PRUEBAS DE HABILIDADES CCNA – FINAL

Presentado por:

FREY HERNÁN RODRÍGUEZ GARZÓN

Diplomado de profundización cisco (diseño e implementación de soluciones integradas LAN)

TUTOR GIOVANNI ALBERTO BRACHO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
INGENIERIA ELECTRÓNICA
ESCUELA DE CIENCIAS BASICAS Y TECNOLOGIAS
CEAD JAG
2019

Contenido

RESUMÉN

Se ha realizado dos escenarios con el fin de desarrollar los conceptos y ponerlos en práctica mediante el software packet tracer, en ella se divide en dos módulos, el primer escenario se puede analizar el direccionamiento IP, en el cual se debe definir una dirección de acuerdo con el número de hosts requeridos, asignar los parámetros básicos y la detección de vecinos directamente conectados, además la red y subred establecidas deberán tener una interconexión total, todos los hosts deberán ser visibles y poder comunicarse entre ellos sin restricciones. Una de las principales partes es Implementar la seguridad en la red, se debe restringir el acceso y comunicación entre hosts de acuerdo con los requerimientos del administrador de red.

Para ello se comprueba el funcionamiento mediante el software packet tracer y se realiza un ánalisis de los dos escenarios.

ABSTRACT

This work has been carried out in order to put into practice the topics covered in modules 1 and 2 of the ccna Diploma, through which two exercises with real and very frequent scenarios in the design of networks are solved.
The first scenario can be seen the division is a network into eight subnets, which is put into practice the IP addresses of the networks and their rules to carry out this subdivision, in addition the allocation of the basic parameters such as the Direct verification of equipment close to these devices.
You can check the communication of the different equipment that make up the subnets, through Telnet and Ping commands, verifying and analyzing the correct operation and guaranteeing the timely communication.
The router access list is configured, which restricts communication to a certain network, and allows communication governed by only one host, which is requested on stage.
Finally, the correct functioning is checked, by means of a table, which allows us to verify the communication of the different hosts of the different subnets.
The second scenario allows us to analyze the basic configuration of the routers, authentication, authorization and accounting (AAA), the configuration of the maximum access time to detect attacks such as establishing a TFTP server to store all the files of the routers.

INTRODUCCIÓN

Este trabajo se ha realizado con el fin de poner en práctica los temas tratados en los módulos 1 y 2 del Diplomad ccna , mediante el cual se resuelve dos ejercicios con escenarios reales y muy frecuentes en el diseño de redes.

El primer escenario se puede apreciar la división se un red en ocho subredes, lo cual se pone en práctica la direcciones ip de las redes y sus reglas para llevar a cabo dicha subdivisión, además se pone de manifiesto la asignación de los parámetros básicos como la verificación directa de los equipos cercanos a estos dispositivos.

Se puede comprobar la comunicación de los distintos equipos que conforman las subredes, por medio de comandos de Telnet y Ping, verificando y analizando el correcto funcionamiento y garantizando la oportuna comunicación.

Se configura la lista de acceso a los routers, los cuales restringen la comunicación a determinada red, y permite la comunicación gobernada solo por un host, lo cual es pedido en el escenario.

Por último se comprueba el correcto funcionamiento, mediante una tabla, que nos permite verificar la comunicación de los distintos host de las diferentes subredes.

El segundo escenario nos permite analizar la configuración básica de los routers, la autenticación, autorización y contabilidad (AAA), la configuración del máximo tiempo de acceso de detectar ataques como el establecer un servido TFTP para almacenar todos los archivos de los routers.

OBJETIVOS

- Estudiar y analizar el propósito y las reglas para realizar sudivisiones de redes, ya que es de gran importancia para redes que se pueden aumentar en capacidad a futuro, para mejoras de la red.

- Poner en práctica las configuraciones básicas de dispositivos de redes como son los routers, los switches y los hots.

- Realizar diagnóstico de conectividad por medio del comando cdp así como del comando Ping, muy útiles para este fin.

- Analizar y ejecutar la configuración de enrutamiento lo cual nos permite restringir la comunicación de dispositivos entre varias redes de un sistema.

- Obtener la mayor seguridad en el acceso a routers, configurando el máximo tiempo al detectar ataques, así como establecer un servidor TFTP para almacenar los archivos que se requieren en ,os routers.

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

DESARROLLO DE LOS 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.

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.

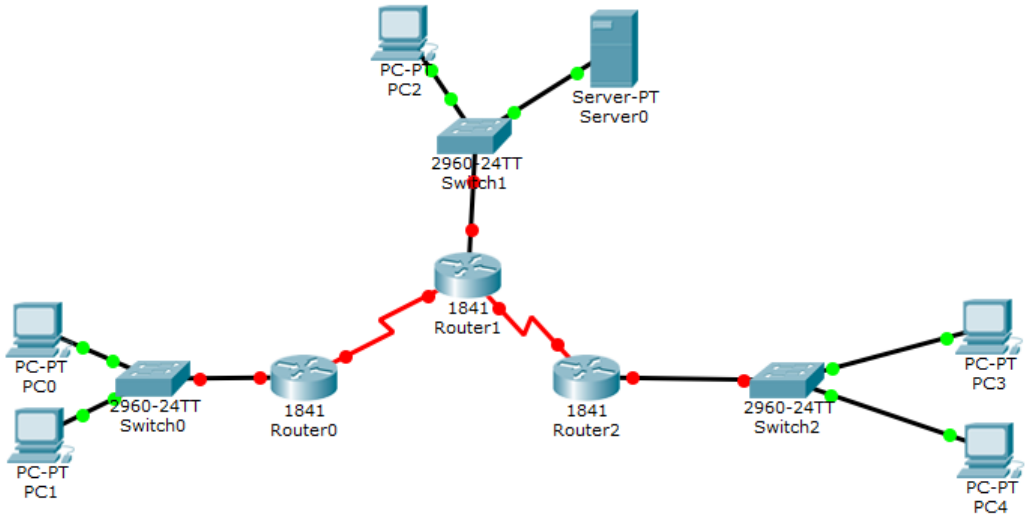


Figura 1. Topología

Desarrollo

Como trabajo inicial se debe realizar lo siguiente.

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

Configuración de los routers y switches

La configuración del R0 tenemos:

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname Medelln
Medelln(config)#no ip domain-lookup
Medelln(config)#line con 0
Medelln(config-line)#password cisco
Medelln(config-line)#login
Medelln(config-line)#line vty 0 4
Medelln(config-line)#password cisco
Medelln(config-line)#login
Medelln(config-line)#exit
Medelln(config)#service password-encryption
Medelln(config)#banner motd $ Unauthorized Acces is prohibited $
Medelln(config)#
```

La configuración de R1, tenemos:

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname Bogot
Bogot(config)#no ip domain-lookup
Bogot(config)#line con 0
Bogot(config-line)#password cisco
Bogot(config-line)#login
Bogot(config-line)#line vty 0 4
Bogot(config-line)#password cisco
Bogot(config-line)#login
Bogot(config-line)#exit
Bogot(config)#service password-encryption
Bogot(config)#banner motd $ Unauthorized Acces is prohibited $
Bogot(config)#
```

Para la configuración de R3, tenemos:

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

```
Router(config)#hostname Cali
Cali(config)#no ip domain-lookup
Cali(config)#line con 0
Cali(config-line)#password cisco
Cali(config-line)#login
Cali(config-line)#exit
Cali(config)#service password-encryption
Cali(config)#banner motd $ Unauthorized Acces is prohibited $
Cali(config)#
```

Configuración de S1:

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname S1
S1(config)#no ip domain-lookup
S1(config)#enable secret class
S1(config)#line con 0
S1(config-line)#password cisco
S1(config-line)#login
S1(config-line)#exit
S1(config)#service password-encryption
S1(config)#banner motd $ Solo personal autorizado $
S1(config)#
```

Configuración de S2:

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname S2
S2(config)#no ip domain-lookup
S2(config)#enable secret class
S2(config)#line con 0
S2(config-line)#password cisco
S2(config-line)#login
S2(config-line)#exit
S2(config)#service password-encryption
S2(config)#banner motd $ Solo personal autorizado $
S2(config)#
```

