Listas de control de acceso y Autenticación.

Se dice que CCNA es prácticamente una puerta de entrada a las redes, ya que explica claramente los conceptos fundamentales. De todas maneras, es un prerrequisito para otros cursos y sobre todo para sumergirse en el mundo de las telecomunicaciones.



ABSTRACT

The development of this work is intended to cover most of the topics discussed and studied during the course of design and implementation of integrated lan / wan solutions, under the Cisco platform and supported by the network simulation program called packet tracer, following the activity guide defined for this purpose. The main activities implemented in the proposed exercises are based on IP addressing, network subnetting, Routing, Access control lists and Authentication. CCNA is said to be practically a gateway to networks, as it clearly explains the fundamental concepts. In any case, it is a prerequisite for other courses and especially to immerse yourself in the world of telecommunications.



INTRODUCCION

Culminamos las actividades planteadas en cada una de las guías perfiladas para el curso de profundización cisco (diseño e implementación de soluciones integradas lan/wan), se desarrolló de manera práctica un taller formativo el cual requirió aplicar los diferentes conceptos y fundamentos estudiados a lo largo del curso para la configuración básica, aspectos físicos y aspectos lógicos de una Red. Construir una LAN simple, significa realizar configuraciones básicas en enrutadores y switches, además de implementar esquemas de direccionamiento ip, infraestructuras de red e Internet; Todo ello abarca el desarrollo de los escenarios planteados más adelante y permiten evidenciar tanto las competencias adquiridas como los niveles de comprensión en la solución de problemas relacionados con networking.

En esta prueba de habilidades se efectuará ejecución de protocolos de routing, configuración de servidor DHCP, Network Address Translation (NAT) y de sobrecarga (PAT), Listas de control de acceso (ACL), Autenticación local con AAA, cifrado de contraseñas, Habilitación de VLANs y establecimiento de servidor ftp entre otros. Todo en pro de implementar la seguridad de una red con políticas de entrada y salida de paquetes para prevenir y supervisar el acceso no autorizado, el uso indebido, la modificación o la denegación de una red informática y sus recursos accesibles.



OBJETIVOS

Objetivos Generales

Efectuar las actividades evaluativas definidas en la prueba de habilidades prácticas CCNA, en las cuales se plantean dos posibles escenarios que se pueden presentar en una empresa, teniendo en cuenta los lineamientos establecidos para direccionamiento IP, protocolos de enrutamiento y demás aspectos que forman parte de la topología de red implementada.

Objetivos específicos

- Desarrollar las actividades pertinentes al primer escenario y concernientes a:
 - Configuración básica de equipos según la topología de red planteada, para Pcs, Routers y Switches.
 - Comprobación del óptimo funcionamiento de la red instalada.
- Desarrollar las actividades pertinentes al segundo escenario y concernientes a:
 - Configuración de equipos (Direcciones ip, enrutamiento, listas control de acceso) según la topología de red planteada para Pcs, Routers y Switches.
 - Comprobación del óptimo funcionamiento de la red instalada.
 - Definir la autenticación local con AAA.
 - Implementar cifrado de contraseñas.
 - Definir un máximo de internos para acceder al router.
 - Establecer un servidor TFTP que almacene todos los archivos necesarios de los routers.
 - Configurar el DHCP para proporcionar solo direcciones a los hosts de Bucaramanga y Cundinamarca
 - Configurar el web server con NAT estático y NAT de sobrecarga (PAT) para el resto de los equipos de la topología.

PLANTEAMIENTO DEL PROBLEMA

Descripción de escenarios propuestos para la prueba de habilidades

Escenario 1

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

Topología de red

Los requerimientos solicitados son los siguientes:

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

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

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

Parte 4: Implementar la seguridad en la red, se debe restringir el acceso y comunicación entre hosts de acuerdo con los requerimientos del administrador de red.

Parte 5: Comprobación total de los dispositivos y su funcionamiento en la red.

Parte 6: Configuración final.

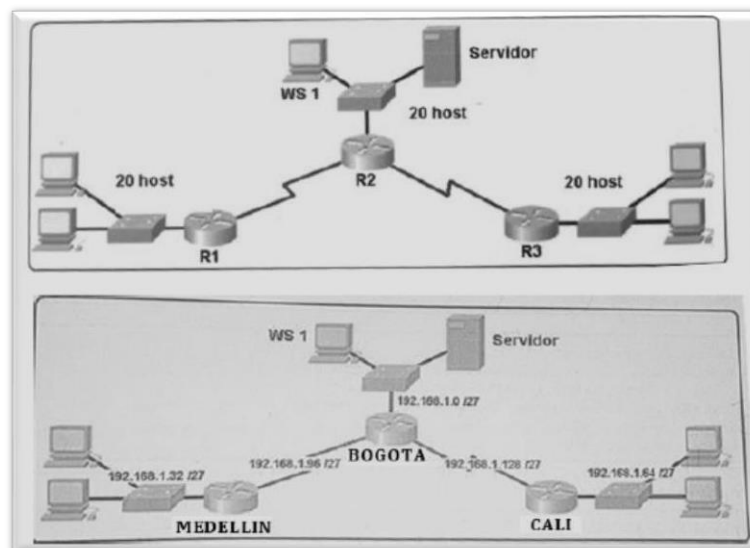


Figura 1. Topología de Red Dispuesta

1. Desarrollo Escenario 1

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.

