PRUEBA DE HABILIDADES CCNA

(DISEÑO E IMPLEMENTACIÓN DE SOLUCIONES INTEGRADAS LAN/ WAN)

JUAN FERNANDO ALVAREZ SALAMANCA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA (ECBTI)
INGENIERÍA ELECTRONICA
SOGAMOSO – BOYACA
2020

PRUEBA DE HABILIDADES CCNA

(DISEÑO E IMPLEMENTACIÓN DE SOLUCIONES INTEGRADAS LAN/ WAN)

JUAN FERNANDO ALVAREZ SALAMANCA

Trabajo final de Diplomado de Profundización CISCO Para optar al título de Ingeniero Electrónico

DIRECTOR

ING. JUAN CARLOS VESGA FERREIRA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA (UNAD)
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA (ECBTI)
INGENIERÍA ELECTRONICA
SOGAMOSO – BOYACA

2020

NOTA DE ACEPTACION

_____

_____

_____

_____

_____

_____

_____

Presidente del jurado

_____

Jurado

_____

Jurado

DEDICATORIA

Le dedico este trabajo en primera instancia a Dios, quien es con sus bendiciones permite realizar los objetivos propuestos, a la empresa donde laboro ya que es la que económicamente me sostiene para sacar adelante los logros, a mi familia, por su apoyo incondicional a lo largo de esta carrera y a mis compañeros que durante este ciclo fueron apoyo y ayuda en el trascurrir de cada semestre.

GLOSARIO

Enrutamiento EIGRP: ES un protocolo de enrutamiento del tipo vector distancia avanzado, propiedad de Cisco, que ofrece las mejores características de los algoritmos vector distancia y de estado de enlace; EIGRP es utilizado en redes TCP/IP y de Interconexión de Sistemas Abierto (OSI)
Dirección IPV6 Es una etiqueta numérica usada para identificar una interfaz de red

Dirección unicast Una dirección unicast identifica un único interfaz de red. El protocolo de Internet entrega los paquetes enviados a una dirección unicast al interfaz específico

Dirección anycast: Una dirección anycast es asignada a un grupo de interfaces, normalmente de nodos diferentes

Dirección Mulitcast Una dirección multicast también es usada por múltiples interfaces, Un paquete enviado a una dirección multicast es entregado a todos los interfaces que se hayan unido al grupo multicast correspondiente.

Servidor FTP: Es un protocolo de red para la transferencia de archivos entre sistemas conectados a una red TCP (Transmission Control Protocol), basado en la arquitectura cliente-servidor

Servidor DNS Es una tecnología basada en una base de datos que sirve para resolver nombres en las redes, es decir, para conocer la dirección IP de la máquina donde está alojado el dominio al que queremos acceder

Un servidor Web: Es un programa que utiliza el protocolo de transferencia de híper texto, HTTP para servir los archivos que forman páginas Web a los usuarios, en respuesta a sus solicitudes, que son reenviados por los clientes HTTP de sus computadoras.

RESUMEN

Durante el desarrollo de este documento se le dará solución las 2 situaciones planteadas como parte de un examen final da habilidades prácticas en el curso CCNA 2; el administrador de la red, deberá hacer la configurar e interconexión de los dispositivos que forman parte de la red, de acuerdo a lo requerido donde se puedan aplicar los conocimientos adquiridos durante este curso, la teoría y las habilidades que se han venido desarrollando con cada una de las practicas realizadas y que han formado una capacidad técnica suficiente para desarrollar este proceso.

TABLA DE CONTENIDO

LISTADO DE FIGURAS

LISTADO DE TABLAS

INTRODUCCION

Durante el trascurso de este curso se han venido desarrollando de manera sistemática una serie de laboratorios realizados por pasos, tratando de entender los conceptos y aplicarlos en estas aplicaciones y aplicando los comandos que darán origen a preguntas con el ánimo de reforzar el procedimiento y afianzar la labor realizada mediante el uso de Packet Tracer que es la herramienta de aprendizaje y simulación de redes interactiva para los instructores y alumnos de Cisco CCNA. Esta herramienta nos permite a los usuarios crear topologías de red, configurar dispositivos, insertar paquetes y simular una red con múltiples representaciones visuales; Packet Tracer se enfoca en apoyar mejor los protocolos de redes que se enseñan durante el programa y afianzar de manera práctica los módulos teóricos desarrollados y evaluados. Uno de los puntos importantes desarrollados durante este trabajo son las rutas estáticas que se utilizan generalmente cuando se enruta desde una red a una red de conexión única que es una red a la que se accede por una sola ruta.

OBJETIVOS

1.1 OBJETIVO GENERAL

Consolidar y aplicar los conocimientos establecidos a lo largo del curso al igual que aplicar las fortalezas adquiridas por medio del desarrollo de las prácticas y que tiene un uso de los diferentes comandos y las habilidades adquiridas en el desarrollo de Packet Tracer en la solución de 2 escenarios por medio de este trabajo.

1.2 OBJETIVOS ESPECIFICOS

Establecer la topología e inicializar los dispositivos

Configurar los parámetros básicos de los dispositivos y verificar la conectividad

Conocer y aplicar la configuración básica para un Switch y un Router.

Identificar los protocolos de seguridad usados en los Switch.

Configurar los puertos de switch para cumplir con los requisitos de red.

Configurar la característica de seguridad de puertos para restringir el acceso a la red.

Configurar y aplicar una ACL nombrada estándar

Configurar rutas estáticas

2 DESARROLLO

2.1 PLANTEAMIENTO DEL PROBLEMA

2.1.1 ESCENARIO 1

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

2.1.2 REQUERIMIENTOS SOLICITADOS EN LA TOPOLOGÍA DE RED 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.

2.1.2.1 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.

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.