Configuración de S3:

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname S3
S3(config)#no ip domain-lookup
S3(config)#enable secret class
S3(config)#line con 0
```

S3(config-line)#password cisco
S3(config-line)#login
S3(config-line)#exit
S3(config)#service password-encryption
S3(config)#banner motd $ Solo personal autorizado $
S3(config)#

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

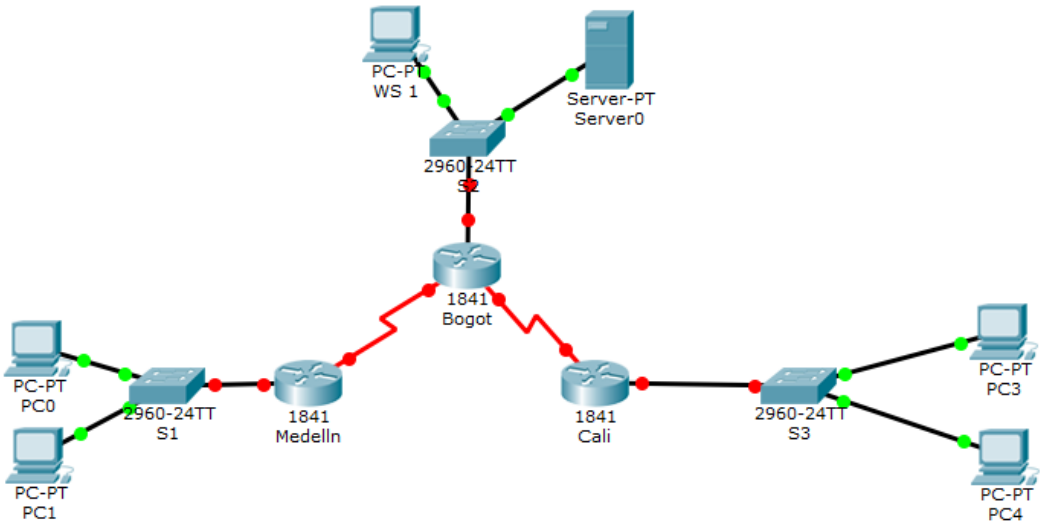


Figura 2. Conexión física

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

Parte 1: Asignación de direcciones IP:

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

De acuerdo a la red podemos observar lo siguiente:
Red Original: 192. 168. 1. 0000. 0000
Máscara de res 255. 255. 255. 0000. 0000
Por lo tanto para obtener 8 partes, entonces tenemos:

$$2^3 = 8$$

192. 168. 1. 0000. 0000
La primera subred, estará comprendida en:
192. 168. 1. 0000. 0001
192. 168. 1. 0000. 0010
192. 168. 1. 0000. 0011
192. 168. 1. 0000. 0100
⋮
192. 168. 1. 0001. 1111
Como toma prestado 3 bits entonces quedará /27.

Y la máscara estará formada por:
255.255.255.224

Teniendo en cuenta lo anterior la primera subred estará compuesta por:
192.168.1.0/27 a 192.168.1.31/27, la primera de red y la última de Broadcast
La segunda red:
192.168.1.32/27 a 192.168.1.63/27
La tercera red:
192.168.1.64/27 a 192.168.1.95/27