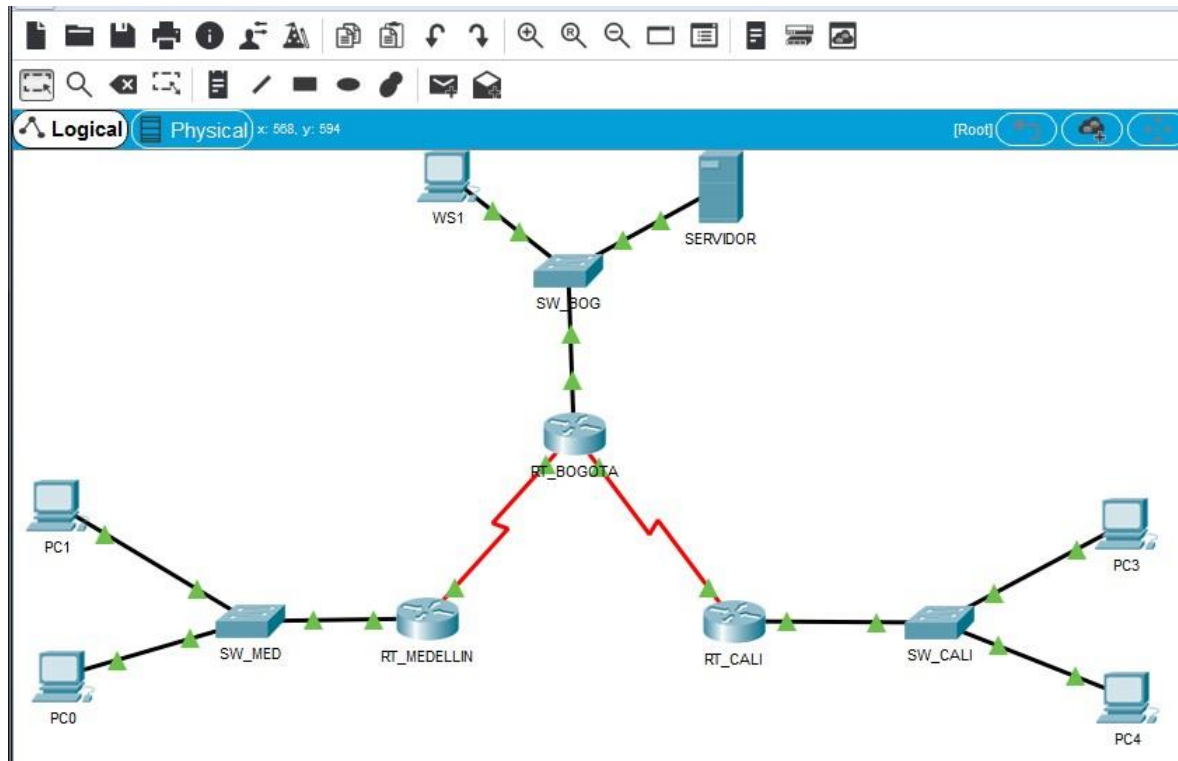


Figura 2. Conectividad Escenario 1.

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

1.1 Asignación de direcciones IP:

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



Para el correspondiente Subneteo se utilizó la fórmula básica de división para Subredes,

- Tomando prestado 1 Bit, tenemos que $2^1 = 2$ Subredes
- En nuestro caso, $2^3 = 8$ Subredes, ya que tomamos prestado 3 bits, lo cual nos indicaría:

```
255.255.255 128 64 32 16 8 4 2 1 (octetos)
255.255.255  0  0  0  0  0  0  0  0
255.255.255  1  1  1  0  0  0  0  0 (prendiendo los tres bits necesarios)
```

- De esta manera nuestra máscara de subred estaría dada por: $128+64+32=224$, entonces, sería igual a **255.255.255.224**

```
192.168.0.0   - 12.168.0.31
192.168.0.32  - 12.168.0.63
192.168.0.64  - 12.168.0.95
192.168.0.96  - 12.168.0.127
192.168.0.128 - 12.168.0.159
192.168.0.160 - 12.168.0.191
192.168.0.192 - 12.168.0.223
192.168.0.224 - 12.168.0.255
```

- Utilizando y comprobando con una calculadora IP también nos indica:

```
Address:      192.168.0.1          11000000.10101000.00000000.000
00001Netmask: 255.255.255.224 = 2711111111.11111111.11111111.111
00000Wildcard: 0.0.0.3100000000.00000000.00000000.000
11111=>Network: 192.168.0.0/27      11000000.10101000.00000000.
000 00000HostMin: 192.168.0.111000000.10101000.00000000.000
00001HostMax: 192.168.0.3011000000.10101000.00000000.000
11110Broadcast: 192.168.0.3111000000.10101000.00000000.000
11111Hosts/Net: 30Class C, Private Internet
```

- b. Asignar una dirección IP a la red.

Esta dada en ejercicio como 192.168.1.1



1.2 Configuración Básica.

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

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

Tabla 1. Configuración Básica

- Configuración puertos RT MEDELLIN

```
configure terminal
interface serial 0/1/0
ip address 192.168.1.99 255.255.255.224
no shutdown
exit
```

```
interface GigabitEthernet0/0
ip address 192.168.1.33 255.255.255.224
no shutdown
exit
```

- Configuración puertos RT BOGOTA

```
configure terminal
interface GigabitEthernet0/0
ip address 192.168.1.1 255.255.255.224
no shutdown
exit
```

```
interface Serial0/1/0
ip address 192.168.1.98 255.255.255.224
no shutdown
exit
```

```
interface Serial0/1/1
ip address 192.168.1.130 255.255.255.224
```



- Configuración puertos RT_CALI

```
configure terminal
interface GigabitEthernet0/0
ip address 192.168.1.65 255.255.255.224
no shutdown
exit
```

```
interface Serial0/1/1
ip address 192.168.1.131 255.255.255.224
no shutdown
exit
```

b. Después de cargada la configuración en los dispositivos, verificar la tabla de enrutamiento en cada uno de los routers para comprobar las redes y sus rutas.

- Router Bogotá:

RT_BOGOTA#**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 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, 00:45:44, Serial0/1/0
D 192.168.1.64/27 [90/2172416] via 192.168.1.131, 00:45:43, Serial0/1/1
C 192.168.1.96/27 is directly connected, Serial0/1/0
L 192.168.1.98/32 is directly connected, Serial0/1/0
C 192.168.1.128/27 is directly connected, Serial0/1/1
L 192.168.1.130/32 is directly connected, Serial0/1/1
```



- Router Medellín:

RT_MEDELLIN#**show ip 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 [90/2172416] via 192.168.1.98, 00:34:34, Serial0/1/0

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, 00:34:34, Serial0/1/0

C 192.168.1.96/27 is directly connected, Serial0/1/0

L 192.168.1.99/32 is directly connected, Serial0/1/0

D 192.168.1.128/27 [90/2681856] via 192.168.1.98, 00:34:34, Serial0/1/0

- Router Cali:

RT_CALI#**show ip 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 [90/2172416] via 192.168.1.130, 00:38:17, Serial0/1/1

D 192.168.1.32/27 [90/2684416] via 192.168.1.130, 00:38:17, Serial0/1/1

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, 00:38:17, Serial0/1/1

C 192.168.1.128/27 is directly connected, Serial0/1/1

L 192.168.1.131/32 is directly connected, Serial0/1/1

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

Teniendo en cuenta la topología planteada y dado que solo tenemos una ruta, se puede decir que no hay balanceo de cargas, como se puede observar en las anteriores configuraciones para cada router con el comando *Show ip route*.