192.168.1.0/27 Mascara 255.255.255.224

Blocksize 32 2^3 -2 =6 redes usables 8 redes reales

Tabla 3 Direccionamientos

Dispositivo	Interface	Dirección IP	Masca de Subred	Puerta de enlace predeterminada
R1	G0/0	192.168.1.33	255.255.255.224	
	S0/0/0	192.168.1.99	255.255.255.224	
R2	S0/0/0	192.168.1.98	255.255.255.224	
	S0/0/1	192.168.1.130	255.255.255.224	
	G0/0	192.168.1.1	255.255.255.224	
R3				
	S0/0/0	192.168.1.131	255.255.255.224	
	G0/0	192.168.1.65	255.255.255.224	
Ws-1	NIC	192.168.1.2	255.255.255.224	192.168.1.1
PC-B	NIC	192.168.1.38	255.255.255.224	192.168.1.33
PC-C	NIC	192.168.1.39	255.255.255.224	192.168.133
PC-D	NIC	192.168.1.68	255.255.255.224	192.168.1.65
PC-E	NIC	192.168.1.69	255.255.255.224	192.168.1.65
SERVIDOR	NIC	192.168.1.5	255.255.255.224	DHCP

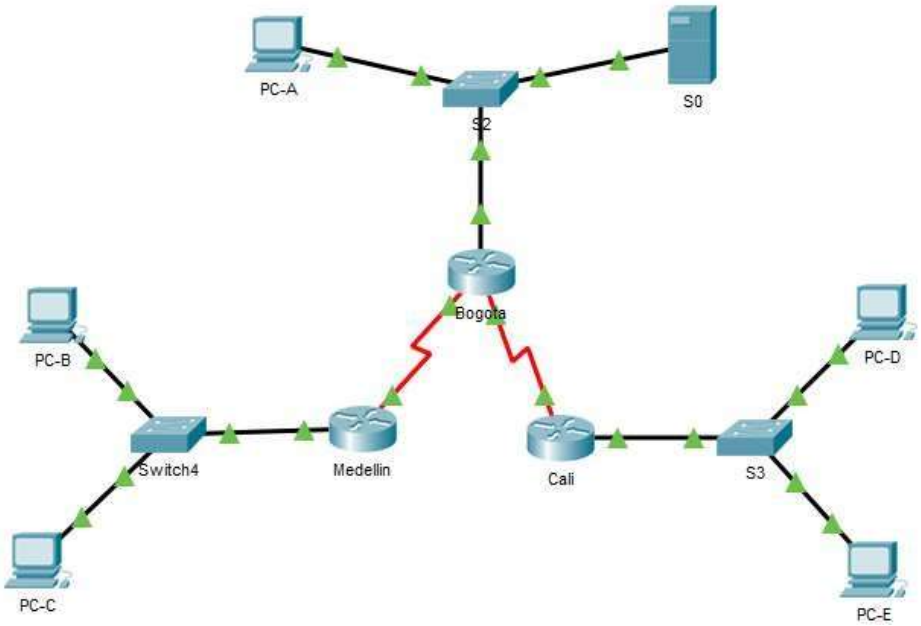
b. Después de cargada la configuración en los dispositivos, verificar la tabla de enrutamiento en cada uno de los routers para comprobar las redes y sus rutas.

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

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

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

Ilustración 3 asignación de los parámetros básicos y la detección de vecinos



C:\>ping 192.168.1.68

Pinging 192.168.1.68 with 32 bytes of data:

Reply from 192.168.1.68: bytes=32 time<1ms TTL=128
Reply from 192.168.1.68: bytes=32 time<1ms TTL=128
Reply from 192.168.1.68: bytes=32 time<1ms TTL=128
Reply from 192.168.1.68: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.68:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:

Reply from 192.168.1.2: bytes=32 time=2ms TTL=126
Reply from 192.168.1.2: bytes=32 time=2ms TTL=124
Reply from 192.168.1.2: bytes=32 time=1ms TTL=126
Reply from 192.168.1.2: bytes=32 time=2ms TTL=124

Ping statistics for 192.168.1.2:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 1ms, Maximum = 2ms, Average = 1ms
C:\>ping 192.168.1.69

Pinging 192.168.1.69 with 32 bytes of data:

Reply from 192.168.1.69: bytes=32 time=1ms TTL=128
Reply from 192.168.1.69: bytes=32 time<1ms TTL=128
Reply from 192.168.1.69: bytes=32 time<1ms TTL=128
Reply from 192.168.1.69: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.69:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:

Reply from 192.168.1.2: bytes=32 time=2ms TTL=126
Reply from 192.168.1.2: bytes=32 time=3ms TTL=124
Reply from 192.168.1.2: bytes=32 time=2ms TTL=126
Reply from 192.168.1.2: bytes=32 time=2ms TTL=124

Ping statistics for 192.168.1.2:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 2ms, Maximum = 3ms, Average = 2ms

C:\>ping 192.168.1.39

Pinging 192.168.1.39 with 32 bytes of data:

Reply from 192.168.1.39: bytes=32 time=47ms TTL=128
Reply from 192.168.1.39: bytes=32 time=1ms TTL=128
Reply from 192.168.1.39: bytes=32 time<1ms TTL=128
Reply from 192.168.1.39: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.39:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 47ms, Average = 12ms

C:\>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:

Request timed out.
Reply from 192.168.1.2: bytes=32 time=1ms TTL=126
Reply from 192.168.1.2: bytes=32 time=1ms TTL=126
Reply from 192.168.1.2: bytes=32 time=1ms TTL=126

Ping statistics for 192.168.1.2:
Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
Minimum = 1ms, Maximum = 1ms, Average = 1ms

C:\>ping 192.168.1.38

Pinging 192.168.1.38 with 32 bytes of data:

Reply from 192.168.1.38: bytes=32 time=1ms TTL=128
Reply from 192.168.1.38: bytes=32 time<1ms TTL=128
Reply from 192.168.1.38: bytes=32 time<1ms TTL=128
Reply from 192.168.1.38: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.38:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:

Reply from 192.168.1.2: bytes=32 time=2ms TTL=126
Reply from 192.168.1.2: bytes=32 time=1ms TTL=126
Reply from 192.168.1.2: bytes=32 time=1ms TTL=126
Reply from 192.168.1.2: bytes=32 time=4ms TTL=126

Ping statistics for 192.168.1.2:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:

Minimum = 1ms, Maximum = 4ms, Average = 2ms

C:\>ping 192.168.1.38

Pinging 192.168.1.38 with 32 bytes of data:

Reply from 192.168.1.38: bytes=32 time=1ms TTL=126
Reply from 192.168.1.38: bytes=32 time=1ms TTL=126
Reply from 192.168.1.38: bytes=32 time=1ms TTL=126
Reply from 192.168.1.38: bytes=32 time=1ms TTL=126

Ping statistics for 192.168.1.38:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 1ms, Maximum = 1ms, Average = 1ms

C:\>ping 192.168.1.39

Pinging 192.168.1.39 with 32 bytes of data:

Reply from 192.168.1.39: bytes=32 time=3ms TTL=126
Reply from 192.168.1.39: bytes=32 time=1ms TTL=126
Reply from 192.168.1.39: bytes=32 time=1ms TTL=126
Reply from 192.168.1.39: bytes=32 time=1ms TTL=126

Ping statistics for 192.168.1.39:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 1ms, Maximum = 3ms, Average = 1ms

C:\>ping 192.168.1.68

Pinging 192.168.1.68 with 32 bytes of data:

Reply from 192.168.1.68: bytes=32 time=2ms TTL=126
Reply from 192.168.1.68: bytes=32 time=2ms TTL=126
Reply from 192.168.1.68: bytes=32 time=1ms TTL=126
Reply from 192.168.1.68: bytes=32 time=3ms TTL=126

Ping statistics for 192.168.1.68:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 1ms, Maximum = 3ms, Average = 2ms

C:\>ping 192.168.1.69

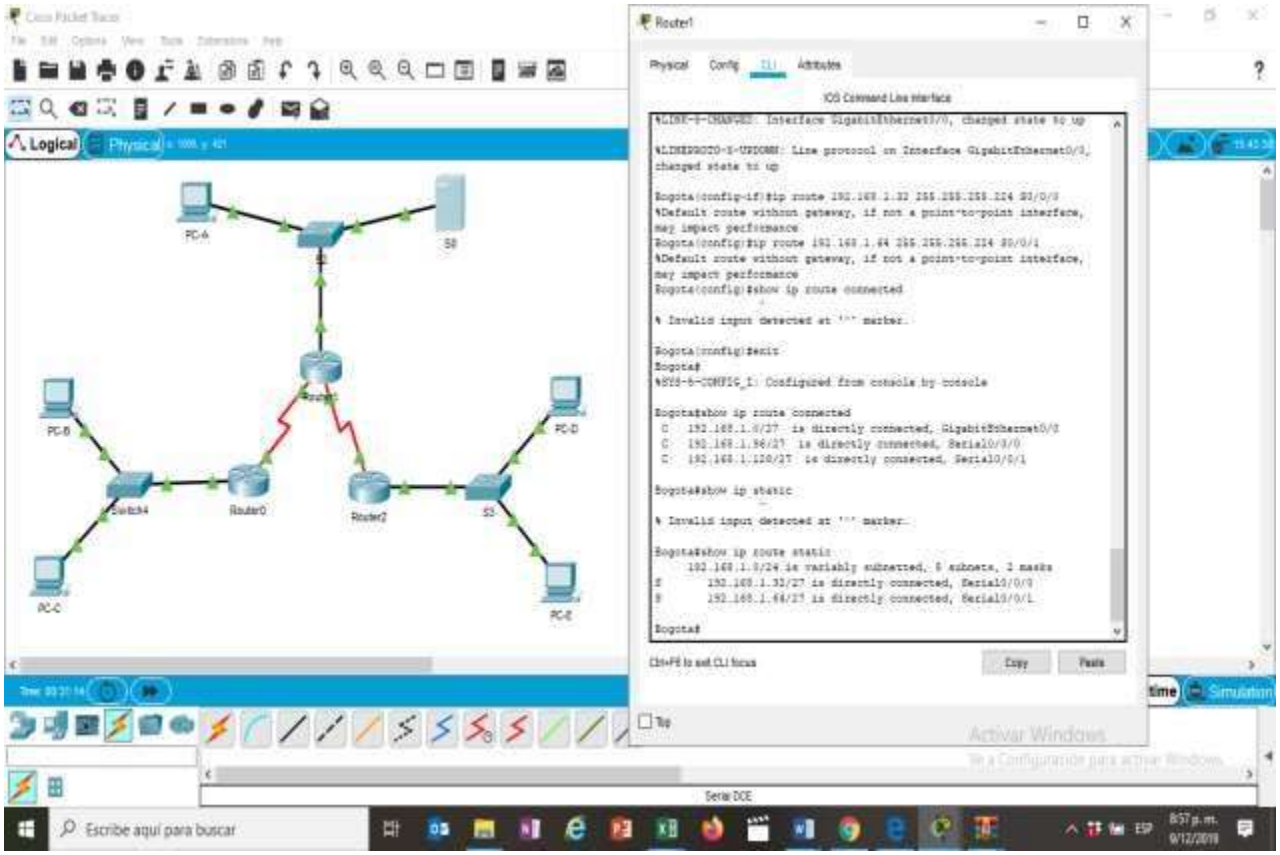
Pinging 192.168.1.69 with 32 bytes of data:

Reply from 192.168.1.69: bytes=32 time=1ms TTL=126
Reply from 192.168.1.69: bytes=32 time=3ms TTL=126
Reply from 192.168.1.69: bytes=32 time=1ms TTL=126
Reply from 192.168.1.69: bytes=32 time=2ms TTL=126

Ping statistics for 192.168.1.69:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:

Minimum = 1ms, Maximum = 3ms, Average = 1ms

Ilustración 4 ROUTER Interface Gigabit Ethernet



```
Medellín>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
S 192.168.1.0/27 is directly connected, Serial0/0/0 [1/0] via 192.168.1.98
C 192.168.1.32/27 is directly connected, GigabitEthernet0/0
L 192.168.1.33/32 is directly connected, GigabitEthernet0/0
S 192.168.1.64/27 is directly connected, Serial0/0/0 [1/0] via 192.168.1.98
C 192.168.1.96/27 is directly connected, Serial0/0/0
L 192.168.1.99/32 is directly connected, Serial0/0/0
S 192.168.1.128/27 is directly connected, Serial0/0/0 [1/0] via 192.168.1.98

Medellín>show ip route static
192.168.1.0/24 is variably subnetted, 7 subnets, 2 masks
S 192.168.1.0/27 is directly connected, Serial0/0/0 [1/0] via 192.168.1.98
S 192.168.1.64/27 is directly connected, Serial0/0/0 [1/0] via 192.168.1.98
S 192.168.1.128/27 is directly connected, Serial0/0/0 [1/0] via 192.168.1.98

Medellín>show ip route connected
C 192.168.1.32/27 is directly connected, GigabitEthernet0/0
C 192.168.1.96/27 is directly connected, Serial0/0/0



Bogotá>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
S 192.168.1.32/27 is directly connected, Serial0/0/0 [1/0] via 192.168.1.99
S 192.168.1.64/27 is directly connected, Serial0/0/1 [1/0] via 192.168.1.99
[1/0] via 192.168.1.131
C 192.168.1.96/27 is directly connected, Serial0/0/0
L 192.168.1.98/32 is directly connected, Serial0/0/0
C 192.168.1.128/27 is directly connected, Serial0/0/1
L 192.168.1.130/32 is directly connected, Serial0/0/1

Bogotá>show ip route static
192.168.1.0/24 is variably subnetted, 8 subnets, 2 masks
S 192.168.1.32/27 is directly connected, Serial0/0/0 [1/0] via 192.168.1.99
S 192.168.1.64/27 is directly connected, Serial0/0/1 [1/0] via 192.168.1.131

Bogotá>show ip route connected
C 192.168.1.0/27 is directly connected, GigabitEthernet0/0
C 192.168.1.96/27 is directly connected, Serial0/0/0
C 192.168.1.128/27 is directly connected, Serial0/0/1

Cali>show ip route connected
C 192.168.1.64/27 is directly connected, GigabitEthernet0/0
C 192.168.1.128/27 is directly connected, Serial0/0/0

Cali>show ip route static
192.168.1.0/24 is variably subnetted, 7 subnets, 2 masks
S 192.168.1.0/27 [1/0] vía 192.168.1.130
S 192.168.1.32/27 [1/0] via 192.168.1.130
S 192.168.1.96/27 [1/0] via 192.168.1.130

Cali>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
S 192.168.1.0/27 [1/0] via 192.168.1.130
S 192.168.1.32/27 [1/0] via 192.168.1.130
C 192.168.1.64/27 is directly connected, GigabitEthernet0/0
L 192.168.1.65/32 is directly connected, GigabitEthernet0/0
S 192.168.1.96/27 [1/0] via 192.168.1.130
C 192.168.1.128/27 is directly connected, Serial0/0/0
L 192.168.1.131/32 is directly connected, Serial0/0/0

Parte 3: Configuración de Enrutamiento.

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

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

Bogota#config t

Enter configuration commands, one per line. End with CNTL/Z.
Bogota(config)#router eigrp ?
<1-65535> Autonomous system number
Bogotá(config)#router eigrp 50
Bogotá(config-router)#network 192.168.1.32 0.0.0.31
Bogotá(config-router)#network 192.168.1.96 0.0.0.31
Bogotá(config-router)#network 192.168.1.128 0.0.0.31
Bogotá(config-router)#network 192.168.1.0 0.0.0.31
Bogotá(config-router)#no auto-summary
Bogotá(config-router)#end
Bogotá#
%SYS-5-CONFIG_I: Configured from console by console

Bogotá#
%DUAL-5-NBRCHANGE: IP-EIGRP 50: Neighbor 192.168.1.99 (Serial0/0/0) is up: new adjacency

%DUAL-5-NBRCHANGE: IP-EIGRP 50: Neighbor 192.168.1.131 (Serial0/0/1) is up: new adjacency

Medellin#config t
Enter configuration commands, one per line. End with CNTL/Z.
Medellín(config)#router eigrp 50