La cuarta red:
192.168.1.96/27 a 192.168.1.127/27
La quinta red:
192.168.1.128/27 a 192.168.1.159/27
La sexta red:
192.168.1.160/27 a 192.168.1.191/27
La séptima:
192.168.1.192/27 a 192.168.1.223/27
La octava:
192.168.1.224/27 a 192.168.1.255/27

Cada subred para una cantidad de hots de:

$$2^5 - 2 = 32 - 2 = 30\ hots$$

b. Asignar una dirección IP a la red

Parte 2: Configuración básica

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

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

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.

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

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

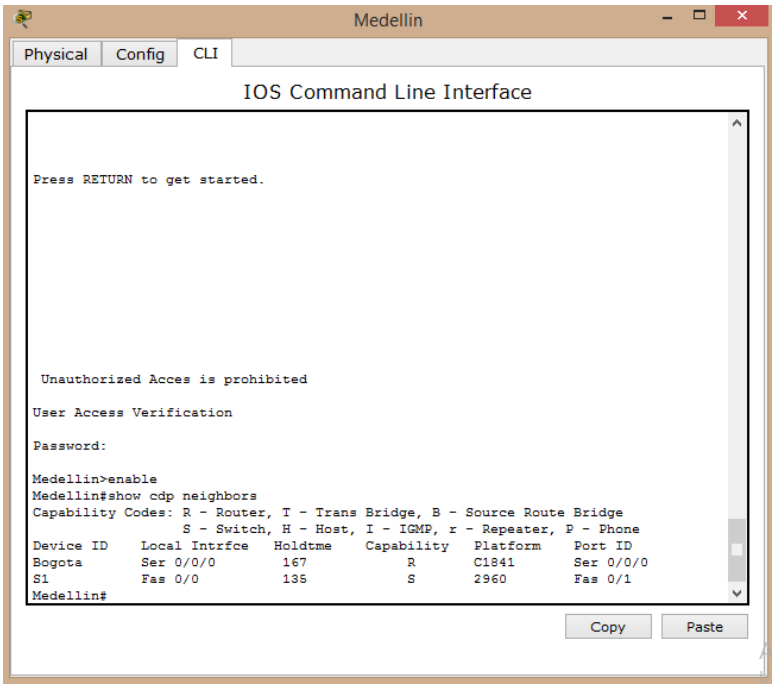


Figura 3. Comando cdp en router Medellín

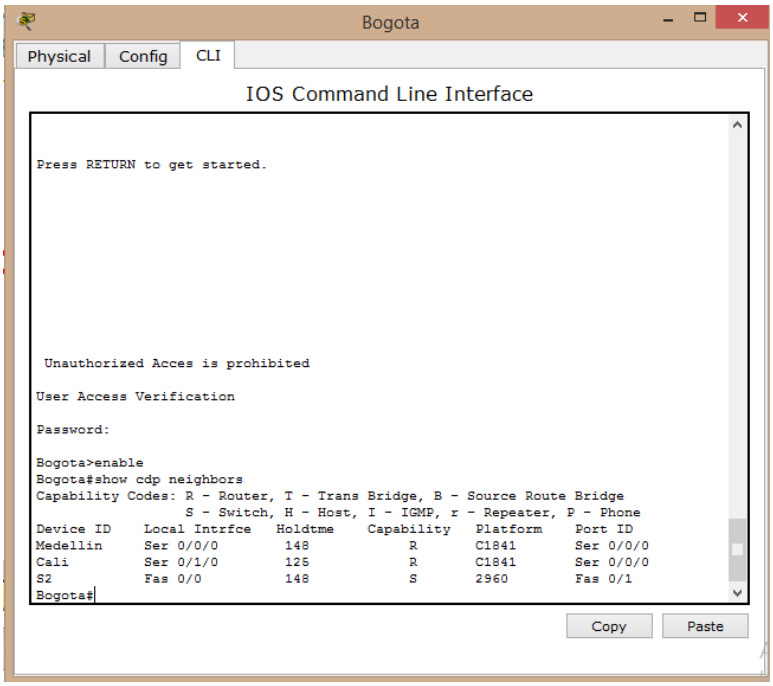


Figura 4. Comando cdp en router Bogotá

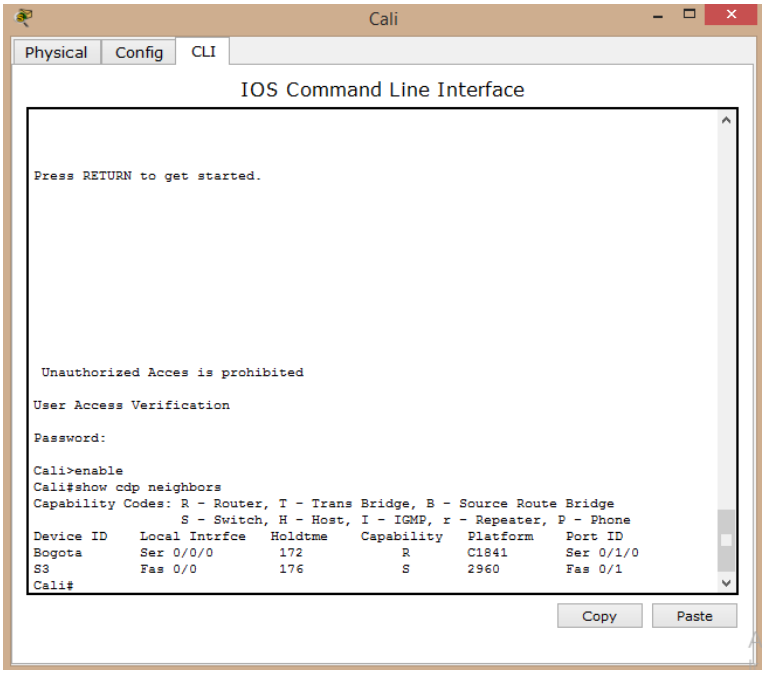


Figura 5. Comando cdp en router Cali

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

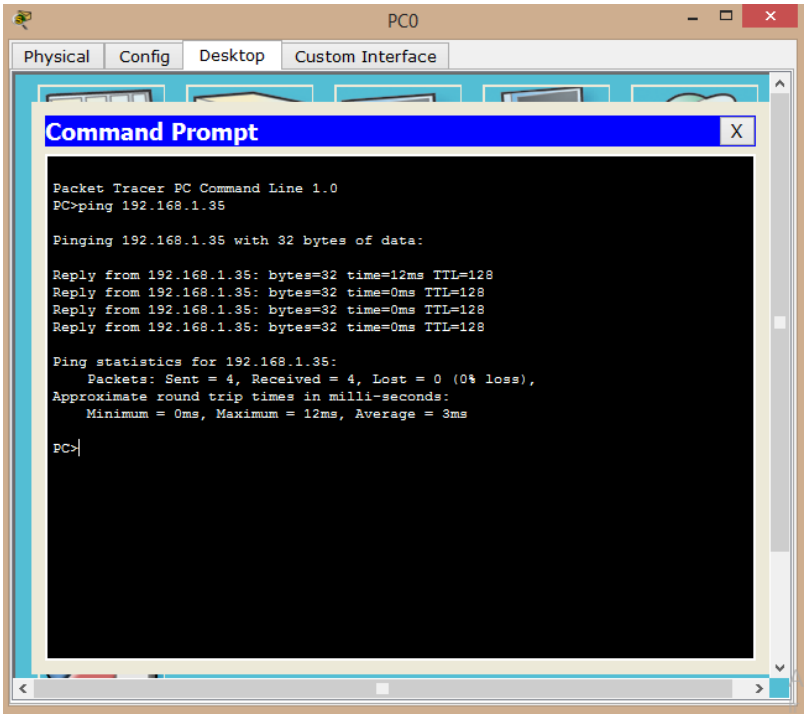


Figura 6. Ping PC0 a PC1

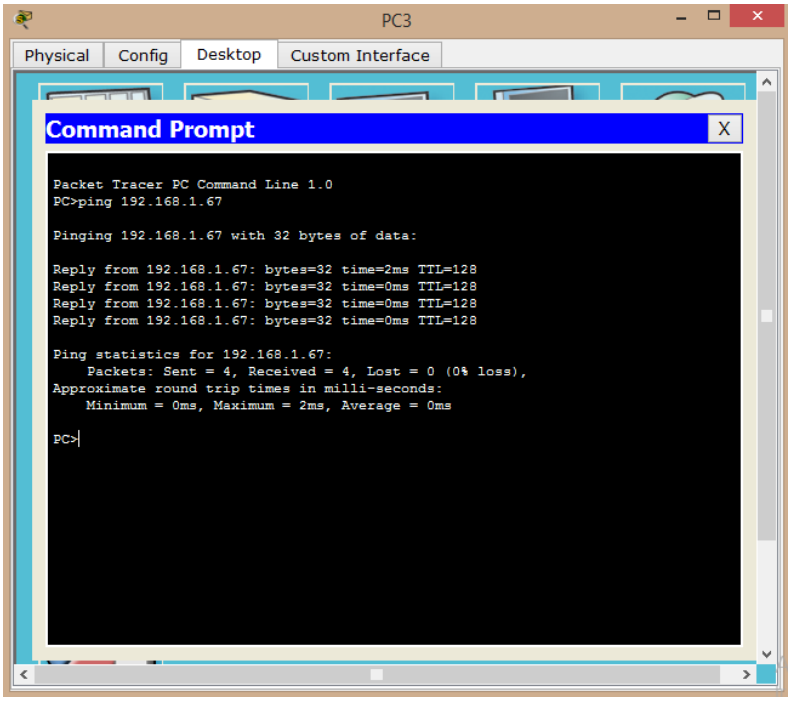


Figura 7. Ping PC 3 a PC 2

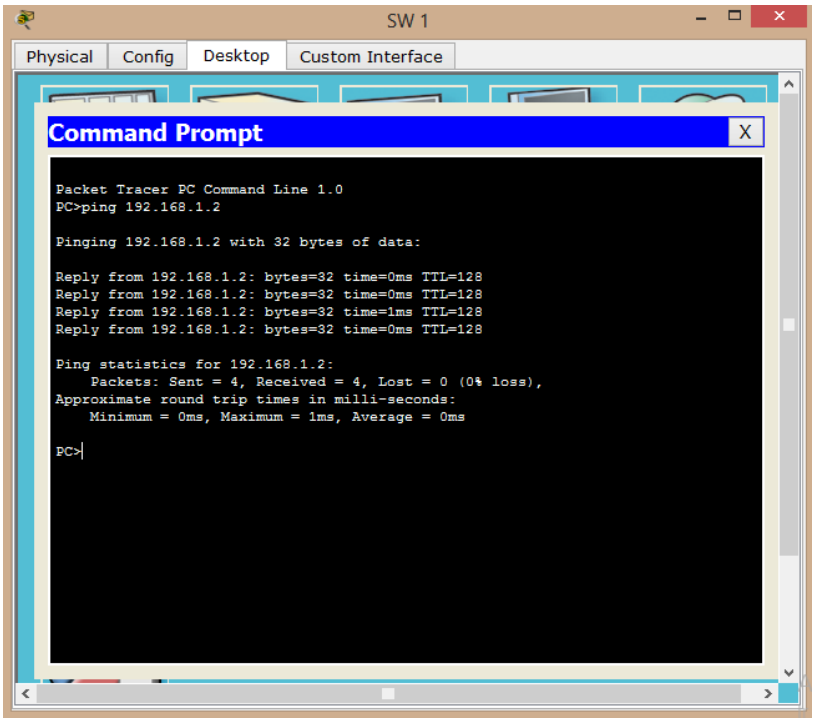


Figura 8. Ping SW1 al Servidor

Parte 3: Configuración de Enrutamiento

a. Asignar el protocolo de enrutamiento EIGRP a los routers considerando el direccionamiento diseñado.
Para el router Medellin, es:

