



DIPLOMADO DE PROFUNDIZACION CISCO

PRUEBA DE HABILIDADES PRÁCTICAS

Presentado a:
GIOVANNI ALBERTO BRACHO
Tutor

Entregado por:
Luis Albeiro Bernal Romero

Grupo: 208002_1

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD
PROGRAMA DE INGENIERIA TELECOMUNICACIONES
CEAD FACATATIVÁ
DICIEMBRE DE 2019

Contenido

INTRODUCCION	4
RESUMEN.....	5
ABSTRACT	6
OBJETIVOS.....	7
General.....	7
Específicos.....	7
CAPITULO 1.....	8
Escenario 1.....	8
Topología de red	8
Parte 1: Asignación de direcciones IP:	10
Parte 2: Configuración Básica.	10
Parte 3: Configuración de Enrutamiento.	13
Parte 4: Configuración de las listas de Control de Acceso.	17
Parte 5: Comprobación de la red instalada.	18
CAPITULO 2.....	21
Escenario 2.....	21
Configuración Basica.....	22
Configuración TFTP	22
Configuración DHCP.....	23
Configuración NAT y PAT	25
Configuración Enrutamiento.....	27
Configuración Listas de acceso	27
Configuración VLSM.....	34
Aspectos para tener en cuenta	34
CONCLUSIONES.....	41
REFERENCIAS BIBLIOGRÁFICAS	42

INDICE DE GRAFICAS

Ilustración 1. Diseño de Red.	8
Ilustración 2. Diseñode red PKT	9
Ilustración 3. Prueba de conectividad 1.....	16
Ilustración 4. Prueba conectividad 2.....	16
Ilustración 5. prueba conectividad 3.....	19
Ilustración 6. Prueba conectividad 4.....	19
Ilustración 7. Diseño de red Cap. 2	21
Ilustración 8.Backup TFTP	22
Ilustración 9. Backup TFTP 1	23
Ilustración 10. Asignacion DHCP	24
Ilustración 11. Asignacion DHCP 1	25
Ilustración 12. Funcionamiento NAT.....	26
Ilustración 13. Funcionamiento NAT 2.....	27
Ilustración 14. Configuración OSPF.....	27
Ilustración 15. Prueba ACL 1	28
Ilustración 16. Prueba ACL 2	29
Ilustración 17. Prueba ACL 3	30
Ilustración 18. Prueba ACL 4	31
Ilustración 19. Prueba ACL 5	32
Ilustración 20. Prueba ACL 6	33
Ilustración 21. Prueba conectividad 4.....	36
Ilustración 22. Tabla DHCP router Tunja.....	38
Ilustración 23. Configuración NAT	38
Ilustración 24. Funcionamiento de NAT.....	39
Ilustración 25. Funcionamiento de Nat 1.....	39
Ilustración 26. Configuración Línea VTY Y Consola	40

INTRODUCCION

El diseño y administración de redes es de gran necesidad para poder contar con una red segura, escalable y funcional es por esto por lo que llevar a la práctica diferentes escenarios nos permite desarrollar cualidades y habilidades para la solución y prevención de problemas que se pueden presentar en nuestras redes. Es por este que en el presente documento plasmamos la solución de dos casos de redes de datos que se nos pueden presentar en un entorno real, de tal manera que podamos contar con los conceptos y conocimientos para analizar, configurar y solucionar diferentes ambientes que se nos registran en una red.

Cuando hablamos de redes de datos hablamos de un mundo muy extenso de soluciones, estándares diseños etc., con el desarrollo del curso de redes cisco se nos ha permitido ampliar nuestros conocimientos referentes a estos temas y mediante esta práctica los pondremos aplicar y consolidar.

RESUMEN

El desarrollo, evolución y manejo de las redes en el mundo actual es muy elevado, por lo tanto, se requiere de personal capacitado para configurarlas, administrarlas y sobretodo entenderlas. Es por esto por lo que el desarrollo del curso de redes Cisco es tan importante, ya que la demanda de personal idóneo para administrar redes es alta y contar con personal calificado y certificado permite a las compañías operar con mayor seguridad y elevar la disponibilidad de la prestación de servicios a usuarios finales.

En este documento mostraremos la solución que se realizó para dos escenarios distintos de red de datos que se podrían presentar en una compañía u organización. Se recibió unos escenarios generales con unos requerimientos técnicos puntuales y yo como administrador me encargue de solucionar o responder cada punto.

Teniendo en cuenta lo anterior el documento cuenta con cada una de las configuraciones que se realizan para configurar los diferentes equipos de red y las respectivas evidencias que permiten identificar que las líneas aplicadas son correctas y brindan una solución o respuesta a lo que el cliente demanda para suplir sus necesidades.

ABSTRACT

The development, evolution and management of networks in today's world is very high, therefore it requires trained personnel to configure, manage and above all understand them. This is why the development of the Cisco network course is so important, since the demand for qualified personnel to manage networks is high and having qualified and certified personnel allows companies to operate with greater security and increase the availability of the provision of services to end users.

In this document we will show the solution that was made for two different data network scenarios that could be presented in a company or organization. General scenarios were received with specific technical requirements and I, as administrator, was responsible for solving or answering each point.

Taking into account the above, the document has each of the configurations that are made to configure the different network equipment and the respective evidences that allow to identify that the applied lines are correct and provide a solution or response to what the client demands for meet your needs.

OBJETIVOS

General

Basados en los conocimientos adquiridos durante el desarrollo del curso de redes CISCO, se de aplicar estos conceptos y brindar solución a los dos escenarios de red planteados.

Específicos

- Realizar las configuraciones básicas de los equipos de red como son routers, switch y pcs.
- Aplicar configuraciones de protocolos de enrutamiento y realizar análisis de su funcionamiento y aplicación en la conectividad de las redes.
- Entender el funcionamiento y aplicación de las listas de acceso para la protección y restricción de diferentes dispositivos.
- Ejecutar análisis y comprobación del funcionamiento de una red luego de aplicar diferentes configuraciones sobre los dispositivos que la componen.

CAPITULO 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.

Topología de red

Los requerimientos solicitados son los siguientes:

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

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

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

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

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

Parte 6: Configuración final.

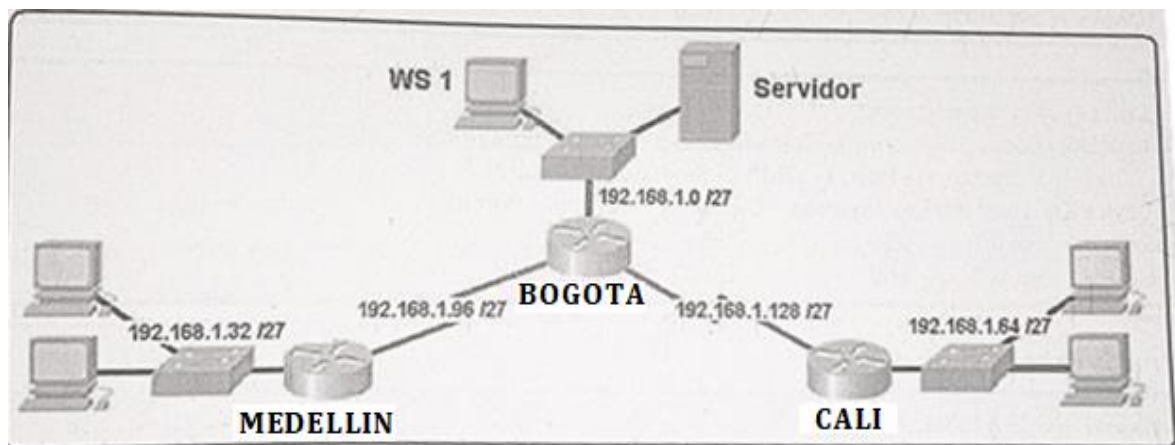


Ilustración 1. Diseño de Red Cap. 1.

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).

En este paso se realizó la configuración básica de los equipos, como credenciales, banner y encriptación de contraseñas.

```
Router(config)#hostname XXXXXXXXX
MEDELLIN(config)#line console 0
MEDELLIN(config-line)#password cisco
MEDELLIN(config-line)#login
MEDELLIN(config-line)#line vty 0 4
MEDELLIN(config-line)#password cisco
MEDELLIN(config-line)#login
MEDELLIN(config-line)#exit
MEDELLIN(config)#banner motd #Acceso restringido solo usuarios UNAD#
MEDELLIN(config)#enable secret class
MEDELLIN(config)#service password-encryption
MEDELLIN(config)# no ip domain-lookup
```

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

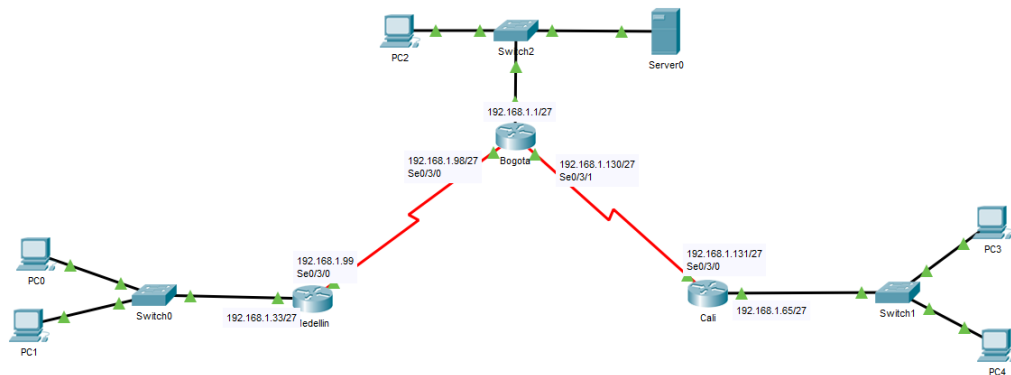


Ilustración 2. Diseño de red PKT

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.
- b. Asignar una dirección IP a la red.

Para Los puntos a y b de acuerdo con el diagrama y la tabla entregada inicialmente el subnetting ya está realizado para la red 192.168.1.0/24 con 8 redes /27, por lo tanto, se mantiene el mismo diseño sin realizar modificaciones ya que cumple con lo requerido en la actividad.

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 Sistema Autónomo	Eigrp 200	Eigrp 200	Eigrp 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.

Se realiza la revision de las rutas mediante el comando show ip route, aun no se tiene protocolo de enrutamiento ni rutas estaticas, por lo tanto conoce las redes configuradas localmente en cada una de la interfaces.