```
Medellín(config-router)#network 192.168.1.32 0.0.0.31
Medellín(config-router)#network 192.168.1.96 0.0.0.31
Medellín(config-router)#
%DUAL-5-NBRCHANGE: IP-EIGRP 50: Neighbor 192.168.1.98 (Serial0/0/0) is up:
new adjacency

Medellín(config-router)#no auto-summary
Medellín(config-router)#end
Medellín#
%SYS-5-CONFIG_I: Configured from console by console
```

```
Cali#config t

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

Cali(config)#router eigrp 50

Cali(config-router)#network 192.168.1.64  0.0.0.31

Cali(config-router)#network 192.168.1.128 0.0.0.31

Cali(config-router)#

%DUAL-5-NBRCHANGE: IP-EIGRP 50: Neighbor 192.168.1.130 (Serial0/0/0) is
up: new adjacency

Cali(config-router)#no auto-summary

Cali(config-router)#end

Cali#

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

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.

SERVIDOR
C:\>PING 192.168.1.5

Pinging 192.168.1.5 with 32 bytes of data:

Reply from 192.168.1.5: bytes=32 time=2ms TTL=126
Reply from 192.168.1.5: bytes=32 time=2ms TTL=124
Reply from 192.168.1.5: bytes=32 time=2ms TTL=126
Reply from 192.168.1.5: bytes=32 time=3ms TTL=124

Ping statistics for 192.168.1.5:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 2ms, Maximum = 3ms, Average = 2ms

PC-E Medellin
C:\>ping 192.168.1.38

Pinging 192.168.1.38 with 32 bytes of data:

Request timed out.
Reply from 192.168.1.38: bytes=32 time=2ms TTL=125
Reply from 192.168.1.38: bytes=32 time=2ms TTL=125
Reply from 192.168.1.38: bytes=32 time=3ms TTL=123

Ping statistics for 192.168.1.38:
Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
Minimum = 2ms, Maximum = 3ms, Average = 2ms

PC_38
C:\>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:

Request timed out.
Reply from 192.168.1.2: bytes=32 time=2ms TTL=126
Reply from 192.168.1.2: bytes=32 time=1ms TTL=126
Reply from 192.168.1.2: bytes=32 time=1ms TTL=126

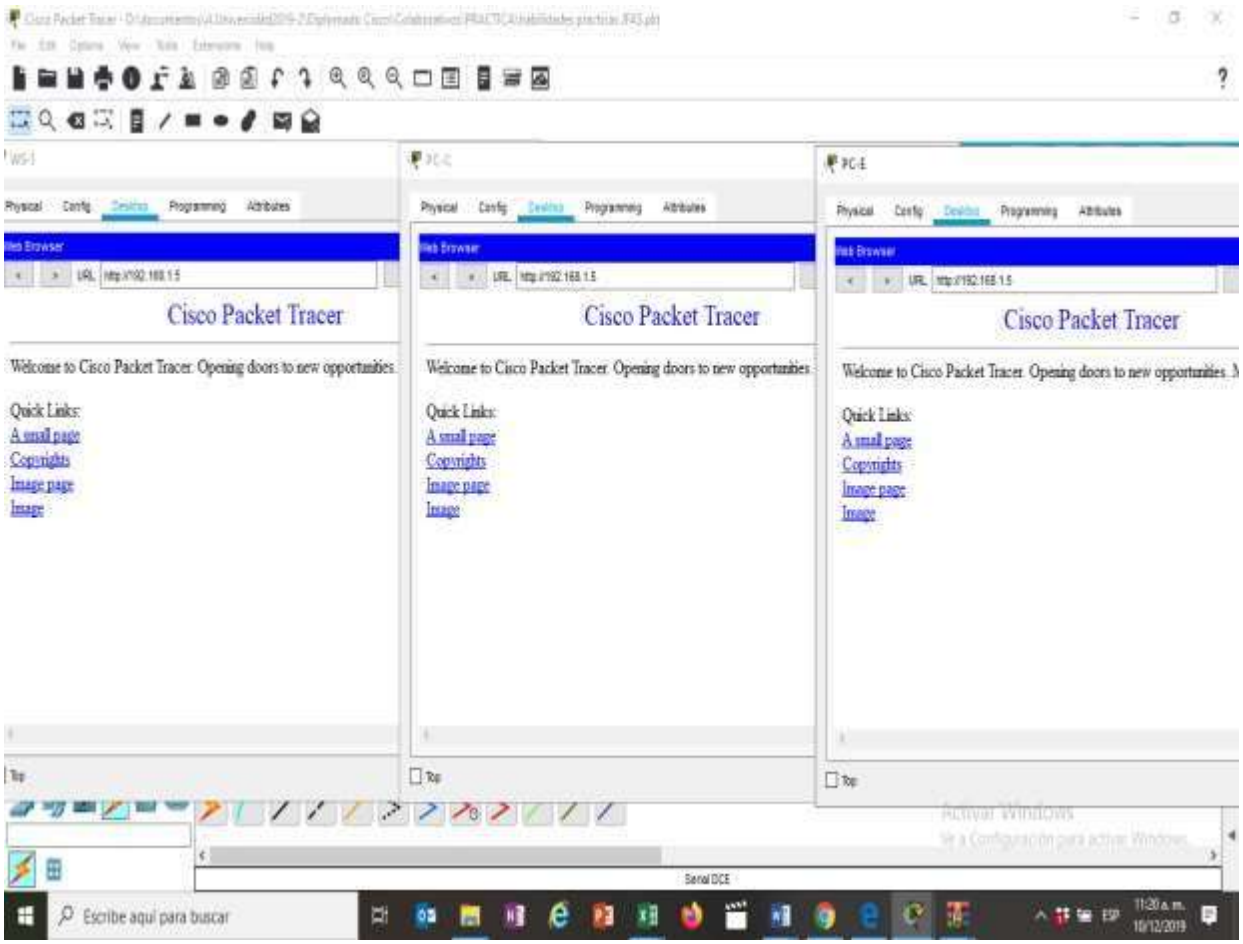
Ping statistics for 192.168.1.2:

Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
Minimum = 1ms, Maximum = 2ms, Average = 1ms

%DUAL-5-NBRCHANGE: IP-EIGRP 50: Neighbor 192.168.1.99 (Serial0/0/0) is up: new adjacency

%DUAL-5-NBRCHANGE: IP-EIGRP 50: Neighbor 192.168.1.131 (Serial0/0/1) is up: new adjacency

Ilustración 5 Comprobaciones

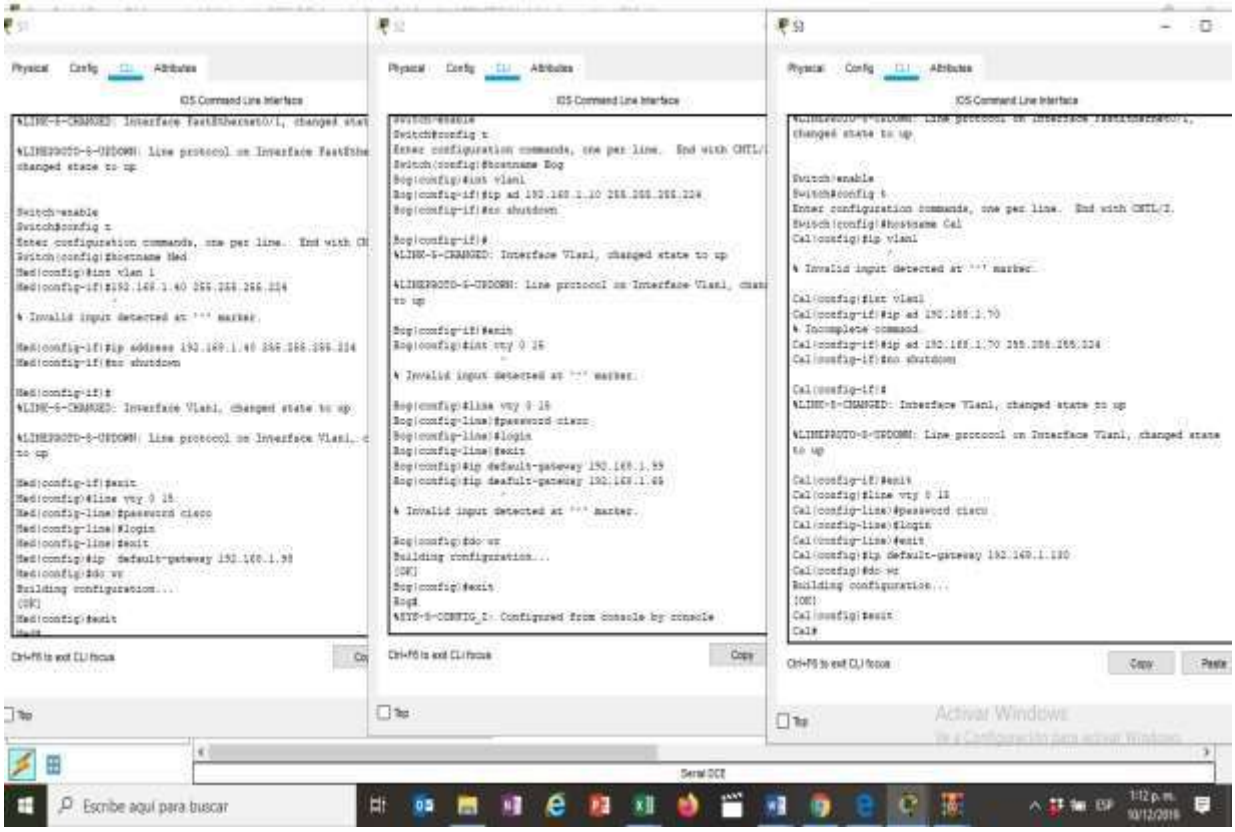


Parte 4: Configuración de las listas de Control de Acceso.

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:

Ilustración 6 Establecer Conexiones



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

TELNET Desde PC-C Entrar a S1

C:\>telnet 192.168.1.40
Trying 192.168.1.40 ...Open
User Access Verification
Password:
Med>

TELNET Desde PC-B Entrar a R1
C:\>telnet 192.168.1.33
Trying 192.168.1.33 ...Open

User Access Verification
Password:
Medellin>

TELNET Desde PC-E entrar a S3

C:\>TELNET 192.168.1.70
Trying 192.168.1.70 ...Open
User Access Verification
Password:
Cal>