```
R1 Medellín
Physical Config CLI Attributes
IOS Command Line Interface
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, 3 masks
D 192.168.1.0/27 [90/2170112] via 192.168.1.98, 00:00:21,
Serial0/3/0
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, 00:00:21,
Serial0/3/0
C 192.168.1.96/27 is directly connected, Serial0/3/0
L 192.168.1.99/32 is directly connected, Serial0/3/0
D 192.168.1.128/26 [90/2691856] via 192.168.1.98, 00:00:21,
Serial0/3/0
Router#
```

Figura 3. B.C. Router Medellín

```
R2 Bogota
Physical Config CLI Attributes
IOS Command Line Interface
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, 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, 00:00:51,
Serial0/3/0
D 192.168.1.64/27 [90/2170112] via 192.168.1.131, 00:03:17,
Serial0/3/1
C 192.168.1.96/27 is directly connected, Serial0/3/0
L 192.168.1.98/32 is directly connected, Serial0/3/0
C 192.168.1.128/27 is directly connected, Serial0/3/1
L 192.168.1.130/32 is directly connected, Serial0/3/1
Router#
Ctrl+F6 to exit CLI focus Copy Paste
```

Figura 4. B.C. Router Bogota.

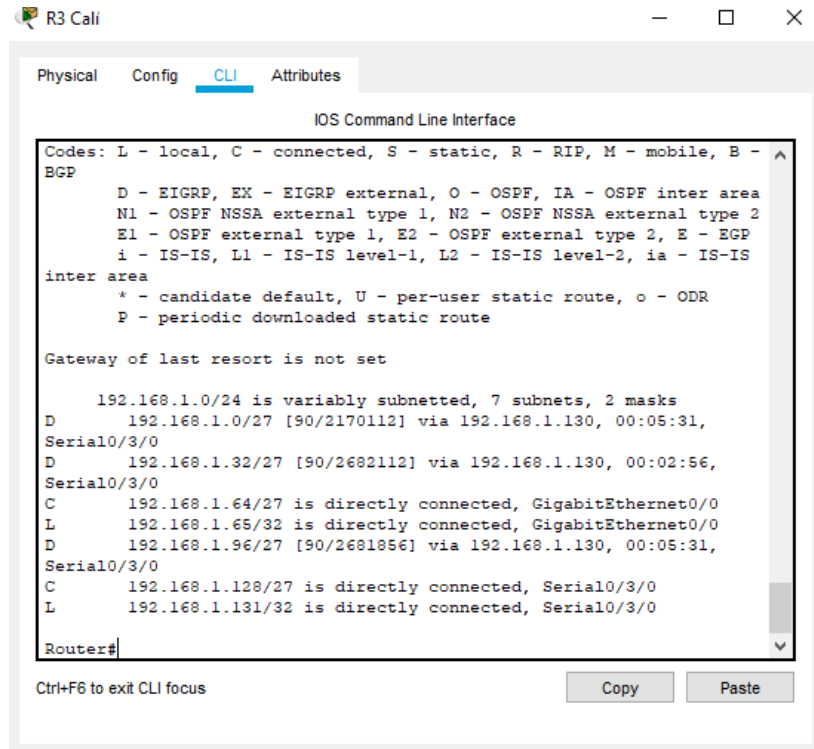


Figura 5. B.C. Router Cali.

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

```
RT_BOGOTA#show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone
Device ID        Local Intrfce   Holdtme    Capability   Platform    Port ID
SW_BOG           Gig 0/0         163        S            2960        Fas 0/1
RT_CALI          Ser 0/1/1       163        R            C1900       Ser 0/1/1
RT_MEDELLIN     Ser 0/1/0       163        R            C1900       Ser 0/1/0
-----
```

```
RT_MEDELLIN#show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone
Device ID        Local Intrfce   Holdtme    Capability   Platform    Port ID
RT_BOGOTA        Ser 0/1/0       135        R            C1900       Ser 0/1/0
SW_MED           Gig 0/0         135        S            2960        Fas 0/1
```

```
RT_CALI#show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone
Device ID        Local Intrfce   Holdtme    Capability   Platform    Port ID
Switch           Gig 0/0         127        S            2960        Fas 0/1
RT_BOGOTA        Ser 0/1/1       127        R            C1900       Ser 0/1/1
-----
```



```
SW_MED#show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone
Device ID      Local Intrfce  Holdtme   Capability  Platform  Port ID
RT_MEDELLIN   Fas 0/1          155      R           C1900     Gig 0/0
```

```
SW_BOG#show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone
Device ID      Local Intrfce  Holdtme   Capability  Platform  Port ID
RT_BOGOTA     Fas 0/1          135      R           C1900     Gig 0/0
```

```
Switch#show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone
Device ID      Local Intrfce  Holdtme   Capability  Platform  Port ID
RT_CALI       Fas 0/1          135      R           C1900     Gig 0/0
```

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

1.2 Configuración de Enrutamiento.

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

- Medellín

```
router eigrp 200
network 192.168.1.0 255.255.255.0
auto-summary
```

- Bogotá

```
router eigrp 200
network 192.168.1.0 255.255.255.0
auto-summary
```

- Cali:

```
router eigrp 200
network 192.168.1.0 255.255.255.0
auto-summary
exit
```

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



Prueba de conectividad entre PC0 (Medellín) hacia PC3 (Cali).

```
C:\>ipconfig
FastEthernet0 Connection:(default port)
Link-local IPv6 Address.....: FE80::2E0:B0FF:FE2E:D90C
IP Address..... : 192.168.1.36
Subnet Mask ..... : 255.255.255.224
Default Gateway..... : 192.168.1.33
```

```
C:\>ping 192.168.1.70
```

Pinging 192.168.1.70 with 32 bytes of data:

```
Reply from 192.168.1.70: bytes=32 time=2ms TTL=125
Reply from 192.168.1.70: bytes=32 time=30ms TTL=125
Reply from 192.168.1.70: bytes=32 time=14ms TTL=125
Reply from 192.168.1.70: bytes=32 time=13ms TTL=125
```

```
Ping statistics for 192.168.1.70:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 2ms, Maximum = 30ms, Average = 14ms
```

- Prueba de existencia de vecindad entre las redes:

```
RT_MEDELLIN#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 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, 01:38:35, Serial0/1/0
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, 01:38:34, Serial0/1/0
C 192.168.1.96/27 is directly connected, Serial0/1/0
L 192.168.1.99/32 is directly connected, Serial0/1/0
D 192.168.1.128/27 [90/2681856] via 192.168.1.98, 01:38:35, Serial0/1/0
```

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



Mediante Show ip route se puede verificar la ruta y las redes que actualmente está preñdiendo cada uno de los routers.

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.

```
C:\>ipconfig
```

```
FastEthernet0 Connection:(default port)
```

```
Link-local IPv6 Address.....: FE80::240:BFF:FE48:CA6  
IP Address..... : 192.168.1.70  
Subnet Mask ..... : 255.255.255.224  
Default Gateway..... : 192.168.1.65
```

```
Bluetooth Connection:
```

```
Link-local IPv6 Address..... :  
IP Address..... : 0.0.0.0  
Subnet Mask ..... : 0.0.0.0  
Default Gateway..... : 0.0.0.0
```

```
C:\> ping 192.168.1.35
```

```
Pinging 192.168.1.35 with 32 bytes of data:
```

```
Reply from 192.168 1.35: bytes=32 time=7ms TTL=125  
Reply from 192.168 1.35: bytes=32 time=15ms TTL=125  
Reply from 192.168 1.35: bytes=32 time=2ms TTL=125  
Reply from 192.168 1.35: bytes=32 time=2ms TTL=125
```

```
Ping statistics for 192.168.1.35:  
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),  
Approximate round trip times in milli-seconds:  
Minimum = 2ms, Maximum = 15ms, Average = 6ms
```

A servidor:

```
C:\>ping 192.168.1.20
```

```
Pinging 192.168.1.20 with 32 bytes of data:
```

```
Reply from 192.168 1.20: bytes=32 time=4ms TTL=126  
Reply from 192.168 1.20: bytes =32 time=1ms TTL=126  
Reply from 192.168 1.20: bytes=32 time=1ms TTL=126  
Reply from 192.168 1.20: bytes=32 time=1ms TTL=126
```

```
Ping statistics for 192.168.1.20:  
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),  
Approximate round trip times in milli-seconds:
```



Minimum = 1ms, Maximum = 4ms, Average = 1ms

1.3 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.

1.3.1 Prueba servidor a Cualquier dispositivo de la red

Ej. PING Servidor – Pc4 Cali, Exitoso.