A continuacion las evidencias de las rutas que se aprenden en cada uno de los equipos:

MEDELLIN:

MEDELLIN#show ip route

Gateway of last resort is not set

192.168.1.0/24 is variably subnetted, 4 subnets, 2 masks

C 192.168.1.32/27 is directly connected, GigabitEthernet0/0
L 192.168.1.33/32 is directly connected, GigabitEthernet0/0
C 192.168.1.96/27 is directly connected, Serial0/3/0
L 192.168.1.99/32 is directly connected, Serial0/3/0

BOGOTA:

BOGOTA#show ip route

Gateway of last resort is not set
192.168.1.0/24 is variably subnetted, 6 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
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

CALI

CALI#show ip route

Gateway of last resort is not set
192.168.1.0/24 is variably subnetted, 4 subnets, 2 masks
C 192.168.1.64/27 is directly connected, GigabitEthernet0/0
L 192.168.1.65/32 is directly connected, GigabitEthernet0/0
C 192.168.1.128/27 is directly connected, Serial0/3/0
L 192.168.1.131/32 is directly connected, Serial0/3/0

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

En este caso no se presenta balanceo ya que no esta configurado protocolos de enrutamiento y solamente se evidencian las rutas directamente conectadas.

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

Mediante el comando show cdp neighbors se reconocen los vecinos que estan conectados directamente a cada dispositivo, a continuación las salidas de los comandos en cada uno de los routers:

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
Switch Gig 0/0 149 S 2960 Fas 0/1

MEDELLIN Ser 0/3/0 149 R C2900 Ser 0/3/0
CALI Ser 0/3/1 149 R C2900 Ser 0/3/0

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 Infrfce Holdtme Capability Platform Port ID
Switch Gig 0/0 137 S 2960 Fas 0/1
BOGOTA Ser 0/3/0 137 R C2900 Ser 0/3/1

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 Infrfce Holdtme Capability Platform Port ID
Switch Gig 0/0 120 S 2960 Fas 0/1
BOGOTA Ser 0/3/0 179 R C2900 Ser 0/3/0

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

Se ejecuta el comando requerido en los tres routers identificando que se tienen conectividad desde Bogotá hacia Cali y Medellín, pero desde Cali solo se alcanza Bogotá y no Medellín y desde Medellín se alcanza Bogotá, pero no Cali, a continuación, la evidencia de la salida:

Prueba desde Bogotá hacia Medellín y Cali

BOGOTA#ping 192.168.1.99
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.99, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/4/12 ms

BOGOTA#ping 192.168.1.131
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.131, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/8 ms

Prueba desde Cali hacia Bogotá y Medellín, este último aún no se alcanza porque no cuenta con enrutamiento.

CALI#ping 192.168.1.130

```
Type escape sequence to abort.  
Sending 5, 100-byte ICMP Echos to 192.168.1.130, timeout is 2 seconds:  
!!!!  
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/3/9 ms
```

```
CALI#ping 192.168.1.98  
Type escape sequence to abort.  
Sending 5, 100-byte ICMP Echos to 192.168.1.98, timeout is 2 seconds:  
.....  
Success rate is 0 percent (0/5)
```

Prueba desde Medellín hacia Bogotá y Cali, este último aun no se alcanza porque no cuenta con enrutamiento.

```
MEDELLIN#ping 192.168.1.98  
Type escape sequence to abort.  
Sending 5, 100-byte ICMP Echos to 192.168.1.98, timeout is 2 seconds:  
!!!!  
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10 ms
```

```
MEDELLIN#ping 192.168.1.131  
Type escape sequence to abort.  
Sending 5, 100-byte ICMP Echos to 192.168.1.131, timeout is 2 seconds:  
.....  
Success rate is 0 percent (0/5)
```

Parte 3: Configuración de Enrutamiento.

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

Se configura el protocolo de enrutamiento dinámico EIGRP con las redes que están directamente conectadas a las interfaces de cada router para su respectiva propagación en la red, en las siguientes líneas se observa como se aplicaron en cada dispositivo:

```
BOGOTA(config)#router eigrp 200  
BOGOTA(config-router)#network 192.168.1.96 0.0.0.31  
BOGOTA(config-router)#network 192.168.1.128 0.0.0.31  
BOGOTA(config-router)#network 192.168.1.1 0.0.0.31
```

```
CALI(config)#router eigrp 200  
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)#end
```

```
MEDELLIN(config)#router eigrp 200
MEDELLIN(config-router)#network 192.168.1.98 0.0.0.31
MEDELLIN(config-router)#network 192.168.1.32 0.0.0.31
MEDELLIN(config-router)#end
```

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

Mediante el comando **show ip eigrp neighbors** se identifica los vecinos que se están conociendo mediante el protocolo EIGRP en cada router, en las siguientes líneas se evidencian cada una de las salidas de los routers:

```
BOGOTA#show ip eigrp neighbors
IP-EIGRP neighbors for process 200
H Address Interface Hold Uptime SRTT RTO Q Seq
(sec) (ms) Cnt Num
0 192.168.1.99 Se0/3/0 13 00:06:24 40 1000 0 9
1 192.168.1.131 Se0/3/1 14 00:04:28 40 1000 0 7
```

```
CALI#show ip eigrp neighbors
IP-EIGRP neighbors for process 200
H Address Interface Hold Uptime SRTT RTO Q Seq
(sec) (ms) Cnt Num
0 192.168.1.130 Se0/3/0 11 00:05:03 40 1000 0 6
```

```
MEDELLIN#show ip eigrp neighbors
IP-EIGRP neighbors for process 200
H Address Interface Hold Uptime SRTT RTO Q Seq
(sec) (ms) Cnt Num
0 192.168.1.98 Se0/3/0 13 00:07:28 40 1000 0 5
```

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

Se lanza de nuevo en todos los routers el comando show ip route con el cual ya se observan todas las redes que se configuraron y que se están recibiendo mediante el protocolo EIGRP.

BOGOTA#show ip 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, 00:09:00, Serial0/3/0
```

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

CALI#sh 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, 00:08:22, Serial0/3/0
D 192.168.1.32/27 [90/2684416] via 192.168.1.130, 00:08:22, Serial0/3/0
C 192.168.1.64/27 is directly connected, GigabitEthernet0/0
L 192.168.1.65/32 is directly connected, GigabitEthernet0/0
D 192.168.1.96/27 [90/2681856] via 192.168.1.130, 00:08:22, Serial0/3/0
C 192.168.1.128/27 is directly connected, Serial0/3/0
L 192.168.1.131/32 is directly connected, Serial0/3/0
```

MEDELLIN#sh 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, 00:11:01, 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 [90/2684416] via 192.168.1.98, 00:09:06, 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 192.168.1.128/27 [90/2681856] via 192.168.1.98, 00:11:01, Serial0/3/0
```

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.

Mediante el comando ping se ejecutan las pruebas de conectividad entre los diferentes dispositivos, confirmando que responden correctamente entre todos, a continuación, las evidencias de las pruebas ejecutadas:

C:\>ping 192.168.1.3

```
Pinging 192.168.1.3 with 32 bytes of data:
Reply from 192.168.1.3: bytes=32 time=1ms TTL=126
Reply from 192.168.1.3: bytes=32 time=1ms TTL=126
Reply from 192.168.1.3: bytes=32 time=4ms TTL=126
Reply from 192.168.1.3: bytes=32 time=13ms TTL=126
```

Ping statistics for 192.168.1.3:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 1ms, Maximum = 13ms, Average = 4ms

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=1ms TTL=128

Reply from 192.168.1.35: bytes=32 time<1ms TTL=128

Reply from 192.168.1.35: bytes=32 time<1ms TTL=128

Reply from 192.168.1.35: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.35:

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

```
C:\>ping 192.168.1.35

Pinging 192.168.1.35 with 32 bytes of data:

Reply from 192.168.1.35: bytes=32 time=1ms TTL=128
Reply from 192.168.1.35: bytes=32 time<1ms TTL=128
Reply from 192.168.1.35: bytes=32 time<1ms TTL=128
Reply from 192.168.1.35: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.35:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>ipconfig

FastEthernet0 Connection: (default port)

Link-local IPv6 Address . . . . . : FE80::2D0:BAFF:FE17:1169
IP Address. . . . . : 192.168.1.34
Subnet Mask . . . . . : 255.255.255.224
Default Gateway . . . . . : 192.168.1.33
```

Ilustración 3. Prueba de conectividad 1

```
Command Prompt

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 13ms, Average = 7ms

C:\>ping 192.168.1.3

Pinging 192.168.1.3 with 32 bytes of data:

Reply from 192.168.1.3: bytes=32 time=1ms TTL=126
Reply from 192.168.1.3: bytes=32 time=1ms TTL=126
Reply from 192.168.1.3: bytes=32 time=4ms TTL=126
Reply from 192.168.1.3: bytes=32 time=13ms TTL=126

Ping statistics for 192.168.1.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 13ms, Average = 4ms
```

Ilustración 4. Prueba conectividad 2

Todas las pruebas son exitosas, se tiene conectividad LAN TO LAN confirmando que la configuración realizada es correcta.

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:

Cada router debe estar habilitado para establecer conexiones Telnet con los demás routers y tener acceso a cualquier dispositivo en la red. El equipo WS1 y el servidor se encuentran en la subred de administración. Solo el servidor de la subred de administración debe tener acceso a cualquier otro dispositivo en cualquier parte de la red.

Se configuran las listas de acceso permitiendo solo la conexión desde redes específicas para cumplir con lo requerido y aumentar la seguridad sobre los dispositivos, las listas fueron llamadas sobre la línea de acceso vty 0 4 que es la que permite la conexión mediante el protocolo telnet.

A continuación, cada una de las líneas de comando aplicada para cada router:

Medellin

```
access-list 110 permit ip 192.168.1.96 0.0.0.31 any
access-list 110 permit ip 192.168.1.130 0.0.0.31 any
access-list 110 permit ip 192.168.1.3 0.0.0.0 any
access-list 110 deny ip any any
```

Bogota

```
access-list 110 permit ip 192.168.1.96 0.0.0.31 any
access-list 110 permit ip 192.168.1.130 0.0.0.31 any
access-list 110 permit ip 192.168.1.3 0.0.0.0 any
access-list 110 deny ip any any
```

Cali

```
access-list 110 permit ip 192.168.1.96 0.0.0.31 any
access-list 110 permit ip 192.168.1.130 0.0.0.31 any
access-list 110 permit ip 192.168.1.3 0.0.0.0 any
access-list 110 deny ip any any
```

```
line vty 0 4
access-class 110 in
```

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

Se configuran las listas de acceso permitiendo solo la conexión a redes específicas para cumplir con lo requerido, las listas fueron llamadas sobre la interfaz gi0/0 que es la que permite la conexión WAN en cada router.

A continuación, cada una de las líneas de comando aplicada para cada router, para cumplir con la necesidad planteada:

Medellin