```
Medellin>enable
Medellin#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Medellin(config)#router eigrp ?
<1-65535> Autonomous system number
Medellin(config)#router eigrp 5
Medellin(config-router)#network 192.168.1.32 0.0.0.31
Medellin(config-router)#network 192.168.1.99 0.0.0.31
Medellin(config-router)#no auto-summary
Medellin(config-router)#end
```

Para el router Bogota, es:

```
Bogota>enable
Bogota#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Bogota(config)#router eigrp ?
<1-65535> Autonomous system number
Bogota(config)#router eigrp 5
Bogota(config-router)#network 192.168.1.98 0.0.0.31
Bogota(config-router)#networ 192.168.1.131 0.0.0.31
Bogota(config-router)#network 192.168.1.1 0.0.0.31
Bogota(config-router)#no auto-summary
Bogota(config-router)#exit
Bogota(config)#exit
```

Para el router Cali, es:

```
Cali>enable
Cali#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Cali(config)#router eigrp ?
<1-65535> Autonomous system number
Cali(config)#router eigrp 5
Cali(config-router)#network 192.168.1.131 0.0.0.31
Cali(config-router)#
%DUAL-5-NBRCHANGE: IP-EIGRP 5: Neighbor 192.168.1.130
(Serial0/0/0) is up: new adjacency

Cali(config-router)#network 192.168.1.65 0.0.0.31
Cali(config-router)#no auto-summary
Cali(config-router)#exit
Cali(config)#exit
Cali#
```

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

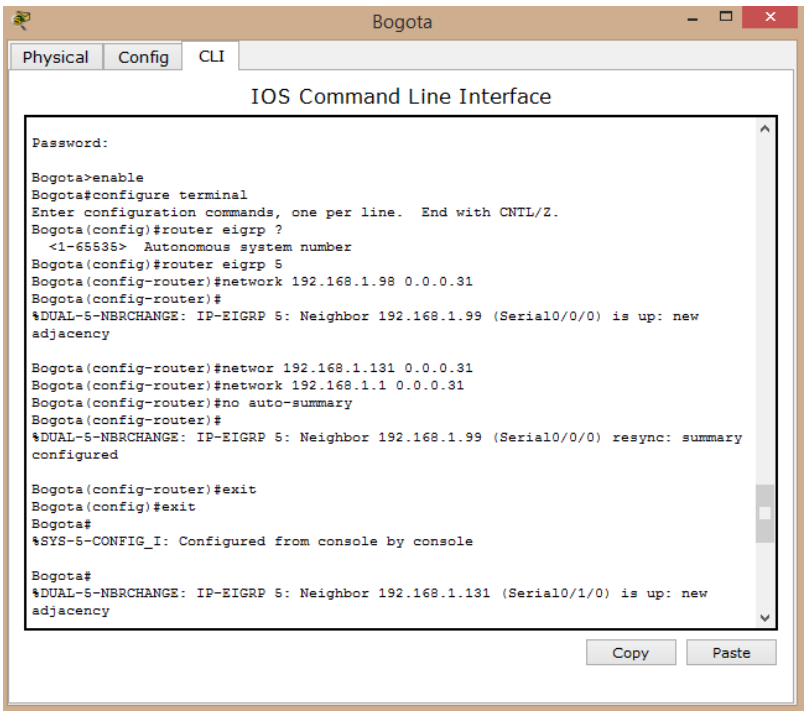


Figura 9. Comando EIGRP

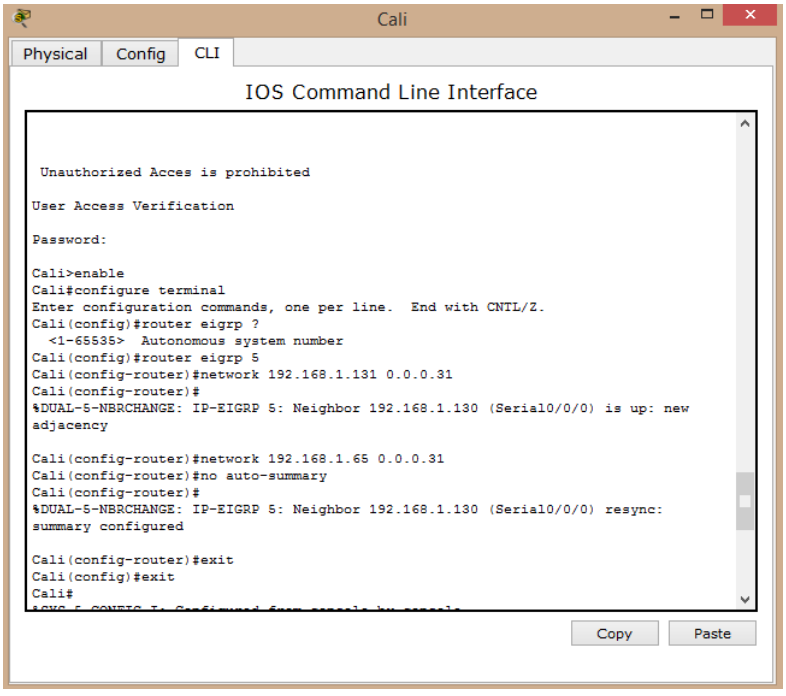


Figura 10. Comando EIGRP

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.

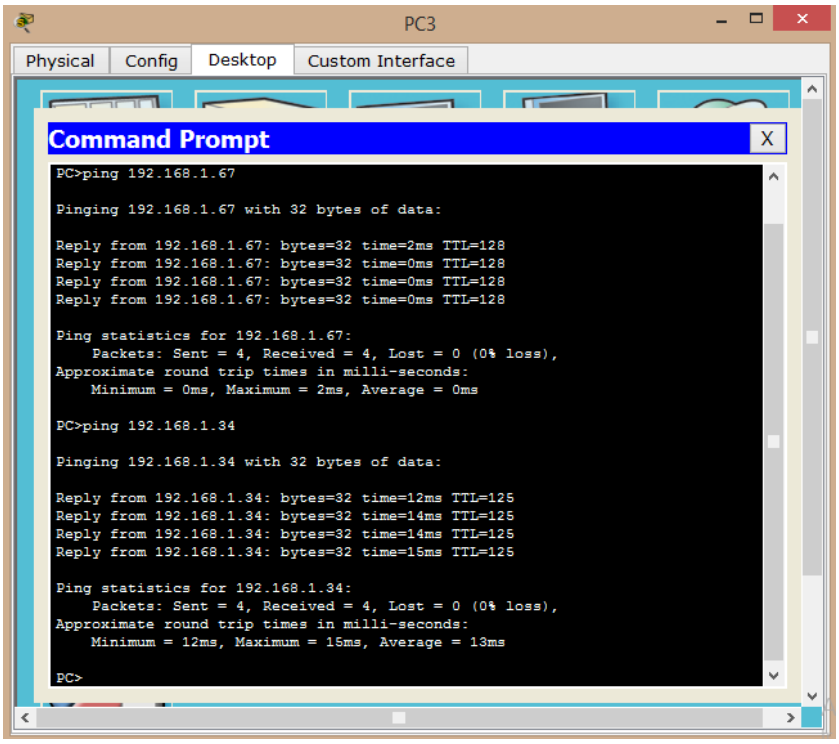


Figura 11. Ping del PC 3 de Cali a PC0 de Medellin

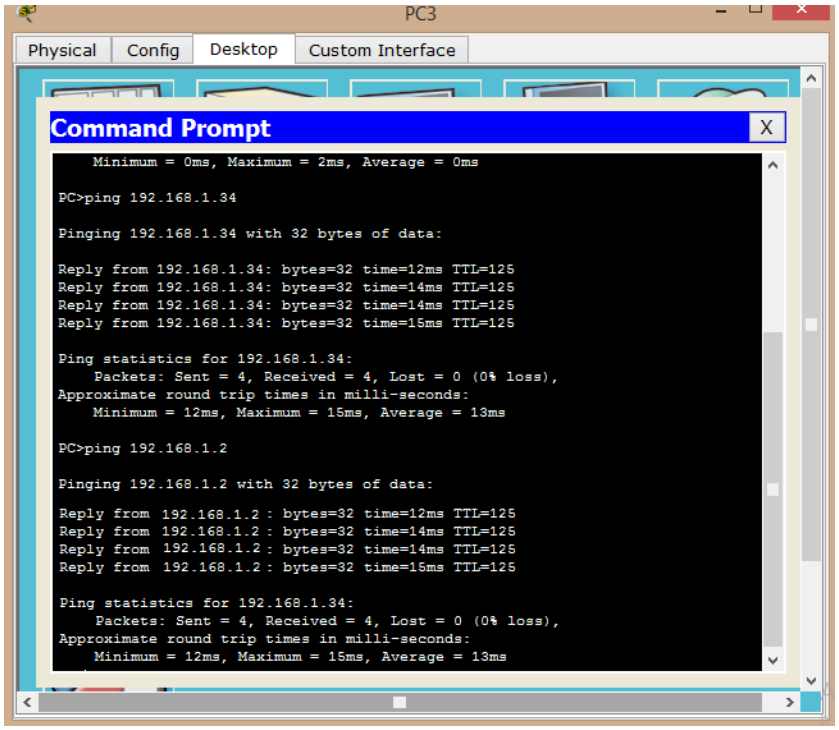


Figura 12. Ping PC3 de Cali al Servidor

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

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

Las condiciones para crear las ACL son las siguientes:

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

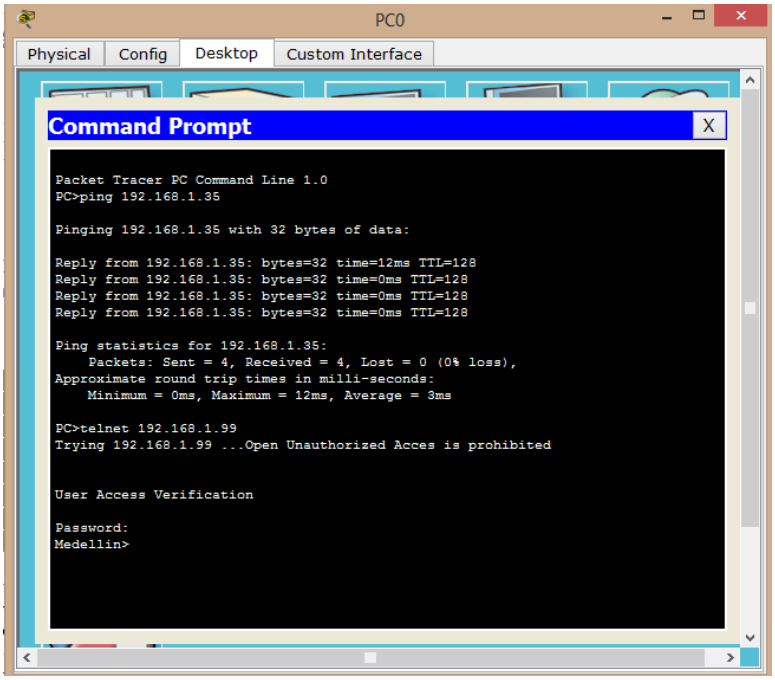


Figura 13. Telnet del PC0 al Router Medellín

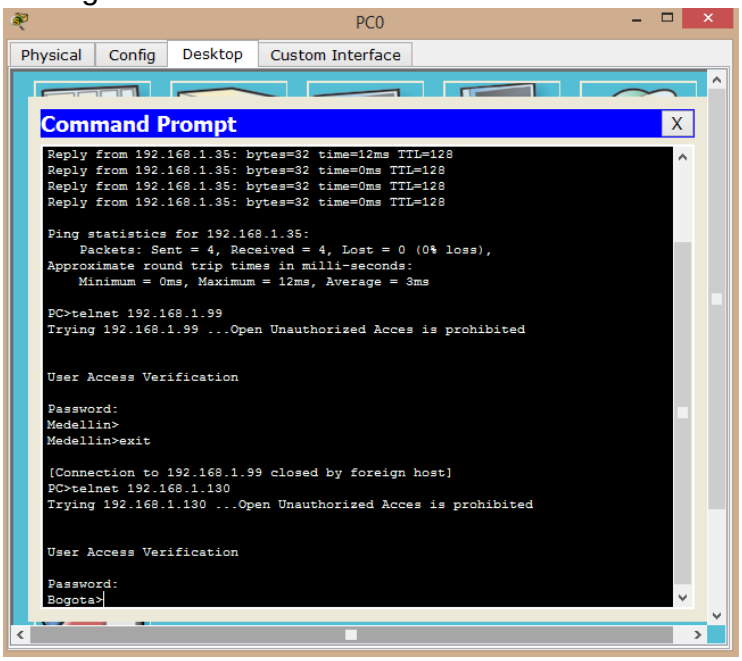


Figura 14. Telnet del PC0 al Router Bogotá

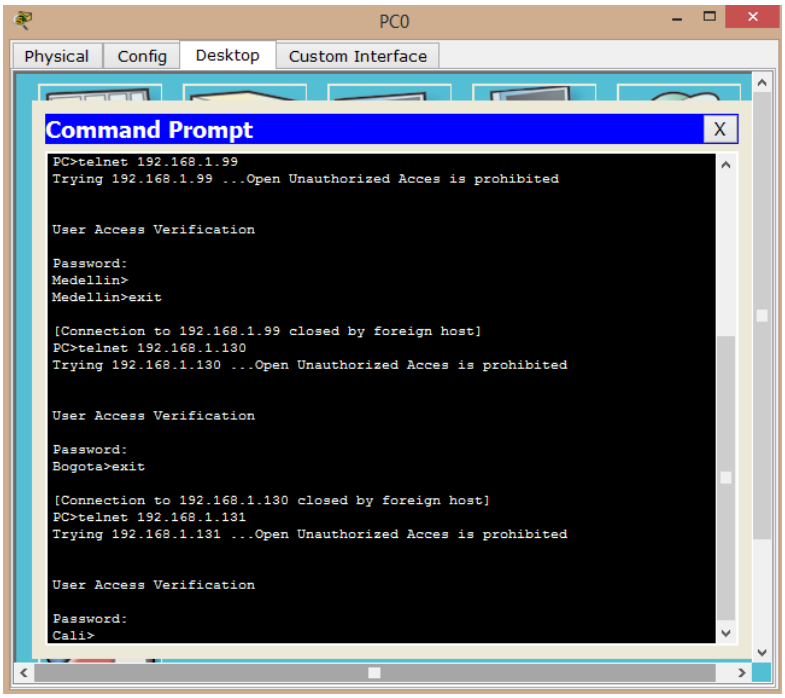


Figura 15. Telnet del PC0 al Router Cali

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.

Router Medellín