```
C:\>ipconfig
FastEthernet0 Connection:(default port)
Link-local IPv6 Address.....: FE80::240:BFF:FE66:2E28
IP Address..... : 192.168.1.20
Subnet Mask ..... : 255.255.255.224
Default Gateway..... : 192.168.1.1
```

```
C:\>ping 192.168.1.71
Pinging 192.168.1.71 with 32 bytes of data:
```

```
Reply from 192.168.1.71: bytes=32 time=16ms TTL=126
Reply from 192.168.1.71: bytes=32 time=12ms TTL=126
Reply from 192.168.1.71: bytes=32 time=12ms TTL=126
Reply from 192.168.1.71: bytes=32 time=12ms TTL=126
```

```
Ping statistics for 192.168.1.71:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 12ms, Maximum = 16ms, Average = 13ms
```

1.3.2 Prueba entre otros dispositivos de la red.

Ej. PING WS1 – Pc4 Cali, No Exitoso.

```
Packet Tracer PC Command Line 1.0
C:\>ipconfig
FastEthernet0 Connection:(default port)
```



```
Link-local IPv6 Address.....: FE80::20D:BDFF:FEDB:A644
IP Address..... : 192.168.1.15
Subnet Mask ..... : 255.255.255.224
Default Gateway..... : 192.168.1.1
```

Bluetooth Connection:

```
Link-local IPv6 Address.....: ::
IP Address..... : 0.0.0.0
Subnet Mask ..... : 0.0.0.0
Default Gateway..... : 0.0.0.0
```

```
C:\>ping 192.168.1.71
Pinging 192.168.1.71 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
```

```
Ping statistics for 192.168.1.71:
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

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.

- RT_MEDELLIN
configure terminal
access-list 100 permit ip any host 192.168.1.20
interface serial xxx
ip access-group 100 out
- RT_CALI
access-list 100 permit ip any host 192.168.1.20

Comprobación de la red instalada.

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

- Desde Red Cali:

```
RT_CALI#show access-lists 100
Extended IP access list 100
permit ip any host 192.168.1.20
```

```
RT_CALI#
RT_CALI#
RT_CALI#
RT_CALI#
```



```
RT_CALI#show access-lists 100
Extended IP access list 100
permit ip any host 192.168.1.20 (3 match(es))
```

- Desde Red Medellín:

```
RT_MEDELLIN#show access-lists 100
Extended IP access list 100
permit ip any host 192.168.1.20 (1 match(es))
```

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

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

Tabla 2. Tabla de Pruebas

TELNET Router Medellín - Router Cali

```
RT_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 [90/2172416] via 192.168.1.98, 01:33:43, Serial0/1/0
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, 01:33:42, Serial0/1/0
C 192.168.1.96/27 is directly connected, Serial0/1/0
L 192.168.1.99/32 is directly connected, Serial0/1/0
D 192.168.1.128/27 [90/2681856] via 192.168.1.98, 01:33:43, Serial0/1/0
```

```
RT_MEDELLIN>telnet 192.168.1.131
Trying 192.168.1.131 ...Open
User Access Verification
```

```
Password:
RT_CALI>
```

TELNET WS1 - Router Bogotá

```
Packet Tracer PC Command Line 1.0
C:\>ipconfig
```

```
FastEthernet0 Connection:(default port)
```

```
Link-local IPv6 Address.....: FE80::20D:BDFF:FEDB:A644
IP Address.....: 192.168.1.15
Subnet Mask .....: 255.255.255.224
Default Gateway.....: 192.168.1.1
```

```
Bluetooth Connection:
```

```
Link-local IPv6 Address.....: ::
IP Address.....: 0.0.0.0
Subnet Mask .....: 0.0.0.0
Default Gateway.....: 0.0.0.0
```

```
C:\>telnet 192.168.1.98
Trying 192.168.1.98 ...Open
```

```
User Access Verification
```

```
Password:
```

```
SW_BOGOTA>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, 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, 01:23:10, Serial0/1/0
D    192.168.1.64/27 [90/2172416] via 192.168.1.131, 01:23:09, Serial0/1/1
C    192.168.1.96/27 is directly connected, Serial0/1/0
L    192.168.1.98/32 is directly connected, Serial0/1/0
C    192.168.1.128/27 is directly connected, Serial0/1/1
L    192.168.1.130/32 is directly connected, Serial0/1/1
```

TELNET Servidor - Router Cali

```
C:\>ipconfig
```

```
FastEthernet0 Connection:(default port)
```

```
Link-local IPv6 Address.....: FE80::240:BFF:FE66:2E28
IP Address.....: 192.168.1.20
Subnet Mask .....: 255.255.255.224
Default Gateway.....: 192.168.1.1
```

```
C:\>telnet 192.168.1.131
Trying 192.168.1.131 ...Open
```

```
User Access Verification
```

```
Password:
```

```
RT_CALI>sh ip route
```

```
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, 01:38:21, Serial0/1/1
D 192.168.1.32/27 [90/2684416] via 192.168.1.130, 01:38:21, Serial0/1/1
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, 01:38:21, Serial0/1/1
C 192.168.1.128/27 is directly connected, Serial0/1/1
L 192.168.1.131/32 is directly connected, Serial0/1/1
RT_CALI>
```

TELNET Lan del Router Cali - Router Cali

```
C:\>ipconfig
```

```
FastEthernet0 Connection:(default port)
```

```
Link-local IPv6 Address.....: FE80::240:BFF:FE48:CA6
IP Address.....: 192.168.1.70
Subnet Mask .....: 255.255.255.224
Default Gateway.....: 192.168.1.65
```



Bluetooth Connection:

Link-local IPv6 Address..... ::
IP Address..... : 0.0.0.0
Subnet Mask : 0.0.0.0
Default Gateway..... : 0.0.0.0

C:\>telnet 192.168.1.131
Trying 192.168.1.131 ...Open

User Access Verification

Password:
RT_CALI>

TELNET Lan del Router Medellin - Router Medellin

Packet Tracer PC Command Line 1.0
C:\>ipconfig

FastEthernet0 Connection:(default port)
Link-local IPv6 Address.....: FE80::2E0:B0FF:FE2E:D90C
IP Address..... : **192.168.1.36**
Subnet Mask : 255.255.255.224
Default Gateway..... : 192.168.1.33