```
access-list 120 permit ip 192.168.1.3 0.0.0.0 any
access-list 120 deny ip any any
interfasce gi0/0
ip access-group 120 out
```

Cali

```
access-list 120 permit ip 192.168.1.3 0.0.0.0 any
access-list 120 deny ip any any
interface gi0/0
ip access-group 120 out
```

Se configuran las listas de acceso para cumplir con lo requerido y se aplican en las interfaces LAN de cada dispositivo.

Parte 5: Comprobación de la red instalada.

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

Evidencias Prueba de Ping desde WS1 y desde servidor.

En esta imagen se observa que de acuerdo con la lista de acceso aplicada desde la red LAN de Bogotá solo se alcanza los equipos de Medellín desde el servidor y desde el pc WS1 esta denegada:

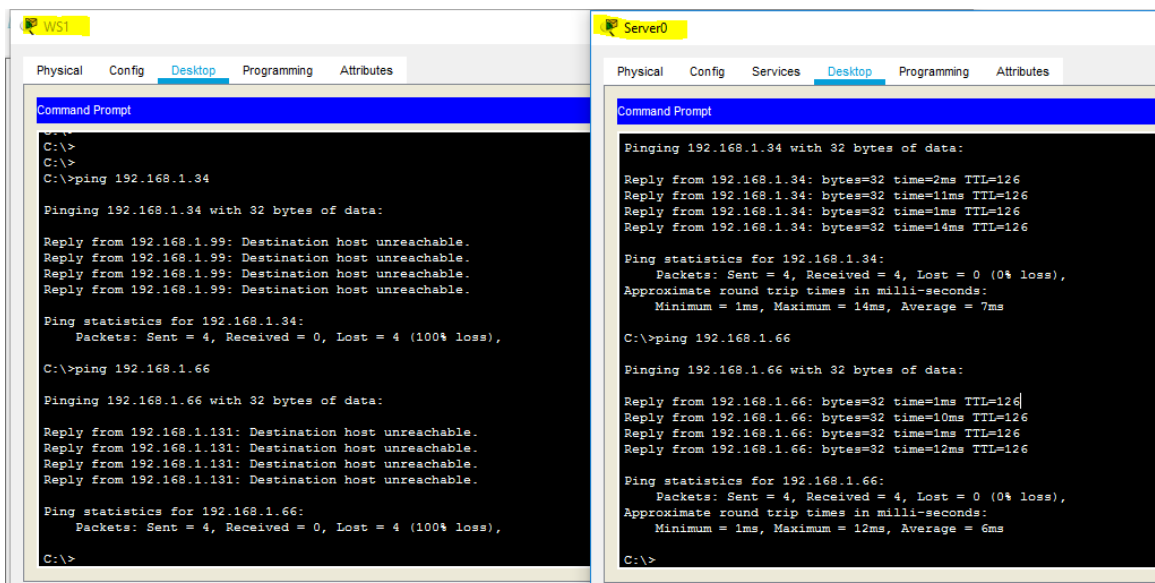


Ilustración 5. prueba conectividad 3

Prueba de telnet desde WS1 y desde servidor.

En esta prueba al igual que la anterior se permitió la conexión al router de Medellín solo desde el servidor y no desde el pc WS1

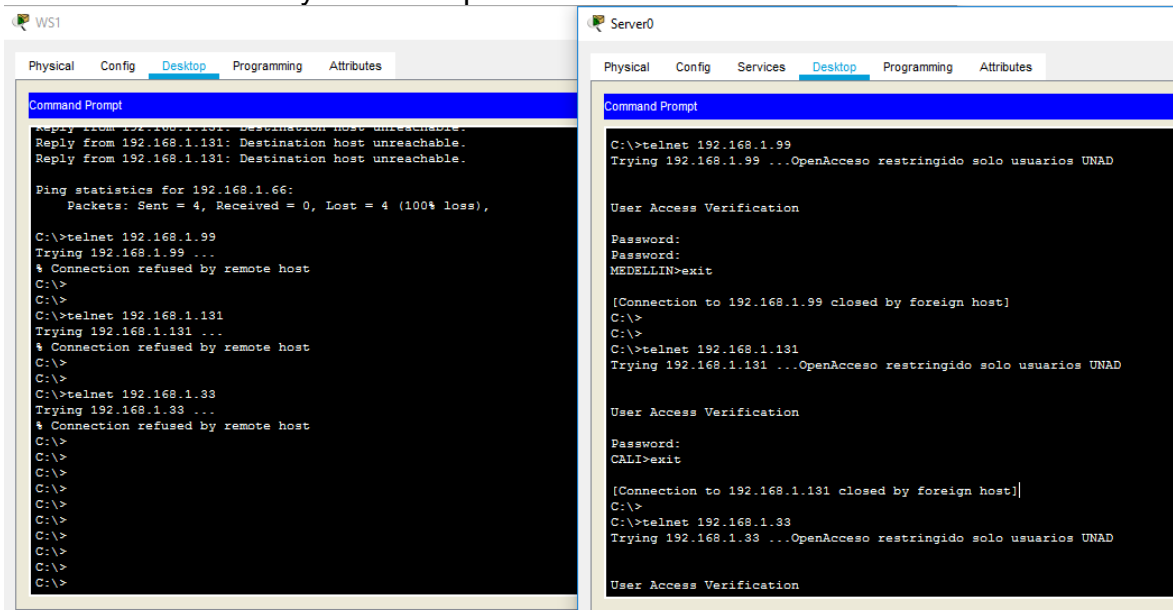


Ilustración 6. Prueba conectividad 4

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	Exitoso
	WS_1	Router BOGOTA	Denegado
	Servidor	Router CALI	Exitoso
	Servidor	Router MEDELLIN	Exitoso
TELNET	LAN del Router MEDELLIN	Router CALI	Denegado
	LAN del Router CALI	Router CALI	Denegado
	LAN del Router MEDELLIN	Router MEDELLIN	Denegado
	LAN del Router CALI	Router MEDELLIN	Denegado
PING	LAN del Router CALI	WS_1	Denegado
	LAN del Router MEDELLIN	WS_1	Denegado
	LAN del Router MEDELLIN	LAN del Router CALI	Denegado
PING	LAN del Router CALI	Servidor	Exitoso
	LAN del Router MEDELLIN	Servidor	Exitoso
	Servidor	LAN del Router MEDELLIN	Exitoso
	Servidor	LAN del Router CALI	Exitoso
	Router CALI	LAN del Router MEDELLIN	Exitoso
	Router MEDELLIN	LAN del Router CALI	Denegado

CAPITULO 2

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.

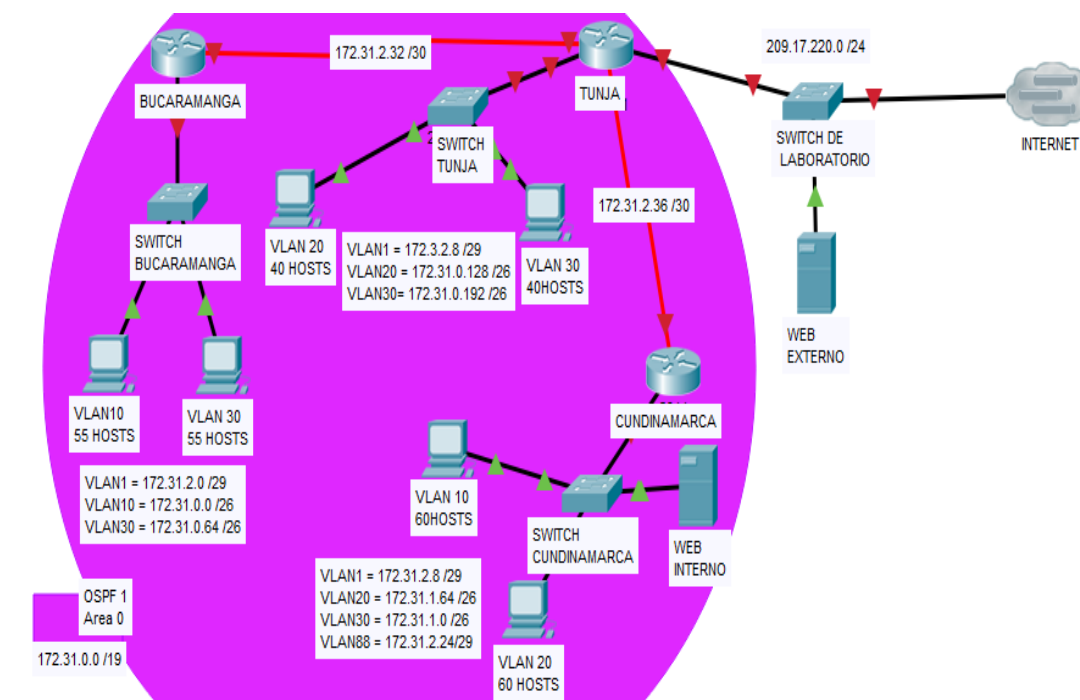


Ilustración 7. Diseño de red Cap. 2

Desarrollo

Los siguientes son los requerimientos necesarios:

Todos los routers deberán tener lo 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.

Configuración Basica

En este paso se realizo al configuración basica de los equipos, como credenciales, banner y encriptacion de contraseñas

```

aaa new-model
no ip domain-lookup
line console 0
password cisco
exec-timeout 5
login
line vty 0 4
password cisco
exec-timeout 5
login
exit
enable password class
service password-encryption
banner motd # Acceso Autorizado Solo Usuarios UNAD#
    