```
Medellin>enable
Medellin#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Medellin(config)#access-list 1 permit
% Incomplete command.
Medellin(config)#access-list 1 permit host 192.168.1.3
Medellin(config)#line vty 0 4
Medellin(config-line)#access-class 1 in
Medellin(config-line)#exit
Medellin(config)#
```

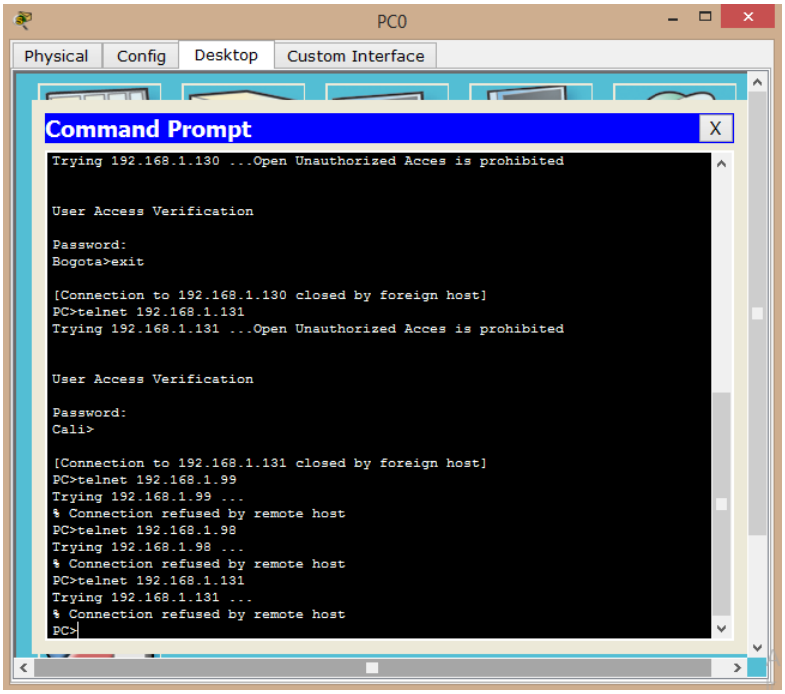


Figura 16. Telnet host PC0 a Router Medellín, Bogotá y Cali

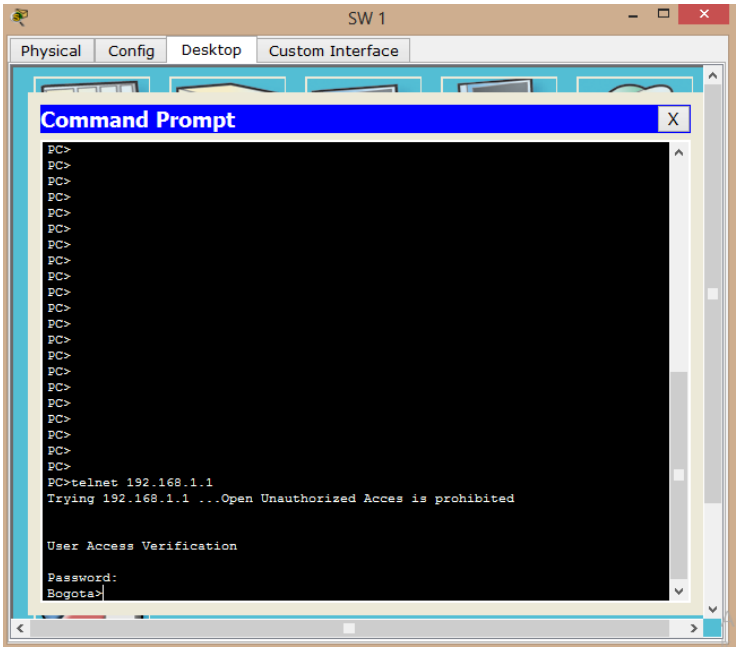


Figura 17. Telnet con router Bogotá

Router Bogotá

Bogota>enable
Bogota#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.