Bluetooth Connection:
Link-local IPv6 Address..... ::
IP Address..... : 0.0.0.0
Subnet Mask : 0.0.0.0
Default Gateway..... : 0.0.0.0

C:\>telnet **192.168.1.99**
Trying 192.168.1.99 ...Open

User Access Verification

Password:
RT_MEDELLIN>

PING Lan del Router Cali - Servidor

C:\>ipconfig

FastEthernet0 Connection:(default port)
Link-local IPv6 Address.....: FE80::20D:BDFF:FE30:E659
IP Address..... : **192.168.1.71**
Subnet Mask : 255.255.255.224
Default Gateway..... : 192.168.1.65

Bluetooth Connection:
Link-local IPv6 Address..... ::
IP Address..... : 0.0.0.0



Subnet Mask : 0.0.0.0
Default Gateway : 0.0.0.0

C:\>ping **192.168.1.20**

Pinging 192.168.1.20 with 32 bytes of data:

Reply from 192.168 1.20: bytes=32 time=13ms TTL=126
Reply from 192.168 1.20: bytes=32 time=12ms TTL=126
Reply from 192.168 1.20: bytes=32 time=14ms TTL=126
Reply from 192.168 1.20: bytes=32 time=14ms TTL=126

Ping statistics for 192.168.1.20:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 12ms, Maximum = 14ms, Average = 13ms

PING Lan del Router Medellín – Servidor

C:\>ipconfig

FastEthernet0 Connection:(default port)

Link-local IPv6 Address.....: FE80::2E0:B0FF:FE2E:D90C
IP Address..... : **192.168.1.36**
Subnet Mask : 255.255.255.224
Default Gateway..... : 192.168.1.33

Bluetooth Connection:

Link-local IPv6 Address..... :
IP Address..... : 0.0.0.0
Subnet Mask : 0.0.0.0
Default Gateway..... : 0.0.0.0

C:\>ping **192.168.1.20**

Pinging 192.168.1.20 with 32 bytes of data:

Reply from 192.168 1.20: bytes=32 time=2ms TTL=126
Reply from 192.168 1.20: bytes=32 time=11ms TTL=126
Reply from 192.168 1.20: bytes=32 time=12ms TTL=126
Reply from 192.168 1.20: bytes=32 time=11ms TTL=126

Ping statistics for 192.168.1.20:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 2ms, Maximum = 12ms, Average = 9ms

PING Servidor – Lan Router Medellín (Pc1)

C:\>ipconfig

FastEthernet0 Connection:(default port)

Link-local IPv6 Address.....: FE80::240:BFF:FE66:2E28



IP Address..... : 192.168.1.20
Subnet Mask : 255.255.255.224
Default Gateway.....: 192.168.1.1

C:\>ping 192.168.1.35

Pinging 192.168.1.35 with 32 bytes of data:

Request timed out.

Reply from 192.168 1.35: bytes=32 time=1ms TTL=126
Reply from 192.168 1.35: bytes=32 time=11ms TTL=126
Reply from 192.168 1.35: bytes=32 time=12ms TTL=126

Ping statistics for 192.168.1.35:

Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
Minimum = 1ms, Maximum = 12ms, Average = 8ms

C:\>ping 192.168.1.35

Pinging 192.168.1.35 with 32 bytes of data:

Reply from 192.168 1.35: bytes=32 time=11ms TTL=126
Reply from 192.168 1.35: bytes=32 time=9ms TTL=126
Reply from 192.168 1.35: bytes=32 time=12ms TTL=126
Reply from 192.168 1.35: bytes=32 time=12ms TTL=126

Ping statistics for 192.168.1.35:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 9ms, Maximum = 12ms, Average = 11ms

PING Servidor – Lan Router Cali (Pc3)

C:\>ipconfig

FastEthernet0 Connection:(default port)

Link-local IPv6 Address.....: FE80::240:BFF:FE66:2E28
IP Address..... : **192.168.1.20**
Subnet Mask : 255.255.255.224
Default Gateway..... : 192.168.1.1

C:\>ping **192.168.1.70**

Pinging 192.168.1.70 with 32 bytes of data:

Reply from 192.168 1.70: bytes=32 time=25ms TTL=126
Reply from 192.168 1.70: bytes=32 time=12ms TTL=126
Reply from 192.168 1.70: bytes=32 time=12ms TTL=126
Reply from 192.168 1.70: bytes=32 time=11ms TTL=126

Ping statistics for 192.168.1.70:



Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 11ms, Maximum = 25ms, Average = 15ms

PING Router Cali – Lan Router Medellin (Pc1)

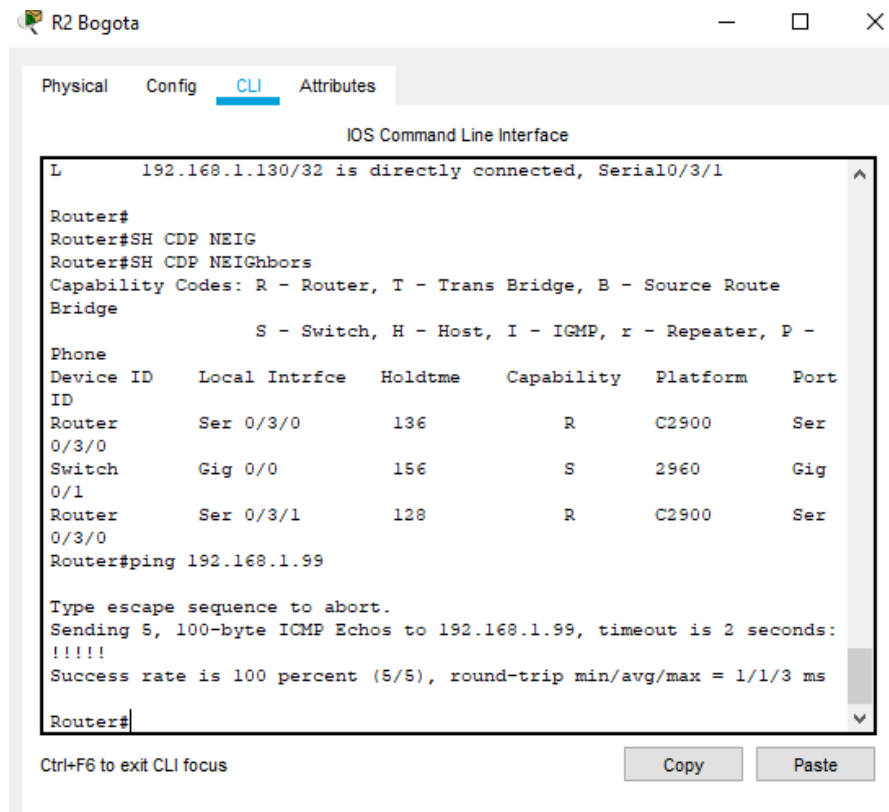
```
RT_CALI>ping 192.168.1.35
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.35, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 2/6/19 ms
```

PING Router Medellin – Lan Router Cali (Pc3)

```
RT_MEDELLIN>ping 192.168.1.70
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.70, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 2/2/3 ms
```

```
RT_MEDELLIN>
```

PRUEBA DE CONECTIVIDAD



Fi0gura 6. Ping Successful Bog- Med.