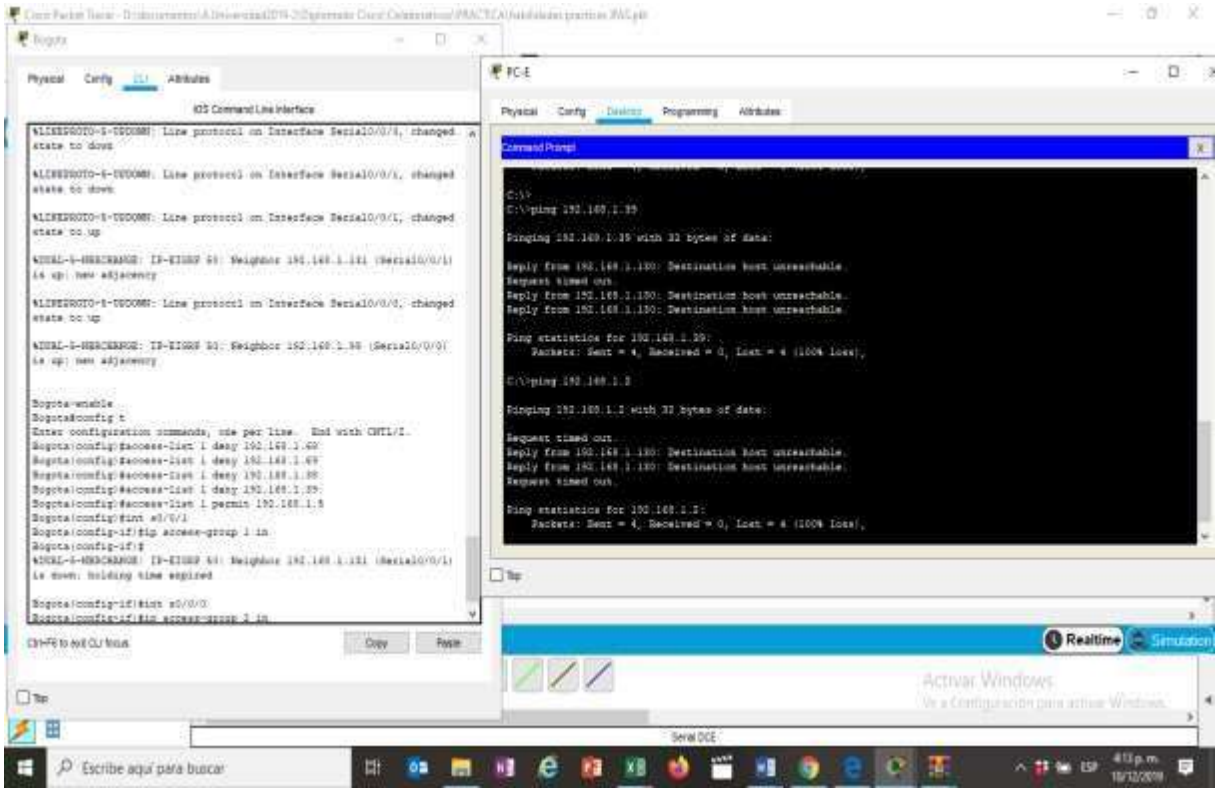
TELNET Desde WS1 entrar a S1

C:\>telnet 192.168.1.10
Trying 192.168.1.10 ...Open
User Access Verification
Password:
Bog>

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

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

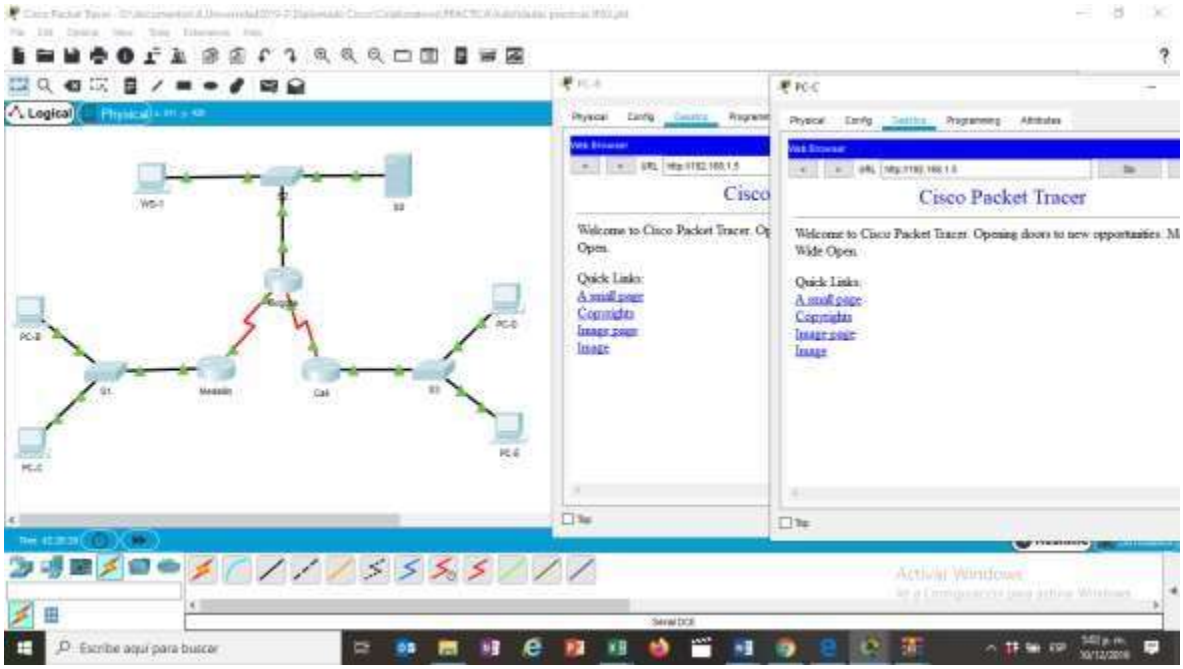
lustración 7 Ping PC-E



Se restringe el acceso fuera de la subred

Bogota#config t
Enter configuration commands, one per line. End with CNTL/Z.
Bogotá(config)#access-list 101 permit ip 192.168.10.0 0.0.0.255
% Incomplete command.
Bogotá(config)#access-list 101 permit ip 192.168.1.68 0.0.0.255 192.168.1.5 0.0.0.255
Bogotá(config)#access-list 101 permit ip 192.168.1.38 0.0.0.255 192.168.1.5 0.0.0.255
Bogotá(config)#access-list 101 permit ip 192.168.1.39 0.0.0.255 192.168.1.5 0.0.0.255
Bogotá(config)#access-list 101 permit ip 192.168.1.69 0.0.0.255 192.168.1.5 0.0.0.255

Ilustración 8 Bogotá Config t



Se habilita para que haya comunicación con el servidor

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.

Tabla 4 Direccionamientos Escenario 2

Dispositivo	Origen	Destino	Resultado
Telnet	Router MEDELLIN	Router CALI	ok
	WS_1	Router BOGOTA	ok
	Servidor	Router CALI	ok
	Servidor	Router MEDELLIN	ok
Telnet	LAN Router MEDELLIN	Router CALI	ok
	LAN Router CALI	Router CALI	ok
	LAN Router MEDELLIN	Router MEDELLIN	
	LAN Router CALI	Router MEDELLIN	ok
Ping	LAN Router CALI	WS1	ok
	LAN Router MEDELLIN	WS1	ok
	LAN Router MEDELLIN	LAN Router CALI	ok
Ping	LAN Router CALI	SERVIDOR	OK
	LAN Router MEDELLIN	SERVIDOR	OK
	Servidor	LAN Router MEDELLIN	OK
	servidor	LAN Router CALI	OK
	Router calí	LAN Router MEDELLIN	OK
	Router Medellín	LAN Router CALI	OK

3.1.3 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.