```

Configuración TFTP

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

Se habilito el servicio tftp en el servidor y se envió la copia de seguridad de la configuración de cada uno de los equipos al servidor con nombre WEB INTERNO, en la siguiente imagen se evidencia el procedimiento realizado en cada uno de los routers para enviar la copia de su configuración hacia el servidor denominado como WEB INTERNO y sobre el servidor se observa que quedaron almacenados los 3 Backus.

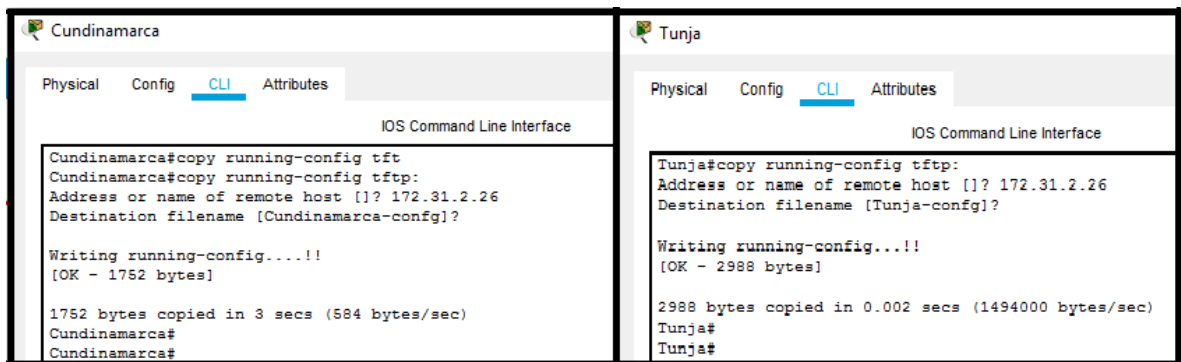


Ilustración 8.Backup TFTP

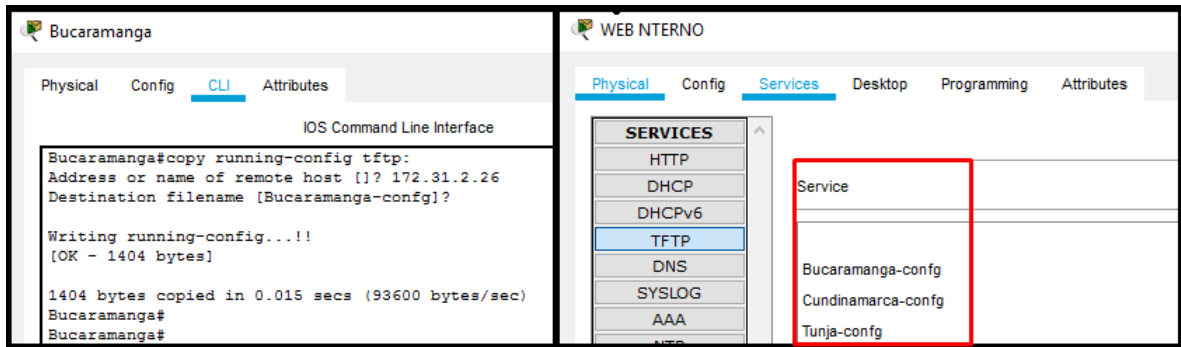


Ilustración 9. Backup TFTP 1

Configuración DHCP

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

Se habilita el DHCP en el router de Bucaramanga y de Cundinamarca, se excluyen las ips de las interfaces del router. En las siguientes líneas se muestra como se configuro el pool DHCP y las exclusiones en cada dispositivo.

Bucaramanga

```
ip dhcp pool vlan10
network 172.31.0.0 255.255.255.192
default-router 172.31.0.1
dns-server 8.8.8.8
ip dhcp pool vlan30
network 172.31.0.64 255.255.255.192
default-router 172.31.0.65
dns-server 8.8.8.8
Bucaramanga(config)#ip dhcp excluded-address 172.31.0.65
Bucaramanga(config)#ip dhcp excluded-address 172.31.0.1
```

En la siguiente imagen se evidencia funcionamiento DHCP en los dispositivos que hacen parte de la red LAN configurada, se les habilita la opción de configuración de IP mediante DHCP y estos la toman automáticamente:

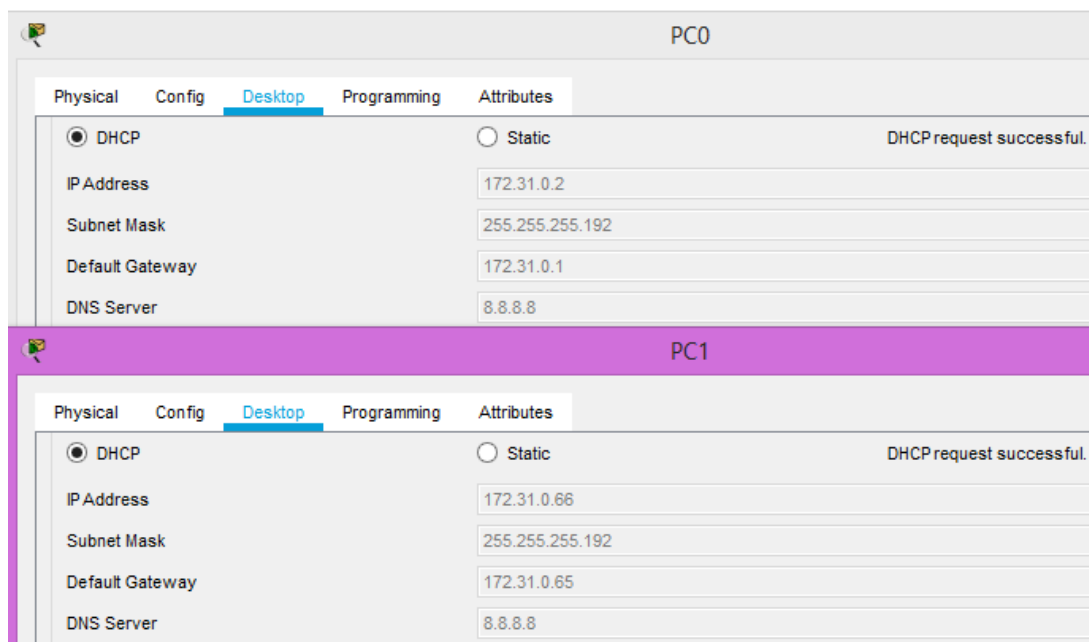


Ilustración 10. Asignacion DHCP

Cundinamarca

```

ip dhcp pool vlan20
network 172.31.1.64 255.255.255.192
default-router 172.31.1.65
dns-server 8.8.8.8
ip dhcp pool vlan30
network 172.31.1.0 255.255.255.192
default-router 172.31.1.1
dns-server 8.8.8.8
ip dhcp pool vlan88
network 172.31.2.24 255.255.255.248
default-router 172.31.2.25
dns-server 8.8.8.8
ip dhcp excluded-address 172.31.1.65
ip dhcp excluded-address 172.31.1.1
ip dhcp excluded-address 172.31.2.25
    
```

Se realizan pruebas de funcionamiento para la red LAN de Bucaramanga, los computadores toman direccionamiento por DHCP de acuerdo con lo configurado, la siguiente imagen muestra el respectivo funcionamiento:

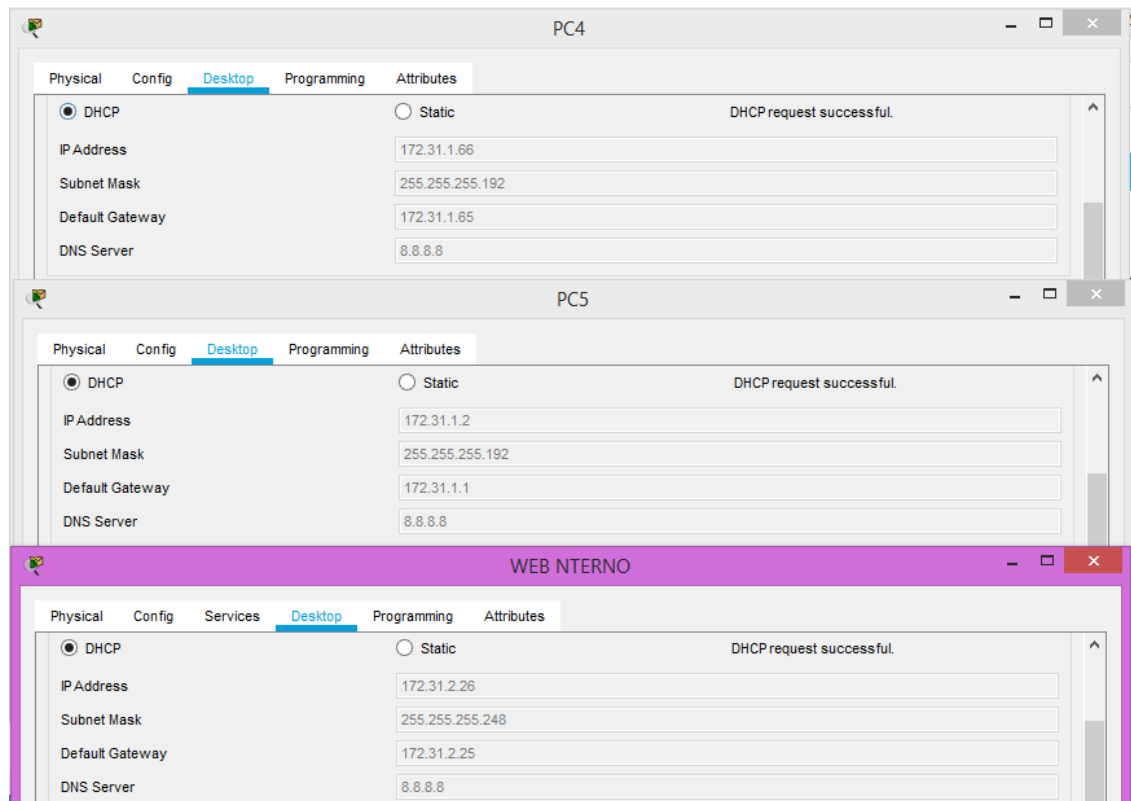


Ilustración 11. Asignacion DHCP 1

Configuración NAT y PAT

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

Se define el NAT con el cual se va a realizar la translación de privadas a publicas y se configura sobre la interface de entrada la opción ip nat inside y sobre la interfaz de salida el ip nat outside para que realice la traslación correspondiente.

Las siguientes líneas muestran la configuración realizada para habilitar el NAT:

NAT ESTATICO Servidor :

```
Tunja#config t
Tunja(config)#ip nat inside source static 172.31.2.25 209.17.220.1
Tunja(config)#end
Tunja(config)#inter se0/0/0
Tunja(config-if)#ip nat outside
Tunja(config-if)#inter se0/1/0
Tunja(config-if)#ip nat inside
Tunja(config-if)#inter fa0/1
```

```
Tunja(config-if)#ip nat inside
Tunja(config-if)#end
```

En esta imagen se evidencia el funcionamiento del NAT, al costado izquierdo la imagen del router haciendo las traslaciones y al costado derecho la prueba de conectividad que indica que se alcanza el equipo indicado:

```
Tunja(config)#ip nat inside source static 172.31.2.25 209.17.220.1
Tunja(config)#end
Tunja#
%SYS-5-CONFIG_I: Configured from console by console