Desarrollo 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.

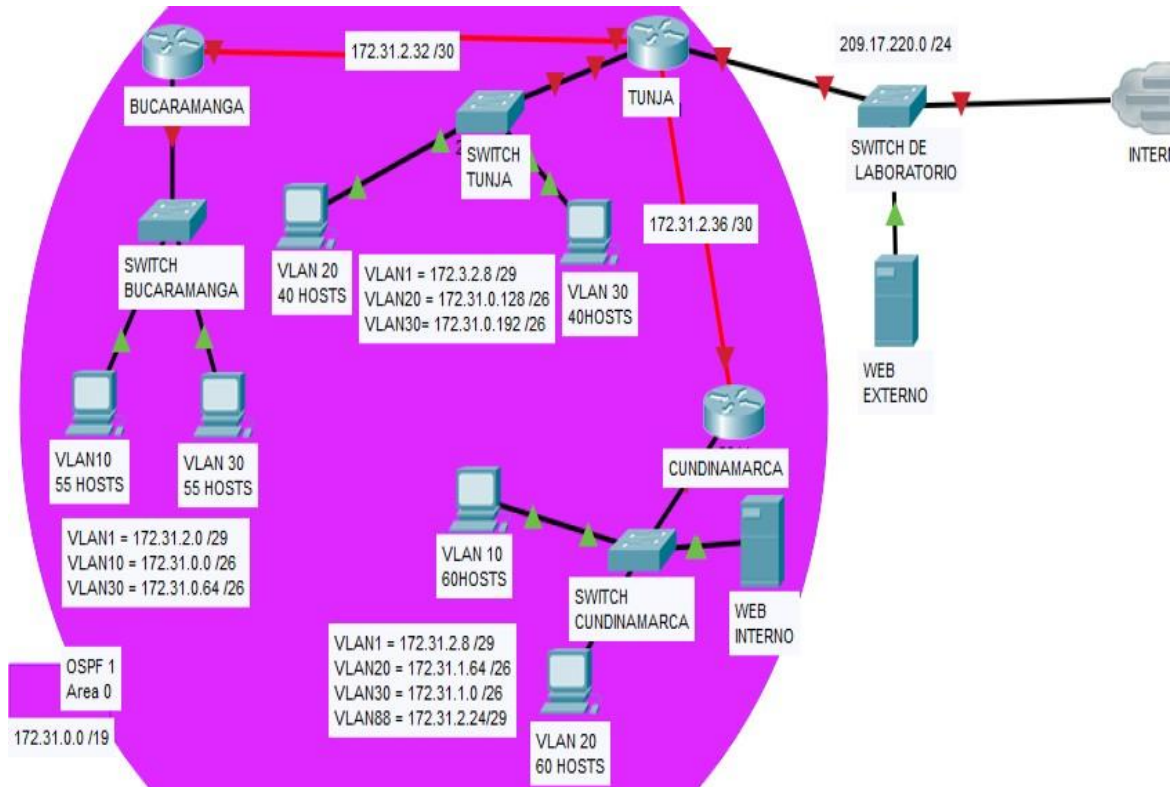


Figura 7. Topología de Red Dispuesta Escenario 2

Desarrollo

Los siguientes son los requerimientos necesarios:

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

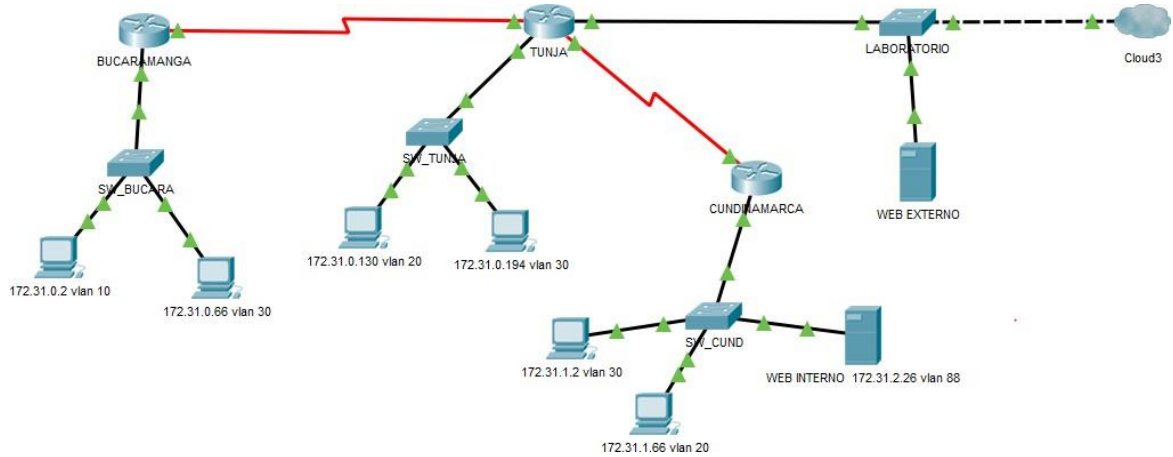


Figura 8. Topología de Red Dispuesta Escenario 2

- Los usuarios para ingresar se crearon como cisco
- Se establecieron todas las contraseñas como cisco

2.1 Autenticación local con AAA.

Habilitación AAA

```
aaa new-model
aaa authentication login default local enable
username cisco password cisco
```

2.2 Verificación de Autenticación de Acceso a Routers Bucaramanga, Tunja y Cundinamarca respectivamente:

```
User Access Verification
Username: cisco
Password:
% Login invalid
Username: cisco
Password:
BUCARAMANGA>
```

```
User Access Verification
Username: cisco
Password:
```



```
User Access Verification
Username: cisco
Password:
CUNDINAMARCA>
```