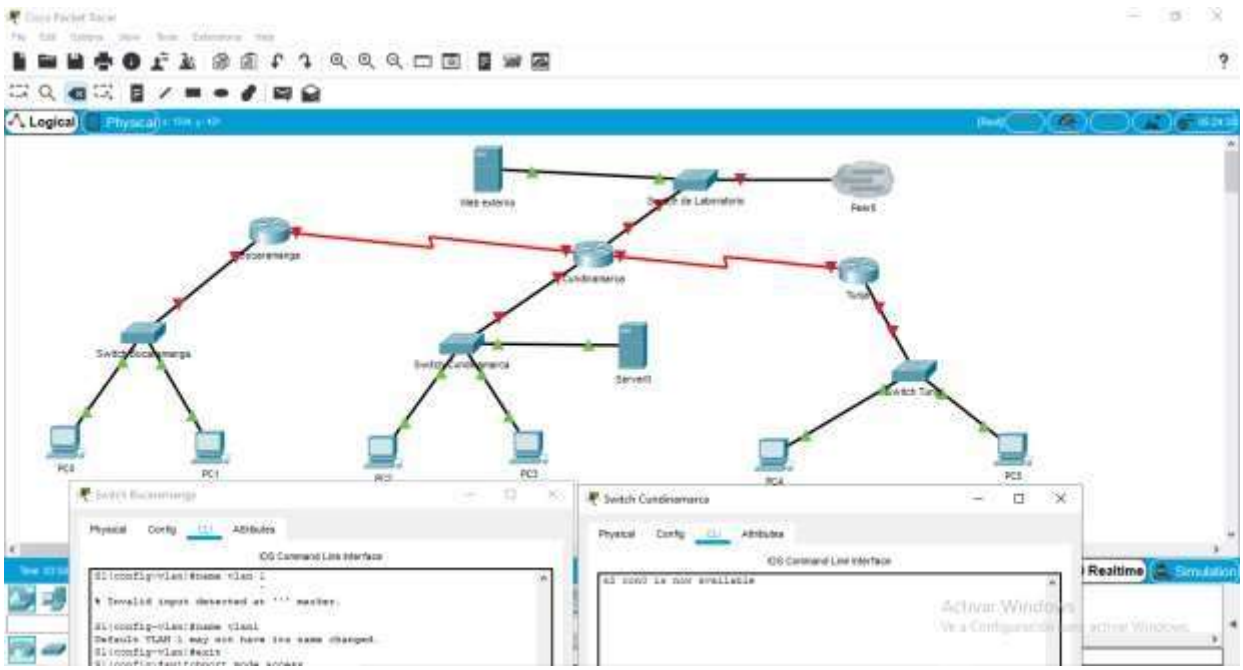
3.1.4 Desarrollo Los siguientes son los requerimientos necesarios:

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.

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

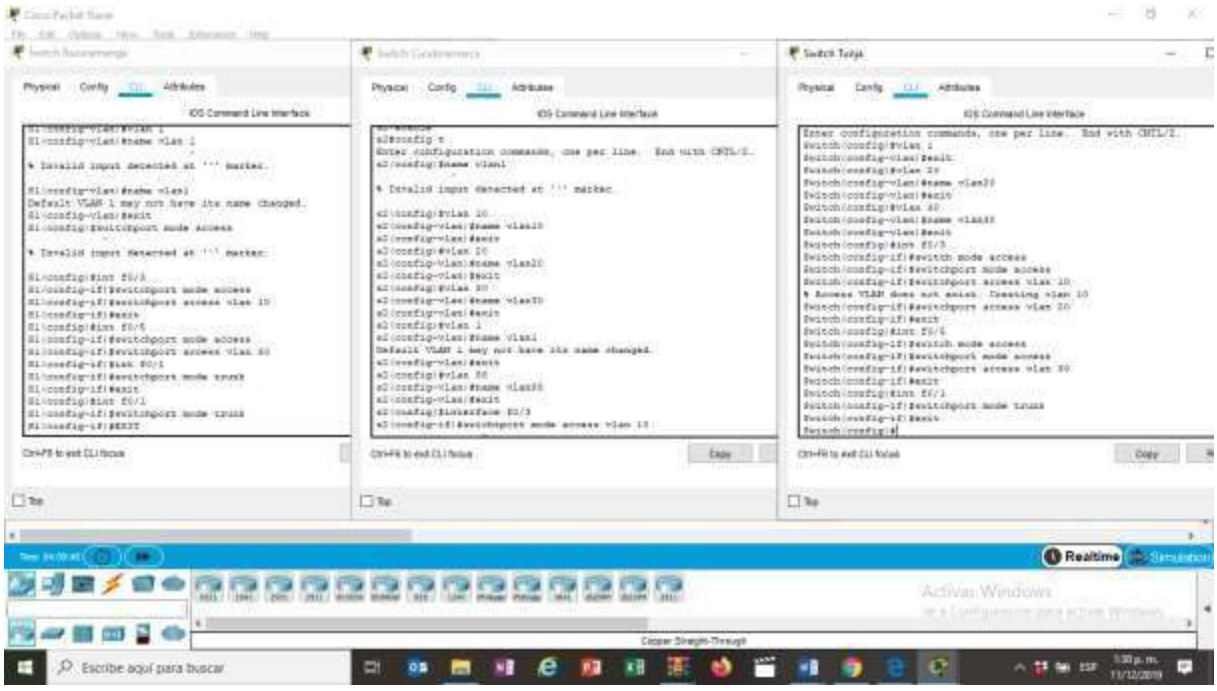
Ilustración 9 DHCP



Switch>enable
Switch#config t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname S1
S1(config)#vlan 10
S1(config-vlan)#name v10
S1(config-vlan)#exit
S1(config)#vlan 30
S1(config-vlan)#name vlan 30
^
% Invalid input detected at '^' marker.
S1(config-vlan)#name vlan30
S1(config-vlan)#vlan 1
S1(config-vlan)#name vlan 1
^
S1(config-vlan)#exit