```
Bogota(config)#access-list 1 permit host 192.168.1.3
Bogota(config)#line vty 0 4
Bogota(config-line)#access-class 1 in
Bogota(config-line)#exit
Bogota(config)#
```

Router Cali

```
Cali>enable
Cali#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Cali(config)#access-list 1 permit host 192.168.1.3
Cali(config)#line vty 0 4
Cali(config-line)#access-class 1 in
Cali(config-line)#exit
Cali(config)#
```

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.

Router Bogotá

Password:

```
Bogota>configure terminal
Bogota#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Bogota(config)#access-list 1 deny 192.168.1.32 0.0.0.31
Bogota(config)#access-list 1 deny 192.168.1.65 0.0.0.31
Bogota(config)#access-list 1 permit any
Bogota(config)#interface fastEthernet 0/0
Bogota(config-if)#ip access-group 1 out
Bogota(config-if)#exit
Bogota(config)#
```

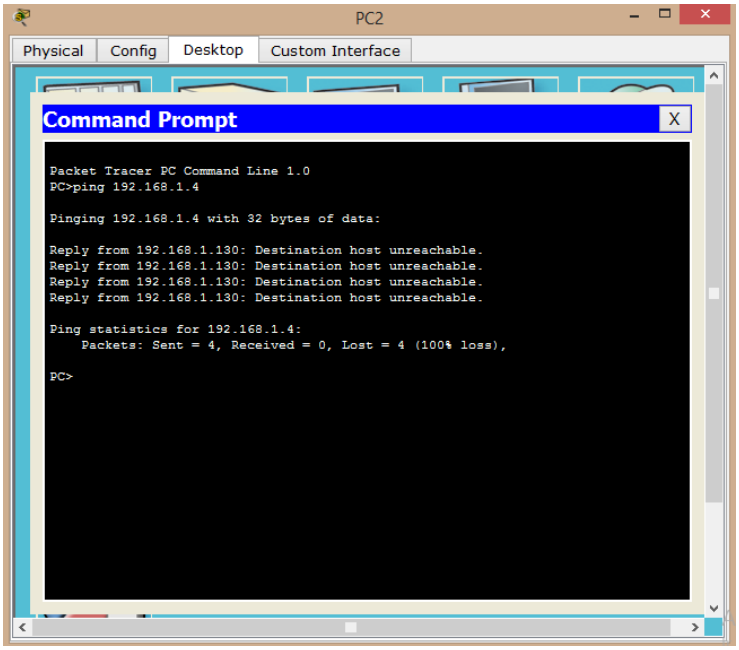


Figura 18. Ping de PC2 a SW1

Parte 5: Comprobación de la red instalada.

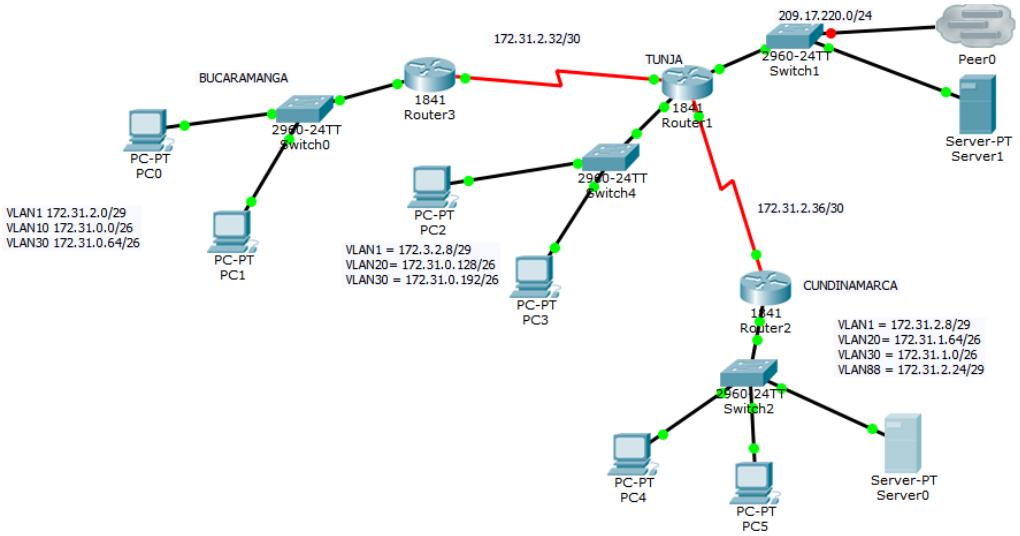
a. Se debe probar que la configuración de las listas de acceso fue exitosa.
b. Comprobar y Completar la siguiente tabla de condiciones de prueba para confirmar el óptimo funcionamiento de la red e.

	ORIGEN	DESTINO	RESULTADO
TELNET	Router MEDELLIN	Router CALI	O.K
	WS_1	Router BOGOTA	O.K
	Servidor	Router CALI	O.K
	Servidor	Router MEDELLIN	O.K
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	O.K
PING	LAN del Router CALI	Servidor	-
	LAN del Router MEDELLIN	Servidor	-
	Servidor	LAN del Router MEDELLIN	O.K

	Servidor	**LAN del Router CALI**	O.K
	Router CALI	**LAN del Router MEDELLIN**	O.K
	Router MEDELLIN	**LAN del Router CALI**	O.K

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, po esa vía, conectarse a internet, pero empleando las direcciones de la red LAN original.



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.

Configuración básica de Router

Configuración básica de R0

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname Bucaramanga
Bucaramanga(config)#no ip domain-lookup
Bucaramanga(config)#line con 0
Bucaramanga(config-line)#password cisco
Bucaramanga(config-line)#login
Bucaramanga(config-line)#line vty 0 4
Bucaramanga(config-line)#password cisco
Bucaramanga(config-line)#login
Bucaramanga(config-line)#exit
Bucaramanga(config)#service password-encryption
Bucaramanga(config)#banner motd $ Unauthorized Acces is prohibited $
Bucaramanga(config)#

Bucaramanga(config)#ip ssh time-out 10
Bucaramanga(config)#ip ssh authentication-retries 5
Bucaramanga(config)#
```