2.3 VLANS

LINEAS DE TERMINAL VIRTUAL

```
line vty 0 15
password xxxxxxx
login
exit
```

```
SW_BUCARA
configure terminal
vlan 10  CREACION DE VLAN 10
exit
```

```
configure terminal
vlan 30  CREACION DE VLAN 30
exit
```

```
interface FastEthernet0/1          Configuración puerto trunk este puerto es el que va directo al router.
switchport trunk allowed vlan 1,10,30
switchport mode trunk
```

```
interface FastEthernet0/2          Configuración puertos de cada pc.
switchport access vlan 10
switchport mode access
```

```
interface FastEthernet0/3          Configuración puertos de cada pc.
switchport access vlan 30
switchport mode access
```

```
SW_TUNJA
configure terminal
vlan 20  CREACION DE VLAN 20
exit
```

```
configure terminal
vlan 30  CREACION DE VLAN 30
```



```
interface FastEthernet0/1
switchport access vlan 20
switchport mode access
```

```
interface FastEthernet0/2
switchport access vlan 30
switchport mode access
```

```
interface FastEthernet0/3
switchport trunk allowed vlan 1,20,30
switchport mode trunk
```

```
SW_CUND
configure terminal
vlan 20 CREACION DE VLAN 20
exit
```

```
configure terminal
vlan 30 CREACION DE VLAN 30
exit
```

```
interface FastEthernet0/1
switchport trunk allowed vlan 1,20,30,88
switchport mode trunk
```

```
interface FastEthernet0/2
switchport access vlan 30
switchport mode access
```

```
interface FastEthernet0/3
switchport access vlan 20
switchport mode access
```

```
interface FastEthernet0/4
switchport access vlan 88
switchport mode access
```

2.4 Cifrado de Contraseñas

```
service password-encryption
!  
line con 0
```



```
password 7 0822455D0A16
!  
line aux 0
!  
line vty 0 4
password 7 0822455D0A16
line vty 5 15
password 7 0822455D0A16
!  
!
```

2.5 Un máximo de internos para acceder al router.

```
User Access Verification
Username: sadsad
Password:
% Login invalid
```

```
Username: dadas
Password:
% Login invalid
```

```
Username: adsad
Password:
% Login invalid
```

Press RETURN to get started!

- Máximo tiempo de acceso al detectar ataques.
- Establezca un servidor TFTP y almacene todos los archivos necesarios de los routers.
 - Establecido en Wb Interno 172.31.2.26 Vlan 88

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

2.6 Configuración DHCP

```
!  
ip dhcp pool BUCARAMANGA
network 172.31.0.0 255.255.255.192
default-router 172.31.0.1
ip dhcp pool BUCARAMANGA1
network 172.31.0.64 255.255.255.192
default-router 172.31.0.65
```



```
ip dhcp pool CUNDINAMARCA
network 172.31.1.64 255.255.255.192
default-router 172.31.1.65
ip dhcp pool CUNDINAMARCA1
network 172.31.1.0 255.255.255.192
default-router 172.31.1.1
ip dhcp pool CUNDINAMARCA2
network 172.31.2.24 255.255.255.248
default-router 172.31.2.25
!
```

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

2.7 Ruta Estática

```
ip nat inside source static 172.31.2.26 209.17.220.252
```

CONFIGURACION DE PAT

```
ip nat pool PAT_SOBRECARGA 209.17.220.250 209.17.220.250 netmask 255.255.255.0
access-list 150 permit ip 172.31.0.0 0.0.31.255 any
ip nat inside source list 150 pool PAT_SOBRECARGA overload
interface GigabitEthernet0/1
ip nat outside
interface serial 0/1/0
ip nat inside
interface serial 0/1/1
ip nat inside
```

Configuración nat estático para el servidor web interno

```
configure terminal
ip nat inside source static 172.31.2.26 209.17.220.1

!
router ospf 1
log-adjacency-changes
network 172.31.0.0 0.0.31.255 area 0
network 209.17.220.0 0.0.0.255 area 0
!
ip nat pool PAT_SOBRECARGA 209.17.220.250 209.17.220.250 netmask 255.255.255.0
ip nat inside source list 150 pool PAT_SOBRECARGA overload
ip nat inside source static 172.31.2.26 209.17.220.252
ip classless
ip route 209.17.220.0 255.255.255.0 GigabitEthernet0/1
!
ip flow-export version 9
!
```



```
!  
access-list 150 permit ip 172.31.0.0 0.0.31.255 any  
!  
!
```

El enrutamiento deberá tener autenticación.

- Configuración Router TUNJA, con Creación de Vlan, Ip de cada Vlan y Enrutamiento OSPF con autenticación

```
interface GigabitEthernet0/0.1  
encapsulation dot1Q 1 native  
ip address 172.3.2.9 255.255.255.248  
ip ospf authentication-key cisco  
interface GigabitEthernet0/0.20  
encapsulation dot1Q 20  
ip address 172.31.0.129 255.255.255.192  
ip ospf authentication-key cisco
```

```
interface GigabitEthernet0/0.30  
encapsulation dot1Q 30  
ip address 172.31.0.193 255.255.255.192  
ip ospf authentication-key cisco
```

```
interface GigabitEthernet0/1  
ip address 209.17.220.1 255.255.255.0  
ip ospf authentication-key
```

```
interface Serial0/1/0  
ip address 172.31.2.34 255.255.255.252  
ip ospf authentication-key
```

```
interface Serial0/1/1  
ip address 172.31.2.37 255.255.255.252  
ip ospf authentication-key
```

```
router ospf 1  
network 172.31.0.0 0.0.31.255 area 0
```

- Configuración Router BUCARAMANGA, con Creación de Vlan, configuración de donde debe buscar las ip por dhcp y enrutamiento OSPF con autenticación

Habilitation AAA
aaa new-model



```
aaa authentication login default local enable
username cisco password cisco
```

```
interface GigabitEthernet0/0.1
 encapsulation dot1Q 1 native
 ip address 172.31.2.1 255.255.255.248
 ip helper-address 172.31.2.34
 ip ospf authentication-key cisco
```

Creacion de vlan en los routers

```
Interface GigabitEthernet0/0
no shutdown
interface gigabitEthernet 0/0.1
 encapsulation dot1Q 1
 ip address 172.31.2.1 255.255.255.248
 ip ospf authentication-key cisco
```

```
interface GigabitEthernet0/0.10
 encapsulation dot1Q 10
 ip address 172.31.0.1 255.255.255.192
 ip helper-address 172.31.2.34
 ip ospf authentication-key cisco
```

```
interface GigabitEthernet0/0.30
 encapsulation dot1Q 30
 ip address 172.31.0.65 255.255.255.192
 ip helper-address 172.31.2.34
 ip ospf authentication-key
```

```
interface Serial0/1/0
 ip address 172.31.2.33 255.255.255.252
 router ospf 1
 network 172.31.0.0 0.0.31.255 area 0
```

- Configuración Router CUNDINAMARCA, con Creación de Vlan, configuración de las ip por dhcp y enrutamiento OSPF con autenticación.

```
Habilitación AAA
aaa new-model
aaa authentication login default local enable
username cisco password cisco
```

```
interface GigabitEthernet0/0.1
 encapsulation dot1Q 1 native
```



```
ip address 172.31.2.9 255.255.255.248  
ip helper-address 172.31.2.37
```

```
interface GigabitEthernet0/0.20  
encapsulation dot1Q 20  
ip address 172.31.1.65 255.255.255.192  
ip helper-address 172.31.2.37
```

```
interface GigabitEthernet0/0.30  
encapsulation dot1Q 30  
ip address 172.31.1.1 255.255.255.192  
ip helper-address 172.31.2.37
```

```
interface GigabitEthernet0/0.88  
encapsulation dot1Q 88  
ip address 172.31.2.25 255.255.255.248  
ip helper-address 172.31.2.37
```

```
interface Serial0/1/1  
ip address 172.31.2.38 255.255.255.252
```

```
router ospf 1  
network 172.31.0.0 0.0.31.255 area 0
```