S1(config)#switchport mode access
^
% Invalid input detected at '^' marker.
S1(config)#int f0/3
S1(config-if)#switchport mode access
S1(config-if)#switchport access vlan 10
S1(config-if)#exit
S1(config)#int f0/5
S1(config-if)#switchport mode access
S1(config-if)#switchport access vlan 30
S1(config-if)#int f0/1
S1(config-if)#switchport mode trunk
S1(config-if)#exit
S1(config)#int f0/1
S1(config-if)#switchport mode trunk
S1(config-if)#EXIT
S1(config)#

Ilustración 10 Switch

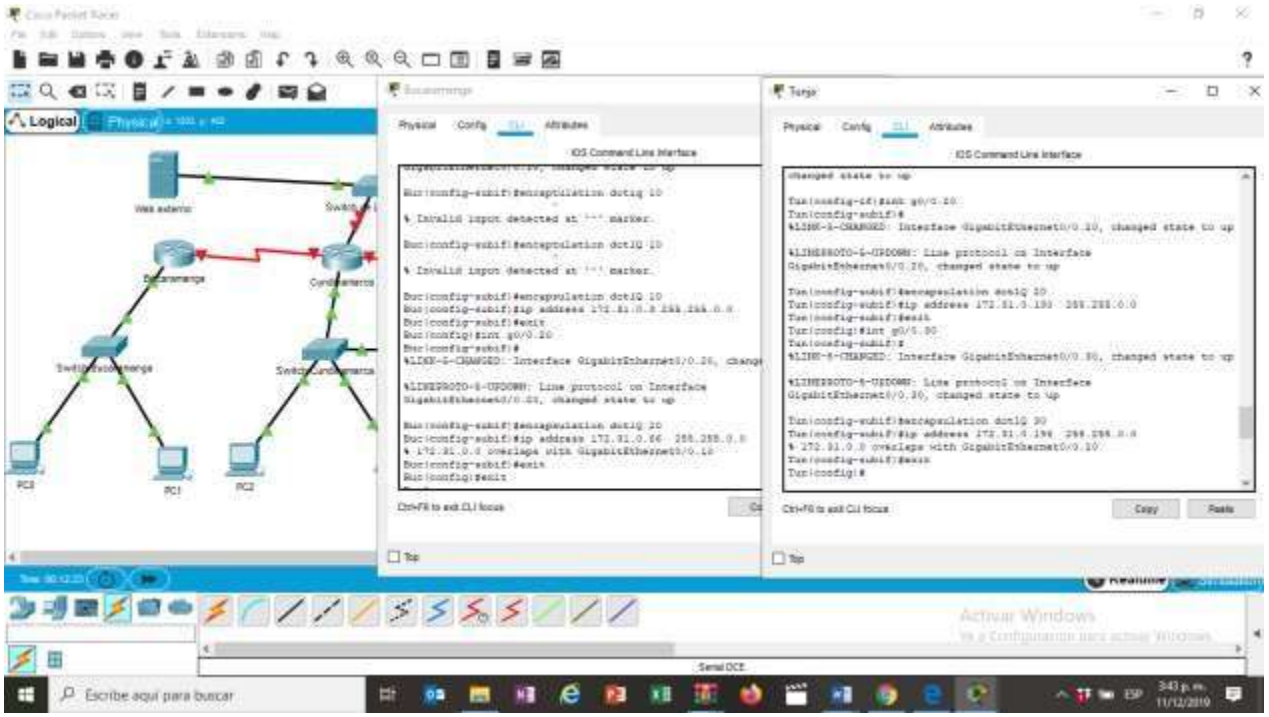


s2(config)#vlan 10
s2(config-vlan)#name vlan10
s2(config-vlan)#exit
s2(config)#vlan 20
s2(config-vlan)#name vlan20

```
s2(config-vlan)#exit
s2(config)#vlan 30
s2(config-vlan)#name vlan30
s2(config-vlan)#exit
s2(config)#vlan 1
s2(config-vlan)#exit
s2(config)#vlan 88
s2(config-vlan)#name vlan88
s2(config-vlan)#exit
s2(config)#interface f0/3
s2(config-if)#switchport mode access
s2(config-if)#switchport access vlan 10
s2(config-if)#exit
s2(config)#interface f0/5
s2(config-if)#switchport mode access
s2(config-if)#switchport access vlan 20
s2(config-if)#exit
s2(config)#int f0/1
s2(config-if)#switchport mode trunk
s2(config-if)#exit
s2(config)#
```

Configuración de los router Bucaramanga, Cundinamarca, Tunja para comunicar las Vlan

Ilustración 11 Interface Línea de comandos



CONCLUSIONES

Mediante el uso de packet tracer se crea la topología física de la red simplemente arrastrando los dispositivos a la pantalla, luego se ingresó a las consolas de configuración, configurando los parámetros que se requerían según el desarrollo de la guía de actividades se realizaron las respectivas simulaciones de conectividad se hacen los pings y traceroutes.

El desarrollo de estos escenarios prácticos es muy importante ya que se fortalecen los conocimientos teóricos que se han adquirido en estas últimas semanas aparte de adquirir una fortaleza en la parte laboral ya que el desarrollo practico hace que se puedan adquirir competencias realmente significativas para un nuevo enfoque o aplicabilidad en las labores o en el campo de desarrollo profesional.

La aplicación de cada uno de los conceptos que Se logran aprender tales como permitir el direccionamiento mediante interfaces específicas en el router que estemos trabajando, la aplicación de comandos para configurar listas de control de acceso (ACL) a los routers y Las condiciones para crear las ACL son como se evidencia en la práctica muy importantes para el desarrollo de redes de acuerdo a requerimientos.

BIBLIOGRAFIA

CISCO. ENRUTAMIENTO DINÁMICO. PRINCIPIOS DE ENRUTAMIENTO Y CONMUTACIÓN. 2014 {en línea} Recuperado de https://sites.google.com/site/comdatosgrupo4/contenidos/cap4_conmutacion-enrutamiento#toc-principios-de-conmutacion-y-enrutamiento

CISCO. INTRODUCCIÓN A REDES CONMUTADAS. PRINCIPIOS DE ENRUTAMIENTO Y CONMUTACIÓN. 2014 {en línea}. Recuperado de: http://www.ie.tec.ac.cr/einteriano/cisco/ccna2/Presentaciones/RS_Chapter1.pdf

CISCO. LISTAS DE CONTROL DE ACCESO. PRINCIPIOS DE ENRUTAMIENTO Y CONMUTACIÓN. 2014 {en línea}. Recuperado de: https://www.cisco.com/c/es_mx/support/docs/security/ios-firewall/23602-confaccesslists.html

WIKIPEDIA. PROTOCOLO DE CONFIGURACION DINAMICA DE HOST. 1997. {en línea}. (s.f.). DHCP. Obtenido de https://es.wikipedia.org/wiki/Protocolo_de_configuraci%C3%B3n_din%C3%A1mica_de_ host