Tunja#
Tunja#
Tunja#
Tunja#sh ip nat trans
Tunja#sh ip nat translations
Pro  Inside global      Inside local      Outside local     Outside global
icmp 209.17.220.1:1     172.31.2.25:1    172.31.2.26:1    172.31.2.26:1
icmp 209.17.220.1:2     172.31.2.25:2    172.31.2.26:2    172.31.2.26:2
icmp 209.17.220.1:3     172.31.2.25:3    172.31.2.26:3    172.31.2.26:3
icmp 209.17.220.1:4     172.31.2.25:4    172.31.2.26:4    172.31.2.26:4
--- 209.17.220.1      172.31.2.25      ---              ---

Tunja#
```

```
C:\>ping 209.17.220.2

Pinging 209.17.220.2 with 32 bytes of data:

Reply from 209.17.220.2: bytes=32 time=2ms TTL=126
Reply from 209.17.220.2: bytes=32 time=1ms TTL=126
Reply from 209.17.220.2: bytes=32 time=2ms TTL=126
Reply from 209.17.220.2: bytes=32 time=2ms TTL=126

Ping statistics for 209.17.220.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 2ms, Average = 1ms
```

Ilustración 12. Funcionamiento NAT

NAT de sobrecarga (PAT). RESTO DE RED

Se configura las listas de accesos con las redes sumarizadas y se configura el ip NAT, se confirma que estan realizando el proceso de translacion por puerto. A continuacion la configuraci3n aplicada sobre el router:

```
Tunja#config t
Enter configuration commands, one per line. End with CNTL/Z.
Tunja(config)#access-list 10 permit 172.31.2.0 0.0.0.15
Tunja(config)#access-list 10 permit 172.31.0.0 0.0.0.255
Tunja(config)#access-list 10 permit 172.31.1.0 0.0.0.127
Tunja(config)#ip nat inside source list 10 interface FastEthernet0/0 overload
Tunja(config)#end
```

Imagen con la evidencia de las translaciones realizadas por el router al momento de lanzar la prueba de conectividad:

```
Tunja#show ip nat translations
Pro  Inside global      Inside local          Outside local         Outside global
icmp 209.17.220.1:18    172.31.0.2:18        209.17.220.2:18     209.17.220.2:18
icmp 209.17.220.1:19    172.31.0.2:19        209.17.220.2:19     209.17.220.2:19
icmp 209.17.220.1:20    172.31.0.2:20        209.17.220.2:20     209.17.220.2:20
icmp 209.17.220.1:21    172.31.0.2:21        209.17.220.2:21     209.17.220.2:21
icmp 209.17.220.1:5     172.31.0.130:5       209.17.220.2:5      209.17.220.2:5
icmp 209.17.220.1:6     172.31.0.130:6       209.17.220.2:6      209.17.220.2:6
icmp 209.17.220.1:7     172.31.0.130:7       209.17.220.2:7      209.17.220.2:7
icmp 209.17.220.1:8     172.31.0.130:8       209.17.220.2:8      209.17.220.2:8
--- 209.17.220.1       172.31.2.25          ---                  ---
Tunja#
```

Ilustración 13. Funcionamiento NAT 2

Configuración Enrutamiento

3. El enrutamiento deberá tener autenticación.

Se configuro protocolo OSPF con autenticación. En la siguiente imagen se muestra las configuraciones aplicadas sobre el router de Tunja, en el cual se declaran mediante la línea network las redes que están directamente conectadas al mismo.

```
router ospf 1
log-adjacency-changes
area 0 authentication
network 172.31.2.36 0.0.0.3 area 0
network 172.3.2.8 0.0.0.7 area 0
network 172.31.0.128 0.0.0.31 area 0
network 172.31.0.192 0.0.0.31 area 0
network 172.31.2.32 0.0.0.3 area 0
```

Ilustración 14. Configuración OSPF

Configuración Listas de acceso

4. Listas de control de acceso:

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

Se crea una lista en la cual se agregan las redes permitidas y el resto de tráfico se deniega, a continuación, la lista aplicada:

CUNDINAMARCA#

```
access-list 120 permit ip 172.31.1.64 0.0.0.31 172.31.0.128 0.0.0.31
access-list 120 permit ip 172.31.1.64 0.0.0.31 172.31.0.192 0.0.0.31
access-list 120 deny ip any any
interface FastEthernet0/0.20
ip access-group 120 in
```

De acuerdo con la lista aplicada en la siguiente imagen se muestra la prueba de conectividad donde se observa que solo se alcanza la red de Tunja y no se tienen salida a internet desde Cundinamarca:

```
PC4
Physical Config Desktop Programming Attributes
Command Prompt
C:\>ping 172.31.0.130

Pinging 172.31.0.130 with 32 bytes of data:

Reply from 172.31.0.130: bytes=32 time=1ms TTL=126
Reply from 172.31.0.130: bytes=32 time=1ms TTL=126
Reply from 172.31.0.130: bytes=32 time=1ms TTL=126
Reply from 172.31.0.130: bytes=32 time=16ms TTL=126

Ping statistics for 172.31.0.130:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 16ms, Average = 4ms

C:\>ping 209.17.220.2

Pinging 209.17.220.2 with 32 bytes of data:

Reply from 172.31.1.65: Destination host unreachable.
Reply from 172.31.1.65: Destination host unreachable.
Reply from 172.31.1.65: Destination host unreachable.
Reply from 172.31.1.65: Destination host unreachable.

Ping statistics for 209.17.220.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Ilustración 15. Prueba ACL 1

- **Los hosts de VLAN 30 en Cundinamarca si acceden a internet y no a la red interna de Tunja.**

Se crea una lista en la cual se agregan las redes que se deben denegar y el resto de tráfico se permite, a continuación, la lista aplicada:

```
access-list 130 deny ip 172.31.1.0 0.0.0.31 172.31.0.128 0.0.0.31
access-list 130 deny ip 172.31.1.0 0.0.0.31 172.31.0.192 0.0.0.31
```

```
access-list 130 permit ip any any
Tunja(config-if)#inter se0/0/0
Tunja(config-if)#ip access-group 130 in
```

De acuerdo con la lista aplicada en la siguiente imagen se muestra la prueba de conectividad donde se observa que no se alcanza la red de Tunja y se tienen salida a internet desde Cundinamarca desde la vlan 30:

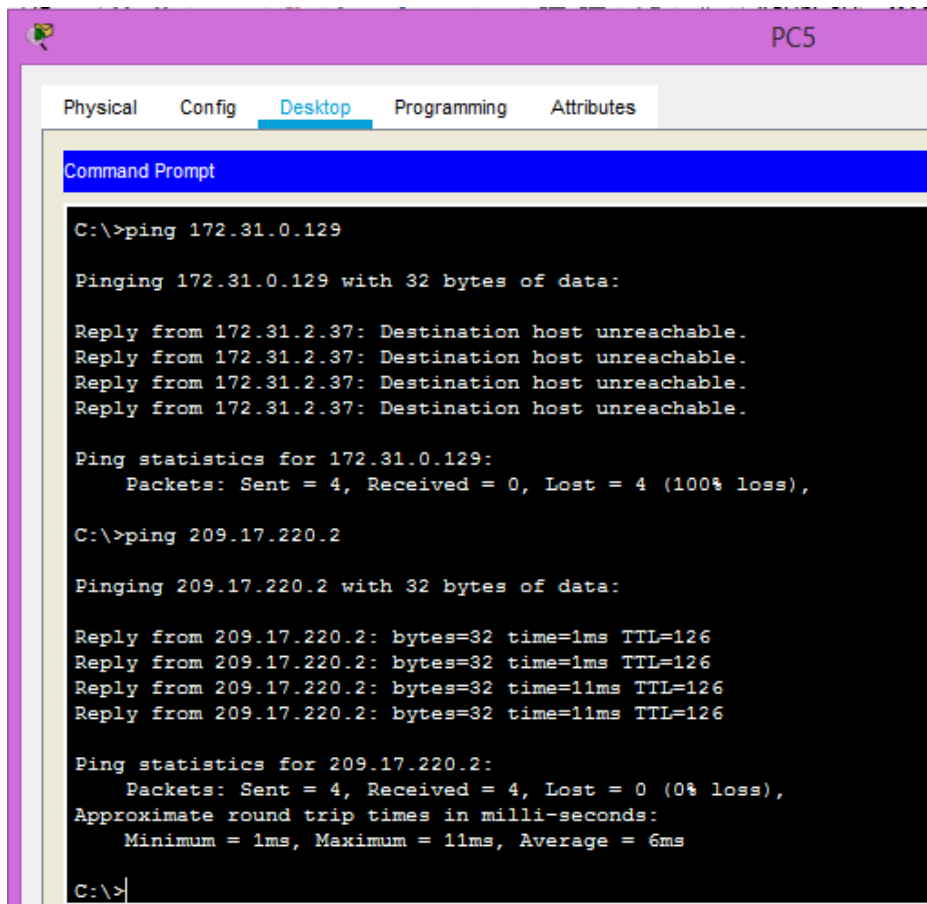


Ilustración 16. Prueba ACL 2

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

Se crea una lista en la cual se agregan las redes que se permiten los protocolos web y ftp, el resto de tráfico se deniega, a continuación, la lista aplicada:

```
access-list 105 permit tcp 172.31.0.192 0.0.0.31 209.17.220.0 0.0.0.255 eq www
access-list 105 permit tcp 172.31.0.192 0.0.0.31 0.0.0.0 0.0.0.0 eq www
```

```
access-list 105 permit tcp 172.31.0.192 0.0.0.31 0.0.0.0 0.0.0.0 eq ftp
access-list 105 deny ip any any
interface FastEthernet0/1.30
description VLAN30
ip access-group 105 in
```

De acuerdo con la lista aplicada en la siguiente imagen se muestra la prueba de conectividad donde se observa que abre sin problemas el sitio web y se alcanza por el protocolo FTP, pruebas como ping son denegadas.