Configuración básica de R1

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname Tunja
Tunja(config)#no ip domain-lookup
Tunja(config)#line con 0
Tunja(config-line)#password cisco
Tunja(config-line)#login
Tunja(config-line)#line vty 0 4
Tunja(config-line)#password cisco
Tunja(config-line)#login
Tunja(config-line)#exit
Tunja(config)#service password-encryption
Tunja(config)#banner motd $ Unauthorized Acces is prohibited $
Tunja(config)#

Tunja(config)#ip ssh time-out 10
Tunja(config)#ip ssh authentication-retries 5
Tunja(config)#
```

Configuración básica R2

```
Router>enable.
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname Cundinamarca
Cundinamarca(config)#no ip domain-lookup
Cundinamarca(config)#line con 0
Cundinamarca(config-line)#password cisco
Cundinamarca(config-line)#login
Cundinamarca(config-line)#line vty 0 4
Cundinamarca(config-line)#password cisco
Cundinamarca(config-line)#login
Cundinamarca(config-line)#exit
Cundinamarca(config)#service password-encryption
Cundinamarca(config)#banner motd $ Unauthorized Acces is prohibited $
Cundinamarca(config)#
```

Autenticación AAA en R0

```
Bucaramanga>enable
Bucaramanga#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Bucaramanga(config)#username Admin1 secret admin123
Bucaramanga(config)#aaa new-model
Bucaramanga(config)#aaa authentication login default local
Bucaramanga(config)#line console 0
Bucaramanga(config-line)#login authentication default
Bucaramanga(config-line)#exit
Bucaramanga(config)#exit
Bucaramanga#
```

Autenticación AAA en R1

```
Tunja>enable
Tunja#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Tunja(config)#username Admin2 secret admin234
Tunja(config)#aaa new-model
Tunja(config)#aaa authentication login default local
Tunja(config)#line console 0
Tunja(config-line)#login authentication default
Tunja(config-line)#exit
Tunja(config)#exit
Tunja#
```

Autenticación en AAA en R2

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

Cundinamarca(config)#username Admin3 secret admin345
Cundinamarca(config)#aaa new-model
Cundinamarca(config)#aaa authentication login default local
Cundinamarca(config)#line console 0
Cundinamarca(config-line)#login authentication default
Cundinamarca(config-line)#exit
Cundinamarca(config)#exit
Cundinamarca#exit

Máximo número de intentos y tiempo de acceso en R0

Bucaramanga(config)#ip ssh time-out 10
Bucaramanga(config)#ip ssh authentication-retries 5
Bucaramanga(config)#

Máximo número de intentos y tiempo de acceso en R1

Tunja(config)#ip ssh time-out 10
Tunja(config)#ip ssh authentication-retries 5
Tunja(config)#

Máximo número de intentos y tiempo de acceso en R2

Cundinamarca(config)#ip ssh time-out 10
Cundinamarca(config)#ip ssh authentication-retries 5
Cundinamarca(config)#

Luego terminamos la configuración de los routers:

Router Bucaramanga

Bucaramanga#
Bucaramanga>enable
Password:
Bucaramanga#
Bucaramanga#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Bucaramanga(config)#interface FastEthernet 0/0.1
Bucaramanga(config-subif)#
%LINEPROTO-5-UPDOWN: Interface FastEthernet0/0.1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on interface FastEthernet0/0.1, changed state to up
Bucaramanga(config-subif)#encapsulation dot1Q 1
Bucaramanga(config-subif)#no shutdown

```
Bucaramanga(config-subif)#exit
Bucaramanga(config)#

Bucaramanga(config)#interface fastEthernet0/0.1
Bucaramanga(config-subif)#ip address 172.31.2.1 255.255.255.248
Bucaramanga(config-subif)#exit
Bucaramanga(config)#
Bucaramanga(config)#interface fastEthernet 0/0.1
Bucaramanga(config-subif)#
%LINK-5-CHANGED: Interface fastEthernet0/0.10, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0.10,
chnaged state to up
Bucaramanga(config-subif)#encapsulation dot1Q 10
Bucaramanga(config-subif)#ip address 172.31.0.1 255.255.255.192
Bucaramanga(config-subif)#no shutdown
Bucaramanga(config-subif)#exit
Bucaramanga(config)#
Bucaramanga(config)#interface fastEthernet0/0.30
Bucaramanga(config-subif)#
%LINK-5-CHANGED:Interface FastEthernet0/0.30, chnged state to up
%LINEPROTO-5-UPDOWN:Line protocol on interface FastEthernet0/0.30,
chnaged state to up
Bucaramanga(config-subif)#encapsulation dot1Q 30
Bucaramanga(config-subif)#ip address 172.31.0.65 255.255.255.192
Bucaramanga(config)#exit
Bucaramanga(config)#exit
Bucaramanga#
%SYS-%-CONFIG_I: Configured from console by console
Bucaramanga#Configure terminal
Bucaramanga(config)#interface serial 0/0/0
Bucaramanga(config-if)#ip address 172.31.2.33 255.255.255.252
Bucaramanga(config-if)#clock rate 64000
Bucaramanga(config-if)#exit
Bucaramanga(config)#exit
Bucaramanga#

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

Router Tunja

```
Tunja#
Tunja>enable
Password:
Tunja#
Tunja#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
```

```
 Tunja(config)#interface FastEthernet 0/1
 Tunja(config-if)#ip address 209.17.220.1 255.255.255.0
 Tunja(config-if)#no shutdown
Tunja(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on interface FastEthernet0/1, changed state to up
Tunja(config-if)#exit
Tunja(config)#

Tunja(conig)#interface fastEthernet 0/0
Tunja(config-if)#no shutdown
Tunja(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up

Tunja(config-if)#exit
Tunja(config)#interface fastEthernet 0/0.1
Tunja(config-subif)#
%LINK-5-CHANGED: Interface FastEthernet0/0.1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0.1, changed state to up

Tunja(config-subif)#encapsulation dot1Q 20
Tunja(config-subif)#ip address 172.31.0.129 255.255.255.192
Tunja(config-subif)#no shutdown
Tunja(config-subif)#exit
Tunja(config)#
Tunja(config)#interface fastEthernet 0/0.30
Tunja(config-subif)#
%LINK-5-CHANGED: Interface FastEthernet0/0.30, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0.30, changed state to up

Tunja(config-subif)#encapsulation dot1Q 30
Tunja(config-subif)#ip address 172.31.0.193 255.255.255.192
Tunja(config-subif)#exit
Tunja(config)#
Tunja(config)#interface serial 0/0/1
Tunja(config-if)ip address 172.31.2.37 255.255.255.252
Tunja(config-if)#clock rate 64000
Tunja(config-if)#exit
Tunja(config)#exit
```

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

Router Cundinamarca
Cundinamarca#
Cundinamarca#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.