2.8 Listas de control de acceso:

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

Acl 100

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

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

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

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

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



- Los hosts de una VLAN no pueden acceder a los de otra VLAN en una ciudad.
- Solo los hosts de las VLAN administrativas y de la VLAN de servidores tienen acceso a los routers e internet.
 - Se establece en router de cada ciudad prevenir ataques de fuerza bruta.

login block-for 10 attempts 10 within 10

ROUTER CUNDINAMARCA

```
access-list 100 permit ip 172.31.1.64 0.0.0.63 172.31.0.128 0.0.0.63
access-list 100 permit ip 172.31.1.64 0.0.0.63 172.31.0.192 0.0.0.63
interface gigabitEthernet 0/0.30
ip access-group 100 in
```

```
access-list 101 deny ip 172.31.1.0 0.0.0.63 172.31.0.128 0.0.0.63
access-list 101 deny ip 172.31.1.0 0.0.0.63 172.31.0.192 0.0.0.63
access-list 101 permit ip any any
interface gigabitEthernet 0/0.20
ip access-group 101 in
```

```
access-list 101 permit ip 172.31.2.0 0.0.0.7 any
interface gigabitEthernet 0/0.1
ip access-group 101 in
```

ROUTER TUNJA

```
access-list 100 permit ip 172.31.0.192 0.0.0.63 209.17.220.0 0.0.0.255
interface gigabitEthernet 0/0.30
ip access-group 100 in
```

```
access-list 101 permit ip 172.31.0.128 0.0.0.63 172.31.0.0 0.0.0.63
access-list 101 permit ip 172.31.0.128 0.0.0.63 172.31.1.64 0.0.0.63
interface gigabitEthernet 0/0.20
ip access-group 101 in
```

```
access-list 102 permit ip 172.31.2.0 0.0.0.7 any
interface gigabitEthernet 0/0.1
ip access-group 102 in
```

ROUTER BUCARAMANGA

```
access-list 100 permit ip 172.31.0.0 0.0.0.63 172.31.1.64 0.0.0.63
access-list 100 permit ip 172.31.0.0 0.0.0.63 172.31.0.128 0.0.0.63
interface gigabitEthernet 0/0.10
ip access-group 100 in
```



```
access-list 102 permit ip 172.31.2.0 0.0.0.7 any
interface gigabitEthernet 0/0.1
ip access-group 102 in
```

```
access-list 103 permit ip 172.31.0.64 0.0.0.63 any
access-list 103 deny ip 172.31.0.64 0.0.0.63 192.168.0.0 0.0.255.255
access-list 103 deny ip 172.31.0.64 0.0.0.63 172.16.0.0 0.0.255.255
access-list 103 deny ip 172.31.0.64 0.0.0.63 10.0.0.0 0.255.255.255
```

```
interface gigabitEthernet 0/0.30
ip access-group 103 in
```

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

Opciones en puerto consola y terminal virtual

```
!
line con 0
password 7 0822455D0A16
!
line aux 0
!
line vty 0 4
password 7 0822455D0A16
line vty 5 15
password 7 0822455D0A16
!
```

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.



CONCLUSIONES

Se estudiaron y aplicaron algunas de las opciones de configuración básica de switches paso a paso, siguiendo como guía las instrucciones planteadas en las guías de actividades correspondientes y que se requieren para mantener un mejor entorno LAN conmutado, disponible y seguro.

Mediante las prácticas efectuadas se pudo aplicar y profundizar sobre las Listas de Control de Acceso (ACL), como aplicación de un concepto de seguridad informático que se usa para fomentar la separación de privilegios, determinando los permisos de acceso apropiados a un determinado objetivo o requerimiento, conceptualizando la idea de que el principal objetivo de las ACL es el de filtrar tráfico, permitiendo o denegando así, el tráfico de red, de acuerdo a las condiciones que se necesiten implementar.

La aplicación de Nat o mejor entendidas como traducción de direcciones de red, nos permitió conocer un mecanismo que permite que múltiples dispositivos compartan una sola dirección IP pública de Internet, de esta manera se puede deducir que el ahorro de direcciones públicas es muy representativo.

De igual manera, entendimos que las direcciones privadas son utilizadas dentro de las redes privadas y no son ruteadas a través de Internet. En otras palabras, que no funcionan a menos de que sean NATeadas antes de salir a Internet.

Respecto a las PAT (también denominada "NAT con sobrecarga") se observó que puede utilizar una única dirección IPv4 pública para cientos, incluso miles de direcciones IPv4 privadas internas, permitiendo que una sola dirección ip sea utilizada por varias máquinas de la intranet.

En general considero, que el curso fue formativo y productivo en cuanto a nociones y conocimiento de infraestructuras y equipamiento de networking se refiere.



REFERENCIAS BIBLIOGRAFICAS

CISCO. (2014). Introducción a redes, Capítulo 9: División de redes IP en subredes, Ing. Aníbal Coto Cortés, Recuperado de, https://www.minagricultura.gov.co/ministerio/recursos-humanos/Actos_Administrativos/Informe_2.pdf

CISCO. (2014). OSPF de una sola área. Principios de Enrutamiento y Conmutación. Recuperado de, <https://static-course-assets.s3.amazonaws.com/RSE50ES/module8/index.html#8.0.1.1>

CISCO. (2014). Listas de control de acceso. Principios de Enrutamiento y Conmutación. Recuperado de, <https://static-course-assets.s3.amazonaws.com/RSE50ES/module9/index.html#9.0.1.1>

UNAD (2014). Principios de Enrutamiento [OVA]. Recuperado de, https://1drv.ms/u/s!AmlJYei-NT1lhgOyjWeh6timi_Tm

Video YOUTUBE, (15 marzo 2012) Packet Tracer - Configurar AAA. Recuperado de, <https://www.youtube.com/watch?v=SqRPTVjU970>

Video YOUTUBE, (16 abril de 2012) Packet Tracer - Tutorial Packet Tracer - 20 - ACL Extendida. Recuperado de, <https://www.youtube.com/watch?v=OtpoVEmPaMU>

Video YOUTUBE, (16 abril de 2012) Lista de Control de Acceso (ACL) Extendida|Tutorial. Recuperado de, https://www.youtube.com/watch?v=jH_NKVhSVq8

Video YOUTUBE, (29 de Septiembre de 2016) Cisco CCNA - Como Crear y Configurar VLAN Cisco Packet Tracer, Recuperado de, <https://www.youtube.com/watch?v=a17mkhZocLc>