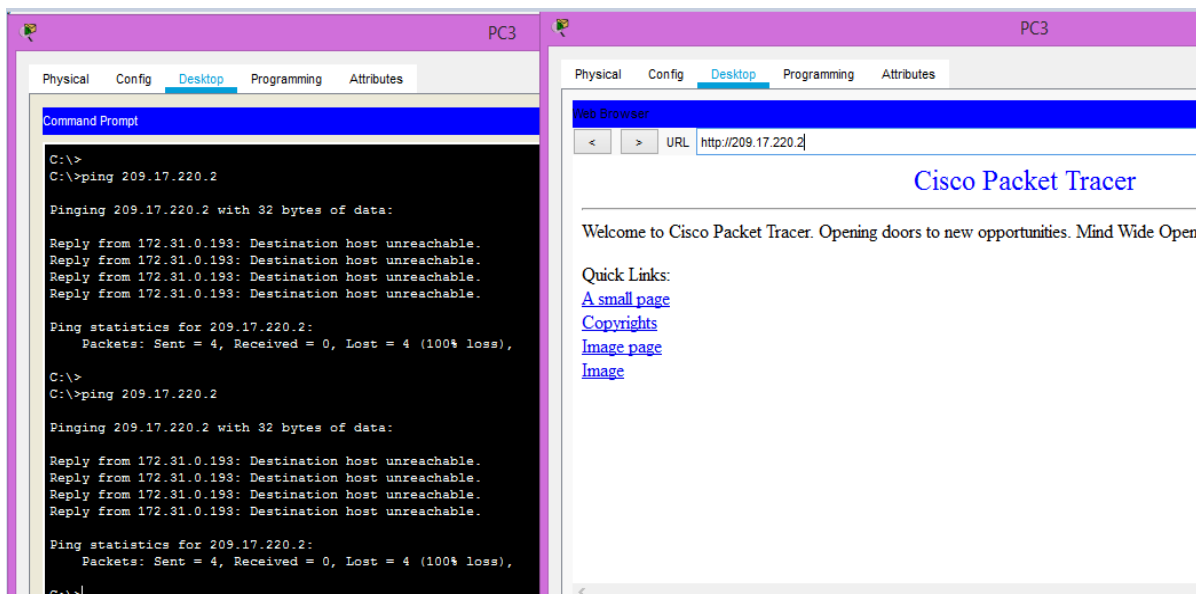


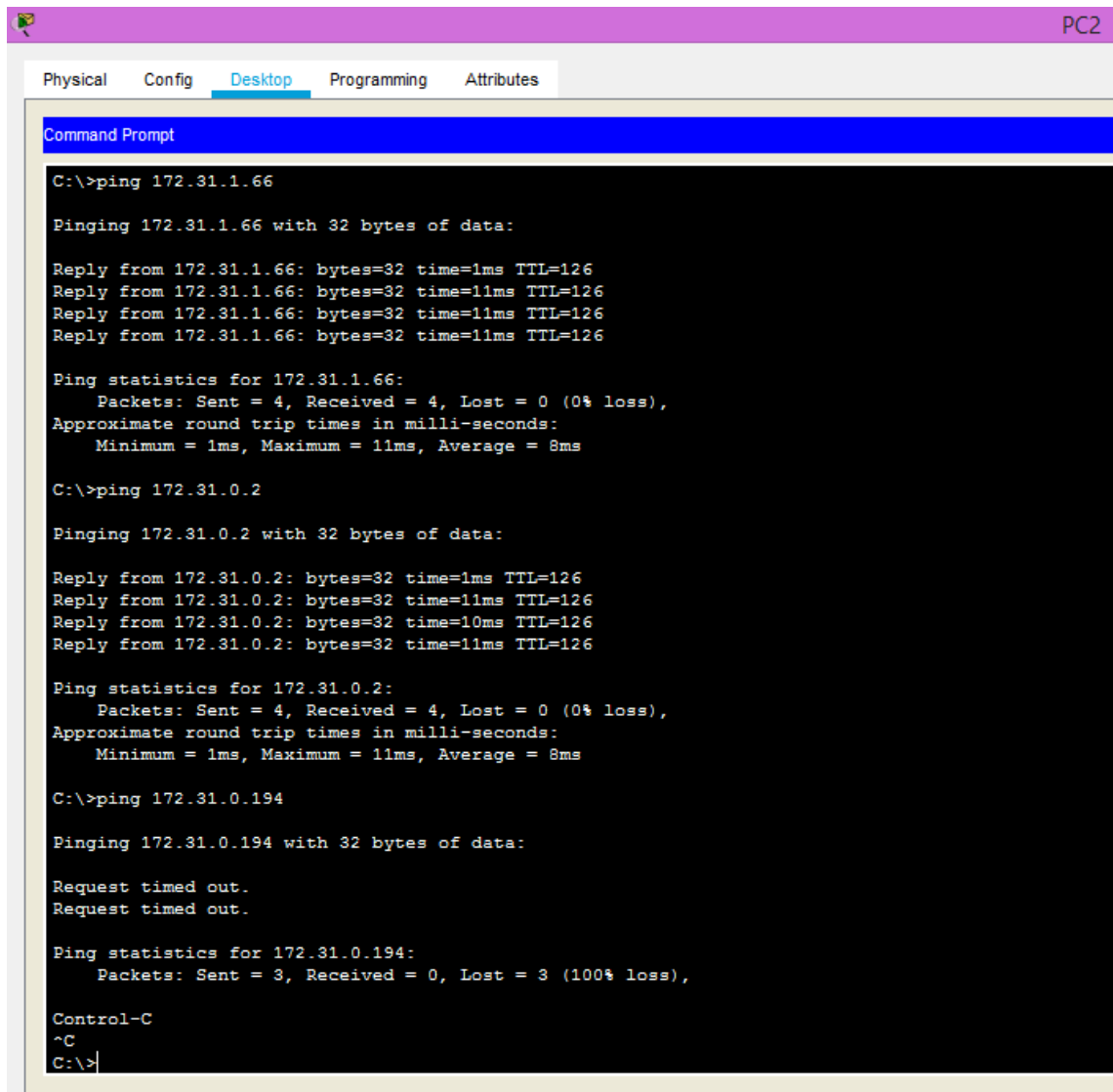
Ilustración 17. Prueba ACL 3

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

Se crea una lista en la cual se agregan las redes que se deben permitir y el resto de tráfico se deniega, a continuación, la lista aplicada:

```
access-list 110 permit ip 172.31.1.64 0.0.0.31 any
access-list 110 permit ip 172.31.0.0 0.0.0.31 any
access-list 110 deny ip any any
```

De acuerdo con la lista aplicada en la siguiente imagen se muestra la prueba de conectividad donde se observa que solo se alcanza la vlan 20 de Cundinamarca y la vlan 10 de Bucaramanga, los otros host no acceden a ningún otro equipo.



```

PC2
Physical Config Desktop Programming Attributes
Command Prompt
C:\>ping 172.31.1.66

Pinging 172.31.1.66 with 32 bytes of data:

Reply from 172.31.1.66: bytes=32 time=1ms TTL=126
Reply from 172.31.1.66: bytes=32 time=11ms TTL=126
Reply from 172.31.1.66: bytes=32 time=11ms TTL=126
Reply from 172.31.1.66: bytes=32 time=11ms TTL=126

Ping statistics for 172.31.1.66:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 11ms, Average = 8ms

C:\>ping 172.31.0.2

Pinging 172.31.0.2 with 32 bytes of data:

Reply from 172.31.0.2: bytes=32 time=1ms TTL=126
Reply from 172.31.0.2: bytes=32 time=11ms TTL=126
Reply from 172.31.0.2: bytes=32 time=10ms TTL=126
Reply from 172.31.0.2: bytes=32 time=11ms TTL=126

Ping statistics for 172.31.0.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 11ms, Average = 8ms

C:\>ping 172.31.0.194

Pinging 172.31.0.194 with 32 bytes of data:

Request timed out.
Request timed out.

Ping statistics for 172.31.0.194:
    Packets: Sent = 3, Received = 0, Lost = 3 (100% loss),

Control-C
^C
C:\>
    
```

Ilustración 18. Prueba ACL 4

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

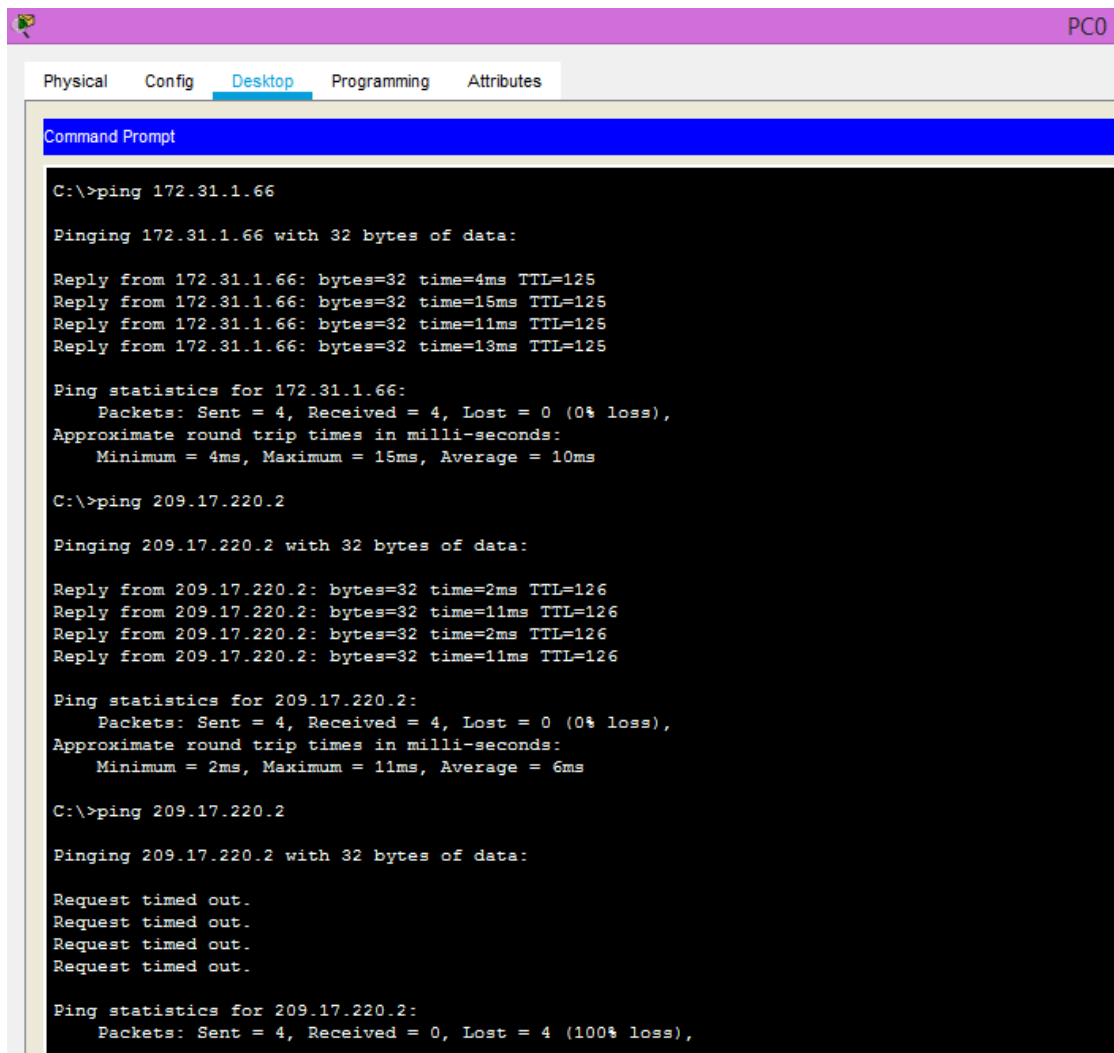
No se aplica Access-list no se identifica una necesidad puntual de aplicarla ya que no especifica que se deniegue algún tipo de conexión.