Cundinamarca(config)#interface fastEthernet 0/0
Cundinamarca(config-if)#no shutdown
Cundinamarca(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up

Cundinamarca(config-if)#exit
Cundinamarca(config)#
Cundinamarca(config)#interface fastEthernet0/0.1
Cundinamarca(config-subif)#
%LINK-5-CHANGED: Interface FastEthernet0/0.1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0.1, changed state to up
Cundinamarca(config-subif)#encapsulation dot1Q 1
Cundinamarca(config-subif)#ip address 172.3.2.9 255.255.255.248
Cundinamarca(config-subif)#no shutdown
Cundinamarca(config-subif)#exit
Cundinamarca(config)#interface fastEthernet 0/0.20
Cundinamarca(config-subif)#
%LINK-5-CHANGED: Interface FastEthernet0/0.20, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0.20, changed state to up

Cundinamarca(config-subif)#encapsulation dot1Q 20
Cundinamarca(config-subif)#ip address 172.31.1.65 255.255.255.192
Cundinamarca(config-subif)#no shutdown
Cundinamarca(config-subif)#exit
Cundinamarca(config)#
Cundinamarca(config)#interface FastEthernet0/0.20
Cundinamarca(config-subif)#
%LINK-5-CHANGED: Interface FastEthernet0/0.30, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0.30, changed state to up

Cundinamarca(config)#
Cundinamarca(config)#interface serial 0/0/0
Cundinamarca(config-config-if)#ip address 172.31.2.38 255.255.2555.252

Cundinamarca(config-if)#exit
Cundinamarca(config)#
Cundinamarca
%SYS-5-CONFIG_I: Configured from console by console

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

Configuración en Bucaramanga:
Bucaramanga#
Bucaramanga>enable
Password:
Bucaramanga#configure terminal
Enter configuration commandas, one per line. End with CNTL/Z
Bucaramanga(config)#ip dchp pool VLAN10
Bucaramanga(dhcp-config)#network 172.31.0.0 255.255.255.192
Bucaramanga(dhcp-config)#default-router 172.31.0.1
Bucaramanga(dhcp-config)#exit
Bucaramanga(config)#
Bucaramanga(config)#ip dhcp excluded-address 172.31.0.1
Bucaramanga(dhcp)#ip dhcp pool VLAN30
Bucaramanga(dhcp-config)#network 172.31.0.61 255.255.255.192
Bucaramanga(dhcp-config)#default-router 172.31.0.65
Bucaramanga(dhcp-config)#exit
Bucaramanga(config)#ip dhcp excluded-address 172.31.0.65
Bucaramanga(config)#exit
Bucaramanga#
%SYS-5-CONFIG_I: Configured from console by console

Bucaramanga#wr
Building configuration...
[OK]

Configuración en Cundinamarca:
Cundinamarca#
Cundinamarca>enable
Password:
Cundinamarca#configure terminal

```
Enter configuration commandas, one per line. End with CNTL/Z
Cundinamarca(config)#ip dchp pool VLAN20
Cundinamarca(dhcp-config)#network 172.31.0.128 255.255.255.192
Cundinamarca(dhcp-config)#default-router 172.31.0.129
Cundinamarca(dhcp-config)#exit
Cundinamarca(config)#
Cundinamarca(config)#ip dhcp excluded-address 172.31.0.129
Cundinamarca(dhcp)#ip dhcp pool VLAN30
Cundinamarca (dhcp-config)#network 172.31.0.192 255.255.255.192
Cundinamarca (dhcp-config)#default-router 172.31.0.193
Cundinamarca (dhcp-config)#exit
Cundinamarca (config)#ip dhcp excluded-address 172.31.0.193
Cundinamarca(dhcp)#ip dhcp pool VLAN88
Cundinamarca (dhcp-config)#network 172.31.0.24 255.255.255.248
Cundinamarca (dhcp-config)#default-router 172.31.2.25
Cundinamarca (dhcp-config)#exit
Cundinamarca (config)#ip dhcp excluded-address 172.31.2.25
Cundinamarca (config)#exit
Cundinamarca #
%SYS-5-CONFIG_I: Configured from console by console

Cundinamarca#wr
Building configuration...
[OK]
```

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

```
Tunja#
Tunja>enable
Password:
Tunja#
Tunja#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Tunja(config)#access-list 1 permit  209.17.220.0 0.0.0.255
Tunja(config)#ip nat inside souerce list 1 interface FastEthernet0/0 overload
Tunja(config)#Interface FastEthernet0/0
Tunja(config-if)#ip nat outside
Tunja(config-if)#Interface FastEthernet0/0.1
Tunja(config-subif)#ip nat inside
Tunja(config-subif)#Interface FastEthernet0/0.20
Tunja(config-subif)#ip nat inside
Tunja(config-subif)#Interface FastEthernet0/0.30
```

```
Tunja(config-subif)#ip nat inside
Tunja(config-subif)# interface serial 0/0/0
Tunja(config-if)#ip nat inside
Tunja(config-if)# interface serial 0/0/1
Tunja(config-if)#ip nat inside
Tunja(config-if)#exit
```

El enrutamiento deberá tener autenticación.

```
Bucaramanga>enable
Password:
Bucaramanga#
Bucaramanga#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Bucaramanga(config)#interface serial0/0/0
Bucaramanga(config-if)#ip ospf authentication message-digest
Bucaramanga(config-if)#ip ospf message-digest-key 1 md5 cisco
Bucaramanga(config-if)#
Bucaramanga(config-if)#exit
Bucaramanga(config)

Tunja>enable
Password:
Tunja#
Tunja#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Tunja(config)#interface serial0/0/0
Tunja(config-if)#ip ospf authentication message-digest
Tunja(config-if)#ip ospf message-digest-key 1 md5 cisco
Tunja(config-if)#
Tunja(config-if)#exit
Tunja(config)
```

Listas de control de acceso:

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

```
Tunja>enable
Password:
Tunja#
Tunja#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Tunja(config)#access-list 1permit icmp 172.31.2.32 0.0.0.3 host 173.31.1.0
```

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

Tunja>enable
Password:
Tunja#
Tunja#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Tunja(config)#access-list 1permit icmp 172.31.2.32 0.0.0.3 host 173.31.2.8

- Los hosts de VLAN 30 en Tunja solo acceden a servidores web y ftp de internet.
  En el servidor Web:

Tunja>enable
Password:
Tunja#
Tunja#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Tunja(config)#access-list 1permit icmp 172.31.1.66 0.0.0.63 host 173.31.0.0
Tunja(config)#

En el servidor FTTP:
Tunja>enable
Password:
Tunja#
Tunja#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Tunja(config)#access-list 1permit icmp 209.17.220.2 0.0.0.255 host 173.31.0.0
Tunja(config)#

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

Cundinamarca>enable
Password:
Cundinamarca#
Cundinamarca#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Cundinamarca(config)#access-list 1permit icmp 172.31.1.64 0.0.0.63 host 173.31.0.128
Cundinamarca(config)#

Bucaramanga>enable
Password:
Bucaramanga#
Bucaramanga#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Bucaramanga(config)#access-list 1permit icmp 172.31.0.0 0.0.0.63 host 173.31.0.128
Bucaramanga(config)#

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

Cundinamarca>enable
Password:
Cundinamarca#
Cundinamarca#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Cundinamarca(config)#access-list 1permit icmp 172.31.1.64 0.0.0.63 host 173.31.0.64
Cundinamarca(config)#

Bucaramanga>enable
Password:
Bucaramanga#
Bucaramanga#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Bucaramanga(config)#access-list 1permit icmp 172.31.2.8 0.0.0.31 host 173.31.0.64
Bucaramanga(config)#

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

De acuerdo a los escenarios propuestos se ponen en práctica los conocimientos adquiridos a través del curso, lo cual se puede dar soluciones a problemas planteados que surgen en la vida real. Por lo tanto se va tomando destrezas de configuración de dispositivos tan importantes como el router y los switches, además de la configuración de direcciones en los hots, para el buen funcionamiento de una red, también se pone en práctica la seguridad ante la configuración de usuarios ajenos que puedan tener acceso a estos equipos.

BIBLIOGRAFÍA

CISCO. (s.f.)(2019). *Cisco Networking Academy de CCNA1 I-2019*:Routing and switching. Obtenido de https://www.netacad.com/es/about-networking-academy.

Cisco. (2019). CCNA *Cisco Networking Academy de CCNA1 I-2019* – configuración DHCP, obtenido de: http://blog.capacityacademy.com/2014/01/09/cisco-ccna-como-configurar-dhcp-en-cisco-router/

Cisco. (2019). CCNA *Cisco Networking Academy de CCNA1 I-2019*- Configurar las ACL de IP, obtenido de: https://www.cisco.com/c/en/us/support/docs/ip/access-lists/26448-ACLsamples.html

Como configurar OPSF en Router http://blog.capacityacademy.com/2014/06/23/cisco-ccna-como-configurar-ospf-en-cisco-router/