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

Se crea una lista en la cual se agregan las redes que se deben denegar y el resto de tráfico se permite, a continuación, la lista aplicada:

```
access-list 110 permit ip 172.31.0.0 0.0.0.31 any
access-list 110 permit ip 172.31.1.64 0.0.0.31 any
access-list 110 deny ip any any
Bucaramanga(config)#inter fa0/0.10
Bucaramanga(config-subif)#ip acces
Bucaramanga(config-subif)#ip access-group 110 in
Bucaramanga(config-subif)#end
```

De acuerdo con la lista aplicada en la siguiente imagen se muestra la prueba de conectividad donde se observa que desde la vlan 10 de Bucaramanga alcanzan la vlan 20 de Bucaramanga y de Tunja y no tienen salida a internet desde dicha vlan:



```
PC0
Physical Config Desktop Programming Attributes
Command Prompt
C:\>ping 172.31.1.66
Pinging 172.31.1.66 with 32 bytes of data:
Reply from 172.31.1.66: bytes=32 time=4ms TTL=125
Reply from 172.31.1.66: bytes=32 time=15ms TTL=125
Reply from 172.31.1.66: bytes=32 time=11ms TTL=125
Reply from 172.31.1.66: bytes=32 time=13ms TTL=125
Ping statistics for 172.31.1.66:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 4ms, Maximum = 15ms, Average = 10ms
C:\>ping 209.17.220.2
Pinging 209.17.220.2 with 32 bytes of data:
Reply from 209.17.220.2: bytes=32 time=2ms TTL=126
Reply from 209.17.220.2: bytes=32 time=11ms TTL=126
Reply from 209.17.220.2: bytes=32 time=2ms TTL=126
Reply from 209.17.220.2: bytes=32 time=11ms TTL=126
Ping statistics for 209.17.220.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 11ms, Average = 6ms
C:\>ping 209.17.220.2
Pinging 209.17.220.2 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Ping statistics for 209.17.220.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Ilustración 19. Prueba ACL 5

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

Se crea una lista en la cual se agregan las redes de los servidores que se deben permitir y el resto de tráfico se deniega, se aplica sobre la línea vty 0 4, a continuación, la lista aplicada:

```
access-list 150 permit ip 172.31.2.0 0.0.0.15 any
access-list 150 deny ip any any
line vty 0 4
access-class 150 in
end
```

De acuerdo con la lista aplicada en la siguiente imagen se muestra la prueba de acceso a los equipos donde se observa que solo se tiene gestión desde las vlans administrativas y de servidores, para las otras redes se les deniega el acceso vía telnet.

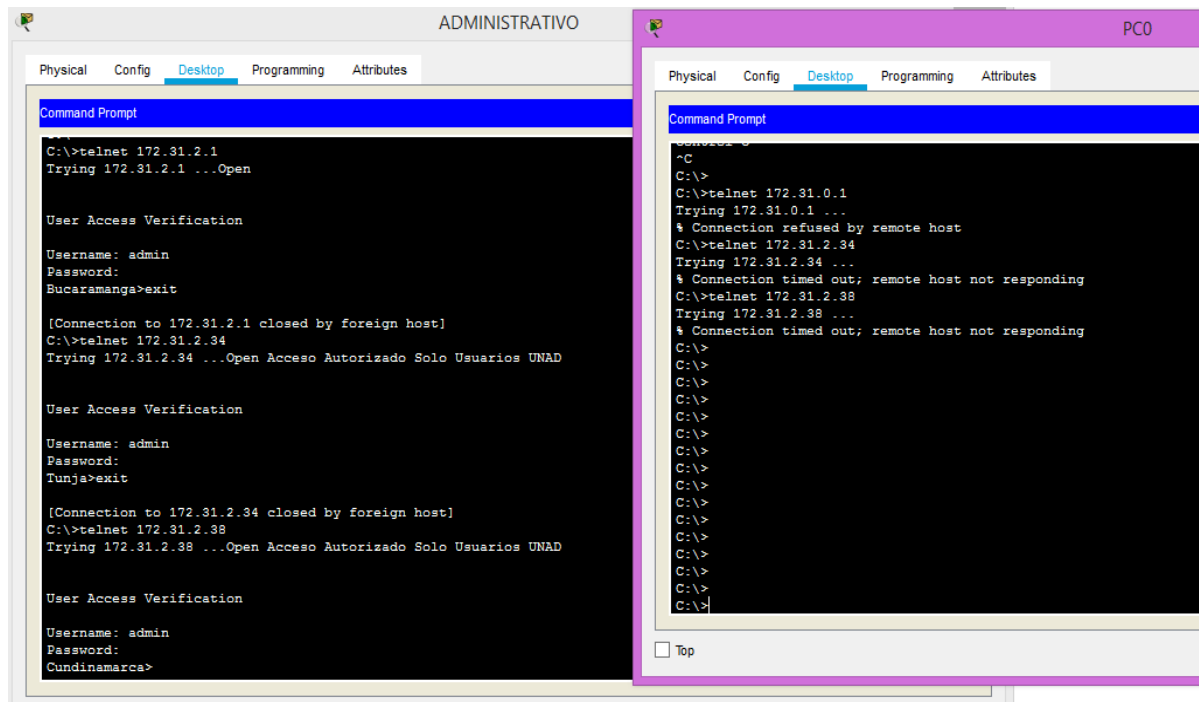


Ilustración 20. Prueba ACL 6

Configuración VLSM

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

Para este caso el diagrama ya contaba con el respectivo VLSM, por lo tanto, no realice ninguna modificación sino me base en lo que estaba, teniendo en cuenta que cumplía con las características requeridas en el diseño planteado.

Sede	Vlan	Rango asignado
Bucaramanga	1	172.31.2.0/29
	10	172.31.0.0/26
	30	172.31.0.64/26
Tunja	1	172.3.2.8/29
	20	172.31.0.128/26
	30	172.31.0.192/26
Cundinamarca	1	172.31.2.8/29
	20	172.31.1.64/26
	30	172.31.1.0/26
	88	172.31.2.24/29

Aspectos para tener en cuenta

- **Habilitar VLAN en cada switch y permitir su enrutamiento.**

Se configuran la interfaz de gestión y la respectiva ruta default en cada switch, a continuación, las líneas aplicadas en cada dispositivo:

SW BUCARAMANGA

```
interface vlan 1
ip add 172.31.2.2 255.255.255.248
no shutdown
ip default-gateway 172.31.2.1
```

SW TUNJA

```
interface vlan 1
ip add 172.3.2.10 255.255.255.248
no shutdown
ip default-gateway 172.3.2.9
```

SWCUNDINAMARCA

```
interface vlan 1
ip add 172.31.2.10 255.255.255.248
no shutdown
ip default-gateway 172.31.2.9
```

- **Enrutamiento OSPF con autenticación en cada router.**

Se configura protocolo OSPF en cada uno de los routers y se confirma conectividad de extremo a extremo, esto previo a la aplicación de listas de acceso. A continuación, las líneas de comando aplicadas sobre cada router para configurar el protocolo requerido:

BUCARAMANGA

```
router ospf 1
log-adjacency-changes
network 172.31.2.0 0.0.0.7 area 0
network 172.31.2.32 0.0.0.3 area 0
network 172.31.0.0 0.0.0.31 area 0
network 172.31.0.64 0.0.0.31 area 0
area 0 authentication
```

TUNJA

```
router ospf 1
log-adjacency-changes
network 172.31.2.32 0.0.0.3 area 0
network 172.31.2.36 0.0.0.3 area 0
network 172.3.2.8 0.0.0.7 area 0
network 172.31.0.128 0.0.0.31 area 0
network 172.31.0.192 0.0.0.31 area 0
area 0 authentication
```

CUNDINAMARCA

```
router ospf 1
log-adjacency-changes
network 172.31.2.36 0.0.0.3 area 0
network 172.31.2.8 0.0.0.7 area 0
network 172.31.2.24 0.0.0.7 area 0
network 172.31.1.64 0.0.0.31 area 0
network 172.31.1.0 0.0.0.31 area 0
area 0 authentication
```

En la siguiente imagen se muestra la prueba de conectividad desde el equipo del extremo de Bucaramanga, hasta equipos intermedios de Tunja y del otro extremo de Cundinamarca, confirmando que se alcanzan de un lado hacia el otro garantizando que la configuración aplicada es correcta.

```

C:\>ping 172.31.2.34

Pinging 172.31.2.34 with 32 bytes of data:

Reply from 172.31.2.34: bytes=32 time=1ms TTL=254
Reply from 172.31.2.34: bytes=32 time=1ms TTL=254
Reply from 172.31.2.34: bytes=32 time=2ms TTL=254
Reply from 172.31.2.34: bytes=32 time=5ms TTL=254

Ping statistics for 172.31.2.34:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 5ms, Average = 2ms

C:\>ping 172.31.2.38

Pinging 172.31.2.38 with 32 bytes of data:

Reply from 172.31.2.38: bytes=32 time=5ms TTL=253
Reply from 172.31.2.38: bytes=32 time=10ms TTL=253
Reply from 172.31.2.38: bytes=32 time=14ms TTL=253
Reply from 172.31.2.38: bytes=32 time=44ms TTL=253

Ping statistics for 172.31.2.38:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 5ms, Maximum = 44ms, Average = 18ms

C:\>ping 172.31.1.66

Pinging 172.31.1.66 with 32 bytes of data:

Request timed out.
Reply from 172.31.1.66: bytes=32 time=16ms TTL=125
Reply from 172.31.1.66: bytes=32 time=14ms TTL=125
Reply from 172.31.1.66: bytes=32 time=15ms TTL=125

Ping statistics for 172.31.1.66:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 14ms, Maximum = 16ms, Average = 15ms
    
```

Ilustración 21. Prueba conectividad 4

- **Servicio DHCP en el router Tunja, mediante el helper address, para los routers Bucaramanga y Cundinamarca.**

Se configura el DHCP en el router de Tunja y se confirma que asignan direccionamiento a las tres sedes, se configura el helper en las interfaces de los routers de Bucaramanga y de Cundinamarca para que envíe la solicitud de DHCP al router de Tunja, a continuación, las configuraciones aplicadas en cada router:

DHCP PARA CUNDINAMARCA

```
ip dhcp pool vlan20_CUND
network 172.31.1.64 255.255.255.192
default-router 172.31.1.65
dns-server 8.8.8.8
ip dhcp pool vlan30_CUND
network 172.31.1.0 255.255.255.192
default-router 172.31.1.1
dns-server 8.8.8.8
ip dhcp pool vlan88_CUND
network 172.31.2.24 255.255.255.248
default-router 172.31.2.25
dns-server 8.8.8.8
```

DHCP PARA BUCARAMANGA

```
ip dhcp pool vlan20_BGA
network 172.31.0.0 255.255.255.192
default-router 172.31.0.1
dns-server 8.8.8.8
ip dhcp pool vlan30_BGA
network 172.31.0.64 255.255.255.192
default-router 172.31.0.65
dns-server 8.8.8.8
```

DHCP PARA TUNJA

```
ip dhcp pool vlan20_TUNJA
network 172.31.0.128 255.255.255.192
default-router 172.31.0.129
dns-server 8.8.8.8
ip dhcp pool vlan30_TUNJA
network 172.31.0.192 255.255.255.192
default-router 172.31.0.193
dns-server 8.8.8.8
```

EXCLUSION DE IPS

```
ip dhcp excluded-address 172.31.1.65
ip dhcp excluded-address 172.31.0.65
ip dhcp excluded-address 172.31.1.1
ip dhcp excluded-address 172.31.0.1
ip dhcp excluded-address 172.31.2.25
ip dhcp excluded-address 172.31.0.193
ip dhcp excluded-address 172.31.0.129
```

Configuración de helper en sedes Bucaramanga y Cundinamarca:

```
Bucaramanga(config)#inter FastEthernet0/0.10
Bucaramanga(config-subif)#ip helper-address 172.31.2.34
Bucaramanga(config-subif)#inter FastEthernet0/0.30
Bucaramanga(config-subif)#ip helper-address 172.31.2.34
Cundinamarca(config)#interface FastEthernet0/0.20
Cundinamarca(config-subif)#ip helper-address 172.31.2.37
Cundinamarca(config)#interface FastEthernet0/0.30
Cundinamarca(config-subif)#ip helper-address 172.31.2.37
Cundinamarca(config-subif)#interface FastEthernet0/0.88
Cundinamarca(config-subif)#ip helper-address 172.31.2.37
```

En la siguiente imagen se muestra el funcionamiento del DHCP en el router de Tunja, se observan las peticiones desde los routers de las otras sedes.

```
Tunja#sh ip dhcp binding
IP address      Client-ID/
                Hardware address      Lease expiration      Type
172.31.1.66     00E0.F740.5925           --                    Automatic
172.31.2.26     0060.47A6.8318           --                    Automatic
172.31.0.2      0001.97E6.4A6E           --                    Automatic
172.31.0.66     0005.5E3A.7218           --                    Automatic
172.31.0.130    0030.A32B.7E74           --                    Automatic
172.31.0.194    0090.0C22.018B           --                    Automatic
Tunja#
```

Ilustración 22. Tabla DHCP router Tunja

- **Configuración de NAT estático y de sobrecarga.**

Se configuran los dos tipos de NAT, a continuación, las evidencias del funcionamiento de la configuración aplicada:

```
Tunja#sh run | incl ip nat inside source
ip nat inside source list 10 interface FastEthernet0/0 overload
ip nat inside source static 172.31.2.25 209.17.220.1
Tunja#
```

Ilustración 23. Configuración NAT

```
Tunja(config)#ip nat inside source static 172.31.2.25 209.17.220.1
Tunja(config)#end
Tunja#
Tunja#
Tunja#
Tunja#sh ip nat trans
Tunja#sh ip nat translations
Pro  Inside global      Inside local      Outside local     Outside global
icmp 209.17.220.1:1      172.31.2.25:1    172.31.2.26:1    172.31.2.26:1
icmp 209.17.220.1:2      172.31.2.25:2    172.31.2.26:2    172.31.2.26:2
icmp 209.17.220.1:3      172.31.2.25:3    172.31.2.26:3    172.31.2.26:3
icmp 209.17.220.1:4      172.31.2.25:4    172.31.2.26:4    172.31.2.26:4
--- 209.17.220.1      172.31.2.25      ---              ---

Tunja#
```

Ctrl+F6 to exit CLI focus

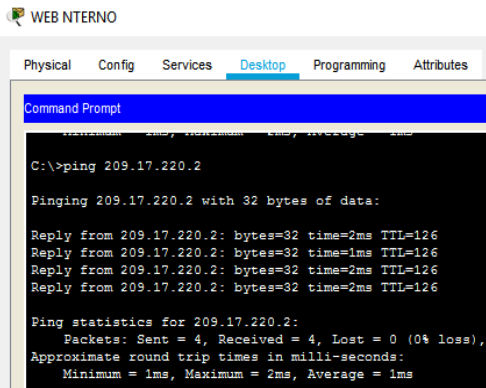


Ilustración 24. Funcionamiento de NAT

```
Tunja#show ip nat translations
Pro  Inside global      Inside local      Outside local     Outside global
icmp 209.17.220.1:18      172.31.0.2:18    209.17.220.2:18  209.17.220.2:18
icmp 209.17.220.1:19      172.31.0.2:19    209.17.220.2:19  209.17.220.2:19
icmp 209.17.220.1:20      172.31.0.2:20    209.17.220.2:20  209.17.220.2:20
icmp 209.17.220.1:21      172.31.0.2:21    209.17.220.2:21  209.17.220.2:21
icmp 209.17.220.1:5      172.31.0.130:5   209.17.220.2:5   209.17.220.2:5
icmp 209.17.220.1:6      172.31.0.130:6   209.17.220.2:6   209.17.220.2:6
icmp 209.17.220.1:7      172.31.0.130:7   209.17.220.2:7   209.17.220.2:7
icmp 209.17.220.1:8      172.31.0.130:8   209.17.220.2:8   209.17.220.2:8
--- 209.17.220.1      172.31.2.25      ---              ---

Tunja#
```

Ilustración 25. Funcionamiento de Nat 1

- **Establecer una lista de control de acceso de acuerdo con los criterios señalados.**

Se aplicaron las listas de acceso se adjuntaron las evidencias en cada punto señalado anteriormente.

- **Habilitar las opciones en puerto consola y terminal virtual**

Se configuraron las líneas VTY y CONSOLA en todos los equipos tanto routers como switches como se evidencia en el punto 1, a continuación, imagen del router de Tunja de como quedo configurado:

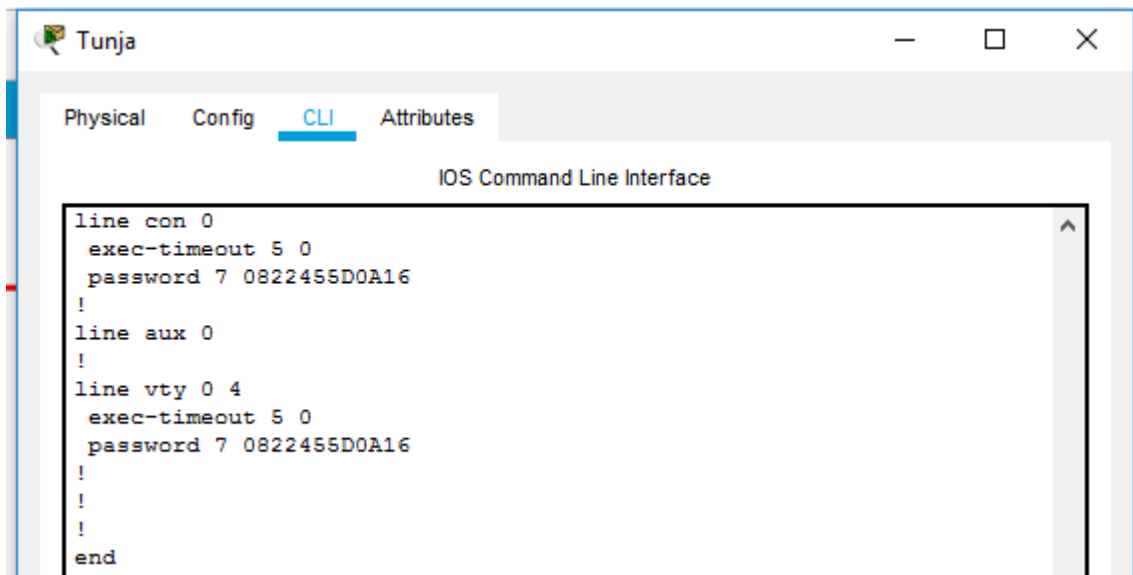


Ilustración 26. Configuración Línea VTY Y Consola

CONCLUSIONES

- Mediante el desarrollo de esta práctica se pusieron a prueba las destrezas y habilidades adquiridas en el curso, demostrando que se cuenta con la capacidad para brindar soluciones a los diseños de red planteados.
- Se aplicaron conceptos de configuración y solución de problemas de enrutamiento, listas de acceso, división de redes y aplicación de seguridad sobre las mismas.
- Se realizó una solución a los diseños planteados identificando múltiples aspectos que se deben tener en cuenta a la hora de implementar una red de datos.

REFERENCIAS BIBLIOGRÁFICAS

Enrutamiento Dinámico

CISCO. (2014). Enrutamiento Dinámico. Principios de Enrutamiento y Conmutación. Recuperado de <https://static-course-assets.s3.amazonaws.com/RSE50ES/module7/index.html#7.0.1.1>

OSPF de una sola área

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>

Listas de control de acceso

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>

DHCP

CISCO. (2014). DHCP. Principios de Enrutamiento y Conmutación. Recuperado de <https://static-course-assets.s3.amazonaws.com/RSE50ES/module10/index.html#10.0.1.1>

LISTAS DE ACCESO. (2019). Retrieved 12 December 2019, from http://atc2.aut.uah.es/~rosa/LabRC/Prac_5/Listas%20de%20Control%20de%20acceso.pdf

Academia Cisco. (2019). Retrieved 12 December 2019, from <https://www.netacad.com/portal/learning>

Cisco Networking Academy. (s.f.). Capítulo 11: Traducción de direcciones de red para IPv4. Recuperado el 12 December de 2019, de UNIDAD 4 Enrutamiento en soluciones de red. Disponible en <https://static-course-assets.s3.amazonaws.com/RSE50ES/module11/index.html#11.0.1